

DELAWARE STATE BAR ASSOCIATION

PRESENTS

RECENT DEVELOPMENTS IN DATA SECURITY AND E-DISCOVERY 2021

LIVE SEMINAR AT DSBA WITH ZOOM OPTION

SPONSORED BY THE E-DISCOVERY AND TECHNOLOGY SECTION
OF THE DELAWARE STATE BAR ASSOCIATION

WEDNESDAY, DECEMBER 15, 2021 | 9:00 A.M. TO 12:15 P.M.

**3.0 Hours of CLE credit in Enhanced Ethics for
Delaware and Pennsylvania Attorneys**



C L E

Property of Delaware State Bar Association
Permission required to reproduce

*Please note that the attached materials are supplied by the speakers and presenters
and are current as of the date of this posting.*

RECENT DEVELOPMENTS IN DATA SECURITY AND E-DISCOVERY 2021

PROGRAM

9:00 a.m. – 10:30 a.m.

Panel I: Recent Developments in Data Security 2021 has been active year for developments in Data Security

- With the change to a new federal administration, data security seems to be gaining traction, as Congress and regulators focus on cybersecurity, misinformation campaigns, and Section 230 of the Communications Decency Act.
- Ransomware and cyber extortion continued to wreak havoc, with even the White House providing guidance for businesses to develop resilience.
- Virginia and Colorado joined California in adopting consumer privacy laws, and other states tackled a variety of privacy and data security topics, like biometric privacy and improvements to data-breach notification standards.
- Cross-Border data-transfer laws continue to create challenges as businesses navigate a post-Brexit Europe and China enacts a privacy law.
- Businesses began transitioning workers back to in-office work, navigating the uncharted waters of hybrid options and vaccine mandates.
- The DSBA Committee on Professional Ethics issued its first opinion in ten years to address issues surrounding remote work by Delaware attorneys.

How do these events affect Delaware lawyers and their clients? Come hear about the latest data privacy and security issues impacting Delaware lawyers and their clients. This panel will discuss recent developments in litigation, legislation and regulations relating to data security and privacy, with an emphasis on recent ethics guidance and incidents involving attorneys and law firms.

William R. Denny, Esquire
Potter Anderson & Corroon LLP
Sara Beth A. R. Kohut, Esquire
Young Conaway Stargatt & Taylor, LLP
Edward J. McAndrew, Esquire
DLA Piper

10:30 a.m. – 10:45 a.m. | Break

10:45 a.m. – 12:15 p.m.

Panel II: Recent Developments in E-Discovery

Come join this panel in discussing substantive developments in e-Discovery, as well as the potential impact of some “ripped from the headlines” discovery abuse stories, including:

- What happens when lawyers “slip” discovery documents into a database without timely notifying opposing counsel?
- Is the frequency of severe discovery abuse increasing, and what is the impact on lawyers and their clients?
- What’s the latest guidance from Delaware courts on discovery protocols and discovery objections?
- What are the most updated best practices from the Sedona Conference, and how might they affect your practice?

This panel will get you up-to-date with the latest e-Discovery developments, including recent court decisions and pending rule changes.

James H.S. Levine, Esquire
Troutman Pepper Hamilton Sanders LLP
Ian D. McCauley, Esquire
Morris James LLP
Laura G. Readinger, Esquire
Potter Anderson & Corroon LLP

COVID-19 POLICY: The DSBA requires that everyone, including speakers and attendees, must be fully vaccinated against COVID-19 to attend live CLE events. In addition, all participants and attendees, regardless of COVID-19 vaccination status, must wear masks except when presenting, eating, or drinking.

This CLE is a HYBRID CLE. You may register for this event as a live participant or by Zoom. Even if you register as a live participant, you will receive a Zoom link by email immediately which you may disregard if not attending by Zoom. (Check spam folders if you do not.) If you are going to attend the live session, you will report to the venue and check in. Only live attendees will receive live CLE credits after 12/31/2022.

REGISTRATION INFORMATION AND RATES

This CLE will be conducted live and via Zoom. To register, visit www.dsba.org/cle and select this seminar, choosing whether you wish to attend live or by Zoom. If registering for EITHER method, you will receive an email back from Zoom immediately providing you with the correct login information. If attending by zoom and you do not receive this email, contact DSBA via email: reception@dsba.org. The Supreme Court of the State of Delaware Commission on Continuing Legal Education cannot accept phone conferencing only. **You must attend through a device that allows DSBA to obtain your Bar ID in order to receive CLE Credit.** Your attendance will be automatically monitored beginning at the scheduled start time and will be completed when the CLE has ended. If you enter or leave the seminar after or before the scheduled start /end time, you will receive credit only for the time you attended. Your CLE credits will be submitted to the Delaware and Pennsylvania Commissions on CLE, as usual. Naturally, if you attend the seminar live, you must sign in and we will use your attendance as the means for reporting the live credit.

Panel I: Recent Developments in Data Security

William R. Denny, Esquire
Potter Anderson & Corroon LLP

Sara Beth A. R. Kohut, Esquire
Young Conaway Stargatt & Taylor, LLP

Edward J. McAndrew, Esquire
DLA Piper

William R. Denny

Partner

William R. Denny has a business and litigation practice, focusing on commercial and corporate transactions, vendor management, mergers and acquisitions, data privacy and security and information technology. Mr. Denny is a Certified Information Privacy Professional (CIPP/US) and a Certified Information Privacy Manager (CIPM) through the International Association of Privacy Professionals (IAPP). He has represented public and privately held companies and government entities in a wide range of technology transactions, including negotiating complex cloud services agreements, software and IT infrastructure development, maintenance and support agreements, long-term materials supply agreements, outsourcing agreements, transition and site services agreements, technology licensing agreements, sales of internet domain names, and website terms of use and privacy policies. Clients include major corporations in the industrial, chemical, medical and technology sectors, as well as technology and information systems service providers and developers.

Mr. Denny has litigated disputes over the interpretation and enforcement of many types of technology contracts, general commercial contracts and liability insurance policies. He has tried jury and non-jury cases in federal and state trial and appellate courts, before arbitration panels, and by use of other alternative dispute resolution techniques.

Mr. Denny took a leading role in drafting and negotiating Delaware's amendment to its computer security breach law, 6 Del. C. §§ 12B-100 *et seq.*, which was enacted in June 2017 and came into force in April 2018.

Mr. Denny writes extensively on technology and business issues, including:

- "Vendor Contracting Project: Cybersecurity Checklist," Second Edition, published by the American Bar Association's Cybersecurity Legal Task Force, April 2021
- "Mitigating Your Business Risk: Board Responsibilities in Cybersecurity," published by Business Law Today, February 2020
- "Legal Obligations and Best Practices for Maintaining Security in the Cloud" and "Warranties, Indemnities and Limitations of Liability in Cloud Contracts," published in Lifshitz, L and Rothchild, J, ed., Cloud 3.0: Drafting and Negotiating Cloud Computing Agreements (American Bar Association 2019)
- "Mitigating Your Business Risk: Board Responsibilities in Cybersecurity," published in *Delaware Business* magazine, November/December 2019



Wilmington
Hercules Plaza
1313 North Market Street, 6th Floor
P.O. Box 951
Wilmington, Delaware 19801

T: 302.984.6039
F: 302.658.1192
wdenny@potteranderson.com

EDUCATION

University of Virginia School of Law,
1987, J.D.

University of Helsinki, 1984

Princeton University, A.B., *cum laude*, 1983

BAR & COURT ADMISSIONS

Delaware, 1988

PRACTICE AREAS

Blockchain

Business & Commercial Litigation

Commercial Litigation

Corporate Counseling

Cybersecurity, Data Privacy and
Information Governance

Insurance Recovery Litigation &
Advice

Intellectual Property

Intellectual Property Litigation

Mergers, Acquisitions & Divestitures

PROFESSIONAL ACTIVITIES AND HONORS

Certified Information Privacy
Professional / U.S. Private Sector;
Chair, KnowledgeNet Delaware
Chapter

Listed in *The Best Lawyers in*

- “Mitigating Risk: Protect your Business Against Ransomware,” published in *Delaware Business* magazine, September/October 2019
- “Mitigating Your Business Risk: Compliance With Data Privacy Laws,” published in *Delaware Business* magazine, July/August 2019
- “Representations and Warranties in M&A Agreements,” published in Smedinghoff, T. and Trope, R., ed., *Guide to Cybersecurity Due Diligence in M&A Transactions* (ABA Publishing 2017).
- “Standing and the Circuit Court Split in Data Breach Litigation” in *Corporate Disputes*, January-March 2018
- “Representations and Warranties in M&A Agreements” in the ABA’s *Guide to Cybersecurity Due Diligence in M&A Transactions*, December 2017
- “What’s Changed Under Delaware’s New Data Breach Law” in *Law360*, August 24, 2017
- “Building Your Cyber Incident Response Plan” in *Delaware Business*, May/June 2017
- “Cybersecurity as an Unfair Practice: FTC Enforcement under Section 5 of the FTC Act” in *Business Law Today*, June 2016
- “Legal Considerations for Business Contracting in Cloud Computing Services” and “Essential IT Due Diligence in Corporate Transactions” in *Internet Law for the Business Lawyer* (Second Edition) (American Bar Association 2012)

Mr. Denny frequently speaks at seminars, programs and meetings on topics including technology, e-discovery and cybersecurity, among others:

- November 18, 2020, at a Delaware State Bar Association panel, Mr. Denny discussed developments in litigation, legislation and regulations relating to **data security and privacy**.
- October 27, 2020, at the Secure Delaware 2020 Workshop, Mr. Denny presented “**Privacy in a Pandemic: Critical Legal Developments and Practical Guidance.**”
- March 29, 2019, at the ABA Section of Business Law Spring Meeting in Vancouver, BC, Canada, Mr. Denny presented: “**Cross-border Cybersecurity Compliance Issues.**”
- November 14, 2018, at a program sponsored by the Delaware State Bar Association on Cybersecurity Recent Developments, Mr. Denny presented on the **California Consumer Privacy Act and the move toward new federal legislation in privacy.**
- October 31, 2018, at the Secure Delaware 2018 Workshop, organized by the State of Delaware’s Department of Technology and

America for Information Technology Law and Commercial Litigation, most recently in the 2022 edition

AV® rated by Martindale-Hubbell

Delaware State Bar Association;
Co-Chair, E-Discovery and Technology Law Section;
Committee on Professional Ethics (former Co-Chair)

American Bar Association;
Business Section, Cyberspace Law Committee; Co-Chair, IT Services and Cloud Computing Subcommittee; Cybersecurity Legal Task Force

Federal Bar Association, Ad Hoc Committee for Electronic Discovery

Richard K. Herrmann Technology American Inn of Court



Innovation, Mr. Denny presented **"Data Privacy and the Double Trouble of the GDPR and the California Consumer Privacy Act of 2018"**.

- September 14, 2018, at the ABA Business Section Annual Meeting in Chicago, Mr. Denny moderated a program entitled **"Blockchain Basics for the Business Lawyer – Smart Contracts, Crypto Offerings and Other Transformative Applications."**
- August 2, 2018, at the ABA Annual Meeting in Chicago, Mr. Denny presented **"Cybersecurity Law: Deciphering the Landscape of Legal Requirements Applicable To Businesses and Law Firms."**
- May 31, 2018, at the Business Law Basics Webinar sponsored by the American Bar Association, Mr. Denny presented on **Data Privacy**.
- May 2, 2018, at a program sponsored by the Delaware Bioscience Association, Mr. Denny presented on **Data Security for IP**.
- April 12, 2018, at the ABA Section of Business Law Spring Meeting in Orlando, FL, Mr. Denny moderated and presented on a program panel entitled, **"Best Practices for Compliance Programs to Mitigate Risks of Cyber Incidents."**
- January 25, 2018, at a Delaware State Bar Association program, Mr. Denny presented **Cybersecurity Recent Developments**.
- December 6, 2017, at a program sponsored by the Delaware Bankers Association, Mr. Denny presented **Staying Secure in the Cloud**.
- October 11, 2017, at the **Secure Delaware 2017 Workshop**, organized by the State of Delaware's Department of Technology and Innovation, Mr. Denny presented **"Trends in Data Breach Disclosure Laws"** and **"After the Breach,"** discussing incident response planning.
- September 14, 2017, at the ABA Section of Business Law Annual Meeting in Chicago, IL, Mr. Denny moderated and presented on a panel entitled **Vendor Risk: The Weakest Link in your Cybersecurity Strategy**.
- November 9, 2016: at a program sponsored by the Delaware State Bar Association, Mr. Denny presented **"Recent Developments in Data Security"**.
- September 28, 2016, at a program sponsored by the Delaware Small Business Development Center, Mr. Denny presented **"Data Breach and Vendor Risk Management."** This presentation focused on necessary due diligence, essential contract terms and follow-up activities to minimize the risk of harm caused by a vendor cyber security event.
- September 7, 2016: 2016 Secure Delaware Workshop, Mr. Denny presented **"Data Breach and Vendors: Strategies to Limit Your Risks of Data Breach and Protect Yourself from Vendor Vulnerabilities."**
- December 15 and 16, 2015: National Business Institute Seminar entitled **"Legal Ethics of Email."** Mr. Denny was one of two principal speakers.
- October 3, 2015: Delaware State Bar Association Seminar, **"Managing E-Discovery Effectively."** Mr. Denny focused on recent developments in e-discovery.
- September 29, 2015: Delaware Cyber Security Workshop, **"Changing Legal Landscape in Cybersecurity: Implications for Business."** Mr. Denny focused on recent developments in cybersecurity laws and regulations at a full-day seminar sponsored by the State of Delaware.
- May 6, 2014: Delaware Cyber Security Workshop. **"Changing Legal Landscape in Cybersecurity: Implications for Business."** This presentation focused on the latest developments and implications for businesses as they seek to protect their critical infrastructure and comply with laws and regulations for data

protection.

- April 10, 2014: ABA Business Section Spring Meeting, Cloud Computing and IT Services Subcommittee. Mr. Denny presented on **recent developments in cloud computing contracting practices**.
- February 6, 2013: Delaware Cyber Security Workshop. Mr. Denny led a roundtable discussion on **data security and data breach notification laws** at the full day conference on cybersecurity sponsored by the State of Delaware.
- January 2013: Technology Inn of Court of Wilmington. Mr. Denny led a panel discussion on **e-discovery**.
- October and November 2013: **Client presentations on indemnification and limitation liability provisions in commercial contracts**.

PUBLICATIONS

Denny Examines Private Sector Actions in Light of the Cybersecurity Executive Order
September 13, 2021

Denny Discusses Federal Efforts to Improve the Nation's Cybersecurity
August 16, 2021

Denny Contributes to New Edition of Vendor Contracting Project: Cybersecurity Checklist
May 5, 2021

Legal Responsibility for Safe Disposal of Personal Data
February 21, 2020

Mitigating Your Business Risk: Board Responsibilities in Cybersecurity
Business Law Today, February 13, 2020

Denny and Noa Contribute to Bloomberg Law Profile on Privacy and Data Security in Delaware
January 2018

Denny and Noa Highlight Standing Issue in Data Breach Litigation
December 20, 2017

RECENT NEWS

Denny, Martin and Wasson Named 'Top Lawyers' by *Delaware Today*
November 3, 2021

43 Potter Anderson Lawyers Recognized in Best Lawyers in America 2022
August 19, 2021

Denny Appointed to New Role With Cyber Security Advisory Council
June 24, 2021

CLIENT ALERT: Actions to Protect Your Cybersecurity After the FireEye Hack
December 14, 2020

CLIENT ALERT: Treasury Warns of Legal Risk of Ransomware Payments
November 2, 2020



41 Potter Anderson Lawyers Recognized in *Best Lawyers in America* 2021
August 20, 2020

CLIENT ALERT: COVID-19: The Legal Consequences of Significant Disruption on Your Contracts
March 30, 2020

33 Potter Anderson Attorneys Named to the 2020 Best Lawyers® List
August 15, 2019

Denny Obtains Information Privacy Manager Certification
May 21, 2019

30 Potter Anderson Attorneys Named to the 2019 Best Lawyers® List
August 15, 2018

Denny Appointed to ABA Cybersecurity Legal Task Force
July 30, 2018

Denny Named IAPP KnowledgeNet Chapter Chair for Delaware
March 23, 2018

Denny Named Among Top E-Discovery/Technology Lawyers by Delaware Today
November 3, 2017

CLIENT ALERT: Update to Delaware Data Breach Disclosure Law
August 17, 2017

22 Potter Anderson Attorneys Named as "The Best Lawyers in America" for 2018
August 15, 2017

William Denny Earns CIPP/US Certification from the International Association of Privacy Professionals
June 6, 2017

Three Potter Anderson Attorneys Named "Lawyers of the Year" and 21 Attorneys Named as "the Best Lawyers in America" for 2017
August 15, 2016

Potter Anderson Attorney Comments on Delaware Federal Court Standards
February 2, 2012

RECENT EVENTS & SPEAKING ENGAGEMENTS

Denny Discusses Latest in Data Security
December 15, 2021

Denny Presents on Vendor Supply Chain Attacks
October 28, 2021

Denny Participates in DSBA Panel on Data Security Developments
November 18, 2020

Denny Presents on Privacy in a Pandemic
October 27, 2020



Denny Presents on Data Privacy Laws

August 6, 2020

Denny Discusses What Delaware Lawyers Need to Know About Privacy Law

June 22, 2020

Denny Moderates Program for Corporate Officers and Directors on Managing Cyber and Privacy Risks

May 19, 2020

Denny Co-Chairs Smart Contracts and Blockchain Meeting

January 24, 2020

Denny Presents on Data Privacy, Security and Mitigating Business Risk

October 2, 2019

Denny Discusses Legal Compliance Challenges at the Intersection of Privacy and Security

September 24, 2019

Denny Leads ABA Program on Board Responsibilities in Cybersecurity

September 12, 2019

Potter Anderson Sponsors ABA Business Law Section's 2019 Annual Meeting

September 12, 2019

Denny and Kelly Weigh in on Blockchain Technology and Smart Contracts

April 11, 2019

Denny Presents at ABA Cyberspace Law Institute on Push for Federal Data Privacy Standard

January 25, 2019

Denny Presents on California Consumer Privacy Act

November 13, 2018

Denny Delivers Keynote Address on Data Breach Disclosure Laws

May 22, 2018

Denny Presents on Data Breach Disclosure Laws, Creating Incident Response Plans

May 17, 2018

Denny Provides Update on Recent Amendment to Delaware's Computer Security Breaches Law

March 1, 2018

Denny Moderates ABA Panel on Blockchain Technology and Smart Contracts

January 27, 2018

Denny Participates in Panel on Cyber Security Threats and Solutions

August 10, 2017

Potter Anderson Hosts Seminar on Protecting Your Business: Cyber Threats, Employees and Financial Security

May 16, 2017

Protecting Your Business - Strategies for Growth and Resilience

February 23, 2016



Sara Beth A.R. Kohut

COUNSEL, CIPM, CIPP/US AND CIPP/E

skohut@ycst.com

[Wilmington](#) | P: 302.571.5004 | F: 302.576.3329

Sara Beth Kohut assists her clients with navigating the complexities of protecting mass tort (mostly asbestos) claimants in bankruptcy cases and settlement trusts. She primarily advises the legal representatives for future claimants in these matters, and also serves as counsel to several post-bankruptcy settlement trusts and service providers. Known for her creativity, thoroughness, and adaptability, Sara Beth draws on broad experience, anchored in her start as a corporate and intellectual property litigator and transactional attorney before moving into bankruptcy matters.

As issues relating to privacy, cybersecurity and data protection increasingly grew in volume and prominence for her clients, Sara Beth immersed herself into this rapidly-evolving field. She works collaboratively with her clients to craft strategies for protecting information assets, and writes and speaks frequently on data protection and technology developments.

FOCUS:

- Mass tort bankruptcy cases and post-bankruptcy personal injury claim settlement trusts, primarily advising the legal representatives for future asbestos claimants.
- Privacy, cybersecurity and data protection matters, including advising on website terms of use, privacy policies, confidentiality agreements, incident-response plans, legal compliance, insurance coverage, security audits, data retention, and vendor contracts.
- Experience also includes litigating corporate, commercial, and intellectual property disputes, and advising clients on the protection of and transactions involving intellectual property assets, such as copyrights, trademarks, domain names, and trade secrets.

Education

- University of Pittsburgh School of Law (J.D., *cum laude*)
- Western Maryland College (B.A., *summa cum laude*)

Bar Admissions

- Delaware
- Pennsylvania

Court Admissions

- U.S. District Court for the District of Delaware
- U.S. Court of Appeals for the Third Circuit

Distinctions

- Certified Information Privacy Manager, International Association of Privacy Professionals
- Certified Information Privacy Professional/United States, International Association of Privacy Professionals
- Certified Information Privacy Professional/Europe, International Association of Privacy Professionals
- Data Privacy and Protection Specialist, Association for Data and Cyber Governance
- Phi Beta Kappa

Memberships and Affiliations

- American Bar Association
- Delaware State Bar Association, Vice Chair of E-Discovery and Technology Law Section
- International Association of Privacy Professionals
- ABA Business Law Section's Cyberspace Law Committee
- ABA Business Law Today, Managing Editor, Internet Law and Cybersecurity

**The DSBA Section of E-Discovery and Technology Law
Presents Recent Developments in Data Security and E-Discovery
Dec. 15, 2021**

Materials and Recommended Reading:

Delaware Lawyers' Rules of Professional Conduct:

<https://courts.delaware.gov/odc/rules.aspx>

Rule 1.1, including Comment 8 – Competence

Rule 1.4 – Communication with clients

Rule 1.6(a) & (c), including Comments 18-20 – Confidentiality

Rules 1.9(c) & 1.6 Comment 21 – Duties to former clients

Rule 1.15 – Safekeeping of client property

Rules 5.1, 5.2, 5.3 – Responsibilities to supervise attorneys and non-attorney assistants

Delaware Supreme Court Commission on Law & Technology:

Leading Practices on technology topics: <http://courts.delaware.gov/declt/practices.aspx>

Delaware Code:

<http://delcode.delaware.gov/>

6 Del. C. § 12B-101 et seq. – Computer Security Breaches

6 Del. C. § 5001C et seq. & 19 Del. C. § 736 – Safe Destruction of Records Containing PII

6 Del. C. § 1201C et seq. – Online and Personal Privacy Protection

14 Del. C. § 8101A et seq. – Student Data Privacy Protection Act

18 Del. C. § 8106 et seq. – Insurance Data Security Act (HB 174, signed into law July 31, 2019)

ABA and Other Formal Opinions:

http://www.americanbar.org/groups/professional_responsibility/publications/ethics_opinions.html

99-413 – Protecting the Confidentiality of Unencrypted E-Mail (Mar. 10, 1999)

06-442 – Review and Use of Metadata (Aug. 5, 2006)

08-451 – Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services (Aug. 5, 2008)

11-459 – Duty to Protect the Confidentiality of E-Mail Communications with One's Client (Aug. 4, 2011)

11-460 – Duty When Lawyer Receives Copies of Third Party's E-mail Comm's with Counsel (Aug. 4, 2011)

17-477R – Securing Communication of Protected Client Information (May 22, 2017)

18-482 – Ethical Obligations Related to Disasters (Sept. 19, 2018)

18-483 – Lawyers' Obligation After an Electronic Data Breach or Cyberattack (Oct. 17, 2018)

20-495 – Lawyers Working Remotely (Dec. 16, 2020)

21-496 – Responding to Online Criticism (Jan. 13, 2021)

21-498 – Virtual Practice (March 10, 2021)

Cal. Formal Op. 2020-203 – Unauthorized Access to Electronic Client Confidential Information

Maine Op. 2019-220 – Cyberattack and Data Breach: the Ethics of Prevention and Response

Pa. 2020-300 – Ethical Obligations for Lawyers Working Remotely

State Bar of Cal. Standing Comm. on Prof. Resp. and Conduct Formal Op. No. 20-0004 (remote work)

DSBA Committee on Professional Ethics Formal Op. 2021-1 (July 9, 2021) (remote work)

Fla. Bar re: Advisory Op. – Out-of-State Attorney Working Remotely from Fla. Home, No. SC20-1220 (Fla. May 20, 2021) (upholding advisory opinion on attorney's remote practice)

Recent Developments in Data Security

Delaware State Bar Association

December 15, 2021

William R. Denny, *Potter Anderson & Corroon LLP*

Sara Beth A.R. Kohut, *Young Conaway Stargatt & Taylor, LLP*

Edward J. McAndrew, *DLA Piper LLP*

The Evolving Cyber Threat Landscape

- Hacking and Exploitation of Stolen Data
- Espionage & Surveillance
- Ransomware - System/Device Disruption & Destruction
- Extortion, Stalking and Threats
- Cyber-facilitated fraud/corruption/violence
- Disinformation campaigns & digital speech
- Non-malicious incidents (data leakage et al.)
- Insider incidents
- Lost/Stolen Devices



Supply Chain & Zero Day Hacking and the Targeting Internet and IT Service Providers

SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president

By Reuters Staff

2 MIN READ



President Brad Smith speaks at the Web Summit, in Lisbon, Portugal, November 6, 2020. Reuters/File Photo

WASHINGTON (Reuters) - A hacking campaign that used a U.S. tech company as a springboard to compromise a raft of U.S. government agencies is "the largest and most sophisticated attack the world has ever seen,"

KrebsOnSecurity

In-depth security news and investigation



[HOME](#) [ABOUT THE AUTHOR](#) [ADVERTISING/SPEAKING](#)

At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software

March 5, 2021

154 Comments

At least 30,000 organizations across the United States — including a significant number of small businesses, towns, cities and local governments — have over the past few days been hacked by an unusually aggressive Chinese cyber espionage unit that's focused on stealing email from victim organizations, multiple sources tell KrebsOnSecurity. The espionage group is exploiting four newly-discovered flaws in Microsoft Exchange Server email software, and has coded hundreds of thousands

Advertisement

**Assess Your
Organization's
Cyber Security**

CBS NEWS NEWS ▾ SHOWS ▾ LIVE ▾   [Login](#)

SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments

60 BY BILL WHITAKER
JULY 4, 2021 / 6:58 PM / CBS NEWS



Kaseya says up to 1,500 businesses compromised in massive ransomware attack

THE WALL STREET JOURNAL.

◆ WSJ NEWS EXCLUSIVE | BUSINESS

Colonial Pipeline CEO Tells Why He Paid Hackers a \$4.4 Million Ransom

Joseph Blount says he needed to quickly restore service after cyberattack threatened East Coast supply

The New York Times

Cyberattack Forces a Shutdown of a Top U.S. Pipeline



'Apex predators': Why the Kaseya ransomware attack has experts worried

The gang behind a supply chain attack used tactics usually reserved for well-resourced nation-state hackers. That could mean a new era of cyberattacks.

CBS NEWS

Colonial Pipeline ransomware attack prompts first cybersecurity mandates for nation's pipelines

The Washington Post

Ransomware attack struck between 800 and 1,500 businesses, says company at center of hack

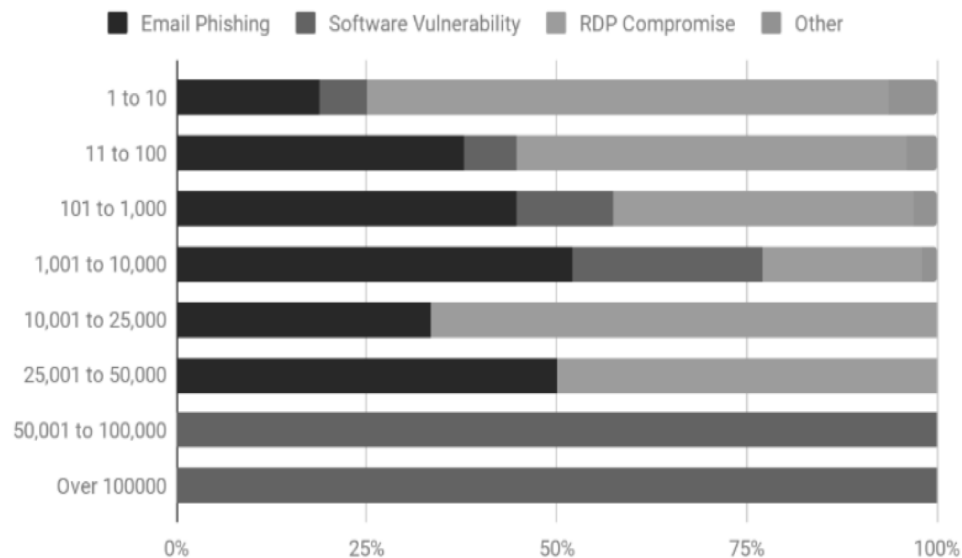
December 10, 2021 | Proprietary and Confidential

**For Drill Purposes Only*

Recent Victim Statistics

- Coveware Q2 2021 Report

Attack Vector by Company Size



Incident Duration and Business Interruption of a Ransomware Attack

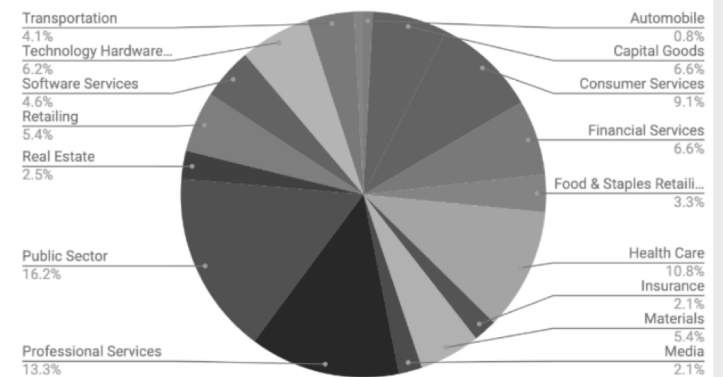
Average Days of Downtime

23

-15% from Q1 2021

Distribution of Ransomware Attacks by Industry in Q2 2021

Common Industries Targeted by Ransomware Q2 2021



Ransomware – By the Dollars

Ransomware: a call for enhanced resiliency

Ransomware is a dynamically evolving risk, impacting organizations around the world with rapidly increasing loss frequency and severity.

AIG's insights are intended to focus conversations around loss preparation and risk management, and help guide well-informed cybersecurity investments.

Cybercrime, and specifically ransomware, is growing exponentially.

By 2025, Global cybercrime damage costs expected to reach

\$10.5 trillion

\$325m
2015



\$20bn

2021

Global ransomware damage costs predicted to reach \$20bn in 2021, up from \$325m in 2015.

Every



A ransomware attack on businesses predicted, by 2021.

Source: Cybersecurity Ventures



Ethics: Del. Rules of Prof'l Conduct

- Rule 1.1 - Competency
- Rule 1.6 - Confidentiality
- Rule 1.9 - Duties to former clients
- Rule 1.15 - Duty to safeguard client property
- Rules 5.1 & 5.3 - Duties to supervise

Rule 1.1 – Competency

- “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”
- Cmt. 8: “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.”

Duty of Technology Competence

- In 2021, California became the 39th state to adopt the duty of technology competence

Source: [Lawsitesblog.com](https://lawsitesblog.com)

Rule 1.6 – Confidentiality

- 1.6(a): “A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent. . . .”
- 1.6(d): “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”
- Cmt. 18: “The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.”

Rule 1.6 – Confidentiality

- Cmt. 18: Factors for reasonableness:
 - Sensitivity of info
 - Likelihood of disclosure if no add'l safeguards used
 - Cost and difficulty in implementing safeguards
 - Extent to which safeguards adversely affect lawyer's ability to represent clients
 - Client may require special security measures or give informed consent to forego security measures
 - Rule does not address other legal obligations

Rule 1.6 – Confidentiality

- Cmt. 19: “When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. . . .”

Rule 1.9 –Former Client Duties

- 1.9(c)(2): “A lawyer who has formerly represented a client . . . shall not thereafter . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client.”
- See also 1.6, cmt. 20: “The duty of confidentiality continues after the client-lawyer relationship has terminated.”

Rule 1.15 – Safekeeping Property

“A lawyer shall hold property of clients or third persons that is in a lawyer’s possession in connection with a representation separate from the lawyer’s own property Other [non-fund] property shall be identified as such and appropriately safeguarded. ”

Rule 5 – Duty to Supervise

5.1(b): “A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.”

5.3(b): “[A] lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person’s conduct is compatible with the professional obligations of the lawyer.”

- law firm staff, but also vendors

ABA Op. 477R - Encrypted Emails

- Attorneys must act competently and must take reasonable measures to protect client confidentiality in all electronic communications.
 - What is reasonable should be determined on a case-by-case basis.
 - Factors to consider:
 - the sensitivity of the information;
 - the likelihood of disclosure if additional safeguards are not employed;
 - the cost of employing additional safeguards;
 - the difficulty of implementing the safeguards; and
 - the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

ABA Op. 477R - Encrypted Emails

- “Using unencrypted email may be appropriate for routine or low sensitivity communications.”
- “[C]yber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email.”
- “[A] fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances.”

ABA Formal Opinion 483

Data Breach Notification Obligations

- When a data breach is either suspected or detected, a lawyer must act reasonably and promptly to contain the breach, mitigate the damage, and notify clients.
- A data breach is a “data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer’s ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.”

ABA Formal Opinion 483

Data Breach Notification Obligations

- Lawyer must notify client of a data breach and keep client reasonably informed of investigative status.
 - Minimum disclosure: “there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred.”
 - “Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact.”
- Continuing duty to keep clients reasonably informed of material developments.

Remote Work Life



PA Formal Opinion 2020-300

- Ethical Obligations for Attorneys Working Remotely
- Overview of Professional Rules 1.1, 1.6, 5.1 and 5.3
- Practical tips:
 - Make sure client communications are confidential (private area, turn off virtual assistants, use encryption)
 - Adopts ABA Formal Op. 477R on Duty of Confidentiality, fact-based analysis
 - Use virtual private networks, secure WiFi, multi-factor authentication
 - Ensure video conferences are secure
 - Take steps to secure your home office
 - Remember to act with civility

ABA Formal Op. 495 – Lawyers Working Remotely

Lawyers can practice remotely but:

- Limited to the law of jurisdictions in which they are licensed
- Not permitted if local jurisdiction has determined remote practice is unlicensed or unauthorized practice of law
- Cannot hold self out as being licensed to practice in local jurisdiction
- Cannot provide or offer legal services in local jurisdiction

ABA Formal Op. 498 – Virtual Practice

- “Virtual practice” = “technologically enabled law practice beyond the traditional brick-and-mortar law firm
- Rules of Prof. Conduct permit virtual practice, but the Rules still apply
- Implicates Rule 1.1 (competence), Rule 1.3 (diligence), Rule 1.4 (communication), Rule 1.6 (confidentiality), and Rules 5.1 and 5.3 (supervision)
- Specific considerations:
 - Secure technology: WiFi, VPN, Portals, password protocols, firewalls, anti-malware software, encryption, paying attention to terms of service for hardware and software, file access and backup, BYOD
 - Virtual meeting platforms – secure online and in remote office environment
 - Turn off smart speakers and virtual assistants
 - Policies to deal with supervision of subordinates, staff and vendors
 - Not everything can be done virtually: mail, checks, accounting

Florida

The Florida Bar re: Advisory Opinion – Out-of-State Attorney Working Remotely from Florida Home, No. SC20-1220 (Fla. May 20, 2021).

- Approved a proposed advisory opinion from Standing Committee on Unlicensed Practice of Law
- The attorney seeking the opinion was:
 - licensed to practice in New Jersey and USPTO, but not in Florida.
 - employed by New Jersey law firm that had not offices in Florida.
 - working remotely from his Florida home
 - handling only federal intellectual property matters (no Fla. Law)
 - without a public presence or profile in Florida as an attorney (using NJ contact info)
 - not soliciting or representing Fla. Clients

Florida

- Attorney testified: “we’ve tried to set up and utilize the technology in a fashion that essentially places me virtually in New Jersey. But for the fact that I’m physically sitting in a chair in a bedroom in Florida, every other aspect of what I do is no different than where I’m physically sitting in a chair in Eatontown, New Jersey and that’s the way I tried to and have structured it so that the public sees a present in, in Eatontown, New Jersey and no other presence.”
- Florida Supreme Court: the facts do not implicate the unlicensed practice of law in Fla.
 - Not providing services to Fla. Residents
 - Not holding himself or firm out as having Fla. Presence
 - Also credited testimony from a Fla. Attorney that after the pandemic, more and more professionals will be working remotely, and that’s not something to discourage (but seems to limit comments to attorney roles where physical presence is not relevant and not soliciting/serving clients in the state where not licensed)

California

- State Bar of Cal. Standing Comm. on Prof. Resp. and Conduct Formal Op. No. 20-0004 (remote work)
 - Concludes that lawyer ethical duties must be upheld when working remotely
 - Firms should enact reasonable measures and policies to meet those duties, especially as to confidentiality, technology competence, communication and supervision.
 - Firm must take steps to ensure the technology it uses, such as cloud providers, is secure
 - Lawyer must protect confidentiality as to household members and maintain ability to communicate with client in an emergency
 - Tech guidance: MFA, strong passwords, auto logoffs, shut off smart speakers
 - Counsel clients on using technology (muting microphones, privilege, etc.)
 - Also consider health as part of duty of competence

Delaware

- DSBA Committee on Professional Ethics Formal Op. 2021-1 (July 9, 2021) (remote work)
- First opinion since 2011
- Largely follows ABA Formal Op. 495
- Concludes that a Delaware-licensed attorney may practice Delaware law while working remotely from a jurisdiction where not licensed under DLRPC 5.5:
 - unless the law or rule of the local jurisdiction prohibits it, and
 - Provided the lawyer doesn't hold self out to be licensed there or have an office there or provide services for matters subject to the local jurisdiction
- Does not address the requirement of maintaining a bona fide office in DE for practicing law

ABA Formal Op. 496

Responding to Online Criticism

- Key is Duty of Confidentiality
- Cannot reveal information relating to client representation or that could lead to discovery of confidential information by another
- Negative review does not qualify under Rule 1.6(b)(5) as a permissible disclosure to defend yourself in defense to a criminal or civil charge
- Recommends:
 - Consider not responding
 - Can invite client to contact offline
 - Say professional obligations preclude a response

Current Threats to Law Firms and Businesses

Attorney, Law Firms & Court Incidents:

New York Courts (Feb. 2021)

- Report of Commission to Reimagine the Future of New York's Court's technology working group issued a report following a survey of judges, court attorneys, and court staff on remote judging
- Found that 42% of the 1,911 respondents were using personal electronic devices to conduct court business remotely
- Also noted failures to protect those personal devices: no MFA, lack of central control
- Recommended court business be done on court-issued devices
- However: only 52% of respondents had court-issued mobile devices
- Judges have devices to work from home, but only 62% have scanners and 83% have printers at home

Attorney, Law Firms & Court Incidents:

Social Media Misfits:

In re O’Gara, Decision and Order Imposing Public Admonishment (Cal. Comm’n Jud. Perf. Sept. 14, 2021)

- L.A. County Superior Judge published and liked comments critical of new District Attorney for L.A. County in a Facebook group with 16,000 members
- The judge also used twitter (under his own name) to post, re-tweet or like content that included partisan viewpoints on controversial issues (politics, BLM protests, gun control, racial bias against Asians, victims of sexual assault, bias against certain religions, death penalty)
- Commission found the comments were partisan and gave the appearance of bias against the D.A., whose office had cases pending before the judge; were a failure to uphold high standards of conduct and promote public confidence in integrity and impartiality of judiciary

Attorney, Law Firms & Court Incidents:

In re Robertelli, No. 084373 (N.J. Sept. 21, 2021)

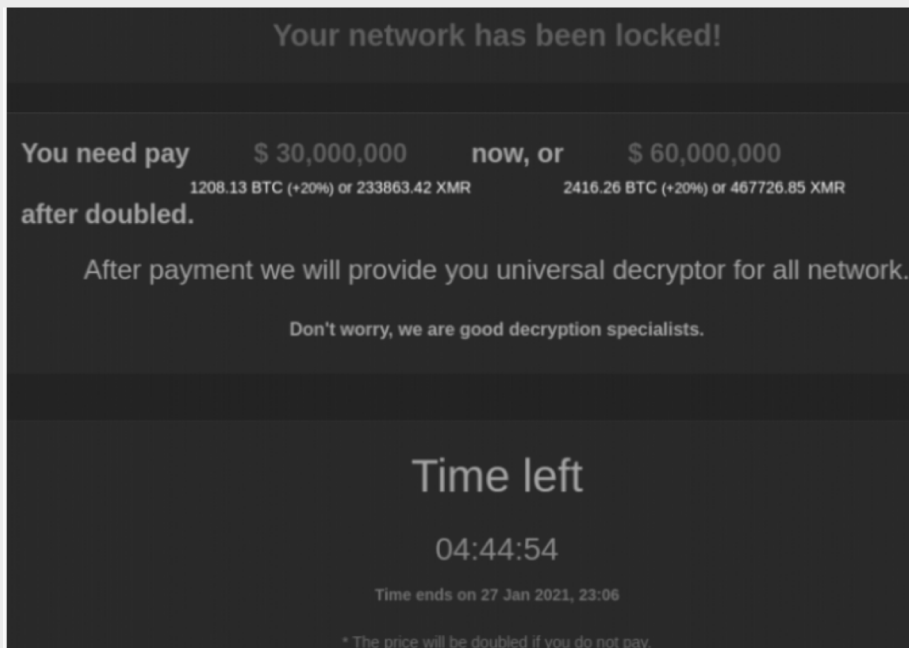
- Attorney had his paralegal do research on a defendant in a personal injury suit. She looked at the defendant's Facebook profile, sent him messages, "friended" him, and downloaded photos that the attorney tried to use in the suit
- Supreme Court of New Jersey concludes that the Office of Attorney Ethics filed to establish an ethical violation by clear and convincing evidence
- Timing: the Facebook contact happened in 2007, before social media was ubiquitous and there was no ethical guidance on using it to research opponents
- Court: Attorney had a "good faith misunderstanding" of Facebook then. Not "tech savvy". Obtained office computer only two years earlier.
- BUT NOW: it's clear an attorney cannot "friend" someone to give access to private information under the Rules of Professional Conduct

Ransomware+ “Double Extortion” Attacks



Negotiating with Hackers

- From Maze to Darkside



The DarkSide ransomware note.

To recover your files, you must pay the ransom.

Your current ransom price should be negotiated.

Message us in chat, to get further details.

This is the BTC address to which you must send bitcoins:

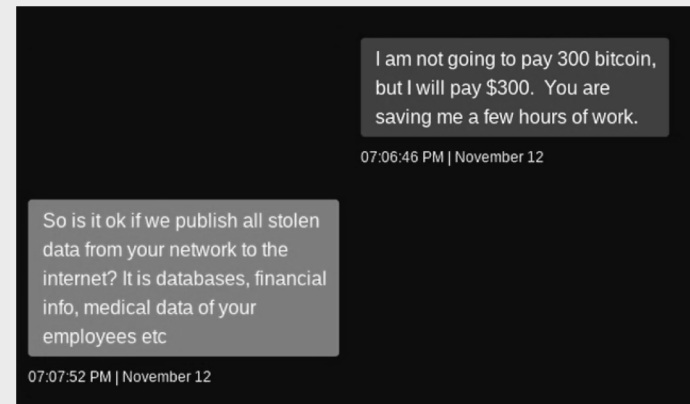
3HNEJTMdmoDbuoNws4guP31e3YfyXmPqqB

To see how to buy the bitcoins, click [Buy Bitcoins](#) at the tab menu on top of the page.

We are providing 3 test decrypts, to prove that we can recover your files.

Click [Test Decrypt](#) at the menu on top of this the page to decrypt 3 files for free.

Attention! We are decrypting only image files for free, as they do not have any significant value to you.



Darkside Attack Chat Excerpts

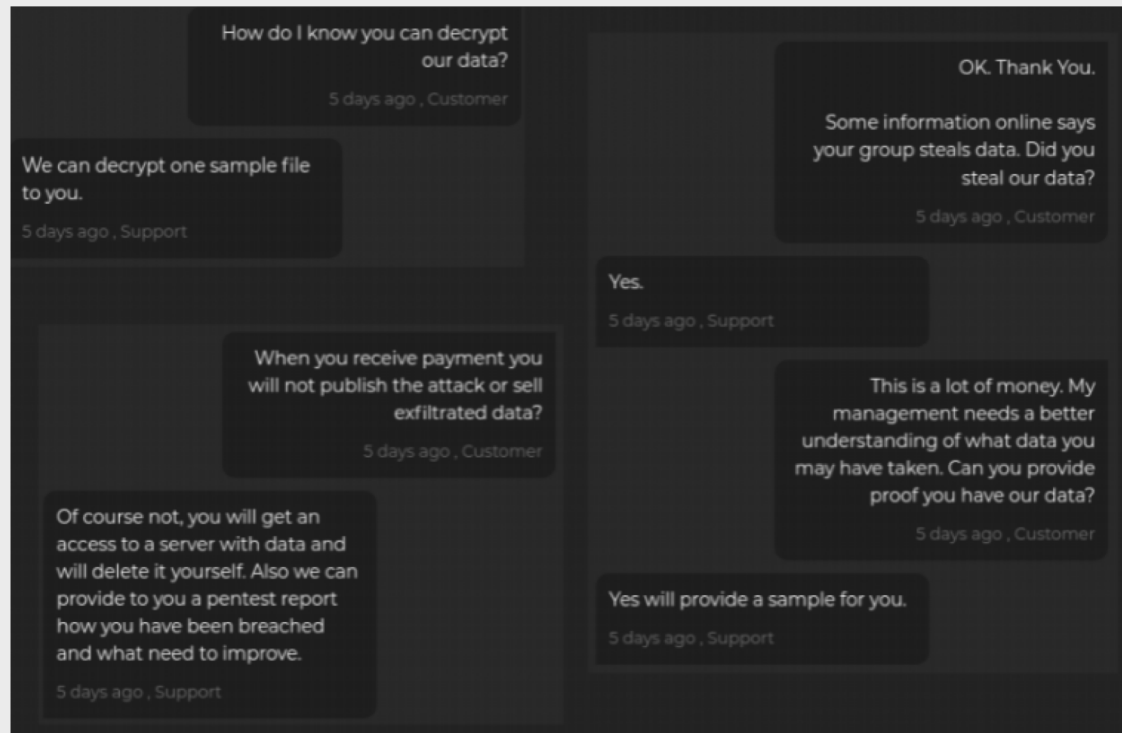


Image: Intel 471.

Darkside Attack Chat Excerpts

The victim firm replies a day later saying they've gotten authority to pay \$4.75 million, and their tormentors agree to lower the demand significantly to \$12 million.

I only have authority for \$4.75 million. That is more than double my offer. Will you accept that? If not, I need additional time to try to get more. It's the middle of night here. I need until Thursday or you can take the \$4.75 million.

4 days ago , Customer

Your last price will be 12 million, provided that you pay 4.7 million now and the remaining amount within 72 hours.

3 days ago , Support

Image: Intel 471.

Darkside Attack Chat Excerpts

The victim replies that this is still a huge amount, and it tries to secure additional assurances from the ransomware group if it agrees to pay the \$12 million, such as an agreement not to target the company ever again, or give anyone access to its stolen data. The victim also tried to get the attackers to hand over a decryption key before paying the full ransom demand.

That is still a lot of money. To resolve this quickly, we will agree to pay on your terms, as long as you turn over the decryption tools with our initial payment of \$4.7 million and agree to immediately disconnect from our systems. Upon payment of the remaining \$7.3 million within 72 hours, you will – 1. provide us access to all of the data you took. 2. agree not to post information about this incident. 3. agree not to sell, share, or retain any copies of our data. 4. provide detail on how you were able to gain access. 5. agree to never target our company again. 6. not give access to or assist anyone else in gaining access. Are these terms acceptable to you?

3 days ago , Customer

Darkside Attack Chat Excerpts

The crime gang responded that its own rules prohibit it from giving away a decryption key before full payment is made, but they agree to the rest of the terms.

We cannot agree to comply with ALL your terms because issuing a decryption tool before full payment violates the Darkside rules, and we cannot change these rules. Darkside values its reputation and you can easily find information that all the conditions have always been met. At this point, we can only promise that we will not launch any new attacks. After full payment, we guarantee: 1. You will get the tool and be able to fully decrypt the encrypted data. 2. We will completely leave your network and it will never be our target again. 3. You will get access to the data, delete it yourself. They will never be published or resold, as it doesn't make sense given the amount of the buyout. 4. You will receive a full report on our actions, how we got into the network and how the attack was carried out. And the report will also contain tips for improving security, and protecting against the penetration of other hackers.

3 days ago , Support

Darkside Attack Chat Excerpts

The victim firm agrees to pay an \$11 million ransom, and their extortionists concur and promise not to attack or help anyone else attack the company's network going forward.

We agree to your terms. We will send the \$4.7 million now and work to get you the remaining \$7.3 million by the end of today – no later than within the deadline. In addition to the points below, please confirm that you will not assist anyone else in targeting our network.

3 days ago , Customer

OK. Our promise - we will not attack your network, and we will not help anyone to attack your network. We will completely leave your network after the transaction is completed. Please note that the payment terms differ depending on the selected coin. Let us know what coin you will use to make the payment, and we will fix the amount and the exchange rate.

3 days ago , Support

Image: Intel 471

Key Issues in Responding to Ransomware Attacks

Detection,
Containment and
Team Scaling

Remediation
Planning –
operationally
down, extortion

Crisis
Management and
Communications

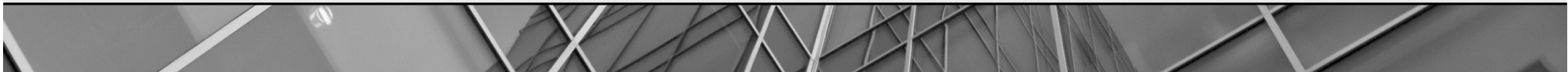
Threat Actor
Engagement and
Ransom
Negotiation

OFAC and Law
Enforcement
Issues

Insurance support,
Documentation
support from
vendor

Legal Disclosure
Obligations

Litigation Planning



Ransomware and Cyber Extortion

OPFAC Updated Advisory – September 2021



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments¹

Date: September 21, 2021

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.²

Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. The U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks.


OFAC Ransomware Guidance

Facilitating a Ransomware Payment May Violate OFAC Regulations

- IEEPA/TWEA -- U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria).
- Any transaction that causes a violation under IEEPA is also prohibited.
 - U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons, which could not be directly performed by U.S. persons due to U.S. sanctions regulations.
- OFAC may impose civil penalties for sanctions violations based on strict liability.
- DOJ may prosecute willful violations of IEEPA/TWEA
 - IEEPA – willfully attempting, conspiring, causing or violating any license, order, regulation or prohibition issued under the statute.
 - TWEA – willfully violating any provision of TWEA or any license, rule, order or regulation issued thereunder.

OFAC Ransomware Guidance

General Factors Affecting Administrative Action -- 31 C.F.R. Pt. 501 App. A, § III

- Willful or Reckless Conduct (knowledge of violation of US law/failure to exercise minimal degree of caution/care, disregard for warning signs)
 - Concealment (hiding conduct to mislead OFAC, federal, state or foreign regulators or other involved parties)
 - Pattern of Conduct (pattern or isolated/atypical occurrence)
 - Prior Notice (reasonably on notice that conduct was illegal)
 - Management Involvement (D&O, supervisory or managerial staff aware or should have been aware)
 - Awareness of Conduct (greater the actual knowledge, greater the penalty)
 - Harm to Sanctions Program Objectives (benefit to sanctioned person/entity; impact on US policy; license eligibility; humanitarian activity)
 - Individual Characteristics (commercial sophistication, operational size and financial condition, transaction volume, sanctions history, compliance program, voluntary corrective action)
 - Cooperation with OFAC (voluntary self-disclosure, production of all relevant information, SOL tolling)
- 

OFAC Ransomware Guidance

Notifying Law Enforcement Prior to Any Ransom Payment is Key

- “OFAC will also consider a company’s self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus.”
- “OFAC will also consider a company’s full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.”
- “Companies involved in facilitating ransomware payments on behalf of victims should also consider whether they have regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations.”
 - FinCEN Guidance, FIN-2020-A006, “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,” October 1, 2020 (AML obligations related to financial institutions in the ransomware context).
 - FI/FS/MSBs are subject to BSA/AML requirements, including filing SARs where they know suspect or have reason to suspect a transaction > \$5K involves proceeds of illicit activity, attempts to disguise funds derived from illegal activity, is designed to evade BSA regs, lacks a business or lawful purpose, or involves use of an FI to facilitate criminal activity.

OFAC Updated Ransomware Guidance – Sept. 2021

Sanctions Compliance Program and Defensive Resilient Measures

- “[t]he existence, nature and adequacy of a sanctions compliance program is a factor” in OFAC enforcement determinations.
 - Implementation of a risk-based compliance program mitigates exposure to sanctions-related violations.
 - Integrate ransomware response activities into existing compliance programs.
- Adoption and improvement of cybersecurity practices “will be considered a significant mitigating factor in any OFAC enforcement response.”
 - See [CISA September 2020 Ransomware Guide](#)
 - Key steps highlighted in OFAC Guidance:
 - Offline data backups
 - Incident response planning
 - Cybersecurity training
 - AV/Anti-Malware updating and software patching
 - Authentication protocols and access management (MFA, etc.)
- “OFAC will consider a company’s self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies . . . made as soon as possible after discovery of an attack . . . to be a voluntary self-disclosure and a significant mitigating factor”
 - “OFAC will also consider a company’s full and ongoing cooperation with law enforcement both during and after a ransomware attack – e.g., providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible – to be a significant mitigating factor.”
- Following the steps above would make it more likely that OFAC would resolve sanctions violations with a non-public response.

DOJ Guidance on Cyber Threat Intel/Purchasing Illicit Data

- Key Factors in DOJ View of Purchasing Stolen Data
 - Legitimate data owner or agent
 - Type of data (possession/transfer itself unlawful)
 - Identity of seller (prohibited person)
- In the last several years, USG has issued executive orders sanctioning Iranian, North Korean, and Russian individuals and entities for national security reasons, including cyber-related misconduct.
- “Because the identity of anyone selling stolen data in a Dark Market is likely to be masked by a pseudonymous online persona, it is unlikely that the true identity of the seller of stolen data will be known or knowable to a buyer. Where a buyer does not know the identity of the seller and, therefore, does not know the buyer is the subject of economic or trade sanctions, a criminal prosecution requiring proof of willful intent might not be possible to bring.”
- Civil enforcement of IEEPA may be imposed on the basis of “strict liability”

Ransomware and Civil Litigation

Silar v. Springhill Medical Center (Ala Cir. Ct. 2021)



A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death

A lawsuit says computer outages from a cyberattack led staff to miss troubling signs, resulting in the baby's death, allegations the hospital denies

Springhill Medical Center delivery room following a 2015 remodel. FRANK MODARELLI/ENVISIA360

By [Kevin Poulsen](#), [Robert McMillan](#) and [Melanie Evans](#)
Sept. 30, 2021 9:36 am ET

SHARE TEXT

292 RESPONSES

Listen to article (11 minutes)

When Teiranni Kidd walked into Springhill Medical Center on July 16, 2019, to have her baby, she had no idea the Alabama hospital was deep in the midst of a [ransomware attack](#).

For nearly eight days, computers had been disabled on every floor. A real-time wireless tracker that could locate medical staff around the hospital was down. Years of patient health records were inaccessible. And at the nurses' desk in the labor and delivery unit, medical staff were cut off from the equipment that monitors fetal heartbeats in the 12 delivery rooms.

Amid the hack, fewer eyes were on the heart monitors—normally tracked on a large screen at the nurses' station, in addition to inside the delivery room. Attending obstetrician Katelyn Parnell texted the nurse manager that she would have delivered the baby by caesarean section had she seen the monitor readout. "I need u to help me understand why I was not notified." In another text, Dr. Parnell wrote: "This was preventable."



Screenshots of texts between obstetrician Katelyn Parnell and the nurse manager, and between Dr. Parnell and another colleague, submitted as evidence in the lawsuit.

Ms. Kidd has sued Springhill, alleging information about the baby's condition never made it to Dr. Parnell because the hack wiped away the extra layer of scrutiny the heart rate monitor would have received at the nurses' station. If proven in court, the case will mark the first confirmed death from a ransomware attack.

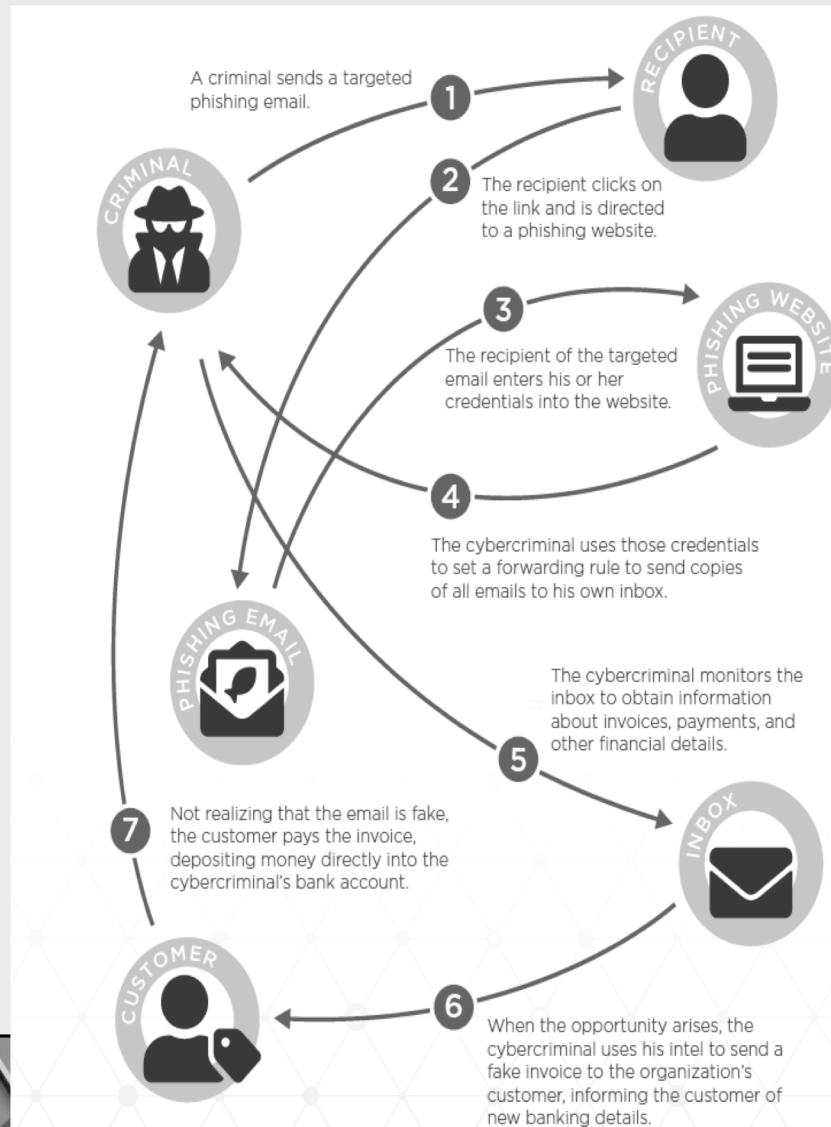
The hospital denies any wrongdoing. In an emailed statement to The Wall Street Journal, Springhill CEO Jeffrey St. Clair said the hospital handled the attack appropriately: "We stayed open and our dedicated healthcare workers continued to care for our patients because the patients needed us and we, along with the independent treating physicians who exercised their privileges at the hospital, concluded it was safe to do so."

SaaS Provider Sued for “Double Extortion” Attack

In re Blackbaud, Inc., Customer Data Breach Litig., MDL No. 2972, 2021 WL 4866393 (D. S.C. Oct. 19, 2021).

- 29 lawsuits against SaaS provider for non-profits and public sector entities consolidated in SC following ransomware/“double extortion” attack.
- SaaS provider has a common law duty to use reasonable care to protect the personal information of third party individuals with whom the provider has no direct relationship.
- SC Supreme Court would recognize a common law tort duty of care under the facts, because: (1) Blackbaud’s contractual relationship with its customers required it to “collect and protect information of third parties (including plaintiffs’ personal and medical information); and (2) Blackbaud exercised the greatest level of control over the security of the data stored in its cloud-based systems and remained best positioned to prevent the harm associated with a data breach of its systems.
- General rule: “there is no general duty to control the conduct of another or to warn a third person or potential victim of danger.”
- Exception applies here because Blackbaud “negligently or intentionally create[d] the risk” of a data breach. In particular, the plaintiffs sufficiently alleged that “Blackbaud had a duty to protect plaintiffs from the criminal conduct of third parties based on Blackbaud’s own negligent conduct in creating the risk by failing to use reasonable security measures.” Moreover, the plaintiffs sufficiently alleged that Blackbaud was aware that a lack of reasonable security could result in a cyberattack, but “failed to correct, update, or upgrade its security protections.”

Social Engineering Schemes – The Business Email Compromise & Phishing



Ways to Send Fraudulent Emails

1. Get unauthorized access and send messages from the victim's email account.
2. Create another email account mimicking the victim's email account, as in the following:
 - ed@dlapiper.com
 - ed@d1apiper.com
3. Spoof the victim's email account to make the "From:" field falsely list his account.

Business Email Compromises Leading to Litigation

Chancery Probes Contract Risks In \$130M Merger Hack



By Leslie Pappas · Listen to article

Law360 (December 9, 2021, 9:04 PM EST) -- A Delaware Chancery Court judge on Thursday strained to understand who was contractually responsible for the loss of a payout to stockholders in a \$130 million merger after hackers diverted the payout to a Chinese bank account, leaving the Utah stockholders, New York payment agent, and the merger parties pointing fingers.

At a hearing on defendants' motions to dismiss the case, Vice Chancellor Sam Glasscock III pushed the parties to explain how the merger contracts laid out who was responsible for what.

"This is a case where there was a third party who came in and stole the money," the vice chancellor said. "The only question for me, really, is how did the parties allocate the risk?"

The shareholders who gave up their stock but never got paid sued the payment agent and the merger parties in Delaware's Court of Chancery in May for breaches of contract, unjust enrichment, negligence and breach of fiduciary duty.

The 2019 merger was a \$130 million acquisition of Graduation Alliance Inc., a Salt Lake City-based education company, by Tassel Parent Inc, a subsidiary of New York investment firm Kohlberg Kravis Roberts & Co. LP.

Useful Tools & Links

- Add to Briefcase
- Save to PDF & Print
- Rights/Reprints
- Editorial Contacts

Related Sections

- Banking
- Commercial Contract
- Cybersecurity & Privacy
- Delaware
- Mergers & Acquisitions
- New York
- Securities

Law Firms

- Bayard PA
- Hodgson Russ
- Kirkland & Ellis
- Kirton McConkie
- Morris James
- Ross Aronstam

Companies

- Shareholder's sue after stock payment is re-directed to cybercriminals.
- Payment to be made to Utah bank, per merger agreement and transmittal letter.
- Shareholders email account hacked and new payment instructions sent to law firm.
- Law firm does not spot fraud and forwards payment instructions to payment agent, which transfers sales proceeds to threat actor account in Hong Kong.

Legal Liability for Business Email Compromises

- Courts look to general contract law principles to determine how a fraud-induced financial loss should be apportioned between the parties.
- UCC Article 3 “Imposter Rule” (UCC § 3-404(d))
 - if a person paying the instrument . . . **fails to exercise ordinary care in paying** . . . the instrument and **that failure substantially contributes to loss** resulting from payment of the instrument, the **person bearing the loss may recover** from the person failing to exercise ordinary care **to the extent the failure to exercise ordinary care contributed to the loss.**
- Relying on UCC and common law, courts employ a multi-factor approach to determine which party had the greater opportunity to discover the fraud and prevent the financial loss.
 - *See, e.g., Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc.*, 759 Fed. App’x 348, 357 (6th Cir. 2018) (applying Ohio law) (“losses attributable to fraud should be borne by the party in the best position to prevent the fraud”); *Arrow Truck Sales, Inc. v. Top Quality Truck & Equipment, Inc.*, No. 8:14-cv-2052-T-30TGW, 2015 WL 4936272, at *1 (M.D. Fla. Aug. 18, 2015); *J.F. Nut Co. v. San Saba Pecan, LP*, No. A-17-CV-00405-SS, 2018 WL 7286493, at *3 (W.D. Tex. July 23, 2018).

Legal Liability for Business Email Compromises

- Courts have emphasized the following factors in their analyses:
 - whether either (or both) parties' email account was compromised and used to facilitate the fraudulent re-direction of payments;
 - whether any email account compromise resulted from negligent cybersecurity practices;
 - whether the party receiving revised wiring instructions by email independently verified the revised instructions by phone call or other method distinct from email;
 - the suspicious nature of the revised wire instructions, such as instructions to wire payments to a different bank, account, or payee than previously communicated or used;
 - the timing of all email communications related to the underlying transaction;
 - whether either party suspected or reasonably should have suspected the potential for fraud based on all known facts, and whether that party warned the other party.

Legal Liability for Business Email Compromises

- Parties generally cannot recover losses from either the sending or receiving banks.
- UCC Article 4A-202
 - A “sender” in whose name a “payment order” (wire transfer) is issued is liable to its bank for the amount of wire transfer if the order is either “authorized” or “verified” pursuant to an agreed-upon “security procedure” which is “commercially reasonable.”
 - The threshold for whether an order is authorized in this context is very low, similar to a “general intent” type of standard whereby the sender’s initiation of the payment – even if it was fraudulently induced by a third party – will satisfy the standard.
 - UCC Article 4A generally preempts common law claims asserted against banks for wire transfers.

State Data Security Laws

- 26 states have enacted general data security laws
- 11 states have adopted a version of the NAIC Model Insurance Data Security Act (as of June 2020)
- Data security laws generally require businesses to:
 - Maintain appropriate security policies, procedures and safeguards (encryption, least privilege, multi-factor authentication)
 - Appoint a cybersecurity leader
 - Create an Incident Response Plan
 - Train employees
 - Oversee service providers
 - Periodically assess risks
 - Monitor their programs
 - Fund their programs
 - Maintain Board Oversight

Business Email Compromise Checklist

Have you been a victim of CEO or Wire Transfer Fraud, commonly known as Business Email Compromise (BEC)? Review the checklist below for immediate actions:

IMMEDIATE ACTIONS

Reporting the Incident

- ☐ Contact your bank
 - ☐ Determine the appropriate contact at your bank, who has the authority to recall a wire transfer
 - ☐ Notify your bank you have been the victim of a Business Email Compromise
 - AND -
 - ☐ Request a wire recall or SWIFT Recall Message
 - AND -
 - ☐ Request they fully cooperate with law enforcement
- ☐ Report the incident (or attempt) to the FBI at www.IC3.gov
 - ☐ Provide all details for the beneficiary: account numbers, contact information, names
- ☐ Contact your local FBI Field Office

Internal Actions

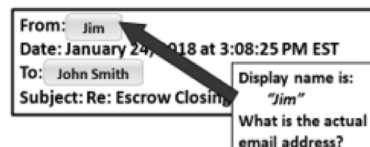
- ☐ Review all IP logs accessing the relevant infrastructure (internal mail servers or other publically accessible infrastructure) – looking for unusual activity
- ☐ Scan for log-in locational data. Was there a log-in from an unknown country or location, specific to that email account?
- ☐ Review the relevant email account(s) which may have been spoofed or otherwise compromised for any rules such as “auto forward” or “auto delete”
- ☐ Inform employees/agents of the situation and require they contact clients and customers who are near the wire transfer stage
- ☐ Review all requests that asked for a change in payment type or location.

****Remain especially vigilant on transactions expected to occur immediately prior to a holiday or weekend. ****



PREVENTION & RECOGNITION

- ☐ Hover your cursor over, or expand contact details on, suspicious email addresses – Looking for indications of Display Name Deception or Spoofing



- ☐ DO NOT hover on **links** within emails, as simply hovering *may* execute commands.
- ☐ Call a known/trusted phone number or meet in person to confirm that the wire transfer information provided to you, matches the other party's information
- ☐ Does the Routing Number or SWIFT Number provided to you, resolve to the expected bank used by the other party?
(Example: Have you received wire information for an account at a Hong Kong bank; however, your other party only banks in the U.S?)
Possible websites to verify a Routing or SWIFT Number:
 - a. Any reputable search engine
 - b. The Federal Reserve www.FRBServices.org
 - c. American Bankers Association <https://routingnumber.aba.com>

- ☐ Regularly check your email account log-in activity for possible signs of email compromise
- ☐ Develop an intrusion detection system to identify emails from extensions that are similar to your company email.
- ☐ Regularly check your email account for new “rules”, such as email forwarding and/or auto delete
- ☐ Be cautious of “new” customers, suppliers, clients and/or others you don't know who ask you to:
 - a. ...open or download any documents they send
 - OR -
 - b. ...sign into a separate window or click on a link to view an invoice or document
 - OR -
 - c. ...provide sensitive Personal or Corporate information
- ☐ Verify the wire instructions you provide to your customers/clients are accurate for both the pertinent bank and pertinent account.
 - a. Where did you get the account data?
 - b. Is this the correct account number?

Key Causes of Action in Data Breach Class Actions

Negligence

Negligence Per Se

Negligent Failure to Warn

Breach of Contract/Implied Contract

Violation of federal/state privacy and information security statutes

Violation of Breach Notification Statutes

Unfair Trade Practices/Consumer Fraud

Fraudulent Misrepresentation

The Marriott Data Breach Cases

Consumer Class Actions Survive Dismissal

- Marriott sued for data breach of Starwood Reservation System that exposed personal information of up to 500 million people. Breach began before and continued after Marriott's 2016 purchase of Starwood for \$13 billion.
- MDL with numerous tracks venued in the District of Maryland.
- Marriott motion to dismiss largely denied on bellweather consumer claims
 - Failure to provide timely data breach notifications (Md & Mich law)
 - Negligence – there is a duty to reasonable safeguard consumer data (Ga, Fla)
 - Breach of contract (Md, NY, Or)
 - Consumer protection statutes (Cal, NY UDAP laws)
- Accenture motion to dismiss largely denied on similar claims (negligence and negligence *per se* in various states)
 - Intimate Nexus Exception to Economic Loss Doctrine applied because Accenture was providing IT and cybersecurity services for systems holding consumer personal information.
 - Duty arose under Section 5 of FTC Act and state common law (Md, Conn, Fla, Ga).

Shareholder Litigation Fails

- June 11, 2021 – Judge Grimm (D. Md.) grants motions to dismiss breach-related securities and derivative suits.
- Consolidated Securities Complaint – Alleged violations of Section 10(b) and 20(a) of Securities Exchange Act of 1934 and Rule 10b-5, based on 73 statements or omissions.
 - P's failed to allege: (1) a false or misleading statement; (2) strong inference of scienter; or (3) loss causation.
 - Statements re due diligence, optimism for merger success; cautionary statements; risk factor disclosures were sufficient. No misrepresentation regarding actual data breach.
 - No intent to deceive based on cybersecurity remediation plan, incident response activities and notification of law enforcement.
- Consolidated Shareholder Derivative Complaint – failure to pled ownership, demand futility, and failure to state a claim.

Firemen's Retirement Sys. v. Sorenson (Del. Ch. Oct. 5, 2021) – Cybersecurity Oversight Under *Caremark*

- VC Will dismisses shareholder derivative action alleging breach of fiduciary duty claims on statute of limitations and failure to plead demand futility.
- Alleged breaches of fiduciary duty
 - Failure to conduct cybersecurity due diligence
 - Failure to implement adequate cybersecurity controls following discovery of deficiencies
 - Concealing data breach between September and November 2018
- All claims barred because demand was not excused, where no director faces a substantial likelihood of liability on a non-exculpated claim.
- First, any claims based on failure to conduct cybersecurity due diligence were barred by 3-year statute of limitations.

Firemen's Retirement Sys. v. Sorenson (Del. Ch. Oct. 5, 2021) – Cybersecurity Oversight Under *Caremark*

- “[A]s the legal and regulatory frameworks governing cybersecurity advance and the risks become manifest, corporate governance must evolve to address them. The corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place.”
- “The growing risks posed by cybersecurity threats do not, however, lower the high threshold that a plaintiff must meet to plead a *Caremark* claim. For either prong of *Caremark*, ‘a showing of bad faith conduct . . . is essential to establish director oversight liability.’ Only a ‘sustained or systemic failure of the board to exercise oversight . . . Will establish the lack of good faith that is a necessary condition to liability.”
- No substantial likelihood of liability under *Caremark*.
 - No showing of: (1) a complete failure to exercise cybersecurity oversight; (2) turning a blind eye to known compliance violations; or (3) conscious failure to remediate cybersecurity failures.
 - No showing of bad faith in failure to provide timely data breach notifications to consumers.

Firemen's Retirement Sys. v. Sorenson (Del. Ch. Oct. 5, 2021) – Cybersecurity Oversight Under *Caremark*

- *Caremark* First Prong – board-level monitoring and reporting systems were in place.
 - Board and Audit Committee were “routinely apprised” on cyber risks and mitigation strategies; received annual risk assessment reports; and engaged outside consultants to improve and auditors to audit Marriott’s cybersecurity practices.
- *Caremark* Second Prong – board did not “consciously fail[] to act after learning about evidence of illegality.”
 - No allegation that board knew of legal or regulatory violations.
 - Violation of industry standards (PCI-DSS) does not equal a legal violation.
 - No allegation board consciously disregarded red flags re Starwood cybersecurity deficiencies.
 - Management provided board with a plan to assess cybersecurity gaps.
 - No allegation that board was made aware of data breach notification requirements or deadlines.
- “[T]he difference between a flawed effort and a deliberate failure to act is one of extent and intent. A *Caremark* violation requires a plaintiff to demonstrate the latter.”

A Tort Duty to Safeguard Personal Data

- *Dittman v. UPMC* (Pa. S. Ct. Nov. 21, 2018)
 - Arose out of data breach impacting personal information of all employees.
 - Reversed dismissal of data breach class action.
 - An employer that collects personal information from employees has a common law duty to exercise reasonable care in securing that information against foreseeable cybersecurity risks.
 - The economic loss doctrine does not prevent the recovery of purely economic damages for a data breach under a negligence theory.
 - Broad rationale easily expandable to all data collectors.
- *In re Rutter's Inc. Data Security Litig.*, slip op. (M.D. Pa. Jan. 5, 2021)
 - Denying motion to dismiss negligence claim in data breach class action
 - Extending rationale of *Dittman* to customer bank card data

Hiscox Data Breach Litigation

Hiscox Ins. Co. v. Warden Grier, LLP (W.D. Mo. Dec. 9, 2021)

- Court denies law firm's motion for summary judgment on legal malpractice claim relating to data breach and cyber extortion attack impacting insurance company policyholder data.
- Insurance Co retains law firm to handle insurance coverage and subrogation disputes and provides law firm with access to sensitive personal information for policyholders.
- On February 14, 2017, "The Dark Overlord" group infiltrates law firm server and then threatens to post stolen Hiscox commercial customers' policyholder PII online if a ransom is not paid.
- Law firm pays \$2.4 million ransom, does not inform Hiscox, and does not report data breach to policyholders or regulators.
- In Spring 2018, "The Dark Overlord" demands a new second ransom payment not to post stolen PII online. Law firm does not inform Hiscox, individuals or regulators.
- "The Dark Overlord" informs Hiscox, which contacts law firm, which finally admits breach and extortionate payments.

Hiscox Data Breach Litigation

Hiscox Ins. Co. v. Warden Grier, LLP (W.D. Mo. Dec. 9, 2021)

- Disputed issues of material fact required jury submission of professional negligence claim relating to data breach and adequacy of response/investigation and fulfillment of legal data breach notification obligations.
- Law firm's argument that it had no legal duty to protect client data was meritless. "[A]ll attorneys owe their clients a 'duty to exercise reasonable care.'"
- Whether law firm's particular actions – or failure to act – goes to the element of "breach" – i.e., whether law firm "failed to exercise that degree of skill and diligence ordinarily used under the same or similar circumstances by members of the legal profession."
- This is a quintessential fact question for the jury.
 - Hiscox claimed that law firm breached duty by failing to conduct investigation into and analysis of compromised PII and to determine whether legal notification obligations arose under all applicable state/federal laws.
- Hiscox claimed damages in the amount of its own investigation and analysis of the data and data breach notification obligations.

Key Court Decisions on Privilege In Cyber Incident Litigation

Wengui v. Clark Hill, PLC (D. D.C. Jan. 12, 2021)

- Duff & Phelps forensic report not protected by attorney-client privilege or work product doctrine and must be produced to plaintiff in data breach litigation.
 - D&P retained by law firm after discovery of incident “to prepare for litigation.”
 - Firm produces communications with eSentire, which worked to “investigate and remediate the attack” and to preserve “business continuity.”
 - Firm refuses to produce D&P forensic report and to answer interrogatory as to “understanding of the facts” of the incident – stating that such understanding is based solely on privileged info.
- No Work Product Protection – CH did not meet burden of proving that the report, or a substantially similar report, would not have been created in the ordinary course of business (or absent the risk of litigation).
 - “discovering how a cyber breach occurred is a necessary business function regardless of litigation or regulatory inquiries.”
 - “it is highly likely CH would have conducted an investigation into the attack’s cause, nature and effect irrespective of the prospect of litigation.”
 - No two-tracking: record shows CH replaced eSentire with D&P (no eSentire docs or report after engagement of D&P).
 - Report shared with CH leadership and IT team (not just legal counsel), and with FBI.
 - “Papering” the engagement through attorneys is not sufficient to invoke work product protection.

Key Court Decisions on Privilege In Cyber Incident Litigation

Wengui v. Clark Hill, PLC (D. D.C. Jan. 12, 2021)

- No Attorney-Client Privilege – D&P report is not a communication between attorney and client for purposes of providing legal advice.
 - A/C privilege can cover forensic reports made at an attorney or client's request where the report puts information obtained from the client into a form usable for providing legal advice.
 - The *Kovel* doctrine is construed narrowly because the A/C privilege is absolute.
 - CH's "true objective was gleaning D&P's expertise in cybersecurity, not in obtaining legal advice from its lawyer."
 - Report provides a summary of findings and "pages of specific recommendations on how CH should tighten its cybersecurity."
 - Report was shared with non-lawyers and third parties, including the FBI.
- CH must produce data regarding all clients impacted by the breach because that information "is directly germane to a central issue in the case – . . . the sufficiency and reasonableness of CH's cybersecurity in September 2017."

Key Court Decisions on Privilege In Cyber Incident Litigation

Mass. Attorney General v. Facebook 487 Mass. 109 (Mar. 24, 2021)

- Facebook ordered to produce some records relating to internal investigation into apps on its platform that may have compromised user data as part of AG's Cambridge Analytica investigation.
- Attorney-Client Privilege
 - CID requests for data sufficient to identify apps and developers that FB's external counsel investigated and other information associated with review of identified apps was not protected by AC privilege.
 - CID did not seek data or communications exchanged between counsel and FB.
 - CID requests for all FB internal communications re categories of apps and developers that counsel investigated was protected by AC privilege; investigation was initiated in part to gather facts needed to advise company on various legal risks it faced.
 - The attorney-client privilege applies to communications between counsel and client made as part of an internal investigation that is undertaken to gather facts for the purposes of providing legal advice.

Key Court Decisions on Privilege In Cyber Incident Litigation

Mass. Attorney General v. Facebook 487 Mass. 109 (Mar. 24, 2021)

- Facebook ordered to produce certain attorney work product relating to internal investigation into apps on its platform that may have compromised user data as part of AG's Cambridge Analytica investigation.
- Work Product Doctrine
 - CID requests for data sufficient to identify apps and developers that FB's external counsel investigated and other information associated with review of identified apps was protected by WP Doctrine.
 - Investigation was staffed by outside counsel and forensic consultants and had methodology distinct from FB's ongoing enforcement program, it was focused on past violations, not ongoing operations, and served to defend FB against vast litigation it was facing, rather than just improving its ongoing operations.
 - AG established substantial need for fact work product that could not be obtained without undue hardship.
 - Factual data was central to investigation, as it identified apps that might have misused user data on a prior version of FB's platform
 - AG had mandate to investigate such potential misuse of user data as well as any misrepresentations by FB
 - It was unlikely AGI would be able to obtain substantial equivalent of information
 - AG undoubtedly would incur enormous costs and delay in her investigation if the information was not disclosed
 - Remand was appropriate to determine whether any materials contained opinion work product.

Key Court Decisions on Privilege In Cyber Incident Litigation

In re Rutter's Data Security Breach Litigation (M.D. Pa. July 22, 2021)

- Rutter's ordered to produce Crowdstrike report and communications relating to incident response, rejecting both attorney-client privilege and work product protection.

Key Court Decisions on Privilege In Cyber Incident Litigation

In re Marriott Customer Data Breach Litigation (D. Md. July 12, 2021)

- SM Facciolla Report & Recommendation denying Plaintiff's motion to compel the production of CrowdStrike IR and compromise assessment reports under Rule 26(b)(3) and (b)(4).
- Rule 26(b)(3) (work product) and 26(b)(4) (non-testifying experts) have distinct analyses.
 - “Substantial Need” to obtain “documents and tangible things that are prepared in anticipation of litigation or for trial”
 - v.
 - “Exceptional Circumstances” to obtain “facts known or opinions held”
- Various prior CrowdStrike reports, agreements and communications were protected from discovery under Rule 26(b)(3) and (b)(4).

Cybersecurity Regulatory Enforcement Accelerates

SEC Activity Increases

- First American Financial – SEC Cyber Consent Order (June 24, 2021)
 - Real estate settlement services company pays \$500,000 for alleged failures to disclose cybersecurity flaw that exposes more than 800 million title insurance records dating back to 2003.
 - IT staff allegedly knew of vulnerability at least 5 months before journalist outed FAF in May 2019.
 - Staff allegedly failed to alert senior executives who filed inaccurate securities disclosures.
 - Alleged violation of Rule 13a-15 of Securities Act of 1934 (issuer must maintain effective disclosure controls).
- Solar Winds Securities Fraud Investigation
- Solar Winds Enforcement Sweep and Amnesty Offer (June 2021)

SEC Activity Increases

- Pearson PLC – SEC Cyber Consent Order (August 16, 2021)
 - Educational publisher and services provider pays \$1 million for alleged misleading statements about a 2018 cyber incident resulting in the theft of 11 million student records and 13,000 school district administrator logins.
 - IT staff allegedly failed to patch software vulnerability known to them since September 2018 until they discovered the data theft in March 2019.
 - Staff allegedly failed to alert senior executives who filed inaccurate securities disclosures noting that a data breach was only a “hypothetical” risk.
 - Alleged violation of Sections 17(a)(2) & (a)(3) of Securities Exchange Act of 1933 and Section 13(a) of Securities Act of 1934.

NYDFS Brings First Cyber Enforcement Actions

- First enforcement action settlement announced in March 2021, imposing a \$1.5 million penalty against a licensed residential mortgage broker based on an email compromise that was not disclosed until questioned in an examination.
- It has since settled 3 other enforcement actions (all against life insurers & totaling \$4.8 million) for phishing attacks and compromises of email accounts that lacked multi-factor authentication.
- DFS recently delayed its first cybersecurity administrative trial from August 2021 to Spring 2022, over the objection of respondent, First American Financial Corporation. The case alleges cybersecurity regulatory violations relating to the leakage of 800 million customer records online.
- DFS has stated that it has conducted an investigation of every ransomware event reported to it and is considering broadening its cybersecurity event reporting obligation.

Cybercrime Developments

Limiting the Scope of the Computer Fraud & Abuse Act – *Van Buren v. United States*, 141 S. Ct. 1648 (2021)

- 18 U.S.C. § 1030 (1986) -- creates criminal and civil liability for any person who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains” virtually any type of information stored on any computer connected to the Internet.
- In its first substantive ruling on the CFAA, SCT held that a person does not “exceed authorized access” to a “protected computer” under the CFAA, when he uses information obtained from accessing that computer for an unauthorized purpose.
- Decision resolves a deep circuit split on the issue and will severely limit both criminal and civil liability under the CFAA.
- Most notably, the decision will largely gut the CFAA as a tool for addressing insider data theft.

Limiting the Scope of the Computer Fraud & Abuse Act – *Van Buren v. United States*

- Georgia police sergeant used his authorized username and password to obtain information from a law enforcement database with the intent to sell it to an FBI confidential informant for \$6,000. As part of the FBI sting operation, the informant requested the information for the ostensible purpose of confirming that a woman of romantic interest to him was not an undercover police officer. Van Buren was authorized to use the database ***for law-enforcement purposes only***. The jury convicted Van Buren of violating the CFAA and the wire fraud statute.
- The Eleventh Circuit affirmed Van Buren’s conviction under Section 1030(a)(2)(C), finding sufficient evidence that Van Buren “intentionally . . . exceed[ed] authorized access [to a computer] and thereby obtain[ed] . . . information from any protected computer” when he accessed the database and obtained information for an unauthorized purpose (*i.e.*, to sell it to a third person).
- The Eleventh Circuit’s interpretation of the “exceeds authorized access” prong of Section 1030(a)(2) was in accord with decisions of the First, Fifth and Seventh Circuits.

Limiting the Scope of the Computer Fraud & Abuse Act – *Van Buren v. United States*

- SCT reversed in a 6-3 decision with Justice Barrett writing for a majority that included Justice Kavanaugh and the Court's liberal block.
- The majority held that Van Buren did not violate the CFAA when he accessed his employer's database and obtained sensitive and confidential information for the purpose of selling it for his own profit.
 - This ruling is consistent with prior decisions issued by the Second, Fourth, Sixth and Ninth Circuits.
- The majority's reasoning was rooted deeply in its textual analysis of Section 1030(e)(6), which defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is *not entitled so to obtain or alter.*"
- The majority focused heavily on the word "so" in the italicized clause as limiting the "exceeds authorized access" prong to situations in which a person "accesses a computer with authorization but then obtains information located in particular areas of the computer – such as files, folders or databases – that are off limits to him."
- The majority announced a new bright line rule that determining whether one accesses a computer "without authorization" or "exceeds authorized access" is a "gates-up-or-down inquiry – one either can or cannot access a computer system, and one either can or cannot access certain areas within the system."

Limiting the Scope of the Computer Fraud & Abuse Act – *Van Buren v. United States*

- Because Van Buren was authorized to access the computer for law enforcement purposes, the Court dismissed as irrelevant his improper purpose in accessing the data.
- Any limits that his employer placed on his authorization to access the computer by policy, terms of use, or contract would require a “circumstance-dependent” analysis that the majority viewed as unsupported by the statutory text.
- Such an approach also would “inject arbitrariness into the assessment of criminal liability.” Pointing to a ‘parade of horrors’ stretching well beyond the facts of any insider data misuse case, the Court also reasoned that a broader interpretation of Section 1030 would criminalize every violation of policy, terms of use, or contract imposed by an employer, computer owner, or Internet platform.
- Justice Thomas (joined by Roberts & Alito) in dissent, pointed out that the majority’s new rule and rationale ignore the plain statutory text, long-settled principles of property law, and the CFAA’s statutory history.
- The dissent focused on the statutory term “entitle” in arguing that Van Buren’s entitlement to accessing the license plate database was limited by the scope and policies of his employment. Under “basic principles of property law,” any entitlement to use another’s property (including computer equipment and data) is “circumstance specific.”
- The dissent went on to offer its own ‘parade of horrors’ under the majority’s rule – including a car rental employee who is authorized to access a computer containing the GPS location history of a rental car to track stolen vehicles, but who instead does so to stalk his ex-girlfriend, or a nuclear scientist who is authorized to access blueprints for an atomic weapon within the scope of his employment, but would be insulated from CFAA liability even if he did so to “help[] an unfriendly nation build a nuclear arsenal.”

Limiting the Scope of the Computer Fraud & Abuse Act – *Van Buren v. United States*

- **Insider Data Theft and Misuse:** The CFAA is unlikely to provide criminal or civil redress to organizations against malicious insiders – those who are authorized to access computerized information for work-related or other limited purposes, but who exceed such authorization by accessing information for an improper purpose. On the facts of *Van Buren* alone, an employee who is authorized to access data in a work computer could not be prosecuted or civilly sued under the CFAA for obtaining confidential and sensitive data to sell to a competitor or a hostile nation, or to leak to a media outlet.
- **The “Exceeds Authorized Access” Prong Appears to Require Circumvention of Technological Barriers:** It is not clear what level of evidentiary support is now needed to prevail on the “exceeds authorized access” prong of Section 1030(a)(2). The Court’s opinion strongly suggests that a technological barrier (i.e., “access control”) must be implemented to preclude an authorized user from accessing data and then circumvented by that user.
- **Terms of Use Violations:** The Court attempts to expressly reserve decision on “whether this inquiry turns only on technological limitations on access, or instead also looks to limits contained in contracts or policies.” It seems clear, though, that violating an entity’s terms of use for a network, website, or other Internet platform – standing alone – will not violate the CFAA’s “exceeds authorized access” prong. Digital platforms will need to consider technical access controls or explicit access prohibitions as a means of falling within the ambit of the CFAA.
- **Data Scraping:** The Court’s holding further solidifies the view that data scraping of publicly facing websites does not violate the CFAA, at least where no technological access barrier is circumvented. *Van Buren* leaves open the question whether the CFAA proscribes the scraping of data that is behind a pay wall or other authentication/access control in violation of a company’s terms of use.

Cyberstalking in the White Collar World



Photo: Diego M. Radzinski/ALM

NEWS

'Relentless Harassment': Former K&L Gates Partner Faces Federal Charges for Allegedly Sending 'Thousands' of Threatening Messages to Past Co-Workers

Willie Dennis, who left the firm in 2019, previously filed discrimination claims against his former employer that have been moved to arbitration.

November 19, 2021 at 03:10 PM

4 minute read

Former eBay supervisor sentenced to 18 months in prison for cyberstalking case targeting Natick couple

By Travis Andersen Globe Staff, Updated July 27, 2021, 1:24 p.m.



The alleged deliveries to a Natick couple included a Halloween mask featuring a bloody pig face and the book "Grief Diaries: Surviving the Loss of a Spouse." ebay cyberstalking HANDOUT VIA FBI BOSTON

A former security supervisor at eBay received an 18-month federal prison sentence Tuesday for his role in a bizarre campaign of cyberstalking aimed at a Natick couple that ran an online newsletter often critical of the e-commerce giant, authorities said.

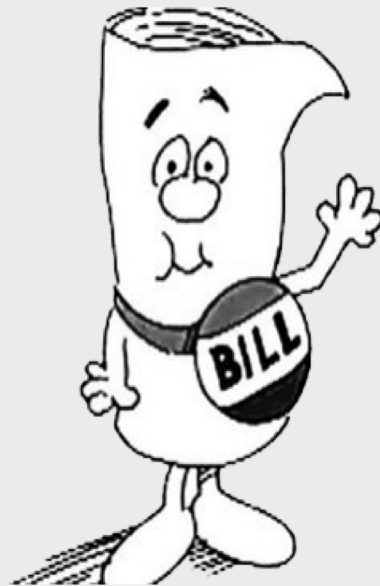
Philip Cooke, 56, of San Jose, Calif., had pleaded guilty in US District Court in Boston in October 2020 to conspiracy to commit cyberstalking and conspiracy to tamper with a witness, legal filings show.⁸³

Assange Extradition & Digital Media Law

IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA Alexandria Division		FILED MAY 23 CLERK, U.S. DISTRICT COURT ALEXANDRIA, VIRGINIA
UNITED STATES OF AMERICA	Criminal No. 1:18-cr-111 (CMH)	
v.	Count 1: 18 U.S.C. § 793(g) Conspiracy To Receive National Defense Information	
JULIAN PAUL ASSANGE,	Counts 2-4: 18 U.S.C. § 793(b) and 2 Obtaining National Defense Information	
Defendant.	Counts 5-8: 18 U.S.C. § 793(c) and 2 Obtaining National Defense Information	
	Counts 9-11: 18 U.S.C. § 793(d) and 2 Disclosure of National Defense Information	
	Counts 12-14: 18 U.S.C. § 793(e) and 2 Disclosure of National Defense Information	
	Counts 15-17: 18 U.S.C. § 793(e) Disclosure of National Defense Information	
	Count 18: 18 U.S.C. §§ 371 and 1030 Conspiracy To Commit Computer Intrusion	
<u>SUPERSEDING INDICTMENT</u>		
May 2019 Term – at Alexandria, Virginia		
THE GRAND JURY CHARGES THAT:		

- WikiLeaks founder indicted in EDVA for CFAA Conspiracy & Disclosure of National Defense Information
- Solicited, encouraged and aided in Chelsea Manning's obtaining and leaking classified information related to the Afghanistan & Iraq Wars, and Gitmo Detainees
- 12/10/21 -- England's High Court reversed denial of extradition based on suicide risk
- Clash between Government & Media over technology facilitated newsgathering
 - Ongoing encrypted communication during data theft
 - Password cracking advice
 - Shared cloud storage
- Examination/Revision of *Bartnicki v. Volper*, 532 US 514 (2001)– First Amendment protects media publication of illegally intercepted and recorded phone call where (1) publisher merely received recorded conversation but played no part in the illegal wiretapping; (2) publisher lawfully obtained access to the recording; (3) the subject matter was of public concern.

Legislation Updates



Overview of Data Privacy Laws

- No overriding data protection law in the U.S.
- Hundreds of laws governing data privacy and security
- State laws – breach notification, biometric privacy, comprehensive consumer privacy
- Federal laws covering certain types of information, *i.e.*, financial, healthcare, education, children, consumer protection and public sectors
- Non-U.S. laws, such as EU's General Data Protection Regulation (**GDPR**), Canada's Personal information Protection and Electronic Documents Act (**PIPEDA**) and Consumer Privacy Protection Act (**CPPA**), and China's Personal Information Protection Law (**PIPL**)

Fair Information Practice Principles (FIPPS)

- Notice/Awareness
- Choice/Consent
- Access/Participation
- Integrity/Security, and
- Enforcement/Redress

FIPPS Variations

- Notice – methods of providing notice
- Choice – opt in or opt out
- Access – degree of control over data
- Security – general requirement or prescriptive
- Enforcement – private right of action or regulator

Comprehensive State Privacy Laws

- California Consumer Privacy Act (CCPA), signed June 2018, effective January 2020
- California Privacy Rights Act (CPRA), passed November 2020, effective January 2023
- Virginia Consumer Data Protection Act (VCDPA), signed March 2021, effective January 2023
- Colorado Privacy Act (CPA), signed July 2021, effective July 2023

Key components of CCPA

- Vastly expanded consumer rights
 - Right of Access
 - Right of Rectification
 - Right of Deletion
 - Right of Restriction
 - Right of Portability
 - Right of Opt-out of Sale
 - Right Against Automated Decision-making
 - Private right of action
- Notice at the point of collection
- Detailed notice requirements
- Risk assessments
- Website updates and consumer rights mechanisms
- Vendor contractual terms

California Privacy Rights Act (CPRA)

- Ballot initiative passed November 2020
- Effective date January 1, 2023.
- Applies to PI collected after January 1, 2022
- Replaces and expands CCPA
- New protections include:
 - New obligations regarding sensitive data
 - Sharing limitations
 - Enhanced protection for minors
 - Creation of California Privacy Protection Agency (CPPA)

VCDPA Overview

- Signed in March 2021, effective January 1, 2023
- Enforcement only by state AG; no private right of action; 30-day cure period
- Incorporates GDPR's controller/processor distinction
- Narrower scope than CPRA and includes broad exceptions
- Creates individual rights for consumers, such as ability to access, correct and delete personal information and opt out of sale and processing of data for targeted advertising
- Requires opt-in consent for processing "sensitive data" including health information, race, ethnicity and precise geolocation data
- Requires companies to conduct a data protection impact assessment

Numerous Differences Between California, Virginia and Colorado Privacy Laws

1. Exemptions for certain types of entities
2. Exemptions for HR and B2B data
3. Scope of opt-out rights
4. Opt-out signals
5. Sensitive data requirements
6. Data protection assessments
7. Contracting requirements
8. Appeals for rights requests
9. Regulator enforcement
10. Cure periods

Pending U.S. Data Privacy Bills

- Over half of states introduced data privacy bills in 2019, stalled due to COVID-19
- 12+ states have bills pending in 2021, including Washington, New York, Florida, Minnesota and Oklahoma
- Big point of contention – private right of action
- Federal legislation major issues
 - Preemption or minimum standard
 - Private right of action vs. FTC or other agency enforcement

Guidance on Compliance

- Data mapping
- Updating privacy policies
- Opt-out compliance
- Updating contracts

Communications Decency Act

47 USC § 230

- Before Section 230, publishers and distributors could be held accountable for the content of publications.
 - *New York Times v. Sullivan*, 376 U.S. 254 (1964) (cases decided based on First Amendment standards and level of scienter needed)
 - *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. 1995) (owner of online bulletin board was liable as publisher of user-created content because it exercised **some** editorial control over the posted messages)
- Congress passed Telecommunications Act in 1996
 - 230 was designed to promote continued and expanded use of the internet while protecting users from objectionable and inappropriate online material.

Major Points of Section 230

- No interactive computer service (ICS) provider or user shall be treated as a **publisher or speaker** of any information provided by another user
- No ICS provider or user shall be held liable due to:
 - Restricting content in good faith that it deems to be “obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable,” or
 - Enabling others the ability to restrict content described above.
- Exceptions to this immunity:
 1. Federal criminal law
 2. Intellectual property law
 3. Electronic Communications Privacy Act
 4. Laws prohibiting sex trafficking (added in 2018)

Why is Section 230 Controversial?

- Some think: Online platforms don't police content enough. They worry about defamation, falsehoods, child predation, extremism and other bad stuff
- Others think: Online platforms police content too much or unequally and are thereby squelching freedom of expression.

Proposals for Revision to Section 230

- Liability for amplifying certain types of harmful content
 - Making personalized recommendations (including targeted advertising) leading to harm
 - Limiting harm to civil rights abuses, terrorism, illegal drugs, child exploitation or cyberbullying
 - Use of algorithms vs. human intervention
- Require greater transparency
- Don't expect bills to target political misinformation or allegations of bias or censorship

Advances in the E.U. in Content Moderation

- In 2021, European Commission announced its digital strategy, including a proposed Data Governance Act (DGA) and Digital Services Act (DSA)
 - DGA would create a framework for secure data sharing
 - DSA would focus on how platforms and other intermediaries interact with user content.
 - One set of rules on content moderation and accountability of online platforms in the EU
 - Assures a higher standard of protection of fundamental rights as well as ensuring safety online
- The world regulates Big Tech while the U.S. dithers.

Cross-Border Data Transfers

- GDPR prohibits transfer of data to countries lacking an “adequate level of protection” absent an approved mechanism.
- EU’s top court decided *Shrems II* on July 16, 2020.
 - Invalidates Privacy Shield, a key data transfer mechanism used by thousands of U.S. companies
 - Requires businesses to assess whether the laws and practices of the destination company to determine if they would prevent them from complying with their obligations under the GDPR, and
 - If not, must implement supplementary measures
- Current backup method, “Standard Contractual Clauses,” gets more complicated.

New Standard Contractual Clauses

- Updated Standard Contractual Clauses (new SCCs) adopt a layered, modular approach
- Transition period
 - On September 27, 2021, all new contracts involving cross-border personal data transfers must incorporate
 - By December 27, 2022, all existing contracts must be updated to the new SCCs
 - Modular, can accommodate multiple scenarios
 - New provisions govern how data importer must react in the face of binding requests for data by government authorities.

Key Highlights of New SCCs

- GDPR Spirit
- Wider range of relationships allowed under “modular” approach
- Obligation on all parties to conduct and record a transfer impact assessment
- Obligations on the importer to notify exporter of public authority access request
- Transparency obligations
- Onward transfers
- Strengthening the data subjects’ rights
- Warranty by the exporter and obligation to inform the importer
- Submission of the importer to a regulator in the EU
- Technical and organizational measures

European Data Protection Board (EDPB) issues Recommendations for Compliance

- Roadmap of steps to determine if supplementary steps are required
- Access to data by public authorities must be considered
- Assess if laws or practices of a third country may impinge on effectiveness of safeguards
- Examples of technical, contractual and organizational measures to increase level of protection
- Use case examples
- Practical steps – mapping international data transfers

EDPB's Key Recommendations for Protections

- Robust encryption
- Pseudonymization prior to transfer
- Due diligence and transparency commitments
- Contractual commitments as to IT solutions in use
- Enhanced technical audit provisions
- Use of “warrant canaries”
- Contractual commitments to resist disclosure requests and give notice to affected parties

EDPB Guidelines on Interplay between Article 3 and Chapter V of the GDPR

- At issue is what constitutes an international transfer
 - When data leaves the physical territory, or
 - When data goes to an entity beyond the jurisdictional scope of the GDPR
- Guidelines published November 18, 2021, open for comment through January 31, 2022.
- Three cumulative criteria that qualify processing as a transfer:
 1. A controller or processor is subject to the GDPR for the given processing.
 2. This controller or processor (“exporter”) discloses by transmission or otherwise makes personal data subject to this processing available to another controller, joint controller or processor (“importer”)
 3. The importer is in a third country or is an international organization, irrespective of whether or not this importer is subject to the GDPR in respect of the given processing in accordance with Article 3.

Practical Guidance

- Understand applicable laws and regulations
- Conduct a risk assessment
- Implement reasonable security and privacy practices
- Prepare a written information security program
- Develop an incident response plan
- Train employees on security and privacy obligations
- Conduct risk assessment on third-party vendors
- Review insurance coverage for cyber-related incidents

RANSOMWARE GUIDE

SEPTEMBER 2020



MS-ISAC[®]
Multi-State Information
Sharing & Analysis Center[®]

Overview

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased, with some demands exceeding US \$1 million. Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

This *Ransomware Guide* includes two resources:

Part 1: Ransomware Prevention Best Practices

Part 2: Ransomware Response Checklist

CISA recommends that organizations take the following initial steps:

- Join an information sharing organization, such as one of the following:
 - Multi-State Information Sharing and Analysis Center (MS-ISAC):
<https://learn.cisecurity.org/ms-isac-registration>
 - Election Infrastructure Information Sharing and Analysis Center (EI-ISAC):
<https://learn.cisecurity.org/ei-isac-registration>
 - Sector-based ISACs - National Council of ISACs:
<https://www.nationalisacs.org/member-isacs>
 - Information Sharing and Analysis Organization (ISAO) Standards Organization:
<https://www.isao.org/information-sharing-groups/>
- Engage CISA to build a lasting partnership and collaborate on information sharing, best practices, assessments, exercises, and more.
 - SLTT organizations: CyberLiaison_SLTT@cisa.dhs.gov
 - Private sector organizations: CyberLiaison_Industry@cisa.dhs.gov

Engaging with your ISAC, ISAO, and with CISA will enable your organization to receive critical information and access to services to better manage the risk posed by ransomware and other cyber threats.



These ransomware best practices and recommendations are based on operational insight from the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The audience for this guide includes information technology (IT) professionals as well as others within an organization involved in developing cyber incident response policies and procedures or coordinating cyber incident response.

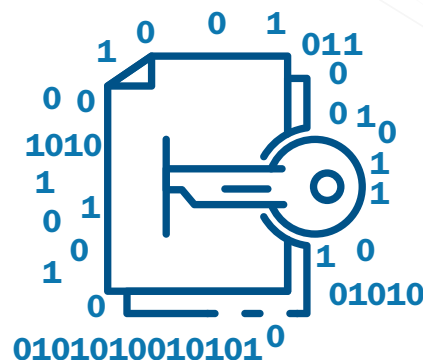
Part 1: Ransomware Prevention Best Practices



Be Prepared

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.
 - Maintain regularly updated “gold images” of critical systems in the event they need to be rebuilt. This entails maintaining image “templates” that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
 - Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred.
 - Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
 - In addition to system images, applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to needed software will help in these cases.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
 - Review available incident response guidance, such as the *Public Power Cyber Incident Response Playbook* (<https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf>), a resource and guide to:
 - Help your organization better organize around cyber incident response, and
 - Develop a cyber incident response plan.
 - The Ransomware Response Checklist, which forms the other half of this *Ransomware Guide*, serves as an adaptable, ransomware-specific annex to organizational cyber incident response or disruption plans.





Ransomware Infection Vector: Internet-Facing Vulnerabilities and Misconfigurations

- Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.
 - CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments: <https://www.cisa.gov/cyber-resource-hub>.
- Regularly patch and update software and OSs to the latest available versions.
 - Prioritize timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins, and document readers—for known vulnerabilities.
- Ensure devices are properly configured and that security features are enabled. For example, disable ports and protocols that are not being used for a business purpose (e.g., Remote Desktop Protocol [RDP] – Transmission Control Protocol [TCP] Port 3389).
- Employ best practices for use of RDP and other remote desktop services. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later propagate ransomware. See CISA Alert AA20-073A, Enterprise VPN Security (<https://us-cert.cisa.gov/ncas/alerts/aa20-073a>).
 - Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multi-factor authentication (MFA), and log RDP login attempts.
- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Based on this specific threat, organizations should consider the following actions to protect their networks:
 - Disable SMBv1 and v2 on your internal network after working to mitigate any existing dependencies (on the part of existing systems or applications) that may break when disabled.
 - Remove dependencies through upgrades and reconfiguration: Upgrade to SMBv3 (or most current version) along with SMB signing.
 - Block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.

Ransomware Infection Vector: Phishing

- Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. Conduct organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.
- Implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the firewall.
- To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification. DMARC builds on the widely deployed sender policy framework and Domain Keys Identified Mail protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email.
- Consider disabling macro scripts for Microsoft Office files transmitted via email. These macros can be used to deliver ransomware.

Ransomware Infection Vector: Precursor Malware Infection

- Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions. CISA recommends using a centrally managed antivirus solution. This enables detection of both “precursor” malware and ransomware.
 - A ransomware infection may be evidence of a previous, unresolved network compromise. For example, many ransomware infections are the result of existing malware infections, such as TrickBot, Dridex, or Emotet.
 - In some cases, ransomware deployment is just the last step in a network compromise and is dropped as a way to obfuscate previous post-compromise activities.
- Use application directory allowlisting on all assets to ensure that only authorized software can run, and all unauthorized software is blocked from executing.
 - Enable application directory allowlisting through Microsoft Software Restriction Policy or AppLocker.
 - Use directory allowlisting rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from **PROGRAMFILES**, **PROGRAMFILES(X86)**, and **SYSTEM32**. Disallow all other locations unless an exception is granted.
- Consider implementing an intrusion detection system (IDS) to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment.



CISA offers a no-cost Phishing Campaign Assessment and other no-cost assessments: <https://www.cisa.gov/cyber-resource-hub>.

For more information on DMARC, see: <https://www.cisecurity.org/blog/how-dmarc-advances-email-security/> and

https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-EnhanceEmailandWebSecurity_S508C.pdf.

Funded by CISA, the MS-ISAC and EI-ISAC provide the Malicious Domain Blocking and Reporting (MDBR) service at no-cost to members. MDBR is a fully managed proactive security service that prevents IT systems from connecting to harmful web domains, which helps limit infections related to known malware, ransomware, phishing, and other cyber threats. To sign up for MDBR, visit: <https://www.cisecurity.org/ms-isac/services/mdbr/>.

CISA and MS-ISAC encourage SLTT organizations to consider the Albert IDS to enhance a defense-in-depth strategy. CISA funds Albert sensors deployed by the MS-ISAC, and we encourage SLTT governments to make use of them. Albert serves as an early warning capability for the Nation's SLTT governments and supports the nationwide cybersecurity situational awareness of CISA and the Federal Government. For more information regarding Albert, see: <https://www.cisecurity.org/services/albert-network-monitoring/>.





Ransomware Infection Vector: Third Parties and Managed Service Providers

- Take into consideration the risk management and cyber hygiene practices of third parties or managed service providers (MSPs) your organization relies on to meet its mission. MSPs have been an infection vector for ransomware impacting client organizations.
 - If a third party or MSP is responsible for maintaining and securing your organization's backups, ensure they are following the applicable best practices outlined above. Using contract language to formalize your security requirements is a best practice.
- Understand that adversaries may exploit the trusted relationships your organization has with third parties and MSPs. See CISA's APTs Targeting IT Service Provider Customers (<https://us-cert.cisa.gov/APTs-Targeting-IT-Service-Provider-Customers>).
 - Adversaries may target MSPs with the goal of compromising MSP client organizations; they may use MSP network connections and access to client organizations as a key vector to propagate malware and ransomware.
 - Adversaries may spoof the identity of—or use compromised email accounts associated with—entities your organization has a trusted relationship with in order to phish your users, enabling network compromise and disclosure of information.

General Best Practices and Hardening Guidance

- Employ MFA for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
 - If you are using passwords, use strong passwords (<https://us-cert.cisa.gov/ncas/tips/ST04-002>) and do not reuse passwords for multiple accounts. Change default passwords. Enforce account lockouts after a specified number of login attempts. Password managers can help you develop and manage secure passwords.
- Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs. Threat actors often seek out privileged accounts to leverage to help saturate networks with ransomware.
 - Restrict user permissions to install and run software applications.
 - Limit the ability of a local administrator account to log in from a local interactive session (e.g., "Deny access to this computer from the network.") and prevent access via an RDP session.



- ❑ Remove unnecessary accounts and groups and restrict root access.
 - ❑ Control and limit local administration.
 - ❑ Make use of the Protected Users Active Directory group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.
 - ❑ Audit user accounts regularly, particularly Remote Monitoring and Management accounts that are publicly accessible—this includes audits of third-party access given to MSPs.
- Leverage best practices and enable security settings in association with cloud environments, such as Microsoft Office 365 (<https://www.us-cert.cisa.gov/ncas/alerts/aa20-120a>).
 - Develop and regularly update a comprehensive network diagram that describes systems and data flows within your organization's network (see figure 1). This is useful in steady state and can help incident responders understand where to focus their efforts.
 - ❑ The diagram should include depictions of covered major networks, any specific IP addressing schemes, and the general network topology (including network connections, interdependencies, and access granted to third parties or MSPs).
 - Employ logical or physical means of network segmentation to separate various business unit or departmental IT resources within your organization as well as to maintain separation between IT and operational technology.

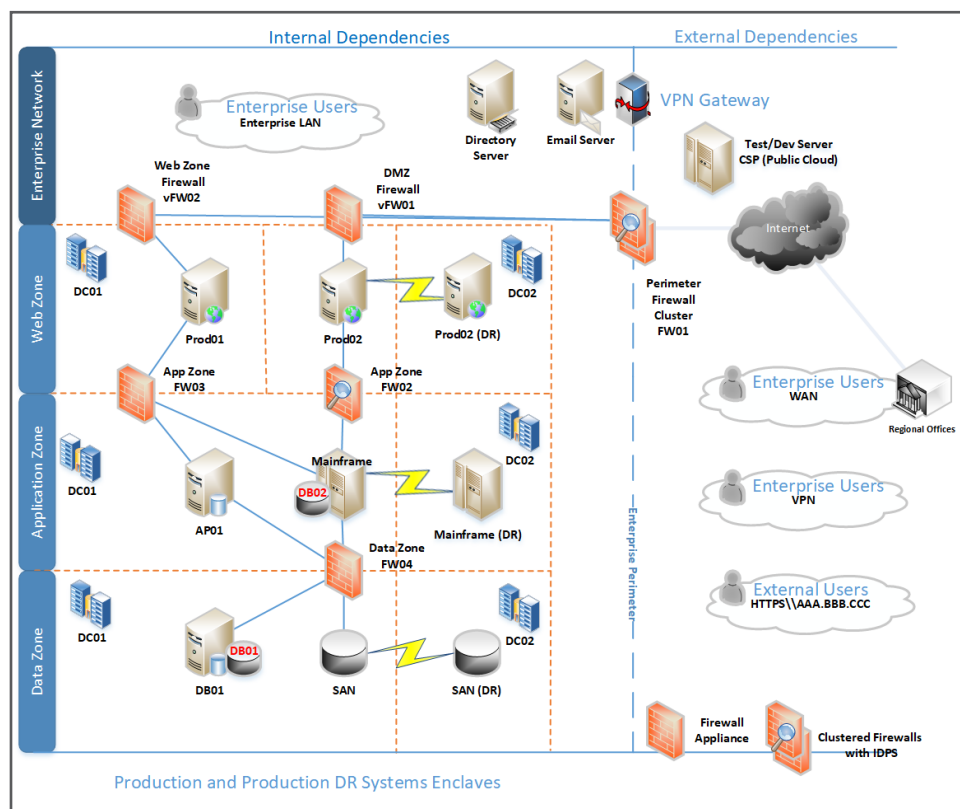


Figure 1. Example Network Diagram

This will help contain the impact of any intrusion affecting your organization and prevent or limit lateral movement on the part of malicious actors. See figures 2 and 3 for depictions of a flat (unsegmented) network and of a best practice segmented network.

- Network segmentation can be rendered ineffective if it is breached through user error or non-adherence to organizational policies (e.g., connecting removable storage media or other devices to multiple segments).
- Ensure your organization has a comprehensive asset management approach.
 - Understand and inventory your organization's IT assets, both logical (e.g., data, software) and physical (e.g., hardware).
 - Understand which data or systems are most critical for health and safety, revenue generation, or other critical services, as well as any associated interdependencies (i.e., "critical asset or system list"). This will aid your organization in determining restoration priorities should an incident occur. Apply more comprehensive security controls or safeguards to critical assets. This requires organization-wide coordination.
 - Use the MS-ISAC Hardware and Software Asset Tracking Spreadsheet: <https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/>.
- Restrict usage of PowerShell, using Group Policy, to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows OSs should be permitted to use PowerShell. Update PowerShell and enable enhanced logging. PowerShell is a cross-platform, command-line, shell and scripting language that is a component of Microsoft Windows. Threat actors use PowerShell to deploy ransomware and hide their malicious activities.
 - Update PowerShell instances to version 5.0 or later and uninstall all earlier PowerShell versions. Logs from PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities.
 - PowerShell logs contain valuable data, including historical OS and registry interaction and possible tactics, techniques, and procedures of a threat actor's PowerShell use.
 - Ensure PowerShell instances (use most current version) have module, script block, and transcription logging enabled (enhanced logging).

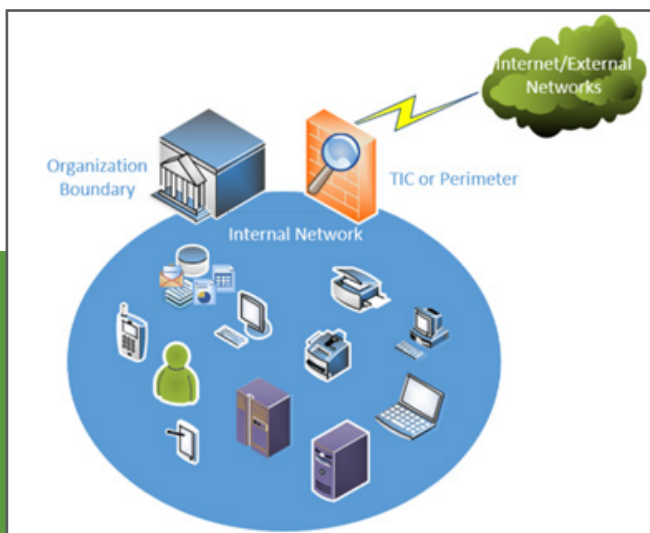


Figure 2. Flat (Unsegmented) Network

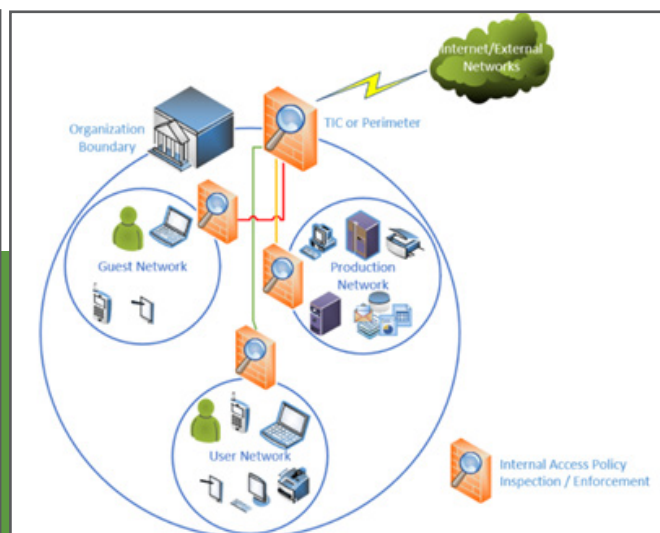
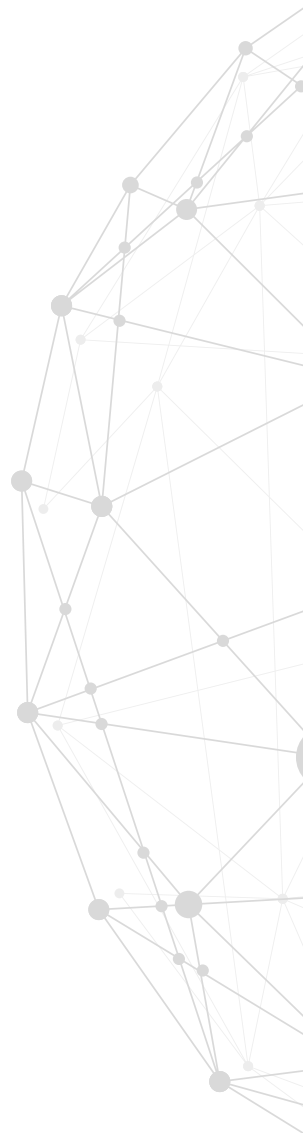


Figure 3. Segmented Network



- The two logs that record PowerShell activity are the “PowerShell” Windows Event Log and the “PowerShell Operational” Log. CISA recommends turning on these two Windows Event Logs with a retention period of 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as possible.
- Secure domain controllers (DCs). Threat actors often target and use DCs as a staging point to spread ransomware network-wide.
 - The following list contains high-level suggestions on how best to secure a DC:
 - Ensure that DCs are regularly patched. This includes the application of critical patches as soon as possible.
 - Ensure the most current version of the Windows Server OS is being used on DCs. Security features are better integrated in newer versions of Windows Server OSs, including Active Directory security features. Use Active Directory configuration guides, such as those available from Microsoft (<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>), when configuring available security features.
 - Ensure that no additional software or agents are installed on DCs, as these can be leveraged to run arbitrary code on the system.
 - Access to DCs should be restricted to the Administrators group. Users within this group should be limited and have separate accounts used for day-to-day operations with non-administrative permissions.
 - DC host firewalls should be configured to prevent internet access. Usually, these systems do not have a valid need for direct internet access. Update servers with internet connectivity can be used to pull necessary updates in lieu of allowing internet access for DCs.
 - CISA recommends the following DC Group Policy settings:
(Note: This is not an all-inclusive list and further steps should be taken to secure DCs within the environment.)
 - The Kerberos default protocol is recommended for authentication, but if it is not used, enable NTLM auditing to ensure that only NTLMv2 responses are being sent across the network. Measures should be taken to ensure that LM and NTLM responses are refused, if possible.
 - Enable additional protections for Local Security Authentication to prevent code injection capable of acquiring credentials from the system. Prior to enabling these protections, run audits against the [lsass.exe](#) program to ensure an understanding of the programs that will be affected by the enabling of this protection.
 - Ensure that SMB signing is required between the hosts and the DCs to prevent the use of replay attacks on the network. SMB signing should be enforced throughout the entire domain as an added protection against these attacks elsewhere in the environment.
- Retain and adequately secure logs from both network devices and local hosts. This supports triage and remediation of cybersecurity events. Logs can be analyzed to determine the impact of events and ascertain whether an incident has occurred.



- Set up centralized log management using a security information and event management tool. This enables an organization to correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact to the organization as a whole.
- Maintain and back up logs for critical systems for a minimum of one year, if possible.
- Baseline and analyze network activity over a period of months to determine behavioral patterns so that normal, legitimate activity can be more easily distinguished from anomalous network activity (e.g., normal vs anomalous account activity).
 - Business transaction logging—such as logging activity related to specific or critical applications—is another useful source of information for behavioral analytics.



Contact CISA for These No-Cost Resources

- **Information sharing with CISA and MS-ISAC (for SLTT organizations)** includes bi-directional sharing of best practices and network defense information regarding ransomware trends and variants as well as malware that is a precursor to ransomware
- **Policy-oriented or technical assessments** help organizations understand how they can improve their defenses to avoid ransomware infection: <https://www.cisa.gov/cyber-resource-hub>
 - Assessments include Vulnerability Scanning and Phishing Campaign Assessment
- **Cyber exercises** evaluate or help develop a cyber incident response plan in the context of a ransomware incident scenario
- **CISA Cybersecurity Advisors (CSAs)** advise on best practices and connect you with CISA resources to manage cyber risk
- **Contacts:**
 - **SLTT organizations:**
CyberLiaison_SLTT@cisa.dhs.gov
 - **Private sector organizations:**
CyberLiaison_Industry@cisa.dhs.gov

Ransomware Quick References

- **Ransomware: What It Is and What to Do About It (CISA):** General ransomware guidance for organizational leadership and more in-depth information for CISOs and technical staff: https://www.us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf
- **Ransomware (CISA):** Introduction to ransomware, notable links to CISA products on protecting networks, specific ransomware threats, and other resources: <https://www.us-cert.cisa.gov/Ransomware>
- **Security Primer – Ransomware (MS-ISAC):** Outlines opportunistic and strategic ransomware campaigns, common infection vectors, and best practice recommendations: <https://www.cisecurity.org/white-papers/security-primer-ransomware/>
- **Ransomware: Facts, Threats, and Countermeasures (MS-ISAC):** Facts about ransomware, infection vectors, ransomware capabilities, and how to mitigate the risk of ransomware infection: <https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/>
- **Security Primer – Ryuk (MS-ISAC):** Overview of Ryuk ransomware, a prevalent ransomware variant in the SLTT government sector, that includes information regarding preparedness steps organizations can take to guard against infection: <https://www.cisecurity.org/white-papers/security-primer-ryuk/>

Part 2: Ransomware Response Checklist



Should your organization be a victim of ransomware, CISA strongly recommends responding by using the following checklist. Be sure to move through the **first three steps in sequence**.

Detection and Analysis

☐ 1. Determine which systems were impacted, and immediately isolate them.

- ☐ If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
- ☐ If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
- ☐ After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods like phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access—already a common tactic—or deploy ransomware widely prior to networks being taken offline.

Note: Step 2 will prevent you from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. It should be carried out **only** if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.

☐ 2. Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.

☐ 3. Triage impacted systems for restoration and recovery.

- ☐ Identify and prioritize critical systems for restoration, and confirm the nature of data housed on impacted systems.
 - Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.
- ☐ Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.

☐ 4. Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.

☐ 5. Using the contact information below, engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.

- ☐ Share the information you have at your disposal to receive the most timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders.



If extended identification or analysis is needed, CISA, MS-ISAC and local, state, or federal law enforcement may be interested in any of the following information that your organization determines it can legally share:

- ☐ Recovered executable file
- ☐ Copies of the readme file – DO NOT REMOVE the file or decryption may not be possible
- ☐ Live memory (RAM) capture from systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- ☐ Images of infected systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- ☐ Malware samples
- ☐ Names of any other malware identified on your system
- ☐ Encrypted file samples
- ☐ Log files (Windows Event Logs from compromised systems, Firewall logs, etc.)
- ☐ Any PowerShell scripts found having executed on the systems
- ☐ Any user accounts created in Active Directory or machines added to the network during the exploitation
- ☐ Email addresses used by the attackers and any associated phishing emails
- ☐ A copy of the ransom note
- ☐ Ransom amount and whether or not the ransom was paid
- ☐ Bitcoin wallets used by the attackers
- ☐ Bitcoin wallets used to pay the ransom (if applicable)
- ☐ Copies of any communications with attackers

Remember: Paying ransom will not ensure your data is decrypted or that your systems or data will no longer be compromised. CISA, MS-ISAC, and federal law enforcement do not recommend paying ransom.

- ☐ Consider requesting assistance from CISA; MS-ISAC; and local, state, or federal law enforcement (e.g., Federal Bureau of Investigation [FBI], U.S. Secret Service [USSS]). See contact information below.
- ☐ As appropriate, coordinate with communications and public information personnel to ensure accurate information is shared internally with your organization and externally with the public.
- ☐ The *Public Power Cyber Incident Response Playbook* (<https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf>) contains guidance for organizational communication procedures as well as templates for cyber incident holding statements for public consumption. Work with your team to develop similar procedures and draft holding statements as soon as possible, as developing this documentation during an incident is not optimal. This will allow your organization to reach consensus, in advance, on what level of detail is appropriate to share within the organization and with the public, and how information will flow.

Containment and Eradication

If no initial mitigation actions appear possible:

☐ **6. Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers). Additionally, collect any relevant logs as well as samples of any “precursor” malware binaries and associated observables or indicators of compromise (e.g., suspected command and control IP addresses, suspicious registry entries, or other relevant files detected). The contacts below may be able to assist you in performing these tasks.**

- ☐ Take care to preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers).

☐ **7. Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants.**

To continue taking steps to contain and mitigate the incident:

☐ **8. Research the trusted guidance (i.e., published by sources such as government, MS-ISAC, reputable security vendor, etc.) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.**

- ☐ Kill or disable the execution of known ransomware binaries; this will minimize damage and impact to your systems. Delete other known, associated registry values and files.

☐ **9. Identify the systems and accounts involved in the initial breach. This can include email accounts.**

☐ **10. Based on the breach or compromise details determined above, contain any associated systems that may be used for further or continued unauthorized access. Breaches often involve mass credential exfiltration. Securing the network and other information sources from continued credential-based unauthorized access may include the following actions:**

- ☐ Disabling virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.

☐ **11. Additional suggested actions—server-side data encryption quick-identification steps:**

- ☐ In the event you learn that server-side data is being encrypted by an infected workstation, quick-identification steps are to:
 1. Review Computer Management > Sessions and Open Files lists on associated servers to determine the user or system accessing those files.
 2. Review file properties of encrypted files or ransom notes to identify specific users that may be associated with file ownership.
 3. Review the TerminalServices-RemoteConnectionManager event log to check for successful RDP network connections.
 4. Review the Windows Security log, SMB event logs, and any related logs that may identify significant authentication or access events.
 5. Run Wireshark on the impacted server with a filter to identify IP addresses involved in actively writing or renaming files (e.g., "smb2.filename contains cryptxxx").

☐ **12. Conduct an examination of existing organizational detection or prevention systems (antivirus, Endpoint Detection & Response, IDS, Intrusion Prevention System, etc.) and logs. Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack.**



Upon voluntary request, CISA and MS-ISAC can assist with analysis (e.g., phishing emails, storage media, logs, malware) at no cost to support your organization in understanding the root cause of an incident, even in the event additional remote assistance is not requested:

- **CISA – Advanced Malware Analysis Center:** <https://www.malware.us-cert.gov/MalwareSubmission/pages/submission.jsf>
- **MS-ISAC – Malicious Code Analysis Platform (SLTT organizations only):** <https://www.cisecurity.org/spotlight/cybersecurity-spotlight-malware-analysis/>
 - ☐ Scans a suspicious file or Uniform Resource Locator (URL) against several antivirus vendors to determine if it matches known malicious signatures
 - ☐ Runs a file or URL in a sandbox to analyze behavior
 - ☐ Provides a user with a summary report of malware behavior, including files accessed, tasks created, outbound connections, and other behavioral traits
 - ☐ Users can opt to keep submissions private and make direct requests for assistance from MS-ISAC; users can also mark submissions for sharing with CISA
 - ☐ Email: mcap@cisecurity.org to set up an account
- **Remote Assistance – Request via CISA Central or MS-ISAC Security Operations Center (see contact information below)**

- Look for evidence of precursor “dropper” malware. A ransomware event may be evidence of a previous, unresolved network compromise. Many ransomware infections are the result of existing malware infections such as TrickBot, Dridex, or Emotet.
 - Operators of these advanced malware variants will often sell access to a network. Malicious actors will sometimes use this access to exfiltrate data and then threaten to release the data publicly before ransomware the network in an attempt to further extort the victim and pressure them into paying.
 - Malicious actors often drop manually deployed ransomware variants on a network to obfuscate their post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromise.
- **13. Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.**
 - Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of external vulnerabilities, etc.
 - Inside-out persistence may include malware implants on the internal network or a variety of living-off-the-land style modifications (e.g., use of commercial penetration testing tools like Cobalt Strike; use of PsTools suite, including PsExec, to remotely install and control malware and gather information regarding—or perform remote management of—Windows systems; use of PowerShell scripts).
 - Identification may involve deployment of endpoint detection and response solutions, audits of local and domain accounts, examination of data found in centralized logging systems, or deeper forensic analysis of specific systems once movement within the environment has been mapped out.
- **14. Rebuild systems based on a prioritization of critical services (e.g., health and safety or revenue generating services), using pre-configured standard images, if possible.**
- **15. Once the environment has been fully cleaned and rebuilt (including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms) issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility. This can include applying patches, upgrading software, and taking other security precautions not previously taken.**
- **16. Based on established criteria, which may include taking the steps above or seeking outside assistance, the designated IT or IT security authority declares the ransomware incident over.**

Recovery and Post-Incident Activity

- **17. Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.**
 - Take care not to re-infect clean systems during recovery. For example, if a new Virtual Local Area Network has been created for recovery purposes, ensure only clean systems are added to it.
- **18. Document lessons learned from the incident and associated response activities to inform updates to—and refine—organizational policies, plans, and procedures and guide future exercises of the same.**
- **19. Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector ISAC/ISA0 for further sharing and to benefit others within the community.**

Contact Information

Consider filling out the following contact information for ready use should your organization become a victim of a ransomware incident. Consider contacting these organizations for mitigation and response assistance or for purpose of notification.

State and Local Response Contacts:

Contact	24x7 Contact Information	Roles and Responsibilities
IT/IT Security Team - Centralized Cyber Incident Reporting		
Departmental or Elected Leaders		
State and Local Law Enforcement		
Fusion Center		
Managed/Security Service Providers		
Cyber Insurance		



Federal Asset Response Contacts

Upon voluntary request, federal asset response includes providing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents while identifying other entities that may be at risk, assessing potential risks to the sector or region, facilitating information sharing and operational coordination, and providing guidance on how to best use federal resources and capabilities.

What You Can Expect:

- Specific guidance to help evaluate and remediate ransomware incidents
- Remote assistance to identify the extent of the compromise and recommendations for appropriate containment and mitigation strategies (dependent on specific ransomware variant)
- Phishing email, storage media, log and malware analysis, based on voluntary submission (full-disk forensics can be performed on an as-needed basis)
- Contacts:
 - CISA:
 - <https://us-cert.cisa.gov/report>, Central@cisa.gov or (888) 282-0870
 - Cybersecurity Advisor (<https://www.cisa.gov/cisa-regions>): [Enter your local CISA CSA's phone number and email address.]
 - MS-ISAC:
 - soc@msisac.org or (866) 787-4722



Federal Threat Response Contacts

Upon voluntary request, federal threat response includes law enforcement and national security investigative activity: collecting evidence and intelligence, providing attribution, linking related incidents, identifying additional affected entities, identifying threat pursuit and disruption opportunities, developing and executing action to mitigate the immediate threat, and facilitating information sharing and operational coordination with asset response.

What You Can Expect:

- Assistance in conducting a criminal investigation, which may involve collecting incident artifacts, to include system images and malware samples.
- Contacts:
 - FBI:
 - <https://www.fbi.gov/contact-us/field-offices>
 - [Enter your local FBI field office POC phone number and email address.]
 - USSS:
 - <https://www.secretservice.gov/contact/field-offices/>
 - [Enter your local USSS field office POC phone number and email address.]

**DEFEND TODAY,
SECURE TOMORROW**
CISA.GOV



MS-ISAC[®]
Multi-State Information
Sharing & Analysis Center[®]

ANNALS OF TECHNOLOGY JUNE 7, 2021 ISSUE

HOW TO NEGOTIATE WITH RANSOMWARE HACKERS

*Kurtis Minder finds the cat-and-mouse energy of
outsmarting criminal syndicates deeply satisfying.*

By Rachel Monroe

May 31, 2021

The rise of ransomware has led to new career opportunities for Kurtis Minder. Photograph by David Williams for The New Yorker



0:00 / 38:46

Audio: Listen to this article. To hear more, download Audm for iPhone or Android.

A few days after Thanksgiving last year, Kurtis Minder got a message from a man whose small construction-engineering firm in upstate New York had been hacked. Minder and his security company, GroupSense, got calls and e-mails like this all the time now, many of them tinged with panic. An employee at a brewery, or a printshop, or a Web-design company would show up for work one morning and find all the computer files locked and a ransom note demanding a cryptocurrency payment to release them.

Some of the notes were aggressive (“Don’t take us for fools, we know more about you than you know about yourself”), others insouciant (“Oops, your important files are encrypted”) or faux apologetic (“WE ARE REGRET BUT ALL YOUR FILES WAS ENCRYPTED”). Some messages couched their extortion as a legitimate business transaction, as if the hackers had performed a helpful security audit: “Gentlemen! Your business is at serious risk. There is a significant hole in the security system of your company.”

The notes typically included a link to a site on the dark Web, the part of the Internet that requires special software for access, where people go to do clandestine things. When victims went to the site, a clock popped up, marking the handful of days they had to fulfill the ransom demand. The clock began to tick down ominously, like a timer connected to a bomb in an action movie. A chat box enabled a conversation with the hackers.

In the past year, a surge of ransomware attacks has made a disruptive period even more difficult. In December, the acting head of the federal Cybersecurity and Infrastructure Security Agency said that ransomware was “quickly becoming a national emergency.” Hackers hit vaccine manufacturers and research labs. Hospitals lost access to chemotherapy protocols; school districts cancelled classes. Companies scrambling to accommodate a fully remote workforce found themselves newly vulnerable

to hackers. In May, an attack by the ransomware group DarkSide forced the shutdown of Colonial Pipeline's network, which supplies fuel to much of the East Coast. The shutdown, which pushed up gas prices and led to a spate of panic-buying, put a spotlight on ransomware's potential to disable critical infrastructure. A week after the attack, once Colonial paid a ransom of \$4.4 million to get its systems back online, eighty per cent of gas stations in Washington, D.C., still had no fuel.

The F.B.I. advises victims to avoid negotiating with hackers, arguing that paying ransoms incentivizes criminal behavior. This puts victims in a tricky position. "To just tell a hospital that they can't pay—I'm just incredulous at the notion," Philip Reiner, the C.E.O. of the nonprofit Institute for Security and Technology, told me. "What do you expect them to do, just shut down and let people die?" Organizations that don't pay ransoms can spend months rebuilding their systems; if customer data are stolen and leaked as part of an attack, they may be fined by regulators. In 2018, the city of Atlanta declined to pay a ransom of approximately fifty thousand dollars. Instead, in an effort to recover from the attack, it spent more than two million dollars on crisis P.R., digital forensics, and consulting. For every ransomware case that makes the news, there are many more small and medium-sized companies that prefer to keep breaches under wraps, and more than half of them pay their hackers, according to data from the cybersecurity firm Kaspersky.

For the past year, Minder, who is forty-four years old, has been managing the fraught discussions between companies and hackers as a ransomware negotiator, a role that didn't exist only a few years ago. The half-dozen ransomware-negotiation specialists, and the insurance companies they regularly partner with, help people navigate the world of cyber extortion. But they've also been accused of abetting crime by facilitating payments to hackers. Still, with ransomware on the rise, they have no lack of clients. Minder, who is mild and unpretentious, and whose conversation is punctuated by self-deprecating laughter, has become an accidental expert. "While I've been talking to you, I've already gotten two calls," he told me when we video-chatted in March.

The man who reached out to him in November explained that the attack, the work of a hacking syndicate known as REvil, had rendered the company's contracts and architectural plans inaccessible; every day the files remained locked was another day the staff couldn't work. "They didn't even have an I.T. person on staff," Minder said. The company had no cyber-insurance policy. The man explained that he had been in touch with a company in Florida that had promised to decrypt the files, but it

had stopped replying to his e-mails. He wanted Minder to negotiate with the hackers to get the decryption key. “The people who reach out to me are upset,” Minder told me. “They’re very, very upset.”

As a child, Minder visited his father at the mill where he worked, in central Illinois, and watched him hoist fifty-pound sacks of flour. His mother, who worked for the state, sat in an air-conditioned office with a cup of coffee. He didn’t quite understand what her job was, other than that it seemed to involve a lot of typing. “I was, like, whatever that typing job is, that’s what I want,” Minder told me.

After college, in the early nineties, he got a tech-support job at a local Internet-service provider. Within a year, he was promoted to assistant systems administrator, a job that entailed keeping tabs on the server logs. He began to notice a strange pattern, which he eventually realized was evidence of hackers. “They would use our routers as what we would now call a pivot point—bouncing off them to attack someone else, so the attack looked like it was coming from us,” he said. The attackers were typically hobbyists who were more interested in showing off their skills than in wreaking real havoc; Minder found the cat-and-mouse energy of outsmarting them deeply satisfying.

By that time, hackers had proved that they could inflict serious damage. In 1989, twenty thousand public-health researchers around the world received a floppy disk purporting to contain an informational program about AIDS. But the disk also included a malicious program that is now considered the first instance of ransomware. After users rebooted their computers ninety times, a text box appeared on the screen, informing them that their files were locked. Then their printers spat out a ransom note instructing them to mail a hundred and eighty-nine dollars to a post-office box in Panama. The malware, which came to be known as the AIDS Trojan, was created by Joseph Popp, a Harvard-trained evolutionary biologist. Popp, whose behavior grew increasingly erratic after his arrest, was declared unfit to stand trial; he later founded a butterfly sanctuary in upstate New York.

Popp’s strategy—encrypting files with a private key and demanding a fee to unlock them—is frequently used by ransomware groups today. But hackers initially preferred an approach known as scareware, in which they infected a computer with a virus that manifested as multiplying pop-ups with ominous messages: “SECURITY WARNING! Your Privacy and Security are in DANGER.” The pop-

ups told users to buy a certain antivirus software to protect their systems. Hackers posing as software companies could then receive credit-card payments, which were unavailable to those deploying ransomware. In the early two-thousands, ransomware hackers typically demanded a few hundred dollars, in the form of gift cards or prepaid debit cards, and getting hold of the money required middlemen, who siphoned off much of the profits.

The calculus changed with the launch of Bitcoin, in 2009. Now that people could receive digital payments without revealing their identity, ransomware became more lucrative. When Minder founded GroupSense, in Arlington, Virginia, in 2014, the cybersecurity threat on everyone's mind was data breaches—the theft of consumer data, like bank-account information or Social Security numbers. Minder hired analysts who spoke Russian and Ukrainian and Urdu. Posing as cybercriminals, they lurked on dark-Web marketplaces, seeing who was selling information stolen from corporate networks. But, as upgrades to security systems made data breaches more challenging, cybercriminals increasingly turned to ransomware. By 2015, the F.B.I. estimated that the U.S. was subjected to a thousand ransomware attacks per day; the next year, that number quadrupled. Mike Phillips, the head of claims for the cyber-insurance company Resilience, told me, “Now it's ransomware first and only, and everything else is a distant second.”

Criminal syndicates are behind most ransomware attacks. In their online interactions, they display a mixture of adolescent posturing and professionalism: they have a fondness for video-game references and the word “evil,” but they also employ an increasingly sophisticated business structure. The larger groups establish call centers to help talk victims through the confusing process of obtaining cryptocurrency, and they promise discounts to those who pay up in a timely fashion. Some ransomware groups, including REvil, work on the affiliate model, providing hackers with the tools to deploy attacks in exchange for a share of the profits. (REvil also handles ransom negotiations on behalf of its affiliates.) “It's way too easy to get into this,” Reiner, of the I.S.T., told me. “You or I could do it—you just hire it out. There's been an incredible commoditization of the entire process.”

Hackers use various techniques to gain access to a company's computers, from embedding malware in an e-mail attachment to using stolen passwords to log in to the remote desktops that workers use to connect to company networks. Many of the syndicates are based in Russia or former Soviet republics; sometimes their malware includes code that stops an attack on a computer if its language is set to

Russian, Belarusian, or Ukrainian. Some of the syndicates employ current or former members of the military, but they seem to care more about money than about geopolitical machinations. “We are apolitical,” a man claiming to be an REvil representative said in an interview with a Russian YouTuber. “No politics at all. We don’t care who’s going to be President. We worked, we work, and we will work.”

Phillips told me, “Paying a ransom, you worry about it being venture capital for this dark-Web Silicon Valley on the other side of the world.” Ransomware groups, like their Silicon Valley counterparts, move fast and break things. In May, 2017, the WannaCry attack infected three hundred thousand computers through old and unpatched versions of Microsoft Windows. In the United Kingdom, ambulances had to be diverted from affected hospitals, and a Renault factory stopped production. Just three years after that attack, though, the REvil representative called this scattershot approach “a very stupid experiment.” The WannaCry hackers had demanded ransoms of only three hundred to six hundred dollars, netting around a hundred and forty thousand dollars.

After WannaCry, ransomware groups concentrated on sectors where a combination of lax security and a low tolerance for disruption makes getting paid more likely and more lucrative—industrial agriculture, mid-level manufacturing, oil-field services, municipal governments. Groups timed disruption for periods of acute vulnerability: schools in August, right before students returned; accounting firms during tax season. Certain syndicates specialize in “big-game hunting,” launching targeted attacks against deep-pocketed companies. The group deploying the Hades ransomware strain focusses on businesses with reported revenues of more than a billion dollars. Another designs custom malware for each job. In 2019, during a Webinar hosted by Europol, the European law-enforcement agency, a security expert mentioned that the cryptocurrency Monero was essentially untraceable; soon afterward, REvil began asking for ransom payments in Monero instead of Bitcoin.

When companies seem reluctant to negotiate, executives receive threatening phone calls and LinkedIn messages. Last year, the Campari Group issued a press release downplaying a recent ransomware attack. In response, hackers launched a Facebook ad campaign, using the profile of a Chicago d.j., whom they had also hacked, to shame the beverage conglomerate. “This is ridiculous and looks like a big fat lie,” they wrote. “We can confirm that confidential data was stolen and we

talking about huge volume of data.” Last year, printers at a South American home-goods chain began spitting out ransom notes instead of receipts.

More recently, syndicates have added extortion to their playbook. They siphon off confidential files before encrypting systems; if their ransom demand isn’t met, they threaten to release sensitive data to the media or auction it off on the black market. Hackers have threatened to publish an executive’s porn stash and to share information about non-paying victims with short sellers. “I’ve seen social-work organizations where ransomware actors threatened to expose information about vulnerable children,” Phillips said.

Before ransomware took over Minder’s life, he had settled into a routine. He walked to work, where he was usually the first to arrive and the last to leave. On the way home, he stopped at a coffee shop for a glass of wine and a salad. Back at his apartment, where he lived alone, he would work at his desk until he fell asleep. His major social outlet was the local motorcycle club, the BMW Bikers of Metropolitan Washington.

Early last year, GroupSense found evidence that a hacker had broken into a large company. Minder reached out to warn it, but a server had already been compromised. The hacker sent a ransom note to the company, threatening to release its files. The company asked Minder if he would handle the ransom negotiations. Initially, he demurred—“It never occurred to me as a skill set I had,” he said—but eventually he was persuaded.

To buy time, Minder suggested that the company acknowledge receipt of the ransom note. He began studying up on negotiation tips, watching MasterClass tutorials and reading books by former hostage negotiators. He learned that he should avoid making counteroffers in round numbers, which can seem arbitrary, and that he shouldn’t make concessions without providing a justification. During the next few weeks, as the conversation with the hacker unspooled, Minder discovered that he had a knack for negotiation. He did his best to engage the hacker, who appeared to be unaffiliated with any of the major ransomware syndicates. When the hacker complained about how much time and effort he’d invested in breaking into the company, Minder complimented him on his skills: “I told him, ‘You’re a very talented hacker, and we’d like to pay you for that. But we can’t pay what you’re asking.’”

The negotiation became all-consuming. On a motorcycle camping trip with his girlfriend, Minder huddled by the campfire with his laptop, using a 3G hot spot to keep talking. Eventually, the hacker agreed to a price that the company's insurer found acceptable. " 'I think I could get him even lower if you gave me a little bit more time,' " Minder recalls saying. "But the cyber-insurance company said, 'This is good enough.' "

Minder soon found more work. Sometimes it was a prominent company facing a multimillion-dollar ransom demand, and the negotiation took weeks. Sometimes it was a small business or a nonprofit that he took on pro bono and tried to wrap up over the weekend. But GroupSense rarely made money from the negotiations. Some ransomware negotiators charge a percentage of the amount that the ransom gets discounted. "But those really profitable approaches are ripe for fraud, or for accusations of fraud," Minder said. Instead, he charged an hourly rate and hoped that some of the organizations that he helped would sign up for GroupSense's core product, security-monitoring software.

Last March, after GroupSense's office shut down, Minder paced in circles in his four-hundred-and-seventy-five-square-foot apartment. "I was, like, I need to go hike," he said. He towed two motorcycles to a rental house in Grand Junction, Colorado. As the world fell apart, the ransomware cases kept coming. Minder handled the negotiations himself; he didn't want to distract his employees, and he found that the work required a certain emotional finesse. "Most of our employees are really technical, and this isn't a technical skill—it's a soft skill," he told me. "It's hard to train people for it."

The initial exchange of messages was crucial. People advocating on their own behalf had a tendency to berate the hackers, but that just riled them up. Minder aimed to convey a kind of warm condescension—"Like, we're friends, but you don't really know what you're doing," he explained. His girlfriend, who speaks Romanian, Russian, Ukrainian, and some Lithuanian, helped him find colloquialisms that would set the right tone. He liked to call the hackers *kuznechik*, Russian for "grasshopper."

Occasionally, Minder was called in to try to rescue negotiations that had gone off the rails. If hackers felt that a negotiation was moving too slowly, or they sensed that they were being lied to, they might cut off communication. Following the advice of Chris Voss, a former F.B.I. hostage negotiator who is

now a negotiation consultant, Minder tried to establish “tactical empathy” by mirroring the hacker’s language patterns.



“You literally could not pay me enough to relive my twenties.”



Cartoon by Suerynn Lee

Most of the time, Minder found himself dealing with a representative from one of the syndicates. “The first person you talk to is, like, level-one support,” he told me. “They’ll say something like ‘I want to work with you, but I have to get my manager’s approval to give that kind of discount.’”

GroupSense partnered with CipherTrace, a blockchain-analysis firm, which allowed Minder to see that a particular cryptowallet had been created and to trace its transactions. Determining the average payments flowing into a wallet gave him a sense of the going rate, so he could avoid overpaying. He came to understand that syndicates were working from a script. “Oftentimes, we can go to the client and say how it’s going to go before it starts,” he told me.

The clients themselves could be more challenging. Minder ran all communications by them, through a secure portal. Some wanted to edit every message to the hackers. “It’s like a spy game to them,” Minder said. Others erupted in anger or frustration. “Sometimes you’re negotiating in two directions at once—with the hacker and with the victim,” he said. “You have to have a personality type where you can be empathetic but also give directions in a way that isn’t confrontational.”

Minder has already seen pressure tactics and ransom demands escalate. In 2018, the average payment was about seven thousand dollars, according to the ransomware-recovery specialist Coveware. In 2019, it grew to forty-one thousand dollars. That year, a large ransomware syndicate announced that it was dissolving, after raking in two billion dollars in ransom payments in less than two years. “We are a living proof that you can do evil and get off scot-free,” the syndicate wrote in a farewell message. By 2020, the average ransom payment was more than two hundred thousand dollars, and some cyber-insurance companies began to exit the market. “I don’t think the insurers really understood the risk they were taking on,” Reiner told me. “The numbers in 2020 were really bad, but, at the end of 2020, everyone looked around and said, 2021 is going to be even worse.”

In 1971, a British manager at an Argentine meatpacking plant was seized by a guerrilla group. Several weeks later, after his employer paid a two-hundred-and-fifty-thousand-dollar ransom, he was freed. The following year, an electronics company paid twice as much to retrieve a kidnapped executive. In 1973, businessmen in Central America kept getting abducted, and their ransoms rose at an alarming rate: Coca-Cola paid a million dollars; Kodak paid \$1.5 million; British American Tobacco paid \$1.7 million; Firestone paid three million. One C.E.O. fetched \$2.3 million; by the time he was kidnapped again, two years later, the price had risen to ten million. Then Juan and Jorge Born, heirs to a multinational food-processing conglomerate, were captured in a scheme involving fake street signs and operatives dressed as telephone workers and police officers. They were eventually ransomed for sixty million dollars, plus a million dollars’ worth of clothing and food to be distributed

to the poor. Taking on the risk of kidnapping was “part of what it means to be an executive,” Gustavo Curtis, an American manager working in Colombia, was told by his employer shortly before his abduction, in 1976.

For much of human history, kidnapping had been largely a local affair, governed by a certain amount of ritual and reciprocity. Globalization, political destabilization, and rising inequality upended those norms. In Italy, criminal gangs abducted wealthy foreigners and farmers’ children; one year, eighty people were held for ransom. John Paul Getty refused to pay more in ransom for his kidnapped grandson than he could deduct on his taxes—reportedly three million dollars.

Kidnap-and-ransom insurance, a field that arose after the Lindbergh baby’s abduction and murder, in 1932, surged. In 1970, the size of the market was around a hundred and fifty thousand dollars; by 1976, it was seventy million dollars. The majority of policies were underwritten by Lloyd’s of London, the world’s main market for specialist insurance. Soon, there were risk analysts, who advised policyholders on how to prevent kidnappings; private security firms that offered on-the-ground protection; and specialist negotiators, who took over if things went south.

Control Risks was founded in 1975, by former members of the British Special Forces, to help the insurance industry deal with its kidnapping problem. Its executives performed their work with a patrician discretion. When, in 1977, two of its founding members were arrested in Colombia—no one was quite sure whether the nascent negotiation industry was legal—they spent their ten-week detention writing a code of conduct for their company. (The members were later exonerated.)

Around three-quarters of Fortune 500 companies eventually invested in kidnap-and-ransom insurance, but there was some discomfort with an industry that turned a profit by funnelling money to the Mafia, terrorist groups, and criminal gangs. “There is a feeling you shouldn’t make too much money,” a Control Risks co-founder told the *Times*, in 1979. Italy, Colombia, and the United Kingdom have all banned kidnap-and-ransom insurance.

But Anja Shortland, a professor of political economy at King’s College London, told me that privatized kidnap intermediaries were key in instituting what she calls “ransom discipline.” Control Risks didn’t merely negotiate ransoms; it also provided security audits, advising companies on how to keep staff from being abducted in the first place. Insurers offered reduced premiums to companies

that beefed up their security, reducing over-all rates of kidnapping. When abductions did happen, skilled negotiators kept ransom demands from spiralling out of control. These days, some ninety per cent of kidnappings are resolved, typically through the payment of a ransom; when specialists are involved, the success rate rises to ninety-seven per cent. Countries that banned kidnap insurance drove negotiations underground.

Shortland specializes in the economics of crime. “A lot of economics is: let’s assume away all the complexities so we can come up with a tractable problem,” she told me. “And I’m just embracing the complexities.” To better understand the kidnap-for-ransom industry, she closely studied the piracy-and-kidnapping market in Somalia, where she saw how private insurers, consultants, and negotiators fostered a certain predictability in a trade that’s typically portrayed as unruly. “There is a pace, a rhythm to these things,” as one negotiator told her.

The orderliness, which relies on a mutual assumption of good faith, benefits all sides, Shortland told me. Kidnappers receive an expected rate of return; the kidnapped can reasonably expect that they’ll be released intact; companies in dangerous areas can assume that their staff won’t be abducted, but, if they are, they almost certainly won’t be killed. And the insurance companies and consultants can collect their fees.

Ransomware has less “kinetic impact” than kidnapping, Bill Siegel, the co-founder of Coveware, told me—that is, no one is sending severed ears in the mail. But, to an economist, the differences are small. “They are creating very similar kinds of institutions to the ones that the kidnap-and-ransom community has created,” Shortland said. “But they’re about eighty years behind.”

When it became clear that ransomware cases weren’t slowing down, Minder trained two of his employees to handle negotiations; one of them was Mike Fowler, a former narcotics detective from North Carolina. Working undercover had taught Fowler how to slip into character, which, he told me, “is part and parcel of being an effective negotiator.”

Last November, Fowler was the designated negotiator for the construction-engineering firm. When he logged on to the dark-Web site, he noticed that the timer showed that three days had already elapsed in the negotiations. In the chat box, a conversation was in progress. “It was shocking for me,”

Fowler said. “This is a whole negotiation—poorly done, but a whole negotiation—that I’m looking at.”

Whoever had been chatting on behalf of the engineering firm was confrontational and aggressive. When the hackers demanded two hundred thousand dollars to unlock the company’s files, the negotiator initially counteroffered ten thousand dollars, and then quickly went up to fourteen thousand, then twenty-five thousand. “What that communicates to the threat actor is: there’s more money here,” Fowler said. The hackers grew frustrated. “You have reported an annual income of \$4 million,” they wrote. “We are not expect small money from you.” The final message in the chat had arrived from the hackers two days earlier: “Are you ready to close with a cost of 65k?”

Fowler and Minder tried to piece together what had happened. The clients insisted that they had never gone to the dark-Web site, much less interacted with the hacker. Then Fowler reminded Minder about a recent post on REvil’s blog, warning about fraudulent middlemen who said that they could decrypt files; instead, the middlemen would secretly negotiate with the hackers before offering the decrypted files at a markup. At the time, it had amused Minder that a cybercrime syndicate was issuing a warning about scammers. But now the clients acknowledged that they had reached out to MonsterCloud, a Florida company that advertises itself as “the world’s leading experts in Cyber Terrorism & Ransomware Recovery.” MonsterCloud’s Web site encouraged victims to use its ransomware-removal services instead of paying a ransom. That pitch likely appealed to the heads of the engineering firm, who were “very, very patriotic,” Minder told me. “It didn’t surprise me at all that they’d rather pay a software company in Florida” than send a ransom to a foreign criminal syndicate.

Minder soon learned that, shortly after the REvil hacker demanded sixty-five thousand dollars, a MonsterCloud representative told the engineering firm that it could recover the files for a hundred and forty-five thousand dollars. (MonsterCloud declined to comment.)

According to an investigation by ProPublica, MonsterCloud has a long track record of secretly negotiating with hackers. ProPublica spoke with a number of former clients who believed that their files had been decrypted without their paying a ransom, even though the ransomware strains in question made this outcome highly unlikely; most are impossible to decrypt unless there is an error in the code. MonsterCloud is one of a handful of U.S.-based data-recovery companies that appear to

follow a similar business model. By purporting to decrypt files using high-tech tools, these firms allow their clients to believe that ransomware can be addressed without sending funds to criminal syndicates—a strategy that’s particularly appealing to MonsterCloud’s publicly funded clients, such as municipalities or law-enforcement departments. Ransomware groups recognize that data-recovery firms can be lucrative partners; one offers a promo code especially for such firms. MonsterCloud declined to discuss its methods with ProPublica. “We work in the shadows,” Zohar Pinhasi, the company’s C.E.O., told the publication. “How we do it, it’s our problem. You will get your data back. Sit back, relax and enjoy the ride.”

When Minder explained the situation to his client, the man let loose a string of expletives. Because the negotiation had already been bungled, there was little chance that Minder could get the hackers to agree to a lower price. The client asked Minder to tell the hackers to go fuck themselves, but Minder says he “respectfully declined.” Instead, the company attempted to rebuild files from backups and old e-mails. Minder encouraged the client to investigate how the breach happened, but the company seemed uninterested. “They said their I.T. guy has theories,” he told me.

Minder reported MonsterCloud to the Federal Trade Commission, but the incident continued to gnaw at him. “If you Google ‘save me from ransomware’ or ‘ransomware response,’ you’re getting these companies that are basically profiteering or fraudulently misrepresenting themselves,” he said. “I’m just nauseous about it.”

Last October, the Treasury Department’s Office of Foreign Assets Control issued an advisory aimed at negotiators, cyber-insurance firms, and incident-response teams, warning that they may be fined for facilitating payments to criminals.

“They did this poorly,” Mike Convertino, the former chief information-security officer for Twitter, told me. “Maybe they got frustrated, but I view it as somewhat irresponsible. Let’s face it—if you’re a two-billion-dollar company and you’re encrypted and you don’t have good backups, they just took away your only option. So you just destroyed a two-billion-dollar company.” (The advisory seemed to have an effect: the number of ransomware victims who paid ransoms declined in the last quarter of 2020.)

In response, Convertino's current employer, the cyber-insurance firm Resilience, participated in a Ransomware Task Force, which included representatives from major cybersecurity vendors and incident-response firms, as well as from the F.B.I. and the Department of Homeland Security, under the umbrella of the Institute for Security and Technology. "Make no mistake, our recommendations aren't about eliminating ransomware as a threat," John Davis, a vice-president at the cybersecurity firm Palo Alto Networks, said at an online event; rather, the goal is to bring it to a level "that can be more effectively managed." Those recommendations included requiring ransom payments to be reported to authorities and creating a fund to support victims who refrain from paying ransoms. In April, the Justice Department announced that it was forming its own ransomware task force to coordinate among the private sector, other federal agencies, and international partners.

Meanwhile, the ransomware syndicates have been working to shore up their images. DarkSide, the group responsible for hacking Colonial Pipeline's system, had vowed that it would not attack schools, hospitals, funeral homes, or nonprofit organizations; it would target only large corporations. In October, DarkSide issued a press release announcing that it had just donated ten thousand dollars in cryptocurrency to two charities. "No matter how bad you think our work is, we are pleased to know that we helped change someone's life," the syndicate wrote. But disabling critical infrastructure brought another level of attention, as well as the threat of a significant law-enforcement response. DarkSide apologized for causing disruption and, sounding like a chastened tech company, promised to invest more in moderation, "to avoid social consequences in the future." A few days later, the syndicate announced that its servers had been shut down and its Bitcoin wallet emptied, potentially an indication of law-enforcement actions. Seemingly spooked by the negative publicity, REvil announced that it would no longer attack targets in the government, health-care, and education sectors.

Shortland saw this kind of brand-burnishing as a good thing. "If this was a complete fly-by-night scenario, then I might despair," she told me. "But people who do this want to do it again." The hackers cared about their reputations, which was a sign that the market was governable. That didn't mean ransomware would go away—at least, if the example of criminal kidnapping was any indication. "There is a certain amount of kidnap that works for everyone," she said. ♦

Published in the print edition of the June 7, 2021, issue, with the headline "The Go-Between."

*Rachel Monroe began contributing to *The New Yorker* in 2017. She is the author of “Savage Appetites: True Stories of Women, Crime, and Obsession.”*

More: [Hackers](#) [Computers](#) [Ransoms](#) [Negotiations](#) [Hacking](#) [Technology](#) [Ransom](#) [Cybercrimes](#)
[Cybersecurity](#) [Gas](#) [Companies](#) [Criminals](#) [Cyber-Attacks](#) [Kidnappings](#) [Organized Crime](#)

THIS WEEK'S ISSUE

Never miss a big *New Yorker* story again. Sign up for This Week's Issue and get an e-mail every week with the stories you have to read.

Enter your e-mail address

Your e-mail address

Sign up

By signing up, you agree to our [User Agreement](#) and [Privacy Policy & Cookie Statement](#).

Read More



MEDICAL DISPATCH

THE COMPLEX BUSINESS OF VACCINE MANDATES

Tougher mandates may be necessary—but we shouldn't ignore the harm that they can cause.

By Dhruv Khullar



ANNALS OF INQUIRY

UNCOVERING THE SECRET OFFSHORE ACCOUNTS OF THE GLOBAL ÉLITE

In an age of rising populism, the International Consortium of Investigative Journalists is exposing the hypocrisy behind the hidden wealth.

By Benjamin Wallace-Wells



A REPORTER AT LARGE

THE MIGRANT WORKERS WHO FOLLOW CLIMATE DISASTERS

A growing group of laborers is trailing hurricanes and wildfires the way farmworkers follow crops, contracting for big disaster-recovery firms, and facing exploitation, injury, and death.

By Sarah Stillman

POLITICS AND MORE PODCAST

HOW WORRIED SHOULD DEMOCRATS BE?

Do the results of the Virginia and New Jersey gubernatorial races mean trouble for the

Democrats in 2022?

Cookies Settings

Combating Ransomware

A Comprehensive Framework for Action:
*Key Recommendations from the
Ransomware Task Force*

Prepared by the Institute for Security and Technology

Contents

A Note from RTF Co-Chairs	3-4
Executive Summary	5-6
Introduction	7-19
<i>Ransomware as a National Security Threat</i>	8
<i>Understanding Ransomware</i>	11
<i>Ransom Payments</i>	12
<i>Cyber Insurance and Ransomware</i>	13
<i>The Role of Cryptocurrency</i>	14
<i>A Global Challenge</i>	15
<i>The Threat Actors</i>	16
<i>Existing Efforts to Mitigate Ransomware Attacks</i>	18
A Comprehensive Framework for Action:	19-48
Key Recommendations from the Ransomware Task Force	
<i>Goal 1: Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy</i>	21
<i>Goal 2: Disrupt the ransomware business model and decrease criminal profits</i>	28
<i>Goal 3: Help organizations prepare for ransomware attacks</i>	35
<i>Goal 4: Respond to ransomware attacks more effectively</i>	42
A Note on Prohibiting Ransom Payments	49-50
Conclusion	51
<i>Summary of Recommendations</i>	52-54
Acknowledgments	55-56
Appendices	57-72
<i>Appendix A: Cyber Insurance</i>	58-61
<i>Appendix B: The Cryptocurrency Payment Process</i>	62-67
<i>Appendix C: Proposed Framework for a Public-Private Operational Ransomware Campaign</i>	68-72
Glossary	73-76
Endnotes	77-81

A Note from the RTF Co-Chairs

We are honored to present this report from the Ransomware Task Force. This report details a comprehensive strategic framework for tackling the dramatically increasing and evolving threat of ransomware, a widespread form of cybercrime that in just a few years has become a serious national security threat and a public health and safety concern.

Ransomware is not just financial extortion; it is a crime that transcends business, government, academic, and geographic boundaries. It has disproportionately impacted the healthcare industry during the COVID pandemic, and has shut down schools, hospitals, police stations, city governments, and U.S. military facilities. It is also a crime that funnels both private funds and tax dollars toward global criminal organizations. The proceeds stolen from victims may be financing illicit activities ranging from human trafficking to the development and proliferation of weapons of mass destruction.

Tackling ransomware will not be easy; there is no silver bullet for solving this challenge. Most ransomware criminals are based in nation-states that are unwilling or unable to prosecute this cybercrime, and because ransoms are paid through cryptocurrency, they are difficult to trace. This global challenge demands an “all hands on deck” approach, with support from the highest levels of government.

Countless people around the world are already working tirelessly to blunt the onslaught of ransomware attacks. But no single entity alone has the requisite resources, skills, capabilities, or authorities to significantly constrain this global criminal enterprise.

For this reason, we convened the Ransomware Task Force — a team of more than 60 experts from software companies, cybersecurity vendors, government agencies, non-profits, and academic institutions — to develop a comprehensive framework for tackling the ransomware threat.

Our goal is not only to help the world better understand ransomware, but to proactively and relentlessly disrupt the ransomware business model through a series of coordinated actions, many of which can be immediately implemented by industry, government, and civil society. Acting upon a few of these recommendations will not likely shift the trajectory, but the Task Force is confident that implementing all of them in coordination, with speed and conviction, will make a significant difference.

While we have strived to be comprehensive, we acknowledge there will be areas we have not addressed, or on which we could not come to consensus. Prohibition of payments is the most prominent example; the Task Force agreed that paying ransoms is detrimental in a number of ways, but also recognized the challenges inherent in barring payments. Just as we have been grateful to stand on the shoulders of those that came before us, we hope our efforts and investigations will fuel the thinking and recommendations of those that come after us.

We urge all those with the ability to act to do so immediately. The ransomware threat continues to worsen by the day, and the consequences of waiting to respond could be disastrous. More than money is at stake; lives, critical infrastructure, public faith in the legitimacy of our institutions, the education system, and in many ways, our very way of life depends on taking action.

As a final note, we would like to offer our sincere thanks to the members of the Ransomware Task Force, who responded to our call and generously dedicated their time and energy into developing the recommendations included in this report.

The Working Group Co-Chairs of the Ransomware Task Force.



John Davis,
*Palo Alto
Networks*



Megan Stifel,
*Global Cyber
Alliance*



Michael Phillips,
Resilience



Kemba Walden,
Microsoft



Jen Ellis,
Rapid7



Chris Painter,
*The Global Forum
on Cyber Expertise
Foundation Board*



Michael Daniel,
*Cyber Threat
Alliance*



Philip Reiner,
*Institute for Security
and Technology*

Executive Summary

Ransomware attacks present an urgent national security risk around the world. This evolving form of cybercrime, through which criminals remotely compromise computer systems and demand a ransom in return for restoring and/or not exposing data, is economically destructive and leads to dangerous real-world consequences that far exceed the costs of the ransom payments alone.

In 2020, thousands of businesses, hospitals, school districts, city governments, and other institutions in the U.S. and around the world were paralyzed as their digital networks were held hostage by malicious actors seeking payouts. The immediate physical and business risks posed by ransomware are compounded by the broader societal impact of the billions of dollars steered into criminal enterprises, funds that may be used for the proliferation of weapons of mass destruction, human trafficking, and other virulent global criminal activity.

Despite the gravity of their crimes, the majority of ransomware criminals operate with near-impunity, based out of jurisdictions that are unable or unwilling to bring them to justice. This problem is exacerbated by financial systems that enable attackers to receive funds without being traced. Additionally, the barriers to entry into this lucrative criminal enterprise have become shockingly low. The “ransomware as a service” (RaaS) model, allows criminals without technical sophistication to conduct ransomware attacks. At the same time, technically knowledgeable criminals are conducting increasingly sophisticated attacks.

Significant effort has been made to understand and address the ransomware threat, yet attackers continue to succeed on a broad and troubling scale. To shift these dynamics, the international community needs a comprehensive approach that influences the behavior of actors on all sides of the ecosystem, including deterring and disrupting attackers, shoring up preparation and response of potential victims, and engaging regulators, law enforcement, and national security experts. We also need international cooperation and adoption of processes, standards, and expectations.

This report outlines a comprehensive framework of actions (48 in total) that government and industry leaders can pursue to significantly disrupt the ransomware business model and mitigate the impact of these attacks in the immediate and longer terms. These recommendations were collaboratively developed by the Ransomware Task Force (RTF) — a broad coalition of volunteer experts from industry, government, law enforcement, civil society, cybersecurity insurers, and international organizations — to provide a strategic framework for a systemic, global approach to mitigating the ransomware problem.

While we have identified some recommendations as priorities, we strongly recommend viewing the entire set of recommendations together, as they are designed to complement, and build on each other. The strategic framework is organized around four primary goals: to deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy; to disrupt the business model and reduce criminal profits; to help organizations prepare for ransomware attacks; and to respond to ransomware attacks more effectively.

Priority recommendations



These priority recommendations are the most foundational and urgent; many of the other recommendations were developed to facilitate or strengthen these core actions:

1. Coordinated, international diplomatic and law enforcement efforts must proactively prioritize ransomware through a comprehensive, resourced strategy, including using a carrot-and-stick approach to direct nation-states away from providing safe havens to ransomware criminals.
2. The United States should lead by example and execute a sustained, aggressive, whole of government, intelligence-driven anti-ransomware campaign, coordinated by the White House. In the U.S., this must include the establishment of 1) an Interagency Working Group led by the National Security Council in coordination with the nascent National Cyber Director; 2) an internal U.S. Government Joint Ransomware Task Force; and 3) a collaborative, private industry-led informal Ransomware Threat Focus Hub.
3. Governments should establish Cyber Response and Recovery Funds to support ransomware response and other cybersecurity activities; mandate that organizations report ransom payments; and require organizations to consider alternatives before making payments.
4. An internationally coordinated effort should develop a clear, accessible, and broadly adopted framework to help organizations prepare for, and respond to, ransomware attacks. In some under-resourced and more critical sectors, incentives (such as fine relief and funding) or regulation may be required to drive adoption.
5. The cryptocurrency sector that enables ransomware crime should be more closely regulated. Governments should require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading “desks” to comply with existing laws, including Know Your Customer (KYC), Anti-Money Laundering (AML), and Combatting Financing of Terrorism (CFT) laws.

The ransomware threat continues to worsen daily. The actions detailed in this report need to be enacted together as soon as possible, and must be coordinated at a national and international level in order to have the necessary impact. We understand the gravity of this challenge, but we believe that if this framework is implemented in full, the international community could see a decrease in the volume of these types of attacks in one year’s time. Proposing this framework is merely the first step, and the real challenge is in implementation. With every recommended action we aimed to work through the practical implications, and in most cases we present immediately actionable recommendations. The Co-Chairs of the RTF welcome the opportunity to discuss these findings and recommendations further to help achieve these goals.

Introduction

Ransomware is a flourishing criminal industry that not only risks the personal and financial security of individuals, but also threatens national security and human life. Businesses, schools, governments, hospitals, and nearly every other type of institution are regularly targeted, disrupted, and held hostage. The problem has steadily grown worse in recent years, and in 2020, nearly 2,400 U.S.-based governments, healthcare facilities, and schools were victims of ransomware, according to the security firm Emsisoft.¹ Multiple organizations have issued reports on the costs of ransomware, and while their exact figures vary, all consistently show a steady increase in the number of attacks — and damaging economic impact.



21
DAYS

**Average downtime
due to ransomware
attacks²**
(Coveware)



287
DAYS

**Average days it takes
a business to fully
recover from an attack³**
(Emsisoft)



\$350
MILLION

**Victims paid in
ransom in 2020
— a 311% increase
over the prior year⁴**
(Chainalysis)



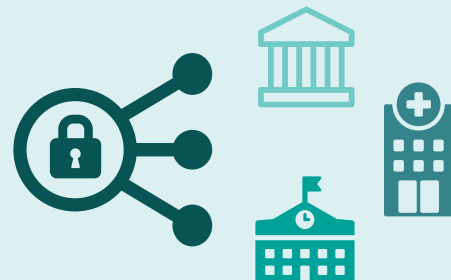
\$312,493

**The average payment
in 2020 — a 171%
increase compared
to 2019⁵**
(Palo Alto Networks)

In 2020, nearly

2,400

**U.S.-based governments,
healthcare facilities, and schools
were victims of ransomware**



Ransomware as a National Security Threat

The costs of ransomware go far beyond the ransom payments themselves. Cybercrime is typically seen as a white-collar crime, but while ransomware is profit-driven and “non-violent” in the traditional sense, that has not stopped ransomware attackers from routinely imperiling lives.

Threats to Critical Infrastructure:

Ransomware attacks have shut down the operations of critical national resources, including military facilities. In 2019, a ransomware attack shut down the operations of a U.S. Coast Guard facility for 30 hours,⁶ and in February 2020, a ransomware attack on a natural-gas pipeline operator halted operations for two days.⁷ Attacks on the energy grid, on a nuclear plant, waste treatment facilities, or on any number of critical assets could have devastating consequences, including human casualties.

Risks to Public Health:

Hospitals and other medical centers are a favorite target for ransomware criminals. In 2020, 560 healthcare facilities were hit by ransomware attacks in the U.S. alone.⁸ These incidents not only cost the victims millions of dollars in recovery, but they also have led to delays in patient treatment, and possibly loss of life. In September 2020, a ransomware attack led to the failure of computer systems at Duesseldorf University Clinic, requiring critically ill patients to be relocated to other facilities, and in the United States, an attack caused delays in treatment for cancer patients at the University of Vermont Medical Care and other facilities.⁹

Societal Impact: Targeting the Health Care Sector



In October 2020, hackers compromised the computer networks of roughly a dozen medical centers across the United States. These attacks forced the cancelations of surgeries and disruptions in patient care; the University of Vermont Medical Center (UVM) was forced to furlough or reassign about 300 employees as the hospital's networks were taken offline in the midst of the COVID pandemic, and patients were turned away from scheduled cancer treatments and other medical procedures. The company's President and COO estimated the attack would cost roughly \$64 million before systems were fully restored.

“It feels like we are all alone and no one understands how dire this is,”

– UVM Nurse to the *New York Times*.¹⁰

Extensive cyber vulnerabilities across the healthcare industry create potentially lucrative targets for malicious ransom-seeking actors, driving the significant increase in attacks against healthcare facilities. Government policy choices regarding ransomware should focus on this critical threat: statistical analysis reveals that ransomware-driven delays in care in these healthcare systems invariably contributes to a loss of life due to the inability of patients to receive timely care.¹¹ This illuminates the risk to human life posed by these attacks – and yet the attackers continue to undertake these assaults with near impunity.

Diversion of Vital Public Resources:

Ransomware attacks on municipal governments are common. Such attacks not only divert public resources into illicit economies, but the victims incur costs that far exceed the ransoms alone. For example, in 2018, the City of Atlanta paid \$50,000 in Bitcoin as ransom, but the total cost of the recovery exceeded \$2.6 million, as the city was forced to pay for digital forensics, increased staffing, crisis communications, and other costs.¹² A ransomware attack similarly debilitated the City of Baltimore, leading to a range of negative impacts.

Loss of Data/Privacy:

Ransomware criminals are increasingly expanding their attacks to include “double extortion,” whereby they first demand ransom to de-encrypt an organization’s data, then threaten to release the data on to the internet unless additional ransom is paid. At the start of 2020, only one major ransomware group exfiltrated data for a second extortion, but by the end of the year, at least 17 other groups used this tactic.¹³ The potential exposure of their data and ensuing legal liability (particularly in countries with strict data security laws) may be a critical factor in leading some victims to pay the ransom.

Disruption of Schools and Colleges:

The education sector has become a top target: during 2020, nearly 1700 schools, colleges, and universities in the United States were impacted by ransomware.¹⁴ According to a report by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), 57% of all reported ransomware attacks in August and September 2020 were targeted at K–12 schools.¹⁵ These attacks not only disrupt the schools’ operations, but often include threats to leak confidential student data on the internet.

Societal Impact: Cities Under Siege

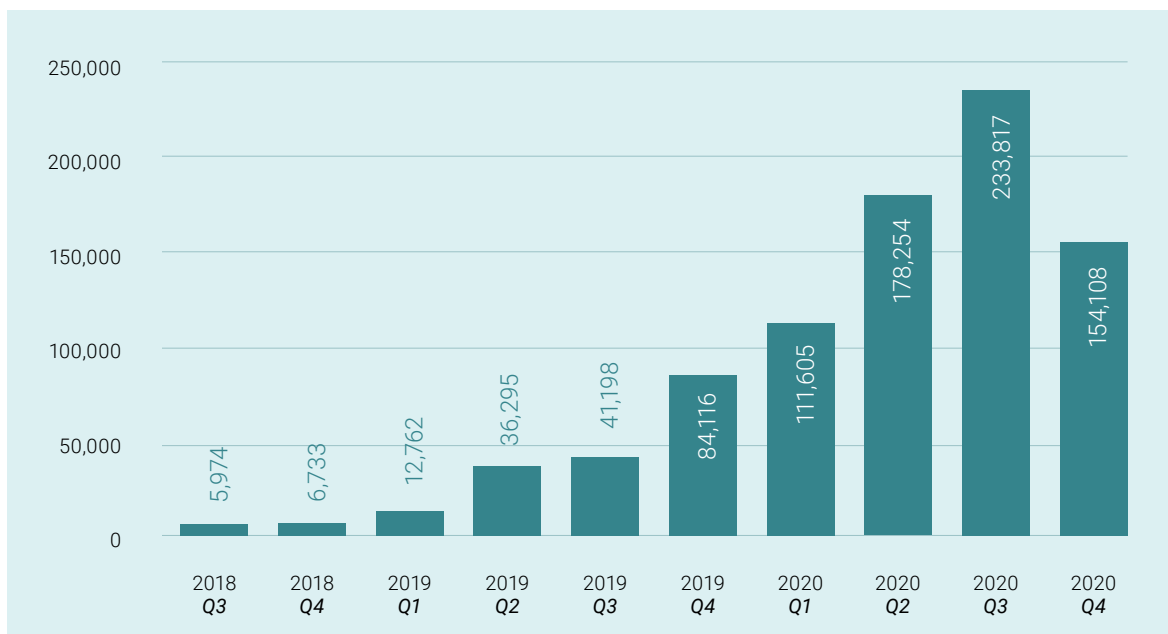
In May 2019, a ransomware attack on the City of Baltimore took critical services offline. The city refused to pay the ransom, but the recovery lasted several weeks and cost \$18.2 million to restore systems back to their original state.¹⁶ Beyond the financial burden on taxpayers and the shutdown of services, the city’s inhabitants were no longer able to pay water bills, property taxes, or parking fines. Some residents who could not pay their bills saw their homes go into foreclosure. Databases tracking street drugs were knocked offline, people were unable to pay water bills and home sales were delayed.¹⁷ The city’s 911 dispatch system was knocked offline, and emergency calls made during that time were not recorded. The criminals threatened to publicly release data stolen during the attack to exert pressure on city officials to pay, in an early example of the “double extortion” tactic that has since become prevalent.¹⁸

Economic Impact:

Ransoms paid by private firms siphon millions of dollars toward criminal enterprise every year. The total amount paid by ransomware victims increased by 311% in 2020, reaching nearly \$350 million worth of cryptocurrency.¹⁹ However, the economic impacts go well beyond the costs of ransoms

alone. Reported ransomware payments do not cover the costs associated with service downtime and recovery. Total remediation costs are typically several times a ransom payment and are often large enough to cripple many small businesses. In addition, money that flows to the criminal networks creates second- and third-order economic effects, since those revenues go on to fund other types of crime.

FIGURE 1 Average ransom in USD



From *The Coveware Quarterly Ransomware Report*

Societal Impact: K-12 Schools



Ransomware attacks on schools have devastating impacts, including loss of instructional time and the leakage of sensitive data. In early 2021, a ransomware attack on the Buffalo Public School system prevented 5,000 students from returning to in-person learning Monday and shut down online learning for thousands more.²⁰

Such attacks also add to budgetary challenges for already under-resourced districts: when Mississippi's Yazoo County School District paid \$300,000 as a ransom to recover files encrypted during a ransomware attack, the cost equaled roughly 1.5% of the district's annual budget.²¹

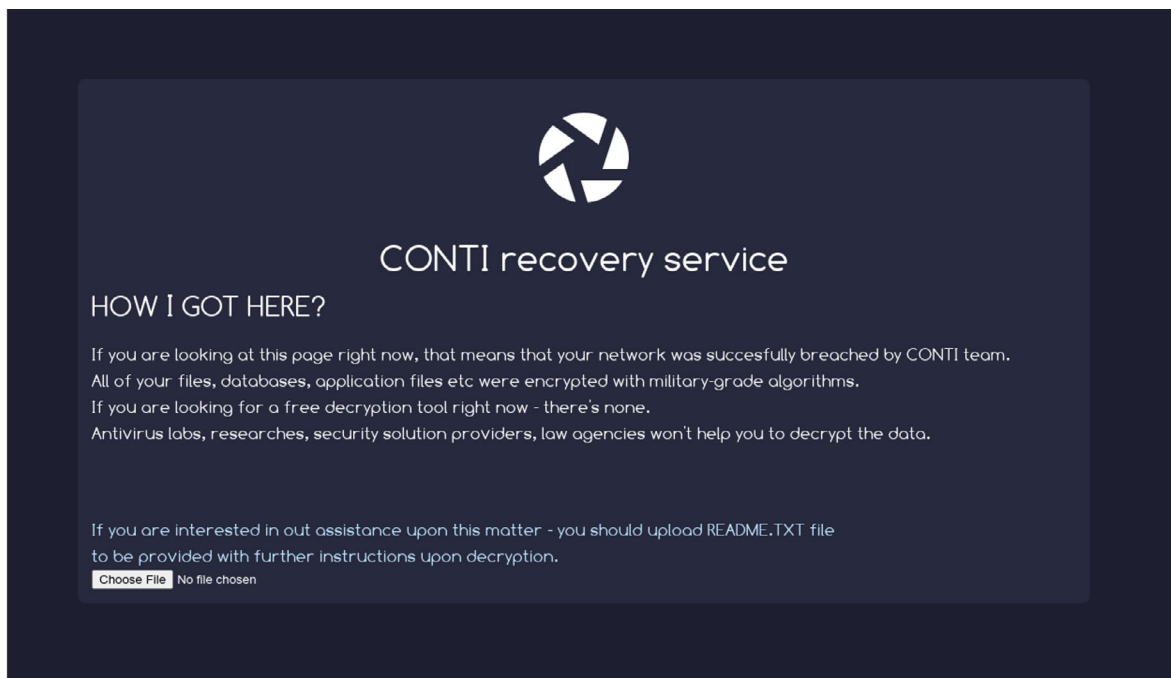
The targeting of schools is not limited to the United States. In March 2021, a ransomware attack left 37,000 students in London and Essex without access to email or coursework. The attack targeted The Harris Federation, which runs 50 primary and secondary schools in the UK.²² The perpetrators are suspected to have stolen personal data about the organization, including financial details, and posted it on the dark web.²³

Understanding Ransomware

Ransomware is a sub-category of malware, a class of software designed to cause harm to a computer or computer network. CISA defines ransomware as “an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.”²⁴

Ransomware proliferates in diverse ways, including through exploitation of vulnerabilities, as well as social engineering tactics, such as “phishing” emails that deceive employees within an organization to open attachments that launch the malware that then infects their networks. Once launched, the malware may connect to a command-and-control server to enable the criminals to move laterally across networks and encrypt and/or exfiltrate the organization’s data. Ransomware victims are typically prompted with a screen informing them that their data has been encrypted, with instructions for how to restore their systems by sending payment via cryptocurrency. Not all attacks result in data encryption, but most do: a 2020 survey of 5000 IT managers found that 51% had been hit by ransomware in the last year, and the criminals succeeded in encrypting the data in 73% of these attacks, according to Sophos.²⁵

Example of a ransomware lock screen



Ransomware victims are typically prompted with a screen informing them that their data has been encrypted, with instructions for how to restore their systems by sending payment via cryptocurrency.

Ransom Payments

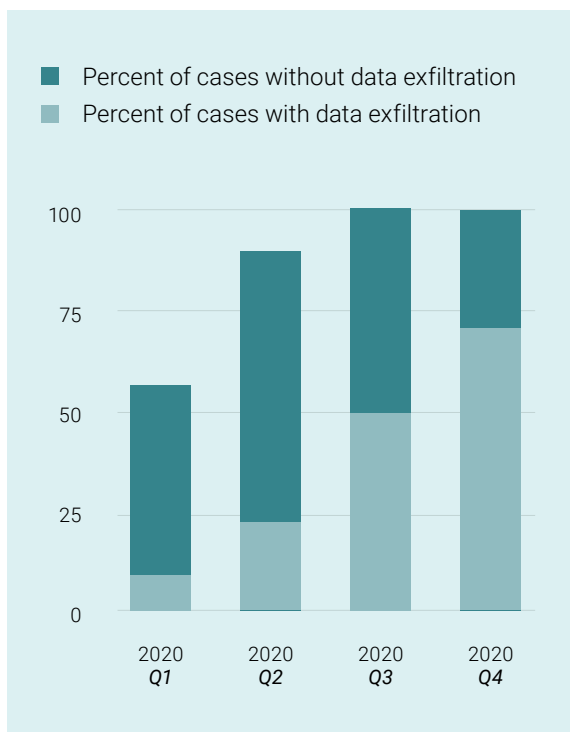
A number of factors can influence whether victims agree to pay the ransom demand, including whether they have cyber insurance, the quality of their data backups, and the estimated costs of the system outage. Legal considerations may also come into play: in the United States for example, firms that pay ransoms (and their facilitators) may find themselves in violation of regulations imposed by the Office of Foreign Assets Controls (OFAC).²⁶

Surveys of global IT professionals have found that, of the organizations reporting a ransomware attack, 27% of victims chose to pay the ransom requested, with small variations at the regional level in terms of the average amounts paid \$1.18 million in APAC, \$1.06 million at EMEA, and \$0.99 million in the United States).²⁷

Victims may be more likely to pay if they are concerned their data will be made public. As a result, the theft and threat of public disclosure of sensitive data — a tactic known as “double extortion” or “data exfiltration” — has become an increasingly common tactic for ransomware attackers, as it intensifies the pressure on entities already struggling to regain operational capacity and protect sensitive data.

FIGURE 2

Percent of attacks involving data exfiltration



From The Coveware Quarterly Ransomware Report



Cyber Insurance and Ransomware

The cyber insurance industry sells policies to firms to cover losses in the event of a ransomware attack or other incident. Cyber insurance policies often include specific coverages for ransomware, including for business interruption losses, data restoration costs, incident response costs, and for a ransom payment, if one is made.

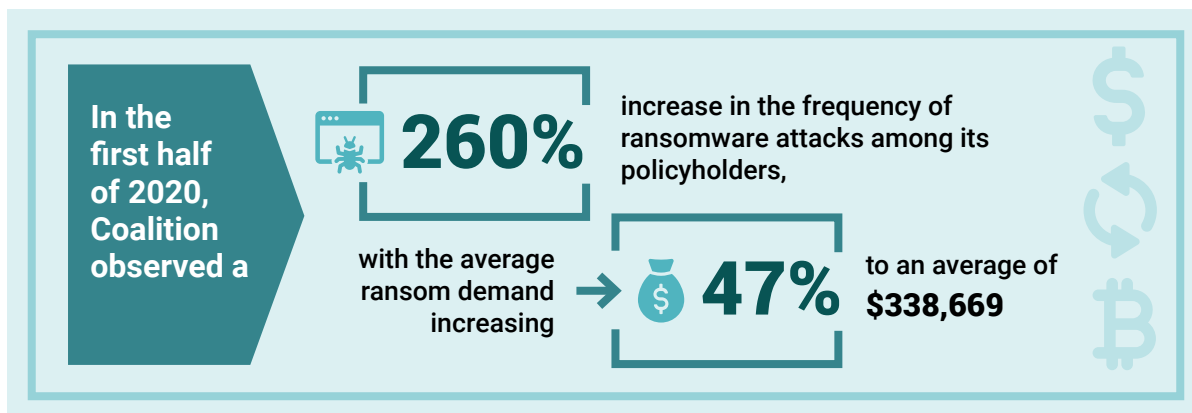
Ransomware attacks are the most common reported cyber insurance claim, according to Coalition, a cyber insurance firm. In the first half of 2020, Coalition observed a 260% increase in the frequency of ransomware attacks among its policyholders, with the average ransom demand increasing 47% to an average of \$338,669.²⁸

The role of cyber insurance in ransomware is complicated. Some argue that the “backstop” support of insurance encourages ransomware attackers, as victims may be more likely to pay if their costs are covered.²⁹ There is evidence that attackers may target companies specifically because they have insurance; in an interview, a ransomware criminal affiliated with the prominent syndicate REvil (also known as Sodinokibi) stated that targeting firms with cyber insurance was “one of the tastiest morsels.”³⁰

On the other hand, more mature insurance providers typically require that their clients adhere to strong baseline security practices, which can significantly reduce the disruption caused by a ransomware attack. They also connect victims to recovery experts and law enforcement, and can leverage a variety of market tools, such as co-insurance, to incentivize security standards and discourage organizations from paying ransoms.

The challenge is that not all cyber insurers are at the same level of sophistication, and some may even view a lack of security baseline requirements to be a unique selling proposition. Given the prevalence and cost of ransomware claims, it is rational to expect that the cyber insurance industry will eventually adopt security baseline requirements broadly as a standard expectation for insurability. When this becomes the status quo, insurers will play a more definitively positive role both in driving adoption of better cyber hygiene, and in providing an important safety net for victims of attacks. However, it will take time to achieve this maturity across the industry.

Acknowledging the ways in which cyber insurance may influence or shape organizational behavior and the ransomware “kill chain”, the insurance-related recommendations in this report are designed to enhance the sector’s role in supporting comprehensive public and private action against ransomware, while accelerating the cyber insurance market’s maturity, solvency, and expertise. For a more detailed overview of cyber insurance, **see Appendix A.**



The Role of Cryptocurrency

The explosion of ransomware as a lucrative criminal enterprise has been closely tied to the rise of Bitcoin and other cryptocurrencies, which use distributed ledgers, such as blockchain, to track transactions. The use of cryptocurrency adds to the challenge of identifying ransomware criminals, as payments with these currencies are difficult to attribute to any individual. Often the money does not flow straight from ransomware victim to criminal; it travels through a multi-step process involving different financial entities, many of which are novel and are not yet part of standardized, regulated financial payments markets.

Ransomware criminals typically demand that victims send their ransom payments via Bitcoin, but after receiving the payment in a designated digital “wallet” (software that stores public and private keys), the criminals typically obfuscate these funds as quickly as possible to avoid detection and tracking. Their methods include “chainhopping,” which involves exchanging funds in one cryptocurrency for another using any of a variety of cryptocurrency exchanges. The funds can be extremely difficult to trace after they have been exchanged, and to further shield themselves, ransomware actors may use money-mule service providers to set up accounts, or use accounts with false or stolen credentials.

Ransomware criminals can also obscure their transactions through cryptocurrency “mixing services,” which muddy the public ledger by mixing in legitimate traffic with illicit ransomware funds. Some groups will also demand payments in currencies known as “privacy coins,” such as Monero, that are designed for privacy and make payments untraceable.³¹ However, privacy coins have not been adopted as widely as might be expected because they are not as liquid as Bitcoin and other cryptocurrencies, and due in part to regulation, this payment method may become increasingly impractical.

Cryptocurrencies add to the challenge of ransomware because they are considered to be “borderless.” The cryptocurrency community is expressly focused on building a set of technologies designed to reduce compliance and financial process costs. After obfuscating the extorted funds, ransomware criminals may either withdraw the funds into hard cash, or because cryptocurrencies have become increasingly common (and their value has been steadily rising), they may keep their profits in cryptocurrency and use them to pay for other illicit activities.

While cryptocurrencies are difficult to trace, blockchain analysis can help interpret public blockchain ledgers and, with the proper tools, government agencies, cryptocurrency businesses, and financial institutions can understand which real-world entities transact with each other. Blockchain analytic companies are able to show that a given transaction took place between two different cryptocurrency exchanges, for example, or between a cryptocurrency exchange and an illicit entity, such as a sanctioned individual or organization. With blockchain analysis tools and Know Your Customer (KYC) information, law enforcement can gain transparency into blockchain activity in ways that are not possible in traditional finance.

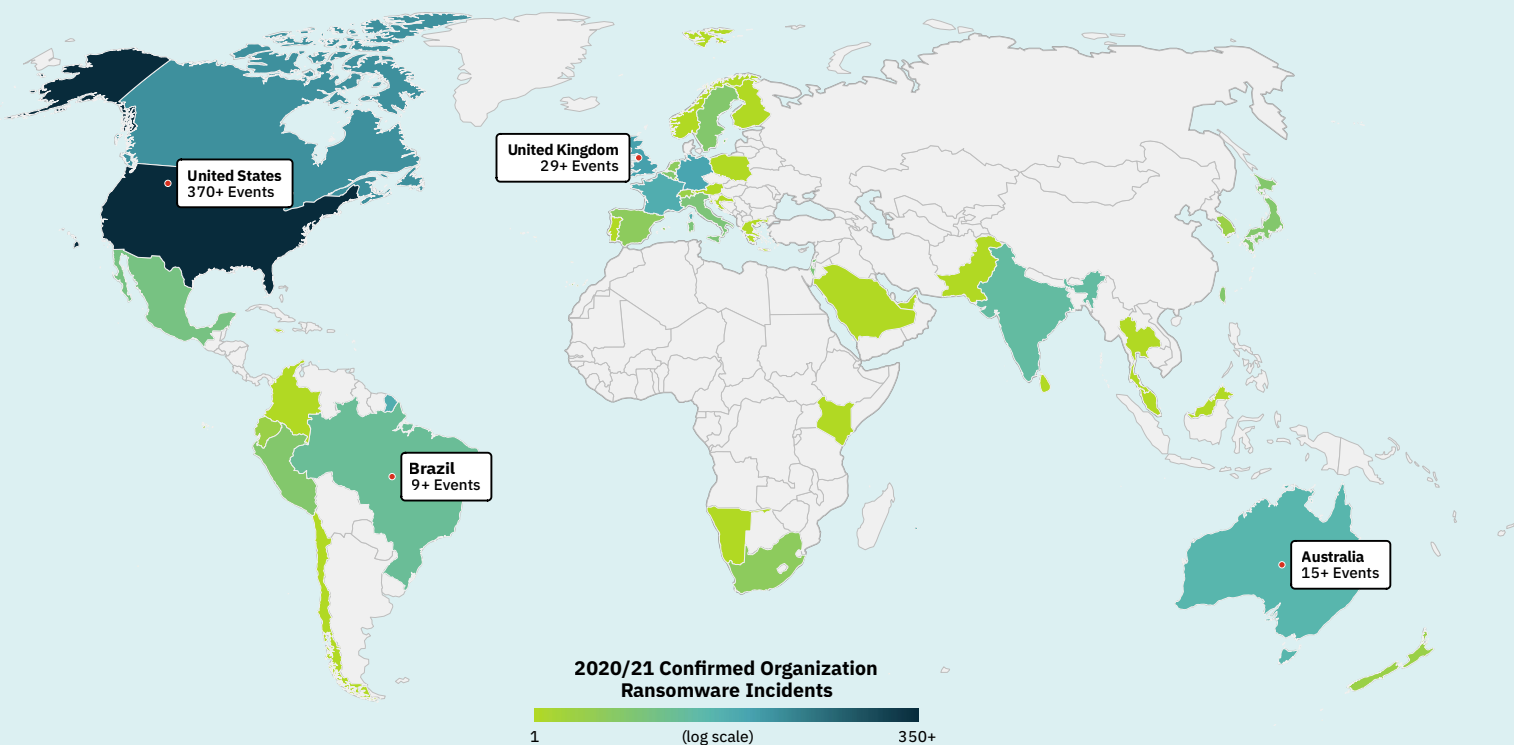
See Appendix B: The Cryptocurrency Payment Process, for a more detailed overview of how ransomware payments work, including where interventions could occur and how they could undermine the ransomware business model.

A Global Challenge

Ransomware is a global challenge, as institutions in all sectors around the world are being increasingly targeted. A single attack can also rapidly spread across borders, intentionally or otherwise: the 2017 WannaCry ransomware attack affected 150 countries.³² A survey by security firm Sophos³³ found the nations with the highest percentage of organizations reporting ransomware attacks in 2020 were India, Brazil, Turkey, Belgium, Sweden, and the United States. However, ransomware attacks occur frequently in Russia, Saudi Arabia, China, and nearly every other nation.³⁴

Reducing the ransomware threat will require global cooperation due to the highly decentralized nature of cryptocurrency, dispersed nature of the criminal networks involved, the internet's basic infrastructure, and the differing legal and regulatory regimes around the world. Ransomware criminals are able to game the system by moving their operations to where legislation and cybercrime enforcement are the most lenient. International institutions have begun to tackle this challenge: in October 2020, for example, finance ministers from the Group of Seven (G7) called upon nations to implement Financial Action Task Force standards to reduce ransomware and other cybercrime.³⁵ However, more must be done to improve global cooperation, reduce safe havens, align international standards, and ramp up enforcement.

FIGURE 3 2020/21 Confirmed Organization Ransomware Incidents



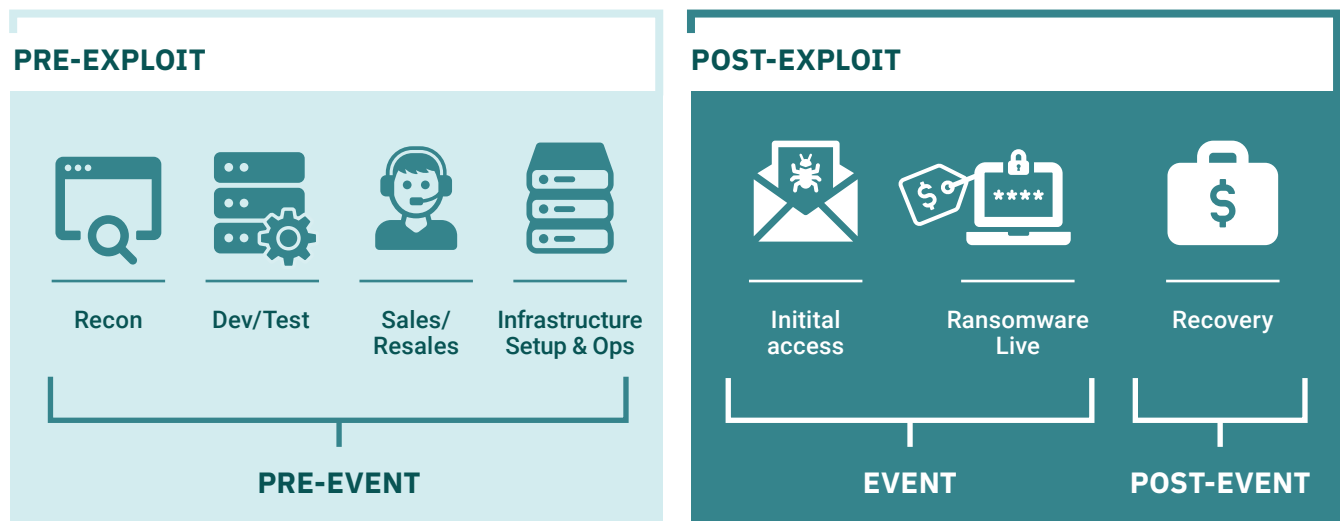
Sources: Palo Alto Unit 42; Scitum; Cloudian; Black Fog; Recorded Future Incidents include victim organizations with data published on leak sites or with publicly disclosed ransoms.

The Threat Actors

The profitability of ransomware has attracted a diverse set of malicious actors, who have built a thriving and evolving criminal ecosystem. While different ransomware attacks may seem similar, they are often executed by a diverse array of attackers with highly variable motivations. Some are organized into ransomware “gangs,” which, like other organized crime units, operate in one cohesive team while developing and executing attacks.

Recent years have seen the rise of the “ransomware as a service” (RaaS) business model. Some national governments have used ransomware to advance their strategic interests, including evading sanctions. This diversity of threats increases the complexity of attributing and countering ransomware attacks and highlights the need for broad pressure along the entire ransomware kill chain.

FIGURE 4 Ransomware “Kill Chain”



Source: World Economic Forum's Partnership against Cybercrime in collaboration with Accenture

Ransomware-as-a-Service

Carrying out a ransomware attack does not require technical sophistication. “Ransomware as a service” (RaaS) is a business model that provides ransomware capabilities to would-be criminals who do not have the skills or resources to develop their own malware. In 2020, two-thirds of the ransomware attacks analyzed by cybersecurity firm Group-IB were perpetrated by cyber criminals using a RaaS model.³⁶ This “as a service” model follows similar evolutions in the mainstream software and infrastructure industries, which have seen success from “software as a service” and “infrastructure as a service” business models.

In the RaaS model, there are at least two parties who establish a business relationship: the *developer* and the *affiliate*. The developer writes the malicious program that encrypts and potentially steals the victim’s data. The developer then licenses this malware to the affiliate for a fixed fee or a share of successful ransom payments. The affiliate executes the attack and collects the ransom, potentially also including additional business arrangements, like purchasing exploits or using cryptocurrency brokers and washers.

In this model, even a non-technical affiliate can successfully execute ransomware attacks by purchasing the necessary exploits and malware. RaaS can be contrasted with more traditional ransomware gangs, in which a cohesive team both builds the malware and executes the attack. The Sobinokibi, Phos, Dharma, and Globelmposter ransomware variants are all known to operate under the RaaS model.³⁷

The Nation-State Nexus

Of particular interest to the Task Force was the relationship between ransomware and national governments. Many ransomware criminals operate with impunity, as their countries' governments are unwilling or unable to prosecute this form of crime. In other cases, the organizations executing ransomware attacks may be state-sponsored, and may in fact be helping nations evade economic sanctions.³⁸ For example, in an April 2021 announcement of new sanctions against Russia, the U.S. Department of Treasury made a direct connection between Russia's Federal Security Service (FSB) and ransomware hackers, noting that "to bolster its malicious cyber operations, the FSB cultivates and co-opts criminal hackers, including the previously designated Evil Corp, enabling them to engage in disruptive ransomware attacks and phishing campaigns."³⁹

Proceeds from ransomware may help finance terrorism, human trafficking, or the proliferation of weapons of mass destruction.⁴⁰ For these reasons, direct affiliation between ransomware attacks and governments is intentionally shrouded in secrecy, making attribution and accountability challenging. Countering state-sponsored attackers will require broad application of "carrot and stick" methods and international cooperation.

Societal Impact: NotPetya



The 2017 NotPetya attack highlighted how this form of cybercrime can have far-reaching consequences. The estimated financial losses exceeded \$10 billion, but the true scale of the damage was far greater. Though the attack was not strictly ransomware as it was not motivated by profit, it did leverage ransomware code, cause the same type of disruptive impact, and present a screen demanding a ransom.

The attack started in Ukraine, where computer systems at two major airports, bus stations, railways, the postal service, and media companies were taken hostage. It infected ATM machines and payment systems, and for the first time after 31 years, the radiation monitors at Chernobyl shut down, forcing workers in hazmat suits to manually monitor radiation levels.⁴¹

The destructive virus was designed to spread, and soon shut down factories in locations as far away as Tasmania. NotPetya affected Merck's production of critical vaccines, and the company had to dip into emergency stockpiles to meet demand. Doctors in Virginia and Pennsylvania were locked out of patient records and prescription systems.

Two years after the attack, railway and shipping systems in Ukraine still were not working at full capacity. Packages that had been lost due to ransomware were still not found, and senior citizens continued to miss pension payments as their records had been lost.

NotPetya was a stark example of how ransomware attacks can affect the very functioning of a society, and erode the trust that citizens hold in public institutions.

Existing Efforts to Mitigate Ransomware Attacks

Ransomware is not a new problem. As attacks have increased in prevalence and impact, significant effort has gone into understanding and addressing the array of associated issues. This includes the development of technical tools, critical research on attacker groups and trends, best practice guides for preparation, established threat intel sharing programs, and attack nullification efforts.

The security field has well-known, pre-existing resources for cyber hygiene,⁴² staff training,⁴³ and securing resources.⁴⁴ Cybersecurity firms can provide network monitoring, anomaly detection, and containment. Incident response teams have been established across government,⁴⁵ industry, and nonprofits, and at a systemic level, federal funding, information sharing, and public-private partnerships have been proposed to improve cyber response across organizations.⁴⁶

Yet adoption of preparedness best practices remains limited, and ransomware attackers continue to find sectors and elements of society that are woefully underprepared for this style of attack. The sheer volume of content published on the topic of ransomware is part of the challenge; with so much information and noise surrounding this threat, time- and resource-constrained organizations and individuals struggle to identify the most relevant and accurate sources of useful information. In addition, many guides are reportedly either too simple, too complicated and overwhelming, or not specific to ransomware. Operational security and IT staff represented in the Task Force reported that it is a struggle to find guidance that is truly actionable and feels relevant to their needs.

Significant effort remains to address the increasing risks posed by ransomware attacks. The sheer volume of attacks hitting such a broad range of sectors leaves even private sector security companies often lacking the capacity to respond to the number of requests for assistance. In response, federal governments have taken steps to coordinate information sharing and raise awareness around the risks posed by ransomware: for example, in January 2021, CISA unveiled the Reduce the Risk of Ransomware Campaign to encourage public- and private-sector organizations to implement best practices, tools, and resources that can help them mitigate ransomware risk.⁴⁷ The U.S. The Dutch National Police, Europol, McAfee, and Kaspersky Lab founded an initiative called “No More Ransom”, which provides decryption keys, information on ransomware, and preventative advice, and has done so for years.⁴⁸ The UK’s National Cyber Security Centre also provides useful information and guidelines on how to mitigate ransomware.⁴⁹ Coordinated global law enforcement actions have led to isolated successes; in January 2021, for example, a coordinated effort led to the disruption of the EMOTET botnet, a major component of ransomware criminals’ infrastructure.⁵⁰

Despite these efforts, ransomware attacks have continued to grow almost unabated, and the criminals behind them continue to operate with near impunity. What began as a relatively minor nuisance to people and business is now causing losses in the billions of dollars, and attackers have continued to target critical public facilities like schools and hospitals. Solutions have been deployed in an uncoordinated, disjointed manner, with different sectors working on siloed solutions. The ransomware threat cannot be stopped via piecemeal solutions; it needs the dedicated, coordinated attention of experts, from policymakers to security engineers to industry leaders.

A Comprehensive Framework for Action: *Key Recommendations from the Ransomware Task Force*

Ransomware has become too large of a threat for any one entity to address; the scale and magnitude of this challenge urgently demands coordinated global action. In response, in early 2021, the Institute for Security and Technology (IST) convened the Ransomware Task Force (RTF), an interdisciplinary group of leaders, for a three-month sprint with the goal of producing a comprehensive framework of actionable solutions and recommendations to help public- and private-sector leaders reduce the threats posed by ransomware in the near and long term.

This strategic framework aims to help policymakers and industry leaders take system-level action — through potential legislation, funding new programs, or launching new industry-level collaborations — that will help the international community build resistance, disrupt the ransomware business model, and develop resilience to the ransomware threat.

The framework is organized around four goals: **deter** ransomware attacks through a nationally and internationally coordinated, comprehensive strategy; **disrupt** the ransomware business model and reduce criminal profits; help organizations **prepare** for ransomware attacks; and **respond** to ransomware attacks more effectively.

These goals are interlocking and mutually reinforcing. For example, actions to disrupt the ransomware payments system will decrease the profitability of ransomware, thereby helping to deter other actors from engaging in this crime. Conversely, without taking the recommended steps to deter ransomware attackers, disruption will be harder to achieve. In a similar vein, many actions taken to better prepare organizations for ransomware attacks, such as informing them about the risks, will also improve their ability to respond, while understanding more about how organizations are responding to ransomware attacks will help improve organizations' collective preparedness. Thus, this framework should be considered as a whole, not merely a laundry list of potential disparate actions.

Recommendations at a glance:

1. **Deter Ransomware Attacks**



2. **Disrupt the ransomware business model**



3. **Help organizations prepare**



4. **Respond to ransomware attacks more effectively**





A Note on the U.S. Focus and International Application

Ransomware, like our digital world, knows no bounds. All of these recommendations seek to leverage the power of multi-stakeholder collaboration, nationally and globally, to combat a crime that transcends borders and attacks indiscriminately. Many recommendations, like enforcing compliance on cryptocurrency entities to drive ransomware actors out of business, will be unsuccessful without international collaboration. A single country's laws or capabilities will be insufficient to tackle this global threat.

While the Ransomware Task Force involved participants from around the world, the majority of members were based in the United States and were primarily familiar with the U.S. legal and policy landscape. As a result, and to help ensure our recommendations are specific and actionable, the findings and recommendations detailed in this report have a decidedly U.S.-focused lens. However, we believe many of the recommendations can and should also be translated to other jurisdictions.

The effort to combat ransomware will only be successful if carried out through a coordinated, international effort. The following recommendations carry universal themes, like improving ransomware preparedness in organizations. We encourage agencies and organizations in other nations — including cybersecurity, law enforcement, government and industry leaders — to adapt these recommendations to their own contexts, and work across borders to coordinate and tackle what is truly a global challenge.



Goal #1

Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy

The number of actors capable of conducting ransomware attacks is large and growing, and to curb the growth of this threat in the long-term, steps must be taken to systemically discourage ransomware attacks. This deterrence must be multilayered and rely on all instruments of national power. We propose a coordinated, effectively messaged, relentlessly executed deterrence campaign directed from the senior-most levels of the U.S. Government in real-time collaboration with international partners. The actions recommended here are to be directly supplemented by the disruption activities recommended in Goal #2.

Objective 1.1:

Signal that ransomware is an international diplomatic and enforcement priority

International governments must cooperate more purposefully and publicly to send an effective signal to ransomware criminals that this form of cybercrime is a diplomatic and law enforcement priority. A clear declarative policy will serve as a foundation to other international and national-level efforts.

Action 1.1.1: Issue declarative policy through coordinated international diplomatic statements that ransomware is an enforcement priority.

Using existing high-level forums (such as the G7, G7 Finance Ministers, G20, Interpol, Europol, and others⁵¹), senior-level officials and ministers from major nations should agree to one or more joint declarations condemning ransomware as a national security concern and/or a threat to critical infrastructure, and commit to pursue ransomware actors. There are several international⁵² precedents⁵³ for this declarative policy. This declaration should outline the steps signatories will mutually agree to take, and include an agreement for each nation to create a domestic action plan.

Timing: *Begin immediately to lay the groundwork; declarations would be issued when the groups meet.*

Lead: *State Department, National Security Council (NSC), Treasury, Department of Homeland Security (DHS), and Department of Justice, in coordination with international partners.*

Action 1.1.2: Establish an international coalition to combat ransomware criminals.

A standing international coalition composed of representatives from key nations is necessary as a conduit for sharing information and other resources related to the ransomware threat. Such a coalition should include representatives from law enforcement using successful models like Europol's Joint Cybercrime Action Taskforce,⁵⁴ but also including the intelligence community, and private industry. It should carry out key shared

tasks, such as building a legal case against criminal actors, pursuing targets/groups through pooling resources and tools, and amplifying takedowns when they happen. This effort would directly coincide with those detailed in 1.1.1 and 1.1.3, but also throughout the actions recommended under Goal #2.

Timing: 3-6 months. **Lead:** White House, in coordination with international partners.

Action 1.1.3: Create a global network of ransomware investigation hubs.

The U.S. Government should lead the development of a network of ransomware investigative hubs across the globe, including by leveraging cyber assistant legal attachés (ALATs) and International Computer Hacking and Intellectual Property (ICHIP) lawyers. The groups within this “team of teams” should be nimble and have access to specialists in each of the kill chain areas of the ransomware criminal organizations. The hubs should ensure their investigative priorities and resources are aligned and coordinated. They should foster a culture of information sharing, be located in diverse geopolitical regions to enable swift sharing of intelligence, and contribute directly to the coalition recommended above in Action 1.1.2, but also to the actions recommended below in Objective 1.2 and many of the actions under Goal #2.

Timing: 9-12 months. **Lead:** State Department, Department of Justice, and international equivalents.

Action 1.1.4: Convey the international priority of collective action on ransomware via sustained communications by national leaders.

Any international effort will need to include coordinated public communications by national leaders to keep the spotlight on combating ransomware as a priority and ensure the success of the broader effort. These communications can take the form of speeches, op-eds, news articles, videos, and other media that draw attention to ransomware as a problem, promote prevention, and highlight enforcement successes.

Timing: Begin immediately to lay the groundwork; declarations must be issued on an ongoing basis.
Lead: White House, in coordination with international partners.

Objective 1.2:

Advance a comprehensive, whole-of-U.S. government strategy for reducing ransomware attacks, led by the White House

Ransomware is an urgent threat that demands a “whole-of-government” strategic response. Within the U.S. Government, establishing structures for cross-agency coordination will be vital for tackling the ransomware challenge, and will reduce the lag time in government response. Leading new joint efforts with industry will also be crucial: no single actor is fully capable of disrupting this threat by themselves, so we must come together to assess the threat and coordinate activities across authorities and capabilities. Although this recommendation is U.S.-focused, a similar approach should be adopted by other national governments. Additionally, since ransomware is a cross-border issue, it will be vital for governments to reach out to, and work with, international partners both on a policy and operational level.

Action 1.2.1: Establish an Interagency Working Group for ransomware.

To ensure this challenge receives sufficient investment of time and resources from the highest levels of the U.S. federal government, the White House should establish an Interagency Working Group (IWG) dedicated to understanding and addressing the ransomware threat at a systemic level, and on an ongoing basis. Doing so will signal to ransomware actors and international partners that this issue rises above other pressing cybersecurity priorities. Ideally led through the National Security Council (NSC) in coordination with the new National Cyber Director (NCD), the Ransomware IWG will serve as a high-level strategic forum for coordinating expertise, shaping policy, sharing information, and directing action for all stakeholders.

The Ransomware IWG will also help ensure that intragovernmental conflicts can be escalated efficiently through the White House policy-coordination and national security decision-making process. The IWG should provide policy direction and leadership for all U.S. Government actions related to ransomware, which will improve accountability and help ensure that agencies work together on signaling and deterrence. In addition, the NSC/NCD, State Department, DHS, DOJ, Treasury, and other relevant members of the IWG should engage international allies and partners to build a like-minded coalition against ransomware and ensure policy coordination, as called for in Action 1.1.2.

Timing: *Immediate.* **Lead:** *White House and international equivalents.*

Action 1.2.2: Establish an operationally focused U.S. government Joint Ransomware Task Force (JRTF) to collaborate with a private-sector Ransomware Threat Focus Hub.

The Interagency Working Group (IWG) described in Action 1.2.1 should direct and oversee the creation of an internal U.S. government Joint Ransomware Task Force (JRTF), whose objective is to coordinate an ongoing, nationwide campaign against ransomware, and identify and pursue opportunities for international cooperation. The JRTF's primary function is to identify targets for disruption and takedown, and clearly designate roles and responsibilities for each. The U.S. government needs this formal interagency structure to avoid uncoordinated activity and to break down the stovepipe structure. The JRTF must be empowered to leverage all tools of national power and should prioritize ransomware threats to critical infrastructure. The JRTF should increase the pace and efficacy of intelligence-driven ransomware infrastructure takedowns, disruptions of ransomware operations, and arrest and prosecution of the people that enable them. A detailed breakdown of a potential structure, roles, and responsibilities for the JRTF are provided in **Appendix C**.

The JRTF should collaborate closely with relevant private-sector organizations that can help defend against and disrupt ransomware operations, such as security vendors, platform providers, telecommunications providers, information sharing organizations, cybersecurity non-profits, and other capable entities. These private-sector activities and groupings can continue to operate on an informal and *ad hoc* basis through the establishment of a Ransomware Threat Focus Hub (RTFH), which can serve as a central, organizing node for informal networks and collaboration as part of a collaborative, sustained public-private anti-ransomware campaign. The structure, roles, and responsibilities of the RTFH are also provided in **Appendix C**.

Timing: *Immediate.* **Lead:** *White House, via the direction of the IWG, in coordination with private industry, and international equivalents.*

Action 1.2.3: Conduct a sustained, aggressive, public-private collaborative anti-ransomware campaign.

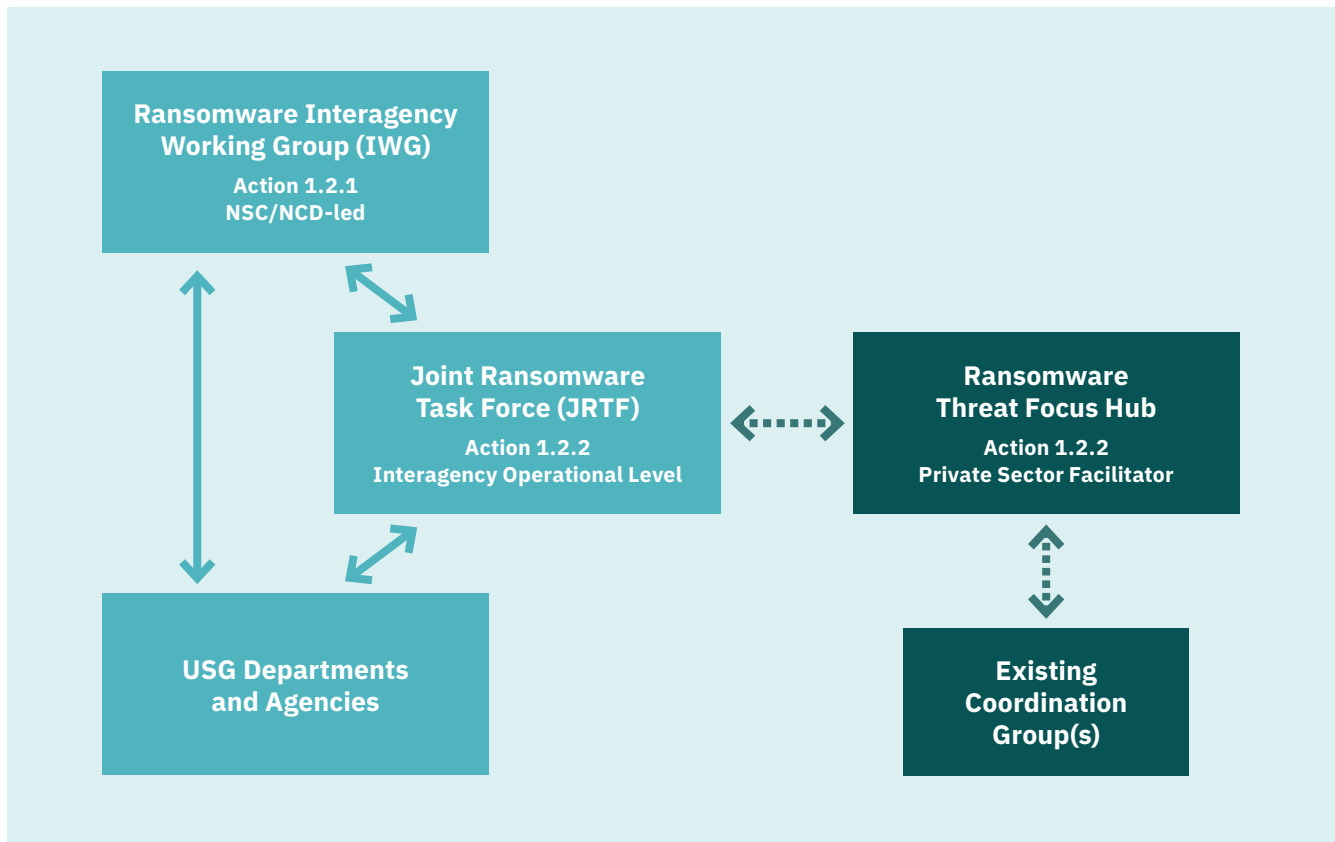
The JRTF should use all tools of national power to sustain an intelligence-driven anti-ransomware campaign that includes target identification, threat hunting, action planning, execution, and communications. The roles and responsibilities covered within the JRTF should include, but not be limited to: law enforcement action, diplomatic efforts, economic tools, technical cyber operations, and intelligence operations as appropriate. The campaign and capabilities utilized should be tailored to target specific vulnerabilities in ransomware groups and their operations as identified in the intelligence assessments recommended in Actions 1.2.5 and 1.2.6. Coordination of operations, and intelligence sharing that supports those operations, should be streamlined with exceptions to policy as needed to be most effective in targeting groups on the designated list. This should include sharing and operational coordination with U.S. government entities, private industry (e.g. cybersecurity companies, service providers, and trust groups), and a coalition of international partners.

The JRTF should enhance operational coordination with their international counterparts to conduct more, and more effective, international investigations and take-downs. This would be directly facilitated through the investigative hubs recommended in Action 1.1.3. The JRTF should, to the greatest extent possible, operate at the unclassified level, which is essential to enable flexibility, quick reaction times, and the incorporation of essential partners who are not JRTF members. To make this possible, the U.S. government should follow the lead of its counterparts in the United Kingdom's National Cyber Security Center and dramatically increase the volume of TS/SCI information made available at the unclassified level, with a singular focus on the ransomware threat.

The JRTF can ensure agreements are in place with designated private-sector partners to allow for field level coordination, and must coordinate early and frequently with all relevant elements of U.S. departments and agencies, for instance, the NCIJTF and select U.S. Attorney Offices.

Via the private-industry Ransomware Threat Focus Hub (RTFH), as detailed in **Appendix C**, non-government participants in these campaigns could include infrastructure providers, platform/OS providers, registrars, endpoint security companies, threat intelligence firms, content delivery networks (CDNs), network operators, non-profits, and industry nodes. Engagement, planning, and execution should not be limited to regularly scheduled meetings; rather, the structure should allow for continuous, responsive, and ad hoc coordination and execution based on constantly changing events.

Timing: 3-6 months. **Lead:** White House, via the direction of the IWG in Action 1.2.1, in coordination with private industry, and international equivalents.

FIGURE 5 Proposed Framework for a Public-Private Operational Ransomware Campaign

Action 1.2.4: Make ransomware attacks an investigation and prosecution priority, and communicate this directive internally and to the public.

The Department of Justice (DOJ) recently formed an internal task force to tackle ransomware and the Acting Deputy Attorney General issued guidance making ransomware an investigatory priority. The Task Force supports this focus on ransomware and recommends that senior officials, such as the Attorney General, the Director of the FBI, and/or the Director of the United States Secret Service, sustain this focus at United States Attorney's Offices (USAOs), FBI field offices, and Secret Service Task Forces to more aggressively pursue cases against ransomware actors. Consistent with this guidance, USAOs should prioritize ransomware prosecutions and seek harsher penalties for attacks on critical infrastructure or for attacks that endanger public health and safety.

Legislation should also be considered to make ransomware and other Computer Fraud and Abuse Act offenses subject to RICO, given the organized crime aspects of these offenses. Additionally, to raise the level of priority and clearly communicate that new status, officials should also pursue asset forfeiture against ransomware actors to the maximum extent allowed by law and signal their intention to use this tool. This recommendation is expanded upon further in Actions 2.1.5 and 2.3.3.

Timing: 9-12 months. **Lead:** U.S. Department of Justice and Congress, and international equivalents.

Action 1.2.5: Raise the priority of ransomware within the U.S. Intelligence Community, and designate it as a national security threat.

The United States must raise the Intelligence Community (IC) collection priority against ransomware actors so that all necessary resources, capabilities, and authorities can be brought to bear to answer the intelligence needs to fulfill the tasks of the IWG and the JRTF. These must include (but are not limited to): signals intelligence (SIGINT) (including computer network operations, or CNO), human intelligence (HUMINT), and imagery intelligence (IMINT). This elevated prioritization must be accompanied by a reduction in the roadblocks that impede greater bidirectional sharing of information between the IC, international IC partners, and private industry, in order to fulfill the intelligence needs of the IWG and the JRTF's campaigns.

To establish the baseline for target development, the NSC should task an Intelligence Community Assessment (ICA) focused solely on ransomware actors and the criminal-state nexus. The goal of this ICA should be to accurately capture: the nature of the ransomware threat to national security; identification of actors and groups who pose the most significant threat (including attribution to individuals involved whenever possible); locations from where they operate; and the infrastructure, tactics, and techniques they commonly use. The ICA should also detail vulnerabilities that may exist within each actor group; any relationships between the actors and their governments that could negatively impact law enforcement's ability to counter the threat; and any intelligence gaps that would need to be filled to more completely understand this threat.

Based on the findings in the ICA and any other relevant intelligence, the IC should clearly designate ransomware actors as a national security threat at the level appropriate to the findings, and raise the priority of actively countering the threat. The designation and priority level should ensure that all tools of national and international power are brought to bear to counter this threat in an aggressive, effective, but proportional, coordinated campaign, as is detailed in 1.2.3.

Timing: 3 months. **Lead:** White House to task DNI, coordinate with Five Eyes Partners and international equivalents.

Action 1.2.6: Develop an international-version of an Intelligence Community Assessment (ICA) on ransomware actors to support international collaborative anti-ransomware campaigns.

International partners should work together to develop an international Intelligence Community Assessment (ICA) on ransomware actors with the same goals described in Action 1.2.5 in order to create a more complete picture of the global security threat posed by ransomware actors, and to serve as the baseline for coordinated international efforts. An international ICA will help raise the global intelligence collection priority against ransomware actors so that all necessary resources can be brought to bear to answer the intelligence needs required to fulfill national and international collaborative efforts.

Timing: 3 months. **Lead:** White House to task DNI, coordinate with Five Eyes Partners and international equivalents.

Objective 1.3:*Substantially reduce safe havens where ransomware actors currently operate with impunity*

Many pernicious ransomware actors are given free reign by the nations where they reside and cannot be easily reached by international law enforcement agencies, either because a host country is actively protecting them, lacks the resources and capabilities to stop them, or does not prioritize the issue. Together with international partners, the U.S. should use a “carrot and stick” approach to motivate these nations to use all tools of national power – including critical law enforcement action – against the criminals operating within their borders or within friendly or neighboring countries.

Action 1.3.1: Exert pressure on nations that are complicit or refuse to take action.

Nations should exert pressure on other nations that refuse to take action against ransomware criminals. These strategies could include economic and trade sanctions; constrain “safe haven” country activity in international financial markets; using evidence of complicity to “name and shame” them in public forums to disrupt their freedom of activity; withholding military or foreign assistance aid; or denying visas to citizens who seek to travel to the United States or other nations. Actions undertaken by the JRTF and the RTFH to disrupt the ransomware business model should proactively be utilized to contribute to the intended deterrent effect of this sustained pressure campaign.

Timing: 3 months, ongoing. **Lead:** U.S. Department of Justice and U.S. Department of State.

Action 1.3.2: Incentivize cooperation and proactive action in resource-constrained countries.

Some nations that serve as home bases for ransomware actors may not understand the gravity of this crime, or they may lack sufficient resources to prosecute ransomware criminals. The United States and other nations should provide training and capacity-building to support these nations’ efforts, and provide direct law enforcement support, for example through joint law enforcement operations. Providing incentives to private-sector partners in those nations may also increase these nations’ willingness to cooperate. Establishing ransomware as a priority in bilateral agreements could further bring these nations to the table.

Timing: 30 days and ongoing. **Lead:** U.S. Department of Justice and Department of State, and international equivalents.



Goal #2

Disrupt the ransomware business model and decrease criminal profits

Ransomware is overwhelmingly a financially motivated crime, and as long as the profits outweigh the risks, attacks will continue. To effectively disrupt this threat, government and industry stakeholders must work collaboratively across borders to reduce the profitability of this criminal enterprise and increase the risk of ransomware execution. Governments can take diverse actions to:

- 1. Disrupt payment systems to make ransomware attacks less profitable;*
- 2. Disrupt the infrastructure used to facilitate attacks; and*
- 3. Disrupt ransomware actors themselves, through criminal prosecution and other tactics.*

This must all be done while minimizing harm to the victims of ransomware and not interfering with their ability to recover their systems.

The flow of money from a victim to a ransomware actor using cryptocurrency is complex. See Appendix B for a detailed guide on this process, and how entities like cryptocurrency exchanges fit within this ecosystem.

Objective 2.1:

Disrupt the system that facilitates the payment of ransoms.

Ransomware attacks are profitable because ransom payments are made through the use of diverse cryptocurrencies, where payments are difficult to trace and can easily be laundered. The challenge for governments is to find new ways to get inside the ransomware payments process. It will be important to set measurable goals to assess progress toward this objective.

Action 2.1.1: Develop new levers for voluntary sharing of cryptocurrency payment indicators.

In addition to the mandatory disclosure of a ransomware payment recommendation in Action 4.2.4, lawmakers should create incentives to share timely and actionable cryptocurrency payment indicators to enable law enforcement to prioritize leads and seize ransom payments when possible. This information may include wallet addresses, transaction hashes, and ransom notes. In exchange for this information, victims should be able to report anonymously, unless a victim is otherwise required to disclose the attack under privacy laws. Congress should broaden the Cybersecurity Information Sharing Act of 2015 to cover this type of information sharing, explicitly preserving attorney-client privilege and implementing parameters that limit how this information could later be used by regulators or as part of civil litigation, to encourage participation.

Timing: 6 to 12 months. **Lead:** Congress, CISA, and other international equivalents.

Recent publicly available analytical reporting estimates that

Just **199** deposit addresses received



of all funds sent by ransomware addresses in 2020

An even smaller group of **25** addresses accounted for



With a broader and deeper understanding of the ransomware landscape, law enforcement would be better equipped to target the most prolific actors.

Cryptocurrency Exchanges

Cryptocurrency exchanges allow users to buy and sell cryptocurrencies in exchange for traditional currencies, as well as convert to other virtual currencies. Exchanges act as middlemen between buyers and sellers.



Cryptocurrency Kiosks

Kiosks that sell, buy, and exchange cryptocurrency. They can be located anywhere and look like ATMs. They tend to charge more than cryptocurrency exchanges. Kiosks act as middlemen between buyers and sellers.



Over-the-Counter (OTC) Trading Desks

Over-the-counter (OTC) cryptocurrency trading allows people to buy from or sell to a “desk,” a business focused on buying and selling cryptocurrency. There is thus no middleman between the seller and buyer, and OTC tends to see larger crypto purchases and sales.



Action 2.1.2: Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading “desks” to comply with existing laws.

Lawmakers need to pursue and enforce consistent licensing and registration requirements for cryptocurrency exchanges, crypto kiosks, and OTC trading desks where criminals “cash out” their cryptocurrency from ransomware payments. These entities are not consistently compliant with or subject to Know Your Customer (KYC), Anti-Money Laundering (AML), and Combatting Financing of Terrorism (CFT) laws, and those that are subject to those laws do not consistently report suspicious transactions to law enforcement or other institutions.⁵⁶ These laws must designate clear enforcement bodies to penalize non-compliant exchanges, kiosks, and OTC desks.

Traditional financial institutions that fund these entities should also impose stricter rules. They should pursue SEC enforcement of cryptocurrency businesses that fail to register as broker-dealers, transfer agents, clearing agencies, and money service businesses (MSBs), with particular focus on mixing services that obfuscate criminal transactions with legal traffic.

Timing: 12 months. **Lead:** *Treasury Department, Securities and Exchange Commission, and other international equivalents.*

Action 2.1.3: Incentivize voluntary information sharing between cryptocurrency entities and law enforcement.

Regulators should incentivize cryptocurrency exchanges, crypto kiosks, over-the-counter trading desks, and financial institutions to increase their reporting of suspicious transactions to federal law enforcement, to facilitate joint disruptive actions. In the U.S., these entities would use Section 314(b)⁵⁷ reports and suspicious activity reports (SARs) to report suspicious transactions to the Financial Crimes Enforcement Network (FinCEN) of the U.S. Treasury Department. In addition, the Department of Treasury should streamline its processes for sharing SARs with exchanges, blacklisting wallets, and sharing with relevant federal and non-federal entities that may take other timely disruptive action.

Timing: 12 months. **Lead:** *U.S. Treasury Department (FinCEN) and international equivalents.*

Action 2.1.4: Centralize expertise in cryptocurrency seizure, and scale criminal seizure processes.

Law enforcement action on the basis of ransomware reporting must be swift as criminals strive to quickly move funds beyond their reach. In the U.S., law enforcement can provide a cryptocurrency exchange with a letter requesting that ransomware funds be frozen at the exchange as proceeds of crime to be seized by the government. If done in time and with cooperation from the exchange, this can make the identified funds unavailable to the ransomware actors. This letter must be followed up with a seizure order from an attorney within the Department of Justice, a process that, at the moment, is scattered across the United States, assigned to different investigations, and assigned to attorneys with varying experience drafting these orders.

Key units within the Department of Justice — including the Computer Crime and Intellectual Property Section (CCIPS), Computer Hacking and Intellectual Property Network (CHIPS), National Security Cyber Specialists (NCSC), the National Security Division (NSD), and the Money Laundering and Asset Recovery Section (MLARS) — should identify attorneys who are knowledgeable in civil and criminal seizures related to cryptocurrency, and engage them to serve as a focal point for seizure orders across ransomware investigations. This should be part of the campaign tasked to the JRTF described in Action 1.2.2 or to the recently formed DOJ ransomware-focused task force. This would dramatically streamline the current process, ensure seizure orders are pursued expeditiously, and increase the number of seizure orders served, thereby making it more difficult for ransomware adversaries to convert virtual currency to fiat.

Timing: 6 to 12 months. **Lead:** *U.S. Department of Justice and international equivalents.*

Action 2.1.5: Improve civil recovery and asset forfeiture processes by kickstarting insurer subrogation.

For individual ransomware victims, the economics of pursuing civil remedies against liable actors may not make sense, given the case may require extensive factual investigation and innovative legal efforts. To solve this problem, insurers and reinsurers should measure and assert their aggregated ransomware losses and establish a common “war chest” subrogation fund to evaluate and pursue strategies aimed at subrogation recoveries, including restitution, recovery, or civil asset seizures, on behalf of victims and in conjunction with law enforcement efforts.

Many insurers currently maintain individual subrogation units, but these do not typically act within the context of ransomware. This is because insurers may not be familiar with the novel legal and investigative expertise needed to pursue ransomware actors; they may believe the chances of recovery are unclear, and the cases may span multiple international jurisdictions where insurers may not typically pursue subrogation. This common “war chest” subrogation fund may sit within a consortium (as described in Action 2.1.7) established by insurers and reinsurers to properly resource and scale novel efforts to pursue civil recoveries against liable actors, kickstarting efforts in civil courts to obtain justice, while pooling the costs associated with any one case, alleviating concerns about uncertain results.

Timing: 6 to 12 months.

Lead: Domestic and international insurance and reinsurance firms.

What is subrogation?



Subrogation refers to an insurer’s assumption of an insured victim’s rights of recovery after a loss is covered and paid by the insurer. Subrogation empowers an insurer to pursue the rights of the insured to recover the amount of a loss from the parties who are legally liable for it. Subrogation thus serves to make both victim and insurer “whole” in the event of a civil recovery. For more information, **see Appendix A: Cyber Insurance.**

For Further Investigation: The Tax Enforcement Opportunity



The IRS and Europol have engaged in efforts to identify taxpayers who have failed to disclose income from cryptocurrency, including developing “tax evasion signatures” within cryptocurrency transactions. In 2021, the IRS’s Office of Fraud Enforcement announced “Operation Hidden Treasure,” convening trained IRS criminal agents and blockchain analysis firms to identify cryptocurrency-related tax fraud.⁵⁸ National and international tax authorities and interested policymakers should further investigate opportunities to leverage tax enforcement efforts like these in the fight against ransomware.

Action 2.1.6: Launch a public campaign tying ransomware tips to existing anti-money laundering whistleblower award programs.

In 2012, the U.S. Securities and Exchange Commission (SEC) launched a whistleblower reward program that has already yielded several billion dollars in penalties that the U.S. would not have otherwise obtained. A public whistleblower campaign in this vein should be targeted toward geographic regions around the world, and provide awards for information leading to the identification of individuals involved with developing ransomware, money laundering of fiat, coding, ransom negotiations, and other roles. In addition to financial awards, such a program could include non-monetary rewards, such as a path to citizenship. Any reward program should be designed in a way to protect the anonymity of the reporter of the criminal activity.

Timing: 6 to 12 months. **Lead:** The Securities and Exchange Commission and international equivalents.

Action 2.1.7: Establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management.

Insurers and reinsurers should voluntarily establish an industry consortium to aggregate and share anonymized, pertinent data to support threat-actor disruption, including both payment information (such as wallet addresses, ransom demands, negotiation outcomes, and transaction hashes) and attack information.

Data sharing at the consortium should also accelerate the maturation of best practices and sustainability of the cyber insurance market, as this data enables further risk modeling and underwriting analysis. This consortium should improve risk management and resolution strategies so that ransomware is less frequent, less destructive, and less profitable for the threat actors. It should also enable insurers and reinsurers to establish certainty with law enforcement and regulators such as OFAC as to the legality of any payment and as with respect to sanctions. Finally, the consortium may serve as the home of any common subrogation “war chest” fund for collaboration, as described in Action 2.1.5. This consortium should also work directly with the JRTF and RTFH as described in actions 1.2.2 and 1.2.3.

Timing: 6-12 months (to establish consortium and initial subrogation effort).

Lead: Domestic and international insurance and reinsurance firms.

Objective 2.2:

Target the infrastructure used by ransomware criminals

Ransomware actors rely on infrastructure to carry out their attacks, including servers and networks that serve as “command and control” for their attacks. Law enforcement agencies have opportunities to disrupt ransomware criminals by targeting this infrastructure.

Action 2.2.1: Leverage the global network of ransomware investigation hubs.

The global network of ransomware investigative hubs recommended in Action 1.1.3 (and utilized by the coalition recommended in 1.1.2 and the JRTF recommended in Action 1.2.2), including leveraging cyber assistant legal attachés (ALATs) and ICHIP prosecutors, should have access to specialists that are empowered to focus efforts

on infrastructure aimed at the “left of boom” elements of the criminal business model. This includes, among other areas, credential theft or other unauthorized access; malware distribution, including the use of malicious domains and criminal and abusive command and controls; criminal surveillance; and theft of intellectual property.

Timing: 6-12 months. **Lead:** U.S. Federal Government and international equivalents.

Action 2.2.2: Clarify lawful defensive measures that private-sector actors can take when countering ransomware.

Currently, private-industry companies — including but not limited to hosting companies, internet service providers, and telecommunications companies — are actively working with law enforcement and other industry partners to disrupt infrastructure associated with ransomware actors. This infrastructure may include malicious servers used to facilitate or conduct attacks against victims. If a service provider is tipped to malicious infrastructure, it should be able to take action against the infrastructure without fear of legal liability. For example, if a hosting company is made aware that a customer is conducting attacks from one of the hosting company’s servers, they can typically shut down the customer’s service due to a violation of the company’s terms of service. In a less clear scenario, if a telecommunications company is provided a signature that identifies malicious network traffic and they block the traffic from transiting their network, thereby disrupting the malicious activity, the company may have some legal liability.

Congress should ensure private industry can actively block or limit traffic when acting in good faith without fear of legal liability. Specifically, Congress should modernize the Computer Fraud and Abuse Act (CFAA) and other cybersecurity laws to take into account activities that cybersecurity companies, security researchers, service providers, and other responsible parties are currently doing “at risk” in gray areas in order to protect their customers.

To be clear, this is not advocating for “hacking back,” rather it is focused on decriminalizing practical security activities necessary to counter modern cybersecurity threats, including against criminal infrastructure like botnets used in ransomware.

Timing: 12 to 24 months. **Lead:** U.S. Congress and international equivalents.

Objective 2.3:

Disrupt the threat actors, including ransomware developers, criminal affiliates, and ransomware variants

Action 2.3.1: Increase government sharing of ransomware intelligence.

The government should increase the sharing of intelligence about ransomware actors with the private and nonprofit sectors, including key data points that specifically lead back to the threat actors. Such information could include threat actor personas, tradecraft, and attribution (including roles and responsibilities); behavioral tactics and techniques; and related technical information (i.e., indicators of compromise). Making such intelligence more broadly available would enable the private sector to protect itself more effectively; better

coordinate with government entities, such as the JRTF and RTFH in Action 1.2.2; and support governments in disrupting ransomware activity.

Timing: 6 months and ongoing. **Lead:** Department of Homeland Security and international equivalents.

Action 2.3.2: Create target decks of ransomware developers, criminal affiliates, and ransomware variants.

To better operationalize and focus resources, the U.S. Government and the security community should work together to create prioritized target decks for ransomware developers, criminal affiliates, and ransomware variants based on how much harm they are doing and the breadth of their operations. The core of this effort must focus on unveiling the threat actors themselves and understanding their organization(s), with the goal of identifying vulnerabilities that can be exploited to disrupt the threat, using all capabilities available to the private industry and governments. This effort should include working more closely with the security community on a routine basis to share information and coordinate operations, to be facilitated by the JRTF and RTFH described in Action 1.2.2.

Timing: 6 to 12 months. **Lead:** U.S. Federal Government and international equivalents.

Action 2.3.3: Apply strategies for combating organized crime syndicates to counter ransomware developers, criminal affiliates, and supporting payment distribution infrastructure.

Ransomware events are not singular, but part of an ongoing campaign of extortion against government and private-sector entities. Kill-chain analyses of ransomware organizations reveal a complex network of associates and entities. These organizations have been established to function as an extortion operation with repeatable outcomes. The various components of the organization include creators of malware, establishment of ransomware affiliates, franchise fees or percentage of ransomware payouts to the operation leaders, digital wallet creation, money laundering, using money mules, and more.

Law enforcement should disrupt the ransomware criminal enterprise by using established frameworks that have been applied successfully to disrupt the activities of the mafia and other criminal organizations. The U.S. government should leverage the power of the RICO statute, as called for above in Action 1.2.4, to prosecute ransomware criminals. The RICO statute (Title 18 USCS § 1962) serves as a “mafia business tax”, and prohibits racketeering. RICO investigations provide influential tools to inspire cooperation of members and supporters of a criminal enterprise, such as enhanced prison terms for any conspirators, and forfeiture and exposure to civil RICO investigations. If deemed necessary, the federal government should undertake immediate action to ensure ransomware crimes are predicates for use of the RICO statutes.

Timing: 12 to 24 months. **Lead:** U.S. Law Enforcement and international equivalents.



Goal #3

Help organizations prepare for ransomware attacks

Any organization can fall victim to ransomware, creating catastrophic disruption for the organization and those it serves. Yet despite extensive press coverage and content on this topic, the threat is poorly understood by many public- and private-sector leaders, and the majority of organizations lack an appropriate level of preparedness to defend against these attacks. Even firms that have invested in cybersecurity broadly may be unaware of how to prepare for, and defend specifically against, ransomware attacks, and information available is in many cases oversimplified or excessively complicated.

The challenge is to increase awareness and build defenses that will be effective both at scale and over time as the threat evolves. To do this, governments and industry leaders need to better connect with key audiences, including both the organizational leaders who need to understand that ransomware is a real and relevant threat to their organization, and also the individuals in operational roles (such as IT and security professionals) who need guidance on how to prioritize mitigation efforts given limited resources. Support should be customized based on each organization's current situation, including to what extent it is already appropriately informed and whether it has appropriately invested in time and resources.

Objective 3.1:

Support organizations with developing practical operational capabilities

Guides and technological tools to mitigate ransomware are currently available; however, many are insufficient, overly simplified, or too complicated, and the general level of noise surrounding this problem is confusing and problematic.

Action 3.1.1: Develop a clear, actionable framework for ransomware mitigation, response, and recovery.

Although multiple organizations have published ransomware guides, no single, authoritative source of best practices exists. The current state of awareness around ransomware is similar to the general environment prior to 2014, when no compilation of best practices existed for cybersecurity. At that time, the U.S. National Institute of Standards and Technology (NIST) led a multi-stakeholder process to develop the *Framework for Improving Critical Infrastructure Cybersecurity*. This framework has been widely adopted by organizations around the world and serves as a foundational cybersecurity risk management resource.

We have reached a similar point with the ransomware threat. The single most impactful measure that could be taken to help organizations prepare for and respond to ransomware attacks would be to create one internationally accepted framework that lays out clear, actionable steps to defend against, and recover from, ransomware.

Ransomware is a global problem, so governments and private-sector organizations around the world should collaborate on this effort to ensure the framework will work internationally. Efforts taken only in one jurisdiction may be regionally effective, but will likely push attackers to focus on different regions; a coordinated international effort will create greater long-term impact and more effectively disrupt the economics of the cybercrime market. It will also drive greater adoption in organizations that operate in more than one country.

As far as is practical, the framework should be consistent with existing cybersecurity frameworks, such as International Standards Organization publications⁵⁹ and the NIST Cybersecurity Framework,⁶⁰ but it should be specific to ransomware. It should build on the work that NIST's National Cybersecurity Center of Excellence has already done as part of the data integrity project and related papers. The framework should clearly identify each recommended action's impact, as well as the required investment of time and other resources. It should include multiple layers for different audiences; similar to the NIST Cybersecurity Framework, the top layer would be intended for executive decision makers, the second and third layers for operational managers, and the fourth layer for front-line implementers.

The ransomware-specific framework should also identify what approaches are most successful in dealing with ransomware and why. The framework should identify what constitutes a reasonable due diligence review prior to payment, consistent with actions 4.1.1 and 4.1.2, which address the creation of ransomware emergency response authorities and a ransomware response fund.

In addition, industry-specific profiles should be developed to tailor the Ransomware Framework to different industries or sectors. Creating different profiles for local governments, small- and medium-sized businesses, and large enterprises, for example, would enable different types of organizations to adapt the framework to their particular situations.

Timing: 12-24 months, and updated yearly thereafter.

Lead: NIST for the US, and international equivalents, with private-sector participation.

Action 3.1.2:

Develop complementary materials to support widespread adoption of the Ransomware Framework.

Additional materials should be developed to accompany the ransomware prevention framework, drawing from existing resources, to further articulate how organizations can leverage specific security capabilities, technologies, and policies to meet the frameworks' identified best practices. Such materials could include:

- Detailed deployment toolkits and guides to assist specific sectors or market segments with applying the framework;
- Mappings to existing popular cybersecurity frameworks, e.g. NIST, ISOs, CIS controls
- A ransomware-specific risk assessment tool;
- Ransomware reference architectures (such as those developed by NIST's National Cybersecurity Center of Excellence);
- A ransomware killchain;
- A checklist to help organizations to hold managed service providers (MSPs) and IT vendors accountable.

Timing: 12-24 months, and updated regularly thereafter.

Lead: NIST for the US, and other international equivalents.

Action 3.1.3: Highlight available internet resources to decrease confusion and complexity.

Many decision aids exist to aid organizations preparing for, and responding to, ransomware attacks. While this volume of content is designed to help, it can in fact hinder preparedness or response as organizations struggle to identify the most relevant and actionable guidance for their situation. It is challenging for organizations to determine which guides can be trusted to provide high-quality, accurate advice. To address these shortcomings, the Task Force recommends a two-pronged approach.

First, internet search companies could take steps to make sorting through online materials easier. For example, during the COVID-19 pandemic, internet search companies took steps to highlight credible content related to the pandemic to make it easier to find the most up-to-date and relevant information, and also to minimize the negative impact of mis- or disinformation. A similar effort focused on ransomware would help IT and security professionals navigate this highly complex and evolving threat landscape, and quickly identify the most important information and guidance. Once the Ransomware Framework and complementary materials are published, these would be prioritized on these search pages.

Second, a nonprofit entity, such as the Cybercrime Support Network, should collect and maintain a reference library of decision aids and best practice guides for responding to a ransomware attack. This step would provide a vetted library of material for organizations to draw on to prepare for and/or respond to a ransomware attack.

Timing: 6-12 months for first iteration, and ongoing thereafter.

Lead: For curation, internet search companies. For aggregation, a nonprofit like the Cybercrime Support Network (CSN) could lead this process in the U.S., together with international partners.

Objective 3.2:

Increase knowledge and prioritization among organizational leaders

There is a stark difference between being aware of ransomware as a threat and having a real understanding of the dynamics, mitigations, and potential impacts of an attack. Organizational leaders need greater understanding about the significance and relevance of the ransomware threat in order to allocate resources and prioritize focus.

Action 3.2.1: Develop business-level materials oriented toward organizational leaders.

Organizational leaders traditionally see security as niche and highly technical. They need to understand ransomware as a whole-organization event, in non-technical, business risk-relevant terms. While the Ransomware Framework described in Action 3.1.1 has a top layer aimed at executives, additional materials should highlight business needs and risks, and aim toward educating organizational leaders about the threat.

These materials should include a simplified and translated overview of the framework; a ransomware primer for business leaders; or a checklist for organizational leaders to address with operational staff. They could also include detailed case studies of real, anonymized attacks related to critical sectors, highlighting how ransomware attacks occurred and the resulting business impact. Any materials should also consider the regulatory landscape,

emphasizing how adhering to preparatory frameworks can reduce the likelihood of fines or other penalties.

Timing: 6-12 months, with updates yearly as needed.

Lead: CISA or equivalent international government agency tasked with capacity-building around cybersecurity.

Action 3.2.2: Run nationwide, government-backed awareness campaigns and tabletop exercises.

A government-backed awareness campaign will not only help raise the profile of ransomware as a serious business issue, but it will also increase the credibility and need for focus among busy organizational leaders. This should be coordinated with efforts addressing operational technical roles. Such a campaign should leverage appropriate international organizations, state and local governmental entities, non-profits, and industry organizations and influencers. It should also be accompanied by tabletop exercises that provide opportunities for learning and collaboration.

Additionally, as many organizational leaders rely on trade or local business networks to learn about challenges facing organizations in their sector or region, we recommend engaging these organizations in awareness campaigns. In the United States, organizations that could be considered include Chambers of Commerce, the National Association of Corporate Directors, the Young Presidents' Organization, and various trade associations. These organizations may need funding in order to be able to take on a campaign of this significance.

Timing: 12-24 months years, and ongoing for as long as relevant.

Lead: U.S. Federal government and international equivalents, appropriate agency leads (e.g., Education or Homeland Security or equivalents), and key nonprofit partners.

A Little Goes a Long Way



Increasing security in a few key areas could make a significant difference for organizations in their effort to prepare for ransomware attacks. Complex security software or complete network rebuilds may not be necessary. For example, as SecurityScorecard notes in a recent report, implementing multi-factor authentication or adopting password managers can dramatically improve an organization's security posture.⁶¹ Although any organization, regardless of its security, can be a target for a ransomware attack, improving baseline security and raising awareness among employees can go far in protecting organizations from attack.

Tabletop Exercises



As part of an awareness-building campaign, national governments could lead multi-stakeholder "tabletop exercises" for states, cities, businesses, and international partners. Tabletop exercises bring together key stakeholders to use scenarios or simulations of ransomware events, and could help organizations hone internal and external organizational collaboration and response processes. Such exercises are valuable in helping organizations understand the importance of prioritizing ransomware preparedness, as well as their personal risks and responsibilities as part of a globally interconnected system. Regular exercises can also help build strong relationships and facilitate more robust ransomware threat information-sharing and incident response collaboration. As an example, the U.S. Department of Homeland Security conducts a bi-annual national cyber exercise called Cyber Storm.

Objective 3.3:

Update existing, or introduce new, cybersecurity regulations to address ransomware

Regulations and standards related to cybersecurity vary widely, and in most cases do not specifically address ransomware. Updating regulations and filling gaps with new regulations will help drive better adoption of ransomware mitigations in core regulated sectors.

For the new regulations proposed below, the government may want to consider a mechanism to address how quickly the technology and threat landscapes evolve, compared to the process for updating laws and regulations. For example, a private- or public-sector standards body (e.g. NIST, the Center for Internet Security, or a group similar to the Payment Card Industry Security Council) could set and annually update minimum required standards, and the law would incorporate this group's standards.

Action 3.3.1: Update cyber-hygiene regulations and standards.

Existing cybersecurity regulations — such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, and the Directive on Security of Network and Information Systems (NIS) in the European Union, as well as non-regulatory standards such as the Payment Card Industry Data Security Standard (PCI DSS) — all set a baseline for cybersecurity in specific regulated sectors where protection of data and essential services is considered critical. Though some targeted guidance exists,⁶² many standards do not specifically address ransomware, despite the significance of this threat. These and other existing cybersecurity regulations and standards should thus be reviewed and, where necessary, updated to incorporate measures that align with the recommended Ransomware Framework (see Action 3.1.1) to more directly mitigate ransomware attacks

Timing: *Dependent on the creation of the Ransomware Framework (Action 3.1.1); likely 12-24 months, with subsequent iterations in the long term (24+ months).*

Lead: *State and federal government(s) or equivalent law-making bodies, with support from state/local entities, think tanks, and nonprofits.*

Action 3.3.2: Require local governments to adopt limited baseline security measures.

Ransomware attacks impacting local governments are catastrophic not only for the organizations themselves, but also for the constituents they serve. Mandating certain behaviors and practices will help local governments better defend against attacks, and may help them provide enhanced support for small-to-medium-sized businesses operating in their jurisdiction. In the United States, required measures could include:

- Joining the Multi-State Information Sharing and Analysis Center (MS-ISAC);
- Signing up for the MS-ISAC's Malicious Domain Blocking and Reporting (MDBR),⁶³ unless already running a comparable DNS filtering service; and
- Signing up for CISA's infrastructure and web application scanning services.⁶⁴

Other measures could include the MS-ISAC offering ransomware-specific training and support to cities, though any additional requirements would likely require funding or financial incentives.

Timing: 6-12 months, and updated yearly thereafter.

Lead: U.S. Federal Government and international equivalents.

Action 3.3.3:

Require managed service providers to adopt and provide baseline security measures.

Managed service providers (MSPs) often cover the IT and security functions for organizations that cannot invest in in-house expertise and technologies. MSPs do not commonly provide extensive security coverage or ransomware mitigations, but doing so would likely create widespread positive impact for small-to-medium-sized organizations. Baseline security measures for MSPs could include:

- Adherence with a cyber-hygiene program (for example, CIS Controls Implementation Group ¹⁶⁵ and the NIST Cybersecurity Framework,⁶⁶
- Mandatory disclosure across the MSP's customer base if there is a ransomware incident involving the MSP's service offering; and
- Forming an MSP-ISAC, an information sharing and analysis center specific to this industry.

Note that some funding or financial incentivization may initially be needed to help MSPs develop cybersecurity capabilities.

Timing: 6-12 months. **Lead:** U.S. Congress and international equivalent lawmakers.

Objective 3.4:

Financially incentivize adoption of ransomware mitigations

Many organizations are under-invested in cybersecurity and resilience, and may lack the resources to manage the ransomware threat. By providing financial incentives, governments can help the most vulnerable and resource-constrained organizations tackle this issue. For some organizations, incentives may be the only means available to prepare for, and defend against, a ransomware attack.

Action 3.4.1: Highlight ransomware as a priority in existing funding provisions.

Where grants or funding are already offered and may be used for cybersecurity activity, we recommend that the accompanying language should be updated to highlight ransomware preparedness as a priority for spending and focus.

According to a Third Way paper on U.S. federal grants for cybersecurity,⁶⁷ eight existing preparedness grants are available to state, local, tribal, and territorial (SLTT) governments, transportation authorities, nonprofits, and private entities through the Federal Emergency Management Agency (FEMA). These have recently been changed to allow recipients to spend funds on cybersecurity, as when FEMA identified cybersecurity as a "priority area" in 2018 for the largest DHS preparedness grant, and required fund recipients to spend at least 5% of their funds on cybersecurity for critical infrastructure. This prioritization and funding expansion should continue across additional grants and should specifically highlight ransomware preparedness as an urgent priority.

Timing: 3-6 months. **Lead:** Relevant fund designation agencies.

Action 3.4.2: Expand Homeland Security Preparedness Grants to encompass cybersecurity threats.

Under current law, Homeland Security Preparedness Grants focus on terrorism. Given the threat that ransomware poses to U.S. state, local, tribal, and territorial government entities, expanding this grant program to encompass cybersecurity threats would provide tremendous benefits. In addition to making SLTTs more resilient to ransomware, these investments will likely improve service delivery as upgrading software and hardware is often the most cost-effective security investment an organization can make. As noted in Action 3.4.3, access to these grants should be conditioned upon demonstrated alignment with the Ransomware Framework after it is developed.

Timing: 6-12 months. **Lead:** Department of Homeland Security, working with Congress.

Action 3.4.3: Offer local government, SLTTs, and critical NGOs conditional access to grant funding for compliance with the Ransomware Framework.

In 2018, the U.S. Congress's Help America Vote Act (HAVA) allocated grant funds to help states bolster their election security. A similar model, through which states manage the delivery of grant funds to municipalities, could be employed to provide grants as financial incentives for demonstrated alignment with the Ransomware Framework. This could help motivate U.S. State, Local, Tribal, and Territorial government entities (SLTTs) to better prepare for and defend themselves against a ransomware attack. Continued provision of such grants should be based on clear measures of progress and advancement toward self-reliance. A similar model could be investigated for suitability in other countries.

Timing: Dependent on the creation of the Ransomware Framework in Action 3.1.1; likely 12-24 months.
Lead: U.S. Federal government and international equivalents.

Action 3.4.4: Alleviate fines for critical infrastructure entities that align with the Ransomware Framework.

A recent amendment to the HITECH ACT⁶⁸ requires the U.S. Department of Health and Human Services, when considering whether an entity should be fined for a HIPAA Security Rule-related violation, to consider the extent to which the entity has demonstrated alignment to an established risk management framework. A similar model could apply to other regulated critical infrastructure sectors to strongly incentivize adherence to established risk management frameworks for ransomware prevention.

Timing: 12-24 months. **Lead:** U.S. Federal government and international equivalents.

Action 3.4.5: Investigate tax breaks as an incentive for organizations to adopt secure IT services.

Governments should offer tax breaks or other financial incentives to businesses that meet certain baseline standards for ransomware preparedness, as laid out in the Ransomware Framework under Action 3.1.1. Such a program should be structured to ensure long-term self-reliance. Leveraging tax breaks could help drive adoption of best practices for preparation for ransomware attacks; however, there are many practical considerations around who would qualify, whether the savings would offset costs, and how organizations would prove their qualification.

Timing: 24 months.
Lead: U.S. Federal government and international equivalents.



Goal #4

Respond to ransomware attacks more effectively

For victim organizations, a ransomware attack can be a stressful, potentially existential event. Crucial decisions about how to respond – including whether to pay the ransom – must be made under intense pressure. Facing the potential threat of losing their data permanently, organizations may make hurried decisions, particularly if they lack understanding about the ramifications of paying a ransom or the full range of alternatives open to them.

In order to improve organizations' ability to respond to ransomware attacks more effectively, government and industry leaders should increase the resources and information available to ransomware victims. At the same time, governments should require organizations to take certain actions before paying a ransom, including reporting the payment to the government. Ultimately, increased support for ransomware victims, including improved awareness of legal requirements prior to payment, will decrease the number of organizations that feel compelled or trapped into paying ransoms.

Objective 4.1:

Increase support for ransomware victims

Ransomware can severely disrupt an organization's business operations, and remediation efforts can take a long time. The resulting revenue loss can prove untenable for many companies, and can be a major crisis for hospitals and other critical infrastructure. Further, for many local governments and small- and medium-sized businesses, the cost of rebuilding networks to avoid paying the ransom is prohibitively expensive. A platform of support resources should be established and made available to help ransomware victims with the recovery process.

Action 4.1.1: Create ransomware emergency response authorities.

Ransomware attacks that have widespread, disruptive effects across society often fall outside the scope of traditional disaster response authorities. To address this gap, national governments should create special authorities to mitigate the effects of ransomware attacks that have impacts beyond the affected organization. The Cyberspace Solarium Commission recommended creating the authority to declare a "cyber disaster."⁶⁹ The Ransomware Task Force supports this idea and recommends that it should explicitly cover ransomware incidents.

A cyber-disaster authority would enable federal agencies to assist victim organizations and local governments, as well as make other resources available, such as incident response support and forensic analysis. Such actions should be limited to dealing with the immediate crisis and not long-term, ongoing engagement. To enable such

“cyber disaster declarations,” Congress could choose to amend the primary law governing natural disaster response activities, typically referred to as the Stafford Act, to explicitly cover cyber incidents, or it could create a new, separate authority.

Timing: 12-24 months. **Lead:** U.S. Federal government, and international equivalents.

Action 4.1.2: Create a Ransomware Response Fund to support victims in refusing to make ransomware payments.

While a company might determine that paying a ransom is economically rational, such a decision supports the criminal enterprise and is rarely in the public interest. To enable more companies to bear the financial cost of remediation, national governments should create “Cyber Response and Recovery Funds” (CRRFs). In addition to other goals, a CRRF should cover restoring IT functionality for local governments, critical national functions, or other entities as they recover from a ransomware attack, particularly when those entities lack access to appropriate cyber insurance or when a cyber insurance policy does not cover the event. This approach would be similar to the Terrorism Risk Insurance Program, which “provides for a transparent system of shared public and private compensation for certain insured losses resulting from a certified act of terrorism.”⁷⁰ If such funding were available for ransomware victims, then cost would play a smaller role in an organization’s decision about whether to pay the ransom. As an incentive to invest in cybersecurity, governments could consider requiring the organization to cover some portion of the ransom as a “deductible.” Governments could also consider additional requirements to access the fund, such as demonstrating use of the Ransomware Framework in Action 3.1.1, to raise organizations’ overall level of cybersecurity.

Timing: 12-24 months. **Lead:** U.S. Federal government in consultation with the insurance industry, and international equivalents.

Action 4.1.3: Increase government resources available to help the private sector respond to ransomware attacks.

Many organizations will seek government assistance during a ransomware attack. In the United States, the Treasury Department’s guidance on ransomware payments essentially requires organizations to consult with the Department if they want to pay the ransom. However, in many countries, agencies cannot fully meet their mandates with existing resources, nor is it always clear which agency has the responsibility or capability to address an inquiry.

Therefore, governments should increase funding for agencies to respond to ransomware-related inquiries so they can meet demand, through a combination of additional staff and improved technology. In addition, in the U.S. context, the Department of Homeland Security’s CISA should consider providing a concierge or ombudsman service for private-sector entities seeking guidance on ransomware-related questions. Under this approach, CISA would not be responsible for interpreting another agency’s guidance, but it would direct the inquiry to the correct office within the Federal government. This assistance would facilitate better decision-making within the private sector.

For example, the U.S. Treasury Department has indicated that ransom payments could violate sanctions against certain individuals or organizations. Treasury’s guidance also indicates that organizations can be held strictly liable for such payments, which means they can be punished for sanctions violations, even if they were unaware

or unable to determine that the recipient is on a prohibited list. As a result, many organizations will want to know whether a potential payment recipient is a sanctioned entity. Given the volume of potential ransomware payments, the Treasury will likely need additional resources to meet demands from the private sector. Second, inquiries may not initially go to the Treasury; CISA could ensure that inquiries it receives regarding Treasury guidance get routed to the correct office.

Timing: 12-24 months. **Lead:** U.S. Federal government, and international equivalents.

Action 4.1.4: Clarify United States Treasury guidance regarding ransomware payments.

In October 2020, the United States Treasury Department's Office of Foreign Assets Control (OFAC) issued an advisory to companies providing services to ransomware victims. This advisory indicates that OFAC will consider ransomware payments as a sanctions violation if the recipient is on the Specially Designated Nationals and Blocked Persons List (SDN List), another blocked person, or covered by comprehensive country or region embargoes. Additionally, the advisory states that a violation by a non-U.S. person that causes a U.S. person to violate any sanctions, or U.S. persons facilitating actions of non-U.S. persons in an effort to avoid U.S. sanctions regulations, are also prohibited. Finally, the advisory notes that any penalties could be assessed under strict liability, which means even if an organization did not know that paying the recipient would constitute a sanctions violation, they can still be held liable for the action.

While this guidance may seem straightforward, Task Force members who have specifically worked within this regime made the point that identifying payment recipients can prove quite challenging, especially under the short timelines of a ransomware attack. Even if an organization asks OFAC whether a particular recipient falls into a prohibited category or seeks a payment license, OFAC is not resourced to provide answers rapidly enough for a company facing tight extortion timelines. Experts have identified other unanswered questions with the advisory. While the Task Force supports Treasury's goal of reducing payments to criminals and in particular to prohibited entities, the advisory does not provide sufficient detail to be effective in achieving this outcome.

Therefore, the Task Force recommends that the U.S. Treasury Department issue additional clarifying guidance to supplement this advisory. This clarifying guidance should address such issues as what constitutes due diligence in determining the payment recipient's identity, the liability OFAC would assign to each stakeholder, the timeline and process for obtaining a payment license (should an organization choose to pursue that route), and to what extent OFAC would consider the harms to people serviced by a ransomware victim in determining whether to grant a license, if required. Taking into consideration the OFAC Advisory, as well as the almost simultaneous Financial Crimes Enforcement Network (FinCEN) Advisory and the Department of Justice Framework issued in October 2020, OFAC should coordinate with these government counterparts to ensure the clarification considers their goals and incorporates them into OFAC's response to this request for clarification.

Timing: 6-12 months. **Lead:** U.S. Treasury Department. *During the update process, the Treasury Department should consult with relevant industry, academia, civil society, and cybersecurity experts.*

Objective 4.2:

Increase the quality and volume of information about ransomware incidents

While everyone agrees that ransomware is a significant problem, there is a lack of reliable, representative data about ransomware's scope and scale. Further, information about ongoing ransomware threats does not yet reach as much of the digital ecosystem as it should – to include both across sectors of private industry or within responsible governmental departments and agencies. Therefore, improving the quality and volume of ransomware information would enable better deterrence, enhance preparedness, and inform disruption activities.

Action 4.2.1: Establish a Ransomware Incident Response Network (RIRN).

To increase the flow of ransomware information, a wide array of public and private organizations should formally agree to share such information rapidly and in standardized formats. To implement this action, the Task Force recommends the creation of the Ransomware Incident Response Network (RIRN). The RIRN would serve several functions, including facilitating receipt and sharing of incident reports, directing organizations to ransomware incident response services, aggregating data, and sharing or issuing alerts about ongoing threats. Not all entities within the RIRN would participate in all RIRN functions. For example, some RIRN organizations might not accept individual incident reports or conduct incident response activities, but they could refer inquiries to another RIRN organization that would.

RIRN entities engaged in the receipt and sharing of specific incident reports would agree to receive and share reports using the standard format developed under 4.2.2; adopt a system of unique identifiers to avoid double-counts while maintaining anonymity; and share the resulting information in an anonymized form with other cyber intelligence organizations and national governments in the network, including law enforcement. RIRN organizations would also agree to direct reporting entities to available public and private resources, including incident responders that could assist the entity through the ransomware attack. The RIRN should consider whether to enable organizations to report anonymously, such that the receiving organization does not know the identity of the submitter.

Other RIRN functions could include sharing or issuing alerts about ransomware threats in non-technical language. Such alerts would be designed to engage as broad an audience as possible and to prompt action to counter specific threats.

The RIRN network should include non-profit organizations, such as the Cybercrime Support Network, Cyber Readiness Institute, Global Resilience Federation, Global Cyber Alliance, Information Sharing and Analysis Organizations, and Cyber Threat Alliance; for-profit entities, including cybersecurity vendors, insurance providers, and incident responders; and national government agencies, including law enforcement.

Timing: 12-24 months to reach full operational capability.

Lead: A nonprofit and international equivalents.

Action 4.2.2: Create a standard format for ransomware incident reporting.

Different organizations require different types of information about ransomware attacks to serve a variety of goals. Cybersecurity providers need technical data about the malware used in the attack to build protections for other customers, while law enforcement may be interested in other information, such as the wallet number and ransom note. At the same time, reporting can be a significant burden to an organization suffering a ransomware attack.

In order to reduce the burden of ransomware reporting while increasing its utility for recipients, a standard ransomware incident report format should be developed through a multi-stakeholder process. Any organization reporting a ransomware incident or reporting on behalf of another organization could use this format. The format should encompass both non-technical information (such as affected organization type or ransom amount) and technical information (such as indicators of compromise). It should also leverage existing formats, such as STIX⁷¹ and the MITRE ATT&CK⁷² framework for technical data and suspicious activity reports, to make integration across reporting systems as easy as possible. The required fields should be kept to a minimum, but the format should enable more technically capable reporting entities to include more detailed information. Creating such a standard format would also make aggregating and anonymizing reports easier.

Timing: 6-12 months. **Lead:** *A nonprofit, such as the Institute for Security & Technology or the Cyber Threat Alliance, and international equivalents.*

Action 4.2.3: Encourage organizations to report ransomware incidents.

National governments should encourage organizations that experience a ransomware attack to report the incident to the RIRN using the common format. This encouragement could take the form of the “See Something, Say Something” campaign, and would note the benefits of reporting, the low level of effort required, and the protections built into the reporting process (for example, that reports can be made anonymously). The government should use different outreach methods for different parts of the ecosystem, for example, using tailored outreach for K-12 engagement versus engagement with the manufacturing sector.

Timing: 6-12 months, updated ongoing as needed.
Lead: *Government cybersecurity agency or cyber center; DHS CISA in the U.S., with support from relevant government, industry, academia, civil society ransomware experts to craft the message.*

Action 4.2.4: Require organizations and incident response entities to share ransomware payment information with a national government prior to payment.

In the US, 54 states and territories have breach disclosure laws, and many sectors also have federal reporting requirements, such as the Gramm-Leach-Bliley Act (in the financial sector) and Sarbanes-Oxley (for publicly traded companies). In the European Union, the Directive on Security of Network and Information Systems (NIS Directive) requires essential entities to report data breaches. Updating breach disclosure laws to include a ransom payment disclosure requirement would help increase the understanding of the scope and scale of the crime, allow for better estimates of the societal impact of these payments, and enable better targeting of disruption activities. Further, requiring ransomware victims to report details about the incident prior to paying the ransom would enable national governments to take actions such as issuing a freeze letter to cryptocurrency exchanges, as called for in Action 2.1.4. Finally, publishing summaries of the information reported under this requirement will help organizations understand how preparative measures need to adapt as attacks evolve.

This mandate should require organizations to report directly to a non-regulatory government agency. In turn, a receiving agency should share the reported information with other appropriate, non-regulatory government agencies as rapidly as possible and, after appropriate anonymization, to the RIRN. To reduce the burden on victim organizations, the mandatory report should only encompass limited information, such as ransom date, demand, payment instructions (e.g., wallet number and transaction hashes), and amount, and it should use the standard reporting format developed through Action 4.2.2. However, the reporting process should allow organizations to provide additional technical information about the incident when they can, and use insurance providers or incident response entities to report on their behalf. In order to avoid forcing organizations to put themselves in potential regulatory jeopardy, the reporting requirement should incorporate limited liability protections, including that the report cannot form the basis for a regulatory or other enforcement action. When enacting this mandate, governments should consider appropriate penalties for organizations that do not comply with the requirement.

Timing: 12-24 months. **Lead:** U.S. Federal government, and international equivalents.

Objective 4.3:

Require organizations to consider alternatives to paying ransoms

While most leaders oppose the idea of paying ransoms and only reluctantly agree to make a payment, they may arrive at the decision based on limited information. A common misperception is that the only alternative to payment is entirely rebuilding the network; that option might be prohibitively costly or take too long for organizations that have critical services that need immediate restoration. However, in many cases, viable alternatives exist between payment and a full network rebuild, such as restoring data from unencrypted shadow copies. Finally, a small minority of organizations might assume that paying the ransom will be the easiest path to restoring operations and may not otherwise review their alternatives.

Requiring organizations to analyze options before paying ransoms could enable more organizations to choose alternative paths. However, even if governments choose not to make these recommendations mandatory, they should still be incorporated as best practices in the Ransomware Framework developed under Action 3.1.1.

Action 4.3.1: Require organizations to review alternatives before making payments.

Although ransomware attackers often try to use time pressure to try to persuade victims to pay, often other options are available. Unencrypted shadow copies of data might be accessible, allowing a victim to recover their business operations, or a decryption key might exist for that particular ransomware. If ransomware victims have a legal requirement to conduct a due diligence review before making a payment, then they would have the ability to push back on demands for immediate payment. This review would also reveal whether options between payment and rebuilding the network from scratch are viable. For example, the mandate could require organizations to consult with initiatives like No More Ransom to determine if their information can be decrypted without paying.

Such reviews should be scaled to the size and criticality of the organization; for SMBs, the review might only consist of two or three actions. If more organizations actively seek alternatives to payment, fewer will feel

compelled to pay. National governments should enact a legal requirement for conducting the review; in the U.S. context, the private sector should develop what constitutes the due diligence review as part of the cost-benefit analysis matrix in Action 4.3.3.

Timing: 12-24 months. **Lead:** U.S. Federal government and international equivalents.

Action 4.3.2: Require organizations to conduct a cost-benefit assessment prior to making a ransom payment.

In addition to searching for payment alternatives, organizations should also compare the costs of paying the ransom with those of not paying. Given the complexities involved, the costs associated with either option are not necessarily obvious without analysis. Many costs will be incurred regardless of whether or not an organization pays the ransom; for example, a company will be liable for breach notification costs regardless of whether the attacker upholds their promise not to further release the data if the ransom is paid. Consequently, such costs should not factor into the decision. In many cases, the analysis could show that paying the ransom is not in fact the cheaper option.

The Task Force recommends that national governments require organizations to conduct a cost-benefit analysis prior to making a ransom payment. Such statutes could also require medium- to large enterprises to document this cost-benefit analysis prior to making a payment or authorizing their insurance provider to make a payment on their behalf. Once a standard cost-benefit analysis matrix is developed, as called for in Action 4.3.3, governments could require the use of the standard matrix to facilitate inter-organization comparisons and data collection.

Timing: 12-24 months Lead. **Lead:** U.S. Federal government and international equivalents.

Action 4.3.3: Develop a standard cost-benefit analysis matrix.

As noted in 4.3.2, analyzing the costs associated with a payment decision can prove challenging. Many organizations would benefit from having a standard analytic matrix to carry out this task. However, most existing decision guides do not explicitly tackle this question and clearly lay out the various cost factors. Therefore, the Task Force recommends that the Ransomware Framework called for in Action 3.1.1 specifically include a cost-benefit matrix. This matrix should enable organizations to identify the costs associated with not paying compared to the costs of paying the ransom, as well as which costs to exclude from the analysis because they are incurred in either case.

Timing: 12-24 months. **Lead:** NIST for the US, and international equivalents, with private sector participation

A Note on Prohibiting Ransomware Payments

The question of whether to prohibit payment of ransoms has become increasingly pressing, and was raised by every working group in the Task Force. The argument in favor of a ransom ban holds that ransomware is primarily motivated by profit, and if the potential for a payout is removed, attackers will shift away from this tactic. A further argument is that ransom profits are used to fund other, more pernicious crime, such as human trafficking, child exploitation, terrorism, and creation of weapons of mass destruction. When viewed with that lens, the case for prohibiting payments is clear.

The challenge comes in determining how to make such a measure practical, as there remains a lack of organizational cybersecurity maturity across sectors, sizes of organization, and geographies. Ransomware attackers require little risk or effort to launch attacks, so a prohibition on ransom payments would not necessarily lead them to move into other areas. Rather, they would likely continue to mount attacks and test the resolve of both victim organizations and their regulatory authorities. To apply additional pressure, they would target organizations considered more essential to society, such as healthcare providers, local governments, and other custodians of critical infrastructure.

Were a government to take a hardline approach on non-payment, perhaps even offering to shore up victims in their jurisdiction in some manner, attackers will look for other potential targets before moving to new sources of revenue. This means they will focus on countries or sectors where governments have not implemented the same policy or are unable to provide a safety net for victims. Even in jurisdictions that offer support for critical entities, organizations that do not qualify for this support may instead pay the ransom without disclosing the incident. This could then open them to further extortion.

As such, any intent to prohibit payments must first consider how to build organizational cybersecurity maturity, and how to provide an appropriate backstop to enable organizations to weather the initial period of extreme testing. Ideally, such an approach would also be coordinated internationally to avoid giving ransomware attackers other avenues to pursue.

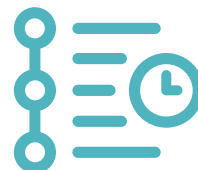
With all these pragmatic considerations in mind, the Ransomware Task Force did not reach consensus on prohibiting ransom payments, though we do agree that payments should be discouraged as far as possible. We recognize, though, that some governments may want to pursue ransomware payment prohibitions based on their policy judgments. Given the potential consequences, the Task Force has identified three factors that governments should consider to reduce the negative impacts of such prohibitions:

Factors to Consider before Pursuing a Ransomware Payment Prohibition

1

Timeline

Governments and organizations need time to adapt to such a dramatic change in the law, so prohibitions cannot be enacted immediately. For example, governments need time to set up victim protection and support programs, as detailed below. Insurance companies need time to update policies to reflect the payment prohibition. The payment facilitator ecosystem would need time to shut down operations in an orderly fashion. Thus, a prohibition statute should establish milestones or conditions that would need to be met before the prohibition would go into effect.

**2**

Phasing

Prohibitions should be implemented in a phased manner, potentially over a matter of years. Phasing could be based on sector: for example, a prohibition could be enacted on public entities before it is extended to the private sector.

**3**

Victim Protection and Support

To help offset the potential burden on victims, governments should provide strong protection and support policies. Examples of such policies include the Cyber Response and Recovery Fund,⁷³ which could be used to help cover business continuity and remediation costs for organizations attacked with ransomware; establish rapid response teams to assist life-line organizations (such as hospitals) to restore functionality quickly; and provide liability protection for business interruptions caused by refusing to pay ransoms.



Conclusion

The Ransomware Task Force developed the recommendations outlined in this report to provide a multi-pronged approach to countering ransomware, and it will be crucial for organizations across sectors to work together and act immediately to tackle this challenge. Make no mistake: reducing the ransomware threat will not be easy, and it will not be accomplished by any individual government or organization alone; this effort will require coordination, collaboration, and investment of time and resources.

The persistence of safe harbors and the challenge of tracing transactions through cryptocurrencies, combined with the complexity of attribution and prosecution, stack the odds in ransomware criminals' favor. The old adage that a cybercriminal only has to be lucky once, while a defender has to be lucky every minute of every day, has never been more true. Without major intervention, the situation will only get worse as ransomware criminals continue to evolve their tactics and the proliferation of devices through the "internet of things" dramatically expands the attack surface. The ever-more lucrative ransomware industry will draw in more threat actors, compounding the problem.

Adding to the challenge, victims of ransomware attacks may increasingly worry about reputational harm and be wary of disclosing details to the public. It is also likely that, as efforts to reduce ransomware become more successful, actors may choose to target increasingly critical systems and networks, and adopt techniques that are more aggressive in order to combat increased defenses or payment obstruction techniques.

Yet failing to act is not an option. Allowing the ransomware challenge to go unchecked could have disastrous consequences. Ransomware actors will only become more malicious, and worsening attacks will inevitably impact critical infrastructure, including communications, transportation, health and safety, distribution and logistics, utilities, and other critical infrastructure. Future attacks could easily combine techniques in ways that cause the infections to spread beyond their intended targets, potentially leading to far-reaching consequences, including loss of life.

The good news is that many of the recommendations outlined in this report may help improve organizations' cybersecurity broadly, and lead to the establishment of new collaborations dedicated to keeping our digital society safe. Indeed, we are still at the dawn of the digital age, and finding new ways to address ransomware and other cyber threats will have benefits that last for decades to come.

Summary of Recommendations



GOAL #1: Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy

Objective 1.1: Signal that ransomware is an international diplomatic and enforcement priority

- Action 1.1.1: *Issue declarative policy through coordinated international diplomatic declarations that ransomware is an enforcement priority*
- Action 1.1.2: *Establish an international coalition to combat ransomware criminals*
- Action 1.1.3: *Create a global network of ransomware investigation hubs*
- Action 1.1.4: *Convey the international priority of collective action on ransomware via sustained communications by national-leaders*

Objective 1.2: Advance a comprehensive, whole-of-U.S. government strategy for reducing ransomware attacks, led by the White House

- Action 1.2.1: *Establish an Interagency Working Group for ransomware*
- Action 1.2.2: *Establish an operationally focused U.S. Government Joint Ransomware Task Force (JRTF) to collaborate with a private-sector Ransomware Threat Focus Hub*
- Action 1.2.3: *Conduct a sustained, aggressive, public-private collaborative anti-ransomware campaign*
- Action 1.2.4: *Make ransomware attacks an investigation and prosecution priority, and communicate this directive internally and to the public*
- Action 1.2.5: *Raise the priority of ransomware within the U.S. Intelligence Community, and designate it as a national security threat*
- Action 1.2.6: *Develop an international-version of an Intelligence Community Assessment (ICA) on ransomware actors to support international collaborative anti-ransomware campaigns*

Objective 1.3: Substantially reduce safe havens where ransomware actors currently operate with impunity

- Action 1.3.1: *Exert pressure on nations that are complicit or refuse to take action*
- Action 1.3.2: *Incentivize cooperation and proactive action in resource-constrained countries*



GOAL #2: Disrupt the ransomware business model and decrease criminal profits

Objective 2.1: Disrupt the system that facilitates the payment of ransoms

- Action 2.1.1: *Develop new levers for voluntary sharing of cryptocurrency payment indicators*
- Action 2.1.2: *Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws*
- Action 2.1.3: *Incentivize voluntary information sharing between cryptocurrency entities and law enforcement*
- Action 2.1.4: *Centralize expertise in cryptocurrency seizure, and scale criminal seizure processes*
- Action 2.1.5: *Improve civil recovery and asset forfeiture processes by kickstarting insurer subrogation*
- Action 2.1.6: *Launch a public campaign tying ransomware tips to existing anti-money laundering whistleblower award programs*
- Action 2.1.7: *Establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management*

Objective 2.2:	Target the infrastructure used by ransomware criminals
Action 2.2.1:	<i>Leverage the global network of ransomware investigation hubs</i>
Action 2.2.2:	<i>Clarify lawful defensive measures that private-sector actors can take when countering ransomware</i>
Objective 2.3:	Disrupt the threat actors, including ransomware developers, criminal affiliates, and ransomware variants
Action 2.3.1:	<i>Increase government sharing of ransomware intelligence</i>
Action 2.3.2:	<i>Create target decks of ransomware developers, criminal affiliates, and ransomware variants</i>
Action 2.3.3:	<i>Apply strategies for combating organized crime syndicates to counter ransomware developers, criminal affiliates, and supporting payment distribution infrastructure</i>



GOAL #3: Help organizations prepare for ransomware attacks

Objective 3.1:	Support organizations with developing practical operational capabilities
Action 3.1.1:	<i>Develop a clear, actionable framework for ransomware mitigation, response, and recovery</i>
Action 3.1.2:	<i>Develop complementary materials to support widespread adoption of the Ransomware Framework</i>
Action 3.1.3:	<i>Highlight available internet resources to decrease confusion and complexity</i>
Objective 3.2:	Increase knowledge and prioritization among organizational leaders
Action 3.2.1:	<i>Develop business-level materials oriented toward organizational leaders</i>
Action 3.2.2:	<i>Run nation-wide, government-backed awareness campaigns and tabletop exercises</i>
Objective 3.3:	Update existing, or introduce new, cybersecurity regulations to address ransomware
Action 3.3.1:	<i>Update cyber hygiene regulations and standards</i>
Action 3.3.2:	<i>Require local governments to adopt limited baseline security measures</i>
Action 3.3.3:	<i>Require managed service providers to adopt and provide baseline security measures</i>
Objective 3.4:	Financially incentivize adoption of ransomware mitigations
Action 3.4.1:	<i>Highlight ransomware as a priority in existing funding provisions</i>
Action 3.4.2:	<i>Expand Homeland Security Preparedness grants to encompass cybersecurity threats</i>
Action 3.4.3:	<i>Offer local governments, SLTTs, and critical NGOs conditional access to grant funding for compliance with the Ransomware Framework</i>
Action 3.4.4:	<i>Alleviate fines for critical infrastructure entities that align with the Ransomware Framework</i>
Action 3.4.5:	<i>Investigate tax breaks as an incentive for organizations to adopt secure IT services</i>



Goal #4: Respond to ransomware attacks more effectively

Objective 4.1: Increase support for ransomware victims

Action 4.1.1: Create ransomware emergency response authorities

Action 4.1.2: Create a Ransomware Response Fund to support victims in refusing to make ransomware payments

Action 4.1.3: Increase government resources available to help the private sector respond to ransomware attacks

Action 4.1.4: Clarify U.S. Treasury guidance regarding ransomware payments

Objective 4.2: Increase the quality and volume of information about ransomware incidents

Action 4.2.1: Establish a Ransomware Incident Response Network (RIRN)

Action 4.2.2: Create a standard format for ransomware incident reporting

Action 4.2.3: Encourage organizations to report ransomware incidents

Action 4.2.4: Require organizations and incident response entities to share ransomware payment information with a national government prior to payment

Objective 4.3: Require organizations to consider alternatives to paying ransoms

Action 4.3.1: Require organizations to review alternatives before making payments

Action 4.3.2: Require organizations to conduct a cost-benefit assessment prior to making a ransom payment

Action 4.3.3: Develop a standard cost-benefit analysis matrix

Acknowledgements

The Institute for Security and Technology is incredibly grateful to the phenomenal group of volunteer experts that came together to make this effort a success. The communities that operate day in and day out to grapple with challenges like ransomware comprise countless unsung heroes, and we are lucky to have been able to convene such a diverse and expansive group of dedicated professionals. They graciously shared considerable amounts of their very limited time to provide their expertise and work through proposed solutions as part of the three-month sprint of the Ransomware Task Force. All of this took place during a period of significant high-level responsibilities across the industry.

Our effort consisted of four main working groups, with an additional three special projects teams, supplemented by numerous sub-working groups focused on everything from cryptocurrencies to “pizza parties” to cyber insurance. The Task Force consisted of members from civil society, private industry (from a range of sectors, including finance, cybersecurity, insurance, healthcare, and high technology), as well as members of government agencies from the United States and around the world.

We want to say a particular word of thanks to the RTF Working Group Co-Chairs, who poured an extraordinary amount of time and energy into organizing and leading large groups of experts, facilitating what were often lively and healthy debates, developing and formulating complicated recommendations, and lending their own extensive knowledge to the entire project. Their leadership elevated the process and this resulting report, and we cannot thank them enough.

We would also like to thank the many members of the Ransomware Task Force and their organizations, which afforded them the opportunity during otherwise exceedingly demanding times. They answered this call to action with dedication and their substantial expertise. We appreciate the resources that each of them brought to the table and the professional connections they have tapped into in order to move the process along and thoroughly vet our proposed solutions.

Lastly, we would like to thank the many unnamed people outside of the Task Force who answered our many questions, discussed ideas, and gave feedback on our recommendations.

We believe the recommendations in this report, if undertaken together and with alacrity, could lead to real change in the trajectory of this threat. All of this has been made possible by the dedication and care of this incredible group of people.

On behalf of all of us at the Institute for Security and Technology, a sincere thank you.

Note: RTF Members and Working Group Members volunteered their time, and contributed to the report in working groups focused on specific problem sets. The resulting suite of recommendations in this document is a combination of all working group efforts, and each recommendation may not necessarily reflect the views of every participant.

RTF Co-Chairs

Megan Stifel, Global Cyber Alliance
John Davis, Palo Alto Networks
Michael Phillips, Resilience

Executive Director
Philip Reiner, Institute for Security and Technology

RTF Working Group Co-Chairs

John Davis, Palo Alto Networks
Megan Stifel, Global Cyber Alliance
Michael Phillips, Resilience
Kemba Walden, Microsoft
Jen Ellis, Rapid7

Chris Painter, The Global Forum on Cyber Expertise Foundation Board
Michael Daniel, Cyber Threat Alliance
Philip Reiner, Institute for Security and Technology

RTF Staff

Sarah Powazek, RTF Program Manager, Institute for Security and Technology
Alexander Riabov, Communications Manager, IST
Leah Walker, Future Digital Security Leader Fellow, IST

Chuck Kapelke, Writing Support
Kathryn Pledger, Pledger Designs
Emma Hollingsworth, Global Cyber Alliance

RTF Membership

Joel de la Garza, a16z
Temí Adebambo, Amazon Web Services
David Forcsey, Aspen Digital
Jeff Troy, Aviation ISAC
Rich Friedberg, Blackbaud
Austin Berglas, BlueVoyant
Lewis Robinson, Center for Internet Security
Roger Francis, CFC Underwriting
Don Spies, Chainalysis
Pamela Clegg, CipherTrace
Brad Garnett, Cisco
Matt Olney, Cisco
Peter Lefkowitz, Citrix
Bill Siegal, Coveware
James Perry, CrowdStrike
Vineet Kumar, CyberPeace Foundation
Stéphane Duguin, The CyberPeace Institute
Yonatan Striem-Amit, Cybereason
Neil Jenkins, Cyber Threat Alliance

Andy Thompson, CyberArk
Ari Schwartz, Cybersecurity Coalition
John Banghart, Cybersecurity Coalition
Ryan Weeks, Datto
Patrice Drake, Deloitte
Keith Mularski, Ernst & Young
Stacy O'Mara, FireEye
Nick Bennett, FireEye
Jill Fraser, Jefferson County, CO
Mark Orsi, K12 SIX
Kent Landfield, McAfee
Ginny Badanes, Microsoft
Kaja Ciglic, Microsoft
Ping Look, Microsoft
Jennifer Coughlin, Mullen Coughlin LLC
John Guerriero, National Governors Association
Justin Herring, New York Department of Financial Services (NYDFS)
Adrian McCabe, Palo Alto Networks

RTF Membership

Sam Rubin, Palo Alto Networks

Sean Morgan, Palo Alto Networks

Bob Rudis, Rapid7

Scott King, Rapid7

Tod Beardsley, Rapid7

Allan Liska, Recorded Future

Katie Nickels, Red Canary

Adam Flatley, Redacted

Davis Hake, Resilience

Michael Convertino, Resilience

Chris Lynam, Royal Canadian Mounted Police's National Cybercrime Coordination Unit (NC3)

Jeff Bonvie, Royal Canadian Mounted Police's National Cybercrime Coordination Unit (NC3)

Kevin Gronberg, SecurityScorecard

Richard Perlotto, The Shadowserver Foundation

Beau Woods, Stratigos Security

James Shank, Team Cymru

Michael Garcia, Third Way

Ciaran Martin, University of Oxford Blavatnik School of Government

Eleanor Fairford, U.K. National Cyber Security Centre (NCSC)

U.K. National Crime Agency (NCA)

Bridgette Walsh, U.S. Cybersecurity and Infrastructure Security Agency (CISA)

U.S. Federal Bureau of Investigation (FBI)

Jonah Hill, U.S. Secret Service (USSS)

Bobby Chesney, U.T. Austin Strauss Center

Who We Are

The Institute for Security and Technology designs and advances solutions to the world's toughest emerging security threats. As a 501(c)(3) non-profit network based in the San Francisco Bay Area, we are dedicated to advancing solutions to critical national security challenges. Our goal is to provide the tools and insights needed for companies and governments to outpace emerging global security threats, creating a bridge between technology and policy leaders.

**IST**Institute for
SECURITY + TECHNOLOGY

Appendix A:

Cyber Insurance

Given the insurance sector's historical role in assessing, managing, pricing, and carrying risks, the cyber insurance industry has been a regular topic of discussion across all of the working groups of the Ransomware Task Force.



This section provides an overview of the cyber insurance market and the role it plays in dealing with ransomware attacks.

Introduction to the Cyber Insurance Market

Many organizations choose to transfer some of their ransomware risk by purchasing insurance. While there are various types of insurance available that may cover losses associated with ransomware, including property insurance, kidnap and ransom insurance, and errors and omissions insurance, most insured ransomware losses are covered by “affirmative” or “stand-alone” cyber insurance. “Affirmative” refers to explicit cyber coverage within the text of an insurance policy; “stand-alone” refers to a dedicated insurance policy for cyber risk, instead of cyber coverage available within a policy dedicated to other types of risk.

The first cyber insurance policies were designed to respond to lawsuits arising out of technology errors and omissions. As the internet developed, organizations digitized their operations, and as states passed laws related to data breach notification and consumer privacy, cyber insurance firms expanded their coverage to respond to the associated risks of data breach and business interruption. Today, cyber insurance has become a standard part of cyber risk management strategies. Many cyber insurers and brokers offer risk management services, education, and security tools to make their insureds more secure, in addition to the traditional risk transfer of an insurance policy.

While many insurance companies actively underwrite cyber risks, the market is led by 20 or so large insurers that write the majority of cyber insurance policies. Less than 15% of organizations globally buy cyber insurance, including about a third of all large companies in the United States. Internationally, the number of companies that have cyber insurance tends to be lower. While cyber insurance is growing, it remains a niche product, and is less than 1% of the size of the greater property and casualty insurance market.⁷⁴

Cyber insurance policies typically cover legal, forensic, and technical experts to help ransomware victims take the most effective steps to recover. (See Table 1, Common Components of a Modern Cyber Insurance Policy.) Insurance concentrates this kind of expertise to help victims best orchestrate their options for recovery. Policies may indemnify victims for any business interruption losses and defend them against any liability arising out of the event. Cyber insurance policies typically cover expertise to help a victim restore

its computer systems from backups and, in the unfortunate circumstances in which the victim has decided it is necessary, expertise to handle a ransom negotiation and effectuate an extortion payment. Cyber insurance policies never require a victim to pay a ransom. Any decision to pay sits with the victim.

TABLE 1: Common Components of a Modern Cyber Insurance Policy

TYPE OF COVERAGE	PARTY	DETAIL
Incident Response Costs	First	The cost of responding to a data breach event, including IT forensics, external services, and specialists that might be employed; internal response costs; legal costs; and costs related to restoring systems to their preexisting condition.
Data Privacy Liability	Third	The cost of dealing with and compensating third-party individuals whose information is or may have been compromised by a data breach event, including notification, compensation, providing credit-watch services, and other third-party liabilities to affected data subjects.
Data Recovery Costs	First	The cost of reconstituting data and/or software that have been deleted or corrupted.
Business Interruption Loss	First	Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a result of cyber attacks or non-malicious IT failures.
Regulatory Defense	Third	Provides coverage for fines, penalties, and defense costs in the face of regulatory actions investigating violations of privacy law.
Cyber Extortion	First	The cost of extortion response expertise to vet and evaluate all possible options for recovery, and, if required, negotiate and execute any ransom payment.
Multimedia Liability	Third	Defense costs and civil damages arising from defamation, libel, slander, copyright/trademark infringement, negligence in publication of any content in electronic or print media, as well as infringement of the intellectual property of a third party.
Reputational Damage	First	Loss of revenues arising from an increase in customer churn or reduced transaction volumes that can be directly attributed to the publication of a defined security breach event.
Network Liability	Third	Third-party liabilities arising from security events occurring within the organization's IT network or passing through it in order to attack a third party.
Contingent Business Interruption Loss	First	Costs of business interruption to the insured resulting from the IT failure of a third party, such as a supplier, critical vendor, utility, or external IT services provider.
Technology Errors & Omissions Liability	Third	Coverage for third-party claims relating to failure to provide adequate technical service or technical products and software, including legal costs and expenses of allegations resulting from a cyber attack, error, or IT failure.
Financial Theft and Fraud	First	The direct financial loss suffered by an organization arising from the use of computers to commit fraud or theft of money, securities, or other property.
Physical Asset Damage	First	First-party loss due to the destruction of hardware or other physical property resulting from cyber attacks.

Thousands of organizations have used cyber insurance to recover from ransomware attacks, including hospitals, cities, and schools, through comprehensive coverage and bringing to bear heavily vetted ransomware response expertise. Each year, cyber insurers pay out hundreds of millions of dollars in cyber losses claimed by their insureds, including business income losses, data recovery costs, and expert fees arising out of ransomware events.⁷⁵ As ransomware has become more frequent and destructive, ransomware losses have increased, impacting both insured and insurer. As a result, a number of insurers have exited the cyber insurance market or reduced their participation. Firms that remain have invested heavily in their ability to properly assess cyber risk. With approximately \$1 trillion in insurance limits exposed, the cyber insurance market is incentivized to reduce the risks posed by ransomware.

In the insurance industry, periods of falling premiums, expanding coverage, and loosening underwriting standards (resulting from increased competition) are referred to as “soft markets,” whereas periods of rising premiums, coverage restrictions, and heightened underwriting standards (due to increased underwriting losses) are often referred to as “hard markets.” According to multiple reports, cyber insurance has entered a “hard market” phase.⁷⁶

In a hard market, the insurance industry can push insured organizations to better manage their risk. Competing insurers may do this through rising underwriting standards and risk management strategies, changes to price, and other innovations that align the insured organization’s incentives toward risk management and risk transfer. This trend has been seen with respect to perils as diverse as fire, piracy, hurricane, and kidnap for ransom; in each instance, the insurance sector has identified and supported risk management practices and technologies that have bent the curve and ameliorated a significant risk, to the mutual benefit of the insured and the insurer. The cyber insurance market should behave similarly; for example, after the major retail payment card breaches of 2013 and 2014, the cyber insurance market pushed compliance with PCI-DSS standards, industry standards promulgated by the payment card industry that establish a base level of payment card cybersecurity.

In a hard market, the insurance industry can push insured organizations to better manage their risk.

Rising Underwriting Standards in Response to Ransomware

The economics of the cyber insurance industry align with the victims of ransomware. As a result, the industry is incentivized to innovate, evolve, compete, and otherwise increase its expertise to prevent insured ransomware losses. As ransomware losses have accelerated, the cyber insurance market has adapted.

Improved cyber-defense:

The key adaptation has been investment in underwriting analysis to identify ransomware risk factors and developing the expertise to help firms secure themselves appropriately against a ransomware attack. Increased scrutiny of prospective insurance buyers is designed to incentivize firms to make appropriate security investments and become prepared. To accurately measure a firm's ransomware risk, cyber insurers are increasingly deploying supplemental ransomware underwriting applications, enlisting third-party cybersecurity firms to conduct additional assessments, and carrying out external scans of firms' web-facing assets. Cyber insurers may deploy in-house security and risk engineering expertise to proactively help insured organizations become more resilient in the face of ransomware risk. A number of cyber insurers and insurance brokerage firms have established or acquired cybersecurity firms to provide managed threat detection, incident response, or security consulting services to insureds in advance of a loss.

Market Strategies:

Another adaptation comes from cyber insurers experimenting with different market strategies to incentivize organizations to increase their cybersecurity to become secure. These strategies include sublimits (i.e. reduced claim limits) for ransomware-related coverage; co-insurance (the joint assumption of a risk by the insured and insurer); increases in premium; and other changes or requirements in the insurance coverage.⁷⁷ Underwriters may refuse to offer insurance coverage to organizations that do not first establish an appropriate level of cybersecurity preparedness. For instance, this may mean that an organization must confirm that it follows a recognized cybersecurity framework, or that it has deployed multi-factor authentication, or is managing the risks associated with remote access to computer networks. While underwriting firms may defer in certain details, the cyber insurance market is coalescing around certain baseline controls as a prerequisite to insurability.⁷⁸ Brokerages and risk management firms have also increased their advisory practices to move organizations toward greater ransomware preparedness and insurability.

Organizations that lack basic cybersecurity hygiene may be uninsurable, which should spur greater investment in ransomware defenses. When the market works properly, organizations should be incentivized to reach an appropriate mix of insurance and security.⁷⁹

Process changes:

Finally, as a third adaptation, cyber insurance companies have modified many internal processes. For example, some insurers have established close connections with national and global law enforcement to facilitate the sharing of data and threat intelligence.⁸⁰

Appendix B:

The Cryptocurrency Payment Process

Ransomware payments are typically made in cryptocurrency. As cryptocurrency ownership records are maintained on the cryptographic ledger of a blockchain, ownership is not easily linked to identifiable individuals. Often the money does not flow straight from victim to criminal; it travels through a multi-step process involving different financial entities, each presenting insights into criminal identities and opportunities for intervention.

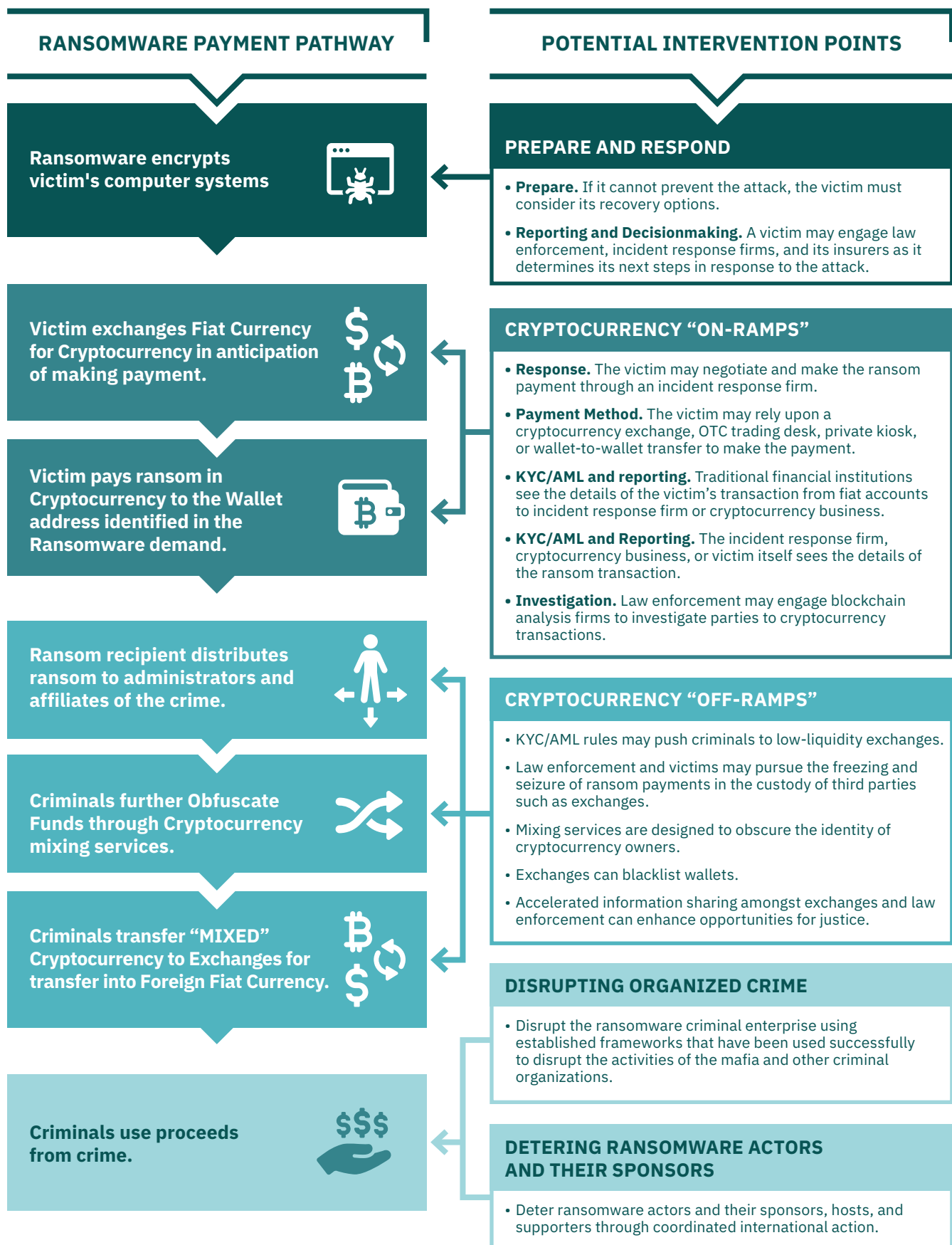


This section expounds on this process, identifies many of the key entities involved, and highlights where interventions could occur and how they could undermine the ransomware business model.



The following is a graphical representation of the cryptocurrency payments process, and various potential points of intervention:

Figure 6 Payment Pathway and Potential Intervention Points



1

Step 1 Victim Response

When a victim is hit with a ransomware attack, they may engage one or more incident response entities to assist in the process of advising on, and potentially paying, the ransom. These firms include the victim's cyber-insurance provider (if they have coverage), law firms, negotiation firms, threat intelligence, and forensic investigators.

Entities like negotiation firms communicate directly with ransomware threat actors and seek to lower the ransom demand. Other organizations (for example, incident response firms, financial institutions, etc.) may perform due diligence to ensure a payment would not violate sanctions, identify the extent of applicable insurance coverage, and confirm that there is no publicly available decryption key. These firms may also assist the victim with deciding whether or not to pay the ransom.

2

Step 2 Ransom Payment

If a victim decides to pay the ransom, either they or an incident response vendor, such as a forensic investigator or negotiation firm, will need to withdraw funds from a financial institution to purchase the cryptocurrency. This cryptocurrency is then transferred from the victim's cryptocurrency wallet, a digital storage service, facilitated by a cryptocurrency exchange, a private kiosk, or simply a wallet-to-wallet transfer to a new wallet address provided by the ransomware criminal. These victim-specific addresses are created by the criminal actors for the purpose of receiving the payments. Often these will have never been used before, to avoid being associated with the threat actor's previous activity, and thus cannot be traced until funds are actually deposited into those wallet addresses by the victim. These are generally un-hosted wallets, which means they are not hosted with any cryptocurrency exchange that handles and monitors transactions.

Cryptocurrencies are outside of any one organization's control, but their blockchains create public, permanent records of activity, whether legal or illicit. Blockchain analysis helps interpret public blockchain ledgers and, with the proper tools, government agencies, cryptocurrency businesses, and financial institutions can understand which real-world entities transact with each other. Blockchain analytic companies, such as Chainalysis and CipherTrace, are able to show that a given transaction took place between two different cryptocurrency exchanges, or between a cryptocurrency exchange and an illicit entity, such as a sanctioned individual or organization. With blockchain analysis tools and Know Your Customer (KYC) information, law enforcement can gain transparency into blockchain activity.

While some illicit actors use privacy coins in an attempt to obfuscate their transactions, this more untraceable form of cryptocurrency has not been adopted as widely as might be expected because they are not as liquid as Bitcoin and other cryptocurrencies. Now that many exchanges have delisted privacy coins following guidance from regulators, this payment method is becoming increasingly impractical. Cryptocurrency is only useful if you can buy and sell goods and services or cash out into fiat, and that is much more difficult with privacy coins.

Step 3 Ransomware Fund Obfuscation

After receiving the ransomware payment in the designated digital wallet, the ransomware criminal often attempts to obfuscate these funds as quickly as possible to avoid detection and tracking. As noted above, Bitcoin transactions are logged in a public ledger, so without obfuscation, a criminal cannot withdraw funds into cash without being tracked. One popular method for obfuscation is to route funds through cryptocurrency mixing services, services that create a series of transactions to mix one set of funds with another, muddying the public ledger by mixing in legitimate “traffic” with illicit ransomware funds.

Cryptocurrency mixing services



Cryptocurrency mixing services (often “mixers” or “tumblers”) are commonly used by ransomware actors and others engaged in illicit activity. As described above, a blockchain is a record of the source and destination of every transaction. As a result, blockchain analytic firms can trace cryptocurrency transactions, supporting both law enforcement efforts to identify criminals and cryptocurrency exchange efforts to screen clients for links to crime. Ransomware actors use mixers to try to prevent such tracing by making it difficult to identify the true source of transactions on the blockchain.

Mixers can function in multiple ways, but typically they rely upon a group of people coming together to pool their cryptocurrency (like bitcoin), with each taking back different bitcoins of the same value. These different bitcoins they receive will have a different source than the ones they submitted for “mixing.” This process is typically managed by a centralized mixing service, which charges a fee — often between 1-10% of the amount mixed. Some mixing services take additional steps to complicate and obfuscate the source of funds, including intermediate trades with privacy coins such as Monero. There are hundreds of mixing services available on the internet.

Another method for obfuscation is “chainhopping,” exchanging funds in one cryptocurrency for another. Tracking funds after they switch currencies can be extremely challenging. These transactions can occur at centralized or decentralized cryptocurrency exchanges, which are discussed further in Step 4, or via atomic swaps and other technical means.

4

Step 4 Cash out

After obfuscating the funds, ransomware criminals may make use of the cryptocurrency, or withdraw the funds into cash. There are several methods for cashing out, including over-the-counter trading desks, crypto kiosks, and exchanges, which are the most prominent. Others include exchanging bitcoin for gift/debit cards and or alternative coins, such as privacy coins.

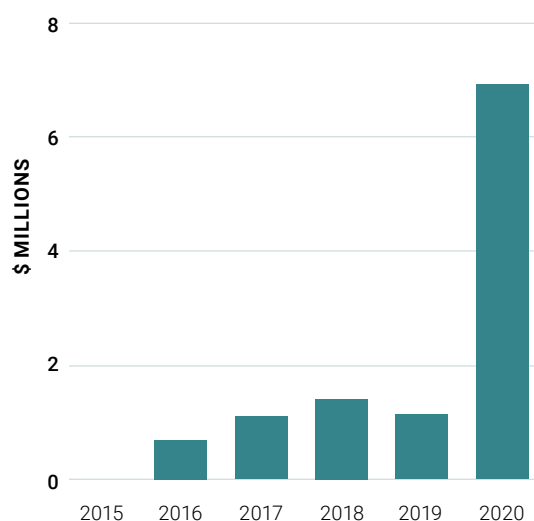
As noted below criminals may make use of cryptocurrency funds by paying for infrastructure to conduct attacks or to pay individuals involved in the criminal organization, such as money launderers and affiliates. Criminals also rely on OTC traders to convert the virtual currency to fiat. A market exists for these OTC transactions because Russian businesses operating in China prefer to operate in Bitcoin to avoid taxes, while criminals operating in Russia prefer cash. Therefore, an OTC trader can connect these individuals with Russian businesses accepting Bitcoin and criminals receiving cash transactions inside Russia.

Where do the funds go?

Ransomware criminals may choose to not immediately withdraw funds into cash for their own use. In the ransomware-as-a-service (RaaS) model described earlier in the report, several criminal affiliates (essentially contractors) are involved in the exploitation, encryption, and ransom demand, all of whom require payouts. Criminal gangs also may use cryptocurrency itself to invest in further malicious infrastructure and services.

In 2020, cryptocurrency-tracing company Chainalysis tracked nearly \$7 million sent from ransomware-tainted cryptocurrency wallets to other known illicit marketplaces.⁸¹ Ransoms paid by victims may go on to fund other criminal enterprises that are facilitated online, as has been detailed in other sections of this report.

Figure 7 Ransomware Wallets Sending to Darknet Marketplaces



Step 4 cont...

Cryptocurrency businesses facilitate the trading of cryptocurrency between buyers and sellers. Ransomware criminals rely on these businesses to exchange their ransomware proceeds for different cryptocurrencies or for government-issued currencies. As relatively new financial institutions, these cryptocurrency businesses exist on a spectrum of legitimacy, regulation, and compliance, and handle varying amounts of transactions with illicit funds. For example, in 2019, Coinbase published a report identifying that most exchanges are not in compliance with Anti Money Laundering or Know your Customer procedures.

Cryptocurrency businesses generally fall into one of three categories:

- **Regulated Cryptocurrency Exchanges:** These are legitimate exchanges with high liquidity that are able to handle a large number of transactions. In the United States, these exchanges are subject to non-bank financial institution anti-money laundering (AML) regulations, which require some Know Your Customer (KYC) identification of customers performing large transactions, among other requirements. Other jurisdictions impose similar KYC and AML requirements as those in the United States, including the United Kingdom, the European Union, Japan, Australia and New Zealand.⁸²
- **Minimally Regulated Cryptocurrency Exchanges:** Located in jurisdictions with less stringent regulatory obligations than the United States and other members of the G7, these cryptocurrency exchanges operate with few controls for identifying potential illicit funds. These exchanges often serve as one of the preferred services for ransomware criminals to cash out illicit funds without oversight. These exchanges include Binance and Huobi, which have much less stringent KYC rules, especially when dealing with OTC traders.
- **Peer-to-Peer (P2P) Cryptocurrency Exchanges (also known as Over-the-Counter or Decentralized Exchanges):** Regardless of geographical limits, users can download freely-available software or access P2P exchanges to buy and sell cryptocurrency directly with one another. This avoids the use of a third-party service like a “traditional” exchange, which may hold user funds in custody, process transactions in fiat currency, and comply with KYC and AML requirements.
- **Over-The-Counter Trading Desks:** Some OTC traders, actors that trade cryptocurrency without an exchange acting as a facilitator or mediator of the trade, provide cryptocurrency laundering services to ransomware threat actors. Although many OTC traders maintain legitimate businesses and comply with stringent financial regulations, some do not, and they provide an important source of liquidity for exchanging ransomware payment.

Tracking payments is difficult due to the variance in standards and enforcement of regulation for exchanges of different categories, or that operate in different countries. Even using regulated exchanges, ransomware actors constantly find new ways to remain hidden by using money mule service providers to set up accounts, or use accounts with false or stolen credentials.

Appendix C:

Proposed Framework for a Public-Private Operational Ransomware Campaign



This appendix provides an overview of how the formal, government-led Joint Ransomware Task Force (JRTF) and the informal Ransomware Threat Focus Hub (RTFH) could collaborate to conduct an operational ransomware campaign.

Background

Over the years, many efforts have attempted to formalize the trust networks that are relied on to keep the internet operating. Some initiatives have been effective without significant formal structure: the Conficker Working Group, convened by Microsoft in the late 2000s to stop the spread and impact of the Conficker worm, is often lauded as an early model. More formal joint collaborative efforts have also been successful: the 2020-2021 takedown of Emotet was an example of a long collaborative effort between global law enforcement, judicial authorities, and private industry to seize and disrupt a massive global botnet. More often, though, public-private information security collaboration occurs primarily when there is a crisis, as was the case with the Cyber Unified Coordination Group (UCG), which the U.S. Government convened in 2021 to focus on the Hafnium case involving vulnerable Microsoft Exchange Servers.

What remains elusive is a standing mechanism for convening operationally focused, sustained, public-private campaigns that are coordinated via formal and informal nodes, and that allow for both the formal requirements needed by government and the informal requirements needed by industry. Much has already been written about potential solutions for launching such an initiative, including Jay Healey's 2018 article on Cyber Incident Collaboration Organizations,⁸³ recent work by the Aspen Institute,⁸⁴ and recommended solutions from the World Economic Forum's Partnership Against Cybercrime.⁸⁵ Ransomware presents a unique opportunity to test new approaches, and the Ransomware Task Force provides below a proposed framework for consideration.

Objective

Use operational collaboration to increase the scope, scale, pace, and efficacy of intelligence-driven takedowns and disruption of ransomware operations and the infrastructure and people that enable them.

Assumptions

Ransomware actors are intelligently taking advantage of the seams between law enforcement and private-sector cooperation mechanisms, and between governmental and private-sector legal authorities. They also move with such alacrity that existing structures cannot respond fast enough to disrupt their activities on a sustained, rapid, and concerted basis.

Existing mechanisms are working to address the problem, but they are siloed in various agencies and not leveraging the full authorities and capabilities of all government agencies. They also do not routinely incorporate private-sector action, nor do they scale to compete with the agility of the criminals.

This public-private operational collaboration mechanism should include actors and organizations that are involved in the full gamut of defending against and disrupting ransomware operations. No single actor or entity is fully capable of disrupting this threat by itself, so public and private actors must come together to assess the threat and coordinate activities across authorities and capabilities.

Private-sector participants must recognize that not all government actions will be shared or coordinated with non-government actors due to security concerns or to protect sources and methods.

Government participants must recognize that private-sector participants may need to take actions quickly to protect their customers and fulfill contractual agreements, and may not always be able to coordinate actions with the government.

A natural governmental response to this collaboration requirement is to create some kind of formal structure. However, a formal private-public Joint Ransomware Task Force would likely hinder private-sector participation. Past experience has shown that private-sector participants are more likely to share information with the government and take actions to defend their customers in coordination with government through existing informal and indirect channels. The U.S. Government, on the other hand, needs formality to function in a joint way; moreover, the need for public accountability requires the government to adhere to formal rules and structures. Departments and agencies, especially those with competing equities, are more likely to work only within their lane of authorities and capabilities unless they are required and incentivized to work with each other.

Thus a formal government task force paired with existing formal and informal private-sector groups in the short-term would build trust and work to develop some early wins. Over time, a combination of formal and informal private-sector structures should develop to interface with the government's Joint Ransomware Task Force (JRTF), working toward a 24/7 operational collaboration mechanism for a public-private anti-ransomware campaign.

Ransomware disruptions will almost always be law enforcement operations at their core. But in order to truly disrupt ransomware actors, we must also consider non-law enforcement options and capabilities that can improve defenses, impose costs, or more fully disrupt ransomware operations. In terms of the intelligence needed for such operations, the government and various private-sector organizations need each other.

*Over time, a combination of formal and informal private sector structures should develop to interface with the government's Joint Ransomware Task Force, working towards a **24/7** operational collaboration mechanism for a public-private anti-ransomware campaign.*



- Private-sector cybersecurity providers are often best positioned to capture indicators of compromise and tactics, techniques, and procedures (TTPs) of the malicious actors to develop protections for their customers and understand active campaigns.
- Cryptocurrency exchanges and analysis firms are best positioned to understand the flow of ransomware payments.
- Government agencies, especially in law enforcement and the Intelligence Community, are best positioned to identify the individuals behind the activity.
- All of these intelligence perspectives must be shared, combined, and understood in order to develop the best possible disruption options.

U.S. Government personnel working with the private sector in a given campaign must be empowered and incentivized by their leadership to engage with the private sector and take action based on what they learn. They should also anticipate the needs of private-sector partners and share information that will lead to disruptions.

To achieve this increased level of operational collaboration, the Ransomware Task Force recommends the following:

Recommendations

1. The U.S. Government should establish the Joint Ransomware Task Force (JRTF) consisting of representatives from the Cybersecurity and Infrastructure Security Agency (CISA; the FBI; United States Secret Service; the Intelligence Community; U.S. Cyber Command; the Departments of Treasury, Justice, and State; the Office of the National Cyber Director; and other departments and agencies as appropriate. The JRTF's mission should be to prioritize ransomware disruption operations and leverage the intelligence-driven disruption planning process to increase the pace and efficacy of ransomware takedowns and disruption. The Departments of Homeland Security, Justice, and Defense should jointly provide the resources needed to establish and operate the Task Force, such as office space, IT infrastructure, and other supplies. The Task Force should coordinate closely with the Joint Cyber Planning Office in CISA, the National Cyber Investigative Joint Task Force (NCIJTF), and other inter-agency cyber-related groups. The NSC-led Interagency Working Group recommended in 1.2.1 of the main RTF report would provide direction, priorities, and oversee the JRTF. The goals of the JRTF should be to:

- Prioritize intelligence-driven operations to disrupt specific ransomware actors;
- Incentivize and empower government agencies and personnel to participate in joint operations in the interagency and with private-sector partners and take action; and
- Anticipate the needs and requests of the private sector

The Administration could create such a Task Force through executive action, just as the Bush Administration created the NCIJTF through National Security Policy Directive-54/Homeland Security Policy Directive-23. The JRTF could be a stand-alone entity, or as U.S. government cyber organizations continue to mature and evolve, it could be folded into an existing organization, such as the Joint Cyber Planning Office, the National Cyber Director's office, or the NCIJTF.

2. An existing non-profit organization should establish a private-sector Ransomware Threat Focus Hub. The participants should include cybersecurity providers, non-profit sharing organizations, cyber threat intelligence firms, threat intelligence researchers and contractors, incident response firms, managed security service providers, telecommunications companies, major platform owners/operators, and hosting providers. The Hub would facilitate and coordinate sustained private-sector actions against an agreed-upon target list, in coordination with the JRTF. The hosting non-profit organization, such as an information-sharing and analysis organization (ISAO), would provide space for information sharing and operational collaboration between participants.⁸⁶ Formal and informal coordination could occur within this Hub, and the Hub would encourage informal and formal groups to work together in tandem. Informal groups would continue to work and collaborate as they do today, while the formal layer would focus on long-term, permanent arrangements with the U.S. or other governments.

The RTF recommends the following general tasks for the JRTF and the RTFH:

Proposed JRTF Tasks

1. Establish a “target list” of the top 10 ransomware threats, in consultation with the private-sector hub, updated on an ongoing basis, to:
 - a. Identify and prioritize targets for threat cells, focused on specific ransomware actors/conglomerates;
 - b. Identify a timeline for the operation; and
 - c. Identify metrics for success.
2. Disrupt criminal actors, associated infrastructure, and their finances.
3. Enable private-sector representatives to move against ransomware actors and infrastructure with rapid legal authority (e.g. court orders) when necessary to take required actions.
4. Enable the private sector to tip and cue law enforcement, network defenders, intelligence community, and, where necessary, U.S. military action.
5. Collect, share, and analyze ransomware trends to inform campaigns.
6. Create “after action reports” that identify successes and failures in an operation to improve subsequent operations.
7. Use non-traditional tools, such as information and influence operations, through online forums or a dedicated web portal

Proposed Ransomware Threat Focus Hub Tasks:

1. Provide input to the JRTF’s top 10 target list.
2. Take synchronized actions against criminal actors, associated infrastructure, and financial operations, based on participants’ legal authority.
3. Enable government-sector representatives to target and disrupt ransomware actors and infrastructure more rapidly.
4. Collect, share, and analyze ransomware trends to inform counter-ransomware campaigns.
5. Create “after action reports” from the private-sector point of view that identify successes and failures in each operation to improve subsequent operations.
6. Use non-traditional tools, such as information and influence operations, via online forums, a dedicated web portal, or other means.

Glossary

AG	Attorney General
ALATs	Assistant Legal Attachés
APAC	Asia-Pacific
Atomic Swaps	A smart contract technique that allows the quick exchange of two different cryptocurrencies, running on distinct blockchain networks, without using centralized intermediaries.
AML	Anti-Money Laundering
CCIPS	Computer Crime and Intellectual Property Section
CDNs	Content Delivery Networks
Centralized Cryptocurrency Exchange (CEX)	Online platforms that are used to buy and sell cryptocurrencies. They are the most common means that investors use to buy and sell cryptocurrency holdings. Most of the control over your account remains in the hands of the third party that runs the exchange
CFAA	Computer Fraud and Abuse Act
CFT	Combating Financing of Terrorism
CHIPS	Computer Hacking and Intellectual Property Network
CISA	Cybersecurity and Infrastructure Security Agency
CNO	Computer Network Operations
CRRFs	Cyber Response and Recovery Funds
CSN	Cybercrime Support Network
Cyber Kill Chain	<p>A series of steps that trace the stages of a cyberattack from the early reconnaissance stages to the exfiltration of data. The steps are as follows:</p> <ol style="list-style-type: none">1. Reconnaissance: The observation stage: attackers typically assess the situation from the outside in to identify both targets and tactics for the attack.2. Intrusion: Based on what the attackers discovered in the reconnaissance phase, they are able to get into the systems: often leveraging malware or security vulnerabilities.3. Exploitation: The act of exploiting vulnerabilities, and delivering malicious code onto the system.4. Privilege Escalation: Attackers often need more privileges on a system to get access to more data and permissions. For this, they need to escalate their privileges, often to an Admin.

5. Lateral Movement: Once in the system, attackers can move laterally to other systems and accounts in order to gain more leverage, whether higher permissions, more data, or greater access to systems.

6. Obfuscation / Anti-forensics: In order to successfully pull off a cyberattack, attackers need to cover their tracks; during this stage, they often lay false trails, compromise data, and clear logs to confuse and/or slow down any forensics team.

7. Denial of Service: Disruption of normal access for users and systems, in order to stop the attack from being monitored, tracked, or blocked.

8. Exfiltration: The extraction stage: getting data out of the compromised system.

Decentralized Cryptocurrency Exchange (DEX)	A peer-to-peer (P2P) marketplace that connects cryptocurrency buyers and sellers. A user remains in control of their private keys when transacting on a DEX platform.
DFIR	Digital Forensics/Incident Response
DHS	Department of Homeland Security
DNS	Denial of Service
DSAR	Data Subject Access Request
EMEA	Europe, the Middle East, and Africa
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
Fiat	Government-issued currency that is not backed by a commodity such as gold; often has government regulations.
FinCEN	Financial Crimes Enforcement Network
FSB	Federal Security Service
HAVA	Help America Vote Act
HIPAA	Health Insurance Portability and Accountability Act
HITECH ACT	Health Information Technology for Economic and Clinical Health Act
HSMs	Hardware Security Models
HUMINT	Human Intelligence
ICA	Intelligence Community Assessment
ICHIP	International Computer Hacking and Intellectual Property
IMINT	Imagery Intelligence
IOS	Indicators of Compromise
IRS	Internal Revenue Service
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization

IWG	Interagency Working Group
JCPO	Joint Cyber Planning Office
JRTF	Joint Ransomware Task Force
KYC	Know Your Customer
Know Your Customer (KYC) Information	A standard in the investment industry that ensures investment advisors know detailed information about their clients' risk tolerance, investment knowledge, and financial position. Sharing KYC information on blockchain would enable financial institutions to deliver better compliance outcomes, increase efficiency, and improve customer experience. Information includes name, date of birth, address, bills, etc.
MDBR	Malicious Domain Blocking and Reporting
Money Mule Service Providers	Someone who transfers or moves illegally acquired money on behalf of someone else. Criminals recruit money mules to help launder proceeds derived from online scams and frauds or crimes.
MS-ISAC	Multi-State Information Sharing and Analysis Center
MSB	Money Service Businesses
MSP	Managed Service Providers
MSSP	Managed Security Services Providers
MXs	Mail Exchangers
NAIC	National Association of Insurance Commissioners
NCD	National Cyber Director
NCIJTF	National Cyber Investigative Joint Task Force
NCSC	National Cyber Security Centre
NDAA	National Defense Authorization Act
NIS Directive	Network and Information Security Directive
NIST	National Institute of Standards and Technology
NSC	National Security Council
NSD	National Security Division
OFAC	Office of Foreign Assets Controls
OFE	Office of Fraud Enforcement
OTC	Over the counter
PCI DSS	Payment Card Industry Data Security Standard
Privacy Coins	A class of cryptocurrencies that power private and anonymous blockchain transactions by obscuring their origin and destination.
RAAS	Ransomware as a Service, a business model used by ransomware developers, in which they lease ransomware variants in the same way that legitimate software developers lease software as a service (SaaS) products.

RCE	Remote Code Execution
RICO	Racketeer Influenced and Corrupt Organizations Act
RIR	Ransomware Incident Report (proposed)
RIRN	Ransomware Incident Response Network (proposed)
RTF	Ransomware Task Force
RTFH	Ransomware Threat Focus Hub (proposed)
SARs	Suspicious Activity Reports
SDN List	Specially Designated Nationals and Blocked Person List
SEC	U.S. Securities and Exchange Commission
SIGINT	Signals Intelligence
SLTTs	U.S. State, local, tribal, and territorial government entities
Trust Group	Communities of security professionals who collaborate between chains of trust. Trust Groups' missions often include maintaining integrity and security of the internet, developing and sharing information, and encouraging and promoting security.
TS/SCI	Top Secret / Sensitive Compartmented Information
TTP	Tactics, Techniques, and Procedures
UCG	Cyber Unified Coordination Group
USAOs	United States Attorney's Office
USIC	United States Intelligence Community

Endnotes

1. Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2020," January 18, 2021, Emsisoft Blog, <https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/>
2. Coveware, "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands," February 1, 2021. <https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020>
3. Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2020," January 18, 2021, Emsisoft Blog, <https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/>
4. Chainalysis Team, "Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think," excerpt from the Chainalysis 2021 Crypto Crime Report, January 26, 2021, <https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021>
5. Unit 42, Palo Alto Networks, "Ransomware Threat Assessments: A Companion to the 2021 Unit 42 Ransomware Threat Report," March 17, 2021, <https://unit42.paloaltonetworks.com/ransomware-threat-assessments>
6. Commandant, U.S. Coast Guard, "Marine Safety Information Bulletin: Cyberattack Impacts MTSA Facility Operations," December 2019. https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf
7. Rundle, James and Nash, Kim S. "Ransomware Attack Exposes Poor Energy-Sector Cybersecurity," Wall Street Journal, February 2020, <https://www.wsj.com/articles/ransomware-attack-exposes-poor-energy-sector-cybersecurity-11582540200>
8. Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2020," January 18, 2021, Emsisoft Blog, <https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/>
9. Eddy, Melissa and Perlroth, Nicole. "Cyber Attack Suspected in German Woman's Death," New York Times, September 18, 2020. <https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomware-death.html>
10. Barry, Ellen and Perlroth, Nicole. "Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack," November 26, 2020. <https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html>
11. Krebs, Brian. "Study: Ransomware, Data Breaches at Hospitals tied to Uptick in Fatal Heart Attacks," KrebsOnSecurity, November 7, 2019, <https://krebsonsecurity.com/2019/11/study-ransomware-data-breaches-at-hospitals-tied-to-uptick-in-fatal-heart-attacks/>
12. Hay Newman, Lily. "Atlanta Spent \$2.6M to Recover From a \$52,000 Ransomware Scare," Wired. April 23, 2018. <https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/>
13. Coble, Sarah. "MAZE Exfiltration Tactic Widely Adopted," Infosecurity Magazine. Accessed April 2, 2021. <https://www.infosecurity-magazine.com/news/maze-exfiltration-tactic-widely/>
14. Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2020," January 18, 2021, Emsisoft Blog, <https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/>
15. Cybersecurity & Infrastructure Security Agency (CISA), "Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data," December 10, 2020. <https://us-cert.cisa.gov/ncas/alerts/aa20-345a>
16. Associated Press. "Baltimore: Ransomware Attack Will Cost at Least \$18M," May 30, 2019. <https://www.nbcwashington.com/news/local/baltimore-ransomware-attack-will-cost-at-least-18m/159464/>
17. Chokshi, Niraj. "Hackers Are Holding Baltimore Hostage: How They Struck and What's Next," New York Times, May 22, 2019. <https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html>
18. Freed, Benjamin. "Baltimore ransomware attack was early attempt at data extortion, new report shows," StateScoop, September 25, 2020. <https://statescoop.com/baltimore-ransomware-crowdstrike-extortion/>
19. Chainalysis Team, "Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think," January 26, 2021. Exerpt from Chainalysis 2021 Crypto Crime Report. <https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021>

20. Buckley, Eileen. "Ransomware attack shutdown all Buffalo school learning," The Rebound Buffalo, March 15, 2021. <https://www.wkbw.com/rebound/state-of-education/ransomware-attack-shutdown-all-buffalo-school-learning>
21. Coble, Sarah. "Cyber-Attack on Mississippi Schools Costs \$300,000," InfoSecurity Magazine, Accessed on April 10, 2021. <https://www.infosecurity-magazine.com/news/cyberattack-on-mississippi-schools/>
22. Palmer, Danny. "A highly sophisticated ransomware attack leaves 36,000 students without email," ZDNet, March 30, 2021. <https://www.zdnet.com/article/a-highly-sophisticated-ransomware-attack-leaves-36000-students-without-email/>
23. Weston, Sabina. "Evidence suggests REvil behind Harris Federation ransomware attack," ITPro, April 9, 2021. <https://www.itpro.com/security/ransomware/359161/evidence-suggests-revil-behind-harris-federation-ransomware-attack>
24. Cybersecurity & Infrastructure Security Agency (CISA), "Ransomware Guidance and Resources," <https://www.cisa.gov/ransomware>
25. Sophos, "The State of Ransomware 2020," May 2020. <http://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/pdf/sophos-the-state-of-ransomware-2020-wp.pdf>
26. United States Department of Treasury, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," October 1, 2020. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
27. Sentonas, Michael. "2020 Global Security Attitude Survey: How Organizations Fear Cyberattacks Will Impact Their Digital Transformation and Future Growth," CrowdStrike Blog, November 17, 2020. <https://www.crowdstrike.com/blog/global-security-attitude-survey-takeaways-2020>
28. Cyber Florida, "The Connection Between Ransomware and Cyber Insurance Claims in 2020," October 20, 2020, Cyber Florida, <https://cyberflorida.org/best-practices/the-connection-between-ransomware-and-cyber-insurance-claims-in-2020/>
29. Dudley, Renee. "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks," <https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks>
30. Smilyanets, Dmitry. "'I scrounged through the trash heaps... now I'm a millionaire:' An interview with REvil's Unknown," The Record. March 16, 2021. <https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/>
31. Freedman, Linn F. "Sodinokibi Hackers Switch Payment Mechanism to Monero," National Law Review, April 16, 2020. <https://www.natlawreview.com/article/sodinokibi-hackers-switch-payment-mechanism-to-monero>
32. Reuters, "Cyber attack hits 200,000 in at least 150 countries: Europol," May 14, 2017. <https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX>
33. Sophos, "The State of Ransomware 2020," May 2020. <http://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/pdf/sophos-the-state-of-ransomware-2020-wp.pdf>
34. Check Point. Live Cyber Threat Map. <https://threatmap.checkpoint.com/>
35. Khan, Abdullah. "G7 finance ministers urge countries to adopt FATF standards against cybercrime," S&P Global Market Intelligence, Oct.13, 2020. <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/g7-finance-ministers-urge-countries-to-adopt-fatf-standards-against-cybercrime-60717238>
36. Skulkin, Oleg; Rezvukhin, Roman; Rogachev, Semyon, "Ransomware Uncovered 2020/2021," Group IB, March 2021, <https://www.group-ib.com/resources/threat-research/ransomware-2021.html>
37. Midler, Marisa. "Ransomware as a Service Threats," Carnegie Mellon University Software Engineering Institute Blog. October 5, 2020. <https://insights.sei.cmu.edu/blog/ransomware-as-a-service-raas-threats/>. See also Kost, Edward, "What is Ransomware as a Service (RaaS)? The dangerous threat to world security," UpGuard Blog, March 5, 2021. <https://www.upguard.com/blog/what-is-ransomware-as-a-service>
38. United States Department of the Treasury, "DPRK Cyber Threat Advisory: Guidance on the North Korean Cyber Threat," April 15, 2020. https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf
39. United States Department of the Treasury, "Treasury Sanctions Russia with Sweeping New Sanctions Authority," Press Release, April 15, 2021. <https://home.treasury.gov/news/press-releases/jy0127>
40. G7, "Ransomware Annex to G7 Statement," October 13, 2020, https://home.treasury.gov/system/files/136/G7-Ransomware-Annex-10132020_Final.pdf

41. Details about the NotPetya ransomware attack from: Perlroth, Nicole. *This is How They Tell Me the World Ends*, New York: Bloomsbury Publishing, 2021; and Greenberg, Andy. *Sandworm*, 2019. New York: Penguin Random House.
42. See, for example, Center for Internet Security, "CIS Controls," <https://www.cisecurity.org/controls/>.
43. See, for example, National Institute of Standards and Technology (NIST), "Small Business Cybersecurity Corner: Training," <https://www.nist.gov/itl/smallbusinesscyber/training>
44. Ibid
45. Cybersecurity & Infrastructure Security Agency (CISA), "Cyber Incident Response," <https://www.cisa.gov/cyber-incident-response>
46. Testimony from Donna F. Dodson, Chief Cybersecurity Advisor, National Institute of Standards and Technology, United States Department of Commerce, "Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure," <https://www.nist.gov/speech-testimony/strengthening-public-private-partnerships-reduce-cyber-risks-our-nations-critical>
47. Cybersecurity & Infrastructure Security Agency (CISA), "CISA Launches Campaign to Reduce the Risk of Ransomware," Press Release, January 21, 2021. <https://www.cisa.gov/news/2021/01/21/cisa-launches-campaign-reduce-risk-ransomware>
48. For more about "No More Ransom," see <https://www.nomoreransom.org>.
49. National Cyber Security Centre (NCSC), "Mitigating malware and ransomware attacks," February 13, 2020. <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>
50. Europol, "World's Most Dangerous Malware EMOTET Disrupted Through Global Action," Press Release, January 27, 2021. <https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action>
51. Other potential forums include the Five Eyes LE Group, Five Eyes AG Group, Tech Accord (PS), Global Banking Associations, Electronic Banking Group, European Banking Federation, Organisation for Security and Cooperation in Europe, World Economic Forum, and Ottawa F5 - AU.
52. Five Country Ministerial, "Five Country Ministerial Statement Regarding the Threat of Ransomware," April 7/8, 2021. <https://www.beehive.govt.nz/sites/default/files/2021-04/Five%20Country%20Ministerial%20Statement%20Regarding%20the%20Threat%20of%20Ransomware.pdf>
53. In October 2020, finance ministers from the Group of Seven called upon nations to implement Financial Action Task Force standards to reduce ransomware and other cyber crime. See Khan, Abdullah. "G7 finance ministers urge countries to adopt FATF standards against cybercrime," S&P Global Market Intelligence, Oct.13, 2020. <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/g7-finance-ministers-urge-countries-to-adopt-fatf-standards-against-cybercrime-60717238>
54. See Europol, "Joint Cybercrime Action Taskforce," <https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce>.
55. Chainalysis Team, "Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think," excerpt from the Chainalysis 2021 Crypto Crime Report, January 26, 2021, <https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021>
56. The Financial Crimes Enforcement Network (FinCEN) has proposed a rule to tighten compliance around convertible virtual currencies and digital assets. See Department of the Treasury, Financial Crimes Enforcement Network, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," <https://public-inspection.federalregister.gov/2020-28437.pdf>
57. See U.S. Department of Treasury, "Section 314(b) Fact Sheet," <https://www.fincen.gov/sites/default/files/shared/314factsheet.pdf>
58. Versprille, Allyson. "IRS's 'Operation Hidden Treasure' Focusing on Crypto Fraud," Bloomberg Tax, March 5, 2021. <https://news.bloombergtax.com/daily-tax-report/irs-operation-hidden-treasure-focusing-on-crypto-fraud>
59. See the International Organization for Standardization (ISO), <https://www.iso.org/publication-list.html>
60. National Institute of Standards and Technology (NIST), "Cybersecurity Framework," <https://www.nist.gov/cyberframework>

61. SecurityScorecard identified 10 security issues more prevalent in ransomware victims than other organizations; if companies addressed these issues they could lower their risk of a successful ransomware attack. See Peng, Tishun Peng and Sohval, Bob. "Organizations with Diligent Cybersecurity Less Likely to Fall Victim to Costly Ransomware," April 15, 2021. <https://securityscorecard.com/blog/organizations-with-diligent-cybersecurity-practices-less-likely-to-fall-victim-to-costly-ransomware-attacks>
62. See, for example, U.S. Department of Health and Human Services (HHS), "Ransomware Fact Sheet," <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>
63. Center for Internet Security, Malicious Domain Blocking and Reporting (MDBR), <https://www.cisecurity.org/ms-isac/services/mdbr/>
64. Cybersecurity & Infrastructure Security Agency (CISA), "Cyber Hygiene Services," <https://www.cisa.gov/cyber-hygiene-services>
65. Center for Internet Security, CIS Controls V7.1 Implementation Groups, <https://www.cisecurity.org/white-papers/cis-controls-v-7-1-implementation-groups/>
66. National Institute of Standards and Technology (NIST), "Cybersecurity Framework," <https://www.nist.gov/cyberframework>
67. Garcia, Michael. "Follow the Money: Few Federal Grants are Used to Fight Cybercrime," Third Way, February 16, 2021. <https://www.thirdway.org/report/follow-the-money-few-federal-grants-are-used-to-fight-cybercrime>
68. See "H.R.7898 - To amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes," <https://www.congress.gov/bills/116th-congress/house-bill/7898/text?r=2&s=1>
69. United States Cyberspace Solarium Commission, March 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QyJFqFkKf10MxIXJGT4yv/view
70. U.S. Department of Treasury, "Terrorism Risk Insurance Program," <https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/federal-insurance-office/terrorism-risk-insurance-program>
71. For more about the Structured Threat Information eXpression (STIX™), see <https://stixproject.github.io/>.
72. For more on the MITRE ATT&CK® Framework, see <https://attack.mitre.org>.
73. Congressional bill S. 4226 (116th): Assessing a Cyber State of Distress Act of 2020. <https://www.govtrack.us/congress/bills/116/s4226/summary>
74. Memorandum from Matthews, Denise, Director, Data Coordination and Statistical Analysis National Association of Insurance Commissioners and the Center for Insurance Policy and Research. "Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement," December 4, 2020. https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final_1.pdf
75. Marsh JLT Specialty, "Setting the Record Straight on Cyber Insurance," <https://www.marsh.com/us/insights/research/setting-the-record-straight-on-cyber-insurance.html>
76. See, for example, "Aon's E&O | Cyber Insurance Snapshot," <https://www.aon.com/cyber-solutions/wp-content/uploads/Aon-errors-and-omissions-cyber-insurance-snapshot.pdf>; "Cyber may never experience another soft market: Gallagher Re," Intelligent Insurer, April 14, 2021, <https://www.intelligentinsurer.com/news/cyber-may-never-experience-another-soft-market-gallagher-re-25350>; 2021 Cyber Insurance Market Conditions Report, <https://www.ajg.com/us/news-and-insights/2021/jan/2021-cyber-insurance-market-report>.
77. Hewitt Jones, John. "Cyber insurers tighten controls as ransomware pain increases," Inside P&C, September 28, 2020, <https://insuranceinsider.com/p-and-c/articles/135862/cyber-insurers-tighten-controls-as-ransomware-pain-increases>
78. See, for example, Doernberg, John, "Ransomware Causes Cyber Insurers to Raise the Bar," Gallagher, <https://www.ajg.com/us/news-and-insights/2021/apr/cyber-insurance-fight-against-ransomware>.
79. Studies addressing how cyber insurance may shape an organization's cybersecurity decision-making include: Romanosky, Sasha, Ablon, Lillian, Kuehn, Andreas, and Jones, Therese. "Content analysis of cyber insurance policies: how do carriers price cyber risk?" Journal of Cybersecurity, February 27, 2019, <https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419>; Harrison, Richard and Herr, Trey (editors). "Cyber Insecurity: Navigating the Perils of the Next Information Age," <https://www.cyberinsecuritybook.org/>; Sullivan, James and Nurse, Jason RC. "Cyber Security Incentives and the Role of Cyber Insurance," Royal United Services Institute for Defence and Security Studies and University of Kent. https://rusi.org/sites/default/files/246_ei_cyber_insurance_final_web_version.pdf

80. See, for example, Stone, Jeff. "FBI turns to insurers to grasp the full reach of ransomware," Cyberscoop, March 30, 2020, <https://www.cyberscoop.com/ransomware-fbi-insurance-companies-data/>; Lyngaas, Sean. "Inside the FBI's quiet 'ransomware summit,'" Cyberscoop, November 16, 2019, <https://www.cyberscoop.com/fbi-ransomware-summit/>
81. Chainalysis Team, "Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think," excerpt from the Chainalysis 2021 Crypto Crime Report, January 26, 2021, <https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021>
82. Protiviti, "Guide to US Anti-Money Laundering Requirements, Frequently Asked Questions, Sixth edition https://www.protiviti.com/sites/default/files/united_states/insights/guide-to-us-aml-requirements-6thedition-protiviti_0.pdf
83. Healey, Jason. "Innovation on cyber collaboration: Leverage at scale," Atlantic Council, May 3, 2018, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/innovation-on-cyber-collaboration-leverage-at-scale/>
84. Aspen Cybersecurity Group, "An Operational Collaboration Framework," November 8, 2018, <https://www.aspeninstitute.org/publications/an-operational-collaboration-framework/>
85. World Economic Forum, "Partnership Against Cybercrime: Insight Report," November 2020, http://www3.weforum.org/docs/WEF_Partnership_against_Cybercrime_report_2020.pdf
86. Cybersecurity & Infrastructure Security Agency (CISA), "Information Sharing and Analysis Organizations," <https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos>

Panel II: Recent Developments in E-Discovery

James H.S. Levine, Esquire

Troutman Pepper Hamilton Sanders LLP

Ian D. McCauley, Esquire

Morris James LLP

Laura G. Readinger, Esquire

Potter Anderson & Corroon LLP

James H. S. Levine

Partner
Wilmington

james.levine@troutman.com

D 302.777.6536



James is a seasoned litigator and trusted counselor. He has led litigation teams in cases involving corporate governance, corporate control, fiduciary duties, breach of contract, fraud, intellectual property, and trade secrets.

Areas of Focus:

- Business Litigation
- Corporate Governance
- Delaware Court of Chancery Litigation
- Patent Litigation
- Securities, Corporate Governance, and D&O Defense Litigation

James regularly represents clients in complex corporate and commercial disputes, including fiduciary duty and bet-the-company litigation, in Delaware state and federal courts, including the Delaware Court of Chancery, and in state and federal courts nationwide. He frequently serves as Delaware counsel in high stakes intellectual property disputes, including patent and trademark litigation. James also advises clients on proxy contests, challenges to corporate control, and transactional matters involving corporate governance principles and Delaware law issues.

He has extensive experience in Delaware corporate litigation, including the following types of matters:

- Breach of fiduciary duty actions brought against corporate officers and directors, LLC members and managers, and partners and limited partners.
- Motions for temporary restraining orders and preliminary injunctions.
- Contract and fraud claims arising out of merger agreements, asset purchase agreements, stock purchase agreements, and other commercial agreements.
- Business divorce and dissolution proceedings.
- Books and records demands and actions.
- Advancement and indemnification proceedings.

- Appraisal actions.
- Petitions to compel or enjoin arbitration.
- Statutory proceedings under the Delaware General Corporation Law.

James has served by judicial appointment as a special master in the Complex Commercial Litigation Division of the Delaware Superior Court, and has represented the Delaware Board of Bar Examiners in appeals related to Bar admission.

Prior to joining the firm, James practiced in the corporate/business services group of a national law firm, where he advised clients on mergers and acquisitions, as well as complex commercial transactions, and provided full life-cycle representation to the firm's corporate clients. He also served as deputy general counsel of an international nonprofit organization, advising the organization's board of directors and staff on legal matters (including fiduciary and constitutional issues), drafting and maintaining compliance and other policies, and coordinating litigation and insurance claims.

James was a member of the team that served as pro bono co-counsel with the American Civil Liberties Union of Delaware (ACLU) and Community Legal Aid Society, Inc. (CLASI) in bringing claims on behalf of mentally ill inmates who were held in solitary confinement by the Delaware Department of Correction. The case resulted in a successful settlement on behalf of the inmates, including improved conditions and mental health treatment services. In recognition of its efforts, the team received a number of awards in 2016-2017, including the ACLU's Clarence Darrow Award, CLASI's Founder's Award, the National Disability Rights Network (NDRN) Advocacy Award, and the Delaware State Bar Association's Christopher W. White Distinguished Access to Justice Leadership Award.

Representative Matters

Corporate/Fiduciary Litigation

- *Exit Strategy, LLC v. Festival Retail Fund BH, L.P., et al.*, C.A. No. 2017-0017-JTL (Del. Ch.) – represented the general partner and fiduciaries of a real estate holding company against claims for breach of contract and breach of fiduciary duties in connection with interpretation of L.P. Agreement.
- *Ogus v. SportTechie, Inc.*, C.A. No. 2018-0869-LWW (Del. Ch.) – represented a sports technology and analytics company in breach of contract/fiduciary duty litigation with co-founder over employment termination and equity valuation in connection with compulsory stock buyback.
- *Milligan v. Salamone, et al.*, Adv. No. 16-01078-tmd (Bankr. Ct. W.D. Tex.) – achieved favorable settlement for former CEO and director of financial services holding company against claims for breach of fiduciary duty, fraudulent transfer, and preferences.
- *iBio, Inc. v. Fraunhofer-Gesellschaft Zur Forderung Der Angewandten Forschung, E.V.*, C.A. No. 2017-0790-TMR (Del. Ch.) – obtained dismissal of \$300 million trade secret misappropriation lawsuit against a leading application-oriented research organization.
- *Aich v. McCarthy, et al.*, C.A. No. 11133-VCN (Del. Ch.) – achieved favorable settlement for acquirer of publicly-traded retail specialty corporation against aiding and abetting breach of fiduciary duty claims.

- *Harland Clarke Holdings Corp., et al. v. Milken*, C.A. No. 14-138-GMS (D. Del.) – achieved a complete defense victory for former CEO of an educational software company in a dispute seeking \$130 million in damages for alleged fraud and other claims arising out of the plaintiffs’ acquisition of the company.
- *Kastis v. Carter, et al.*, C.A. No. 8657-CB (Del. Ch.) – achieved favorable settlement for directors of biopharmaceutical company against claims for breach of fiduciary duty in connection with payment of contractual bonuses to company executives, and implementation of fee-shifting bylaw.
- *In re Solar Trust of America, LLC*, C.A. No. 12-11136(KG) (Bankr. Ct. D. Del) – obtained favorable settlements for liquidation trustee in multiple adversary proceedings, including actions for breach of contract, fraudulent transfers, and equitable subordination against former joint ventures, and breach of fiduciary duties against debtors’ former officers and directors.
- *In re Freeport-McMoran Copper & Gold Inc. Derivative Litig.*, C.A. No. 8145-VCN (Del. Ch.) – represented independent directors of acquirer against fiduciary duty claims in connection with \$20 billion acquisitions of two publicly traded oil and gas exploration corporations.
- *Weiss v. e-Scrub Systems, Inc. et al.*, C.A. No. 13-710-GMS (D. Del) – obtained dismissal of breach of fiduciary claims against former corporate director brought by corporate creditor (affirmed on appeal to Third Circuit).
- *Lindsey, et al. v. Zettacore, Inc., et al.*, C.A. No. 8550-VCL (Del Ch.) – represented acquirer of biotechnology assets against aiding and abetting breach of fiduciary duty claims.
- *Barovic v. Lechleiter, et al.*, C.A. No. 49D02-1308-MI-030458 (In. Super.) – successfully represented directors of global pharmaceutical company against fiduciary duty and waste claims in connection with settlement of FCPA claims against the company.
- *In re eResearchTechnology, Inc. Shareholders Litig.*, C.A. No. 7414-VCL (Del. Ch.) – achieved favorable settlement for directors of technological services and medical device company against claims for breach of fiduciary duty in connection with sale of the company to private acquirer.

Corporate Statutory Proceedings

- *Whalen v. Decision Sciences Int’l Corp.*, C.A. No. 2019-0997-JTL (Del. Ch.) – obtained favorable settlement for former CEO of security technology company in indemnification/advancement dispute.
- *Ephrat, et al. v. medCPU, Inc., et al.*, C.A. No. 2018-0852-MTZ (Del. Ch.) – obtained advancement for founders and former executives of medical technology company for fees incurred in business divorce and trade secret misappropriation action.
- *Dryden Capital Fund, LP vs. Special Diversified Opportunities, Inc.*, C.A. No. 2017-0347-AGB (Del. Ch.) – represented stockholder in action to compel production of books and records concerning proposed insider transactions and related claims of corporate mismanagement.
- *Lauderdale Holdings I, LLC v. Sunrise Detox III, LLC*, C.A. No. 12273-SG (Del. Ch.) – represented member of LLC operator of drug detoxification centers in action to compel production of books and records concerning company finances and operations.

- *McElroy v. Freeport-McMoRan Copper & Gold Inc.*, C.A. No. 8352-VCN (Del. Ch.) – represented a publicly traded mining company in action where stockholder seeking to inspect books and records failed to comply with statutory requirements.
- *Litterst v. Zenph Sound Innovations, Inc.*, C.A. No. 7700-ML (Del. Ch.) – represented dissolved Delaware corporation in action to inspect books and records, where the demanded records were no longer in the corporation’s possession.
- *Danenberg v. Fittracks, Inc.*, C.A. No. 6454-VCL (Del. Ch.) – secured advancement for former CEO of footwear technology company in underlying action alleging misrepresentations in merger negotiations.
- *Dlesk Family Fund v. Circuport, Inc.*, C.A. No. 7166-ML (Del. Ch.) – represented corporation opposing books and records demand on the ground that the demanding party was not actually a stockholder.
- *Levinhar, et al. v. MDG Medical, Inc.*, C.A. No. 4301-CS (Del. Ch.) – represented founders of Delaware corporation in post-merger appraisal proceedings to determine value of corporation stock.

Restrictive Covenants/Trade Secrets

- *U.S. Legal Support, Inc. v. Lucido, et al.*, C.A. No. 2021-0289-MTZ (Del. Ch.) – successfully defended preliminary injunction motion seeking to prevent former employee from competing and soliciting former employer’s clients.
- *CSC ServiceWorks, Inc. v. Rozsa, et al.*, C.A. No. 2021-0864-LWW (Del. Ch.) – represented former employee and new employer in action to enforce restrictive covenants and prevent employee from working in same industry but in a different capacity.
- *Hargray Communications Group, LLC et al. v. Abbasi*, C.A. No. 2021-0757-SG (Del. Ch.) – represent telecommunications company in action to prevent former employee from using former employer’s trade secrets and confidential information in similar position for new employer.
- *GOLO, LLC v. Seay, et al.*, C.A. No. 2017-0859-TMR (Del. Ch.) – obtained favorable settlement for nutraceutical company in disputes with terminated executive and new employer over disposition of company assets, tortious interference with contract, and trade secret misappropriation.
- *Rock-It Cargo USA, LLC v. Adis, et al.*, C.A. No. 2017-0615-TMR (Del. Ch.) – represented a logistics and live event planning company in dispute with former key employee over trade secret misappropriation and tortious interference with contract by new employer.

Commercial Litigation

- *The George Washington University, et al. v. District Hospital Partners, L.P., et al.*, C.A. No. 2019 CA 008019 B (D.C. Super) – represented a leading national university and its affiliated physician practice in breach of contract/fiduciary duty dispute with joint venture partner over operation of branded hospital.
- *Royce Management, Inc., et al. v. Bank of America, N.A., et al.*, C.A. No. OCN L 001353-21 (N.J. Super.) – defended a leading financial institution in dispute over compliance with subpoena for depositor records, where depositor alleges breach of contract and violation of rights under N.J. Constitution.

- *Nokia Solutions and Networks OY v. Collision Communications, Inc.*, C.A. No. N19C-10-262 AML CCLD (Del. Super.) – represented licensor in breach of contract dispute concerning licensing and development of software for use in cellular products.
- *Ephrat, et al. v. medCPU, Inc., et al.*, C.A. No. 2017-0493-MTZ (Del. Ch.) – represented founders and former executives of medical technology company in breach of contract action, and defended counterclaims for breach of contract and trade secret misappropriation.
- *Wilmington Savings Fund Society, FSB v. Foresight Energy LLC*, C.A. No. 11059-VCL (Del. Ch.) – represented borrower entities in dispute over terms of bond indenture and impact of alleged change of control transaction.
- *ESG Capital Partners II, LP, et al. v. Passport Special Opportunities Master Fund, LPA*, C.A. No. 11053-VCL (Del. Ch.) – represented limited partners in dispute over distribution of partnership proceeds.
- *Markow, et al. v. Synageva BioPharma Corp.*, C.A. No. N15C-06-152 WCC CCLD (Del. Super.) – represented a publicly traded biopharmaceutical company in putative class action concerning alleged breach of terms of new employees’ stock option grants.
- *NewSpring Mezzanine Capital II, L.P. v. Hayes, et al.*, C.A. No. 14-1706-GAM (E.D. Pa.) – represented post-closing purchaser in action for indemnification, fraud and breach of contract claims against sellers, or alternatively seeking rescission of transactions, including defending cross-claims by sellers for fraud, breach of contract, and securities law violations.
- *Platypus Holdings, LLC v. Russell, et al.*, C.A. No. 14-00999-NIQA (E.D. Pa.) – defended limited partners against breach of contract claims and prosecuted counterclaims seeking rescission of capital contributions to investment vehicle secured by, and breach of contract arising from, general partner’s misrepresentations.
- *Goldfinger v. MPC Holding Establishment, et al.*, C.A. No. 6207-CS (Del. Ch.) – successfully represented investor in action to pierce the corporate veil and damages for fraudulent transfers in connection with efforts to collect on multimillion dollar judgment in prior action between the parties.

Escrow/Earnout/Working Capital Disputes

- *Thorp v. PerkinElmer Holdings, Inc.*, C.A. No. 8060-VCP (Del. Ch.) – represented stockholder representative in action concerning calculation of post-closing earnout payment.
- *Alco Industries, Inc. v. Quest Specialty Coatings, LLC, et al.*, C.A. No. 9357-VCP (Del. Ch.) – represented seller of business division in dispute over post-closing indemnification and pre-closing compliance with agreement terms.
- *Utilipath, LLC v. Hayes, et al.*, C.A. No. 9992-VCP (Del. Ch.) – successfully represented post-closing purchaser in action to compel arbitration in dispute over post-closing net working capital adjustment.
- *Shareholder Representative Services LLC v. Hospitalists Management Group, LLC*, C.A. No. 7772-VCN (Del. Ch.) – represented stockholder representative in action challenging indemnity claim against an escrow fund established in connection with merger transaction.

Business Divorce

- *Weiss v. Preston, et al.*, C.A. No. 2017-0818-MTZ (Del. Ch.) – represented member in suit to compel judicial dissolution of two joint ventures that operate continuing care retirement communities.
- *Auritec Pharmaceuticals, Inc. v. Eupraxia Holdings, Inc.*, C.A. No. 2017-0019-TMR (Del. Ch.) – represented stockholder in suit to compel judicial dissolution of joint venture pharmaceutical company, including assertion of counterclaims for breach of contract, fraudulent inducement, and negligent misrepresentation.

Health Care Litigation

- *Talley v. Christiana Care Health System, et al.*, C.A. No. 17-926-CJB (D. Del.) – obtained dismissal of antitrust claims and summary judgment in favor of largest health system in Delaware and its executives on breach of contract, tortious interference, and defamation claims arising from termination of former staff physician’s privileges.
- *The Nemours Foundation v. Unison Health Plan of Delaware Inc.*, C.A. No. 15-319-RGA (D. Del.) – represented large pediatric medical services provider in dispute with health insurer over insurer’s compliance with the parties’ agreements.

Securities Litigation

- *In re Wilmington Trust Securities Litig.*, C.A. No. 10-990-RGA (D. Del.) – represented independent directors of an international commercial bank against claims arising under Sections 11 and 15 of the Securities Act of 1933 and 10(b) and 20(a) of the Securities Exchange Act of 1934.
- *Frater v. Hemispherx BioPharma, Inc., et al.*, C.A. No. 12-7152-WY (E.D. Pa.) – achieved favorable settlement for biopharma company and certain of its officers against claims arising under 10(b) of the Securities Exchange Act of 1934.
- *Anderson v. PolyMedix, Inc.*, C.A. No. 12-3721-MAM (E.D. Pa.) – achieved favorable settlement for former corporate officers of biopharma company against claims arising under 10(b) of the Securities Exchange Act of 1934.

Intellectual Property Litigation

- *Align Technology, Inc. v. 3Shape A/S, et al.*, multiple actions (D. Del.) – represented the developer and manufacturer of dental 3D scanners and software solutions in multiple actions for patent infringement.
- *Acera Surgical, Inc., et al. v. Nanofiber Solutions, LLC, et al.*, C.A. No. 20-980-CFC (D. Del.) – defended the designer and manufacturer of nanofiber products against claims of patent infringement.
- *Nanexa AB v. VitriVax, Inc.*, C.A. No. 21-764-CFC (D. Del.) – represented a patent owner drug delivery company in infringement dispute with competitor over nanoparticle technology.
- *TableSafe, Inc. v. DinerIQ, Inc.*, C.A. No. 20-699-LPS (D. Del.) – represented patent owner pursuing claims of patent infringement and inducement for use of proprietary retail payment technology.
- *In-Depth Test LLC v. Vishay Intertechnology Inc.*, C.A. No. 14-888-CFC (D. Del.) – successfully defended semiconductor manufacturer against claims of patent infringement arising from claimed patent for testing process (patent was invalidated on Section 101 motion).

- *Green Mountain Glass et al v. Saint-Gobain Containers, Inc.*, C.A. No. 14-392-GMS (D. Del.) – defended glass manufacturer against patent infringement claims arising from method for mixing colored cullet glass.
- *Collection Marketing Center, Inc., et al. vs. Apollo Enterprise Solutions, Inc.*, C.A. No. 10-870-BMS (D. Del) – successfully represented patent holder in declaratory judgment action for non-infringement and patent invalidity.

Financial Services Litigation

- *Bank of America, N.A. v. Sea-Ya Enterprises, LLC, et al.*, C.A. No. 11-445-RGA (D. Del.) – obtained summary judgment for lender against borrower and guarantors following default on \$6 million commercial aircraft loan.
- *Lambert v. TD Bank, N.A.*, C.A. No. N10C-07-267 RRC (Del. Super.) – obtained dismissal of putative class action concerning alleged overcharging of administrative fees to holders of bank-issued gift cards.
- *Browning v. Data Access Systems, Inc., et al.*, C.A. No. N09C-10-248-FSS (Del. Super.) – obtained dismissal of putative class action alleging conversion, breach of contract, breach of the implied covenant of good faith and fair dealing, tortious interference, civil conspiracy, and unjust enrichment Delaware in connection dispute over withholding third party funds in ATM security dispute.
- *Data Access Systems, Inc. v. First Bank of Delaware, et al.*, C.A. No. 4784-CS, 4790-CS (Del. Ch.) – obtained favorable settlement of claims alleging conversion, negligence, breach of contract, and tortious interference, and affirmative claims of fraud and breach of contract, in dispute concerning financial institution’s sponsorship termination of affiliate members of Visa and MasterCard networks.
- *Premier Payments Online Inc vs First Bank of Delaware*, C.A. No. 6544-VCP (Del. Ch.) – obtained favorable settlement of dispute concerning termination of merchant ISO agreement.

Related Practices and Industries

- Delaware Court of Chancery Litigation
- Corporate Governance
- Business Litigation
- Litigation
- Securities, Corporate Governance, and D&O Defense Litigation
- Class Action

Publications

- Co-author, “[Common M&A Provision Precludes Private Equity Buyer From Escaping an Aiding and Abetting Claim](#),” *Troutman Pepper*, December 10, 2021.
- Co-author, “[Legal or Not, It’s Working: Mandatory Board Diversity for Publicly-held Companies Headquartered in the Golden State](#),” *Westlaw Today*, April 7, 2021.

Speaking Engagements

- Panelist, “[Recent Developments in Data Security and E-Discovery 2021](#),” Delaware State Bar Association, December 15, 2021.
- Presenter, [Troutman Pepper’s Annual Antitrust CLE Event](#), December 8, 2021.
- Moderator, “[Hot Topics in Blockchain Technology 2021](#),” Delaware State Bar Association, July 13, 2021.
- Panelist, “[Recent Developments in Data Security and E-Discovery](#),” Delaware State Bar Association, November 18, 2020.
- Panelist, “The Litigator and Corporate Counsel—Who Needs What?,” Litigation Section of the Delaware State Bar Association, November 10, 2020.
- Co-speaker, “[What Delaware Lawyers Need to Know About Privacy Law](#),” E-Discovery & Technology Section of the Delaware State Bar Association, June 22, 2020.
- Speaker, “[Recent Developments in Data Security and E-Discovery](#),” E-Discovery & Technology Section of the Delaware State Bar Association, October 8, 2019.
- Speaker, “[Recent Developments in Data Security and E-Discovery](#),” E-Discovery & Technology Section of the Delaware State Bar Association, November 14, 2018.
- Speaker, “[Sophisticated Deposition Strategies](#),” National Business Institute, October 19, 2018.
- Moderator, “[Blockchain II: Where No Contract Has Gone Before](#),” DSBA’s 2018 Bench and Bar Conference, June 15, 2018.
- Speaker, “[Sophisticated Deposition Strategies](#),” National Business Institute, November 17, 2017.
- Speaker, “[Recent Developments in Data Security and E-Discovery](#),” E-Discovery & Technology Section of the Delaware State Bar Association, November 14, 2017.
- Speaker, “[Preparing for Electronic Discovery in Litigation](#),” National Business Institute’s Advanced Employment Law Seminar, December 14, 2016.
- Moderator, “[Managing E-Discovery Effectively: Meeting the Expectations of Your Clients and the Court](#),” Delaware State Bar Association, October 15, 2015.
- Moderator, “[E-Discovery for the Mid-Size Case](#),” E-Discovery & Technology Section of the Delaware State Bar Association, April 30, 2015.

Professional and Community Involvement

- Member, Board of Editors, *Delaware Lawyer*
- Associate Member, Delaware Board of Bar Examiners
- Chair, E-Discovery & Technology Law Section; Council Member, Litigation Section; Member, Corporation Law Section, Delaware State Bar Association
- Immediate Past President of the Delaware Chapter, Villanova Law Alumni Association
- Barrister Group Leader, Richard S. Rodney American Inn of Court

Rankings and Recognition

- *Best Lawyers: Ones to Watch*: Commercial Litigation (2021, 2022), Corporate Law (2022)

- Rated AV Preeminent by *Martindale-Hubbell®* (2014-2020)
- Selected for inclusion on the 2017 *Delaware Rising Stars* list

Bar Admissions

- Delaware
- New Jersey
- Pennsylvania

Court Admissions

- U.S. District Court, District of Delaware
- U.S. District Court, Eastern District of Pennsylvania
- U.S. District Court, District of New Jersey
- U.S. Court of Appeals, Third Circuit

Education

- Villanova University Charles Widger School of Law, J.D., *magna cum laude*, 2007; Articles Editor, *Villanova Law Review*; Chairman, Honor Board; Order of the Coif
- University of Delaware, B.A., 2000; Criminal Justice; President, Kappa Sigma Fraternity; Delaware Undergraduate Student Congress

Clerkships

- Hon. Lawrence F. Stengel, U.S. District Court for the Eastern District of Pennsylvania, 2006



Ian D. McCauley

Partner T: 302.888.6919 F: 302.504.9738

imccauley@morrisjames.com

500 Delaware Avenue, Suite 1500
Wilmington, DE 19801

Ian McCauley is a Partner in Business Litigation group and leads the firm's eDiscovery practice. Ian's practice is focused on electronic discovery from the anticipation to the conclusion of litigation. Ian has significant experience advising litigants in the Court of Chancery, Superior Court, and District Court on making defensible, efficient, and strategic decisions regarding the preservation, collection, and production of electronically stored information (ESI). Ian's approach employs common sense solutions while emphasizing effective project management and leveraging of emerging technology. His approach is designed to defensibly control the ever-growing costs associated with discovery while providing his clients with a strategic advantage in litigation. In addition to eDiscovery, Ian advises clients and co-counsel on litigation readiness, information governance, and data privacy issues.

Ian has been recognized by his peers as a Top Lawyer in the area of eDiscovery in Delaware Today Magazine. He frequently presents on eDiscovery topics and has been invited to speak at LegalTech New York, the Master's Conference, Widener University Delaware Law School, and the Delaware Department of Justice.

Experience

- Drafting and implementing preservation and collection plans for and in anticipation of litigation
- Participating in Rule 26(f) conferences and negotiating ESI protocols and agreements among various groups of counsel
- Serving as eDiscovery liaison in Delaware Bankruptcy matters
- Drafting discovery related motion practice
- Developing repeatable but flexible best practices for the handling of all aspects of the EDRM (Electronic Discovery Reference Model)

My goal is to demystify eDiscovery for my clients, ensuring that the process is efficient while providing a strategic advantage in litigation.

Practice Areas

eDiscovery

Corporate and Fiduciary
Litigation

Honors

Delaware Today Top Lawyers,

- E-Discovery/Technology, 2014 - 2020
- Cyber Security + Technology, 2021

Clerkships

Extern for The Honorable
Anthony A. Sarcione, Court of
Common Pleas of Chester
County

Admissions

Delaware, 2013
Pennsylvania, 2008
U.S. District Court for the District
of Delaware

Education

Villanova University School of
Law, JD, 2007
Cornell University, BA, 2001

Ian D. McCauley (Continued)

- Managing large-scale reviews of ESI for both internal investigative and production purposes

Speaking Engagements

- Recent Developments in Data Security and E-Discovery (November 14, 2018)
- Annual Convention of the Delaware Trial Lawyers Association – Discovery Overview (June 15, 2018)
- Annual Meeting of the Employment Section of the DSBA - The State of Delaware Privacy Law (March 27, 2018)
- LegalTech New York 2018 - Forecast Calls for Cloud Computing - Lawyers Are In Full Bloom When They Embrace What the Cloud Can Do For Them (January 30, 2018)
- Delaware Department of Justice - eDiscovery Basics (January 24, 2018)
- Recent Developments in Data Security and E-Discovery (November 14, 2017)
- The Master's Conference - Washington, DC 2017 - Forces Changing eDiscovery (October 13, 2017)
- ALFA International's Business Litigation Practice Group Seminar - Materials Only (September 15, 2017)
- Philadelphia eDiscovery Speaker Series – The Art of the Litigation Hold (April 4, 2017)
- Annual Meeting of the Employment Section of the DSBA – E-Discovery: A Practical Guide (March 28, 2017)
- The Master's Conference – Washington, DC 2016 - eDiscovery Project Management (October 18, 2016)
- The Master's Conference – New York 2016 - From Case Management to Case Intelligence: Surfacing Legal Business Intelligence (July 11, 2016)
- 2016 DSBA Women and the Law Section Retreat – Enough With the Selfie (March 4, 2016)
- Delaware Department of Justice 2015 Retreat (October 30, 2015)
- Managing E-Discovery Effectively (October 15, 2015)
- National Bar Institute - Discovery Under the New Federal Rules of Civil Procedure (September 25, 2015)
- Delaware Department of Justice 2014 Retreat (October 16, 2014)

Professional Affiliations

Delaware Supreme Court Commission on Law and Technology, Associate Member
Richard K. Herrmann Technology American Inn of Court, Executive Committee Member
Delaware State Bar Association
American Bar Association
International Legal Technology Association

Community Affiliations

Committee of Seventy Voter Protection Program
Free to Breathe

Ian D. McCauley (Continued)

Articles & Publications

Vendor Contracting for Privacy and Security

September 2017

Law Journal Newsletters, Cybersecurity Law & Strategy

What Non-Delaware Lawyers Need to Know About e-Discovery in Delaware

April 14, 2016

LJN'S Legal Tech Newsletter

Laura G. Readinger

eDiscovery Counsel

Pronouns: she / her / hers

Laura G. Readinger is eDiscovery Counsel in the firm's Corporate Litigation and Commercial Litigation groups. She counsels clients and co-counsel on the many challenges associated with eDiscovery. She provides cost-effective and efficient project management solutions to clients in what is a complex and continually changing area of the law. Laura is also a Certified E-Discovery Specialist (CEDS) by the Association of Certified E-Discovery Specialists.

Laura has considerable experience working on cases in both Delaware and Pennsylvania. She has practiced in the Court of Chancery, the Superior Court, including the Complex Commercial Litigation Division, and the District Court. Laura has been recognized by her peers as a Top Lawyer in the area of eDiscovery and Technology in *Delaware Today* Magazine for the last five years.

Laura speaks fluent Spanish.

REPRESENTATIVE MATTERS

- Consulting on document preservation and defensible document collections
- Conducting custodian interviews
- Drafting document collection plans
- Drafting discovery-related motions and responses
- Selecting and communicating with vendors
- Using early case assessment and advanced analytic techniques, such as threading and predictive coding
- Managing large-scale reviews of electronically stored information in various platforms, including Relativity, Logikcull, Eclipse, Concordance, and Ringtail
- Conducting in-depth confidentiality and privilege analysis
- Drafting privilege logs
- Managing the review and production of documents for discovery, deposition preparation, and trial
- Advising on eDiscovery best practices



Wilmington
Hercules Plaza
1313 North Market Street, 6th Floor
P.O. Box 951
Wilmington, Delaware 19801

T: 302.984.6167
F: 302.658.1192
lreadinger@potteranderson.com

EDUCATION

The Ohio State University Moritz
College of Law, J.D., 2007
Cornell University, B.A., 2004

BAR & COURT ADMISSIONS

Delaware, 2016
Pennsylvania, 2011
New York, 2008
Ohio, 2008 (inactive)

PRACTICE AREAS

Business & Commercial Litigation
Commercial Litigation
Corporate Law
Corporate Litigation

PROFESSIONAL ACTIVITIES AND HONORS

- Delaware State Bar Association
- American Bar Association
Business Law Section,
Business and Corporate
Litigation Committee, Co-Chair
of the Communications and
Technology Subcommittee and
Vice Chair of the eDiscovery
Subcommittee
- Richard K. Herrmann
Technology American Inn of
Court, eDiscovery Pupilage

RECENT NEWS

Potter Anderson Announces New eDiscovery Counsel
Laura G. Readinger Joins Leading Delaware Law Firm
December 1, 2020

RECENT EVENTS & SPEAKING ENGAGEMENTS

Readinger Weighs in on Recent Developments in E-Discovery
December 15, 2021

- Richard S. Rodney Inn of Court
- Delaware Hispanic Bar Association, President (former Vice President)
- Hispanic Bar Association of Pennsylvania, Advisory Board Member (former Treasurer, Vice President, and Vice President of Communications)
- Hispanic National Bar Association (former Deputy Regional President of Region IV) – Top Lawyers Under 40 Award 2020
- Women in eDiscovery
- The Office of the Child Advocate, Delaware, counsel on behalf of abused and neglected children
- *Delaware Today* Top Lawyers, eDiscovery and Technology, 2016-2020



Vince Catanzaro is Senior Counsel, eDiscovery for FedEx. Vince is a nationally recognized innovator and team builder with 20+ years' experience in litigation and discovery contexts on both large and small scale projects. He is responsible for providing e-discovery and legal technology support to litigation teams and e-discovery program managers and for maintaining, enhancing, and providing strategic guidance regarding e-discovery tools, protocols, and best practices. Previously Vince was Senior Counsel in the eData Practice group of Morgan, Lewis, & Bockius, LLP and Of Counsel at Shook, Hardy, & Bacon LLP where he worked with clients to develop eDiscovery best practices as well as untangling issues related to data preservation, litigation management and international and cross-border collection. Vince began his career in eDiscovery at DuPont where he served as Senior Counsel, Global Discovery Manager as he was responsible for counseling the Company concerning how best to comply with evolving legal standards relating to discovery and information management including use of social media, guiding and supporting the legal teams in the development of e-discovery response strategies and the use of litigation technology.

**The DSBA Section of E-Discovery and Technology Law
Presents Recent Developments in Data Security and E-Discovery
Dec. 15, 2021**

Materials and Recommended Reading:

Delaware Lawyers' Rules of Professional Conduct:

<https://courts.delaware.gov/odc/rules.aspx>

Rule 1.1, including Comment 8 – Competence

Rule 1.4 – Communication with clients

Rule 1.6(a) & (c), including Comments 18-20 – Confidentiality

Rules 1.9(c) & 1.6 Comment 21 – Duties to former clients

Rule 1.15 – Safekeeping of client property

Rules 5.1, 5.2, 5.3 – Responsibilities to supervise attorneys and non-attorney assistants

Delaware Supreme Court Commission on Law & Technology:

Leading Practices on technology topics: <http://courts.delaware.gov/declt/practices.aspx>

Delaware Code:

<http://delcode.delaware.gov/>

6 Del. C. § 12B-101 et seq. – Computer Security Breaches

6 Del. C. § 5001C et seq. & 19 Del. C. § 736 – Safe Destruction of Records Containing PII

6 Del. C. § 1201C et seq. – Online and Personal Privacy Protection

14 Del. C. § 8101A et seq. – Student Data Privacy Protection Act

18 Del. C. § 8106 et seq. – Insurance Data Security Act (HB 174, signed into law July 31, 2019)

ABA and Other Formal Opinions:

http://www.americanbar.org/groups/professional_responsibility/publications/ethics_opinions.html

99-413 – Protecting the Confidentiality of Unencrypted E-Mail (Mar. 10, 1999)

06-442 – Review and Use of Metadata (Aug. 5, 2006)

08-451 – Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services (Aug. 5, 2008)

11-459 – Duty to Protect the Confidentiality of E-Mail Communications with One's Client (Aug. 4, 2011)

11-460 – Duty When Lawyer Receives Copies of Third Party's E-mail Comm's with Counsel (Aug. 4, 2011)

17-477R – Securing Communication of Protected Client Information (May 22, 2017)

18-482 – Ethical Obligations Related to Disasters (Sept. 19, 2018)

18-483 – Lawyers' Obligation After an Electronic Data Breach or Cyberattack (Oct. 17, 2018)

20-495 – Lawyers Working Remotely (Dec. 16, 2020)

21-496 – Responding to Online Criticism (Jan. 13, 2021)

21-498 – Virtual Practice (March 10, 2021)

Cal. Formal Op. 2020-203 – Unauthorized Access to Electronic Client Confidential Information

Maine Op. 2019-220 – Cyberattack and Data Breach: the Ethics of Prevention and Response

Pa. 2020-300 – Ethical Obligations for Lawyers Working Remotely

State Bar of Cal. Standing Comm. on Prof. Resp. and Conduct Formal Op. No. 20-0004 (remote work)

DSBA Committee on Professional Ethics Formal Op. 2021-1 (July 9, 2021) (remote work)

Fla. Bar re: Advisory Op. – Out-of-State Attorney Working Remotely from Fla. Home, No. SC20-1220 (Fla. May 20, 2021) (upholding advisory opinion on attorney's remote practice)

Court of Chancery Materials:

Guidelines to Help Lawyers Practice in the Court of Chancery –

- <https://courts.delaware.gov/forms/download.aspx?id=99468>
- DG BF, LLC, et al. v. Michael Ray, et al.*, C.A. No. 2020-0459-MTZ (Nov. 19, 2021)
 - <https://courts.delaware.gov/Opinions/Download.aspx?id=326670>
- Fortis Advisors LLC v. Johnson & Johnson, et al.*, C.A. No. 2020-0881-LWW (Sept. 21, 2021)
 - <https://courts.delaware.gov/Opinions/Download.aspx?id=324610>
- In Re Howard Midstream Energy Partners, LLC*, C.A. No. 2021-0487-LWW (Sept. 22, 2021)
 - <https://courts.delaware.gov/Opinions/Download.aspx?id=324620>
- In re WeWork Litigation*, C.A. No. 2020-0258-AGB (Dec. 22, 2020)
 - <https://courts.delaware.gov/Opinions/Download.aspx?id=314490>

Internet E-Discovery “Ripped From the Headlines” Resources

- Sandy Hook/Alex Jones
 - https://www.abajournal.com/news/article/infowars-host-who-called-sandy-hook-shootings-a-giant-hoax-is-liable-in-defamation-default-judgment?utm_medium=email&utm_source=salesforce_451631&sc_sid=00121300&utm_campaign=monthly_email&promo=&utm_content=&additional4=&additional5=&sfmc_id=451631&sfmc_s=45491561&sfmc_l=1528&sfmc_ib=20003&sfmc_mid=100027443&sfmc_u=13235217
- Arnold & Porter, Inserted Documents
 - https://www.abajournal.com/news/article/arnold-porter-slipped-discovery-documents-into-database-without-notice-referee-says?utm_medium=email&utm_source=salesforce_451631&sc_sid=00121300&utm_campaign=monthly_email&promo=&utm_content=&additional4=&additional5=&sfmc_id=451631&sfmc_s=45491561&sfmc_l=1528&sfmc_ib=20003&sfmc_mid=100027443&sfmc_u=13235213
- Jon Gruden/NFL Investigation
 - <https://www.wsj.com/cdn.ampproject.org/c/s/www.wsj.com/amp/articles/jon-gruden-emails-investigation-washington-football-team-11634079234>
 - <https://www.mikemcbrideonline.com/2021/10/an-important-ediscovery-lesson-from-jon-gruden/>

Formatted: Font: Arial Narrow, Bold

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: Not Bold, Italic

Formatted: Normal, Indent: Left: 0", First line: 0", Right: 0", No widow/orphan control

Formatted: List Paragraph, Right: 0", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5", No widow/orphan control

Formatted: Normal, Indent: Left: 0", First line: 0", Right: 0", No widow/orphan control

Formatted: Font: Bold

Formatted: Font: Arial Narrow

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: List Paragraph, Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1.25"

Field Code Changed

Formatted: Hyperlink, Font: Arial Narrow

Formatted: Font: Arial Narrow

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: Arial Narrow

Formatted: List Paragraph, Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1.25"

Field Code Changed

Formatted: Hyperlink, Font: Arial Narrow

Formatted: Font: Arial Narrow

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: Arial Narrow

Formatted: List Paragraph, Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1.25"

Field Code Changed

Formatted: Hyperlink, Font: Arial Narrow

Formatted: Font: Arial Narrow

Formatted: List Paragraph, Right: 0", Bulleted + Level: 2 + Aligned at: 0.75" + Indent at: 1.25", No widow/orphan control

Field Code Changed

Formatted: Hyperlink, Font: Arial Narrow



Recent Developments in E- Discovery

Vince Catanzaro, Esq.

James Levine, Esq.

Federal Express Corporation Troutman Pepper Hamilton Sanders LLP

Ian McCauley, Esq.

Laura Readinger, Esq.

Morris James LLP

Potter Anderson & Corroon LLP



Disclaimer

The views, opinions, or information expressed during this CLE are solely those of the speakers and do not necessarily reflect those of their employers or clients.



Agenda

- Delaware Trends
- Delaware Case Law
- National Trends
- National Case Law
- Ripped From the Headlines



Delaware Trends

- Court of Chancery Guidelines Have Been Revised
 - Mission Statement – goose and gander
 - Preservation
 - eDiscovery is now default
 - Meet and confer is now default
 - Scope of privilege
 - Non-party subpoenas
 - Expedited Discovery
 - Emphasis on Discovery Facilitators



Delaware Case Law Emphasis

- Control Issues
- Privilege Issues
- Transparency and document searching issues



Key Delaware Cases

- *In re WeWork Litigation*, C.A. No. 2020-0258-AGB (Dec. 22, 2020)
In re Dell Technologies Inc., Consol. C.A. No. 2018-0816-JTL (Sept. 17, 2021)
 - Both cases deal with custodians using non-company email accounts
 - Also involves scope of privilege based on the usage of those email accounts.
- *Fortis Advisors LLC v. Johnson & Johnson, et al.*, C.A. No. 2020-0881-LWW (Sept. 21, 2021)
 - Case deals with several issues related to custodians and proportionality
- *In Re Howard Midstream Energy Partners, LLC*, C.A. No. 2021-0487-LWW (Sept. 22, 2021)
 - When adversity arises and its impact on privilege
- *DG BF, LLC, et al. v. Michael Ray, et al.*, C.A. No. 2020-0459-MTZ (Nov. 19, 2021)
 - General discovery misconduct resulting in dismissal



National Trends

- The impact of the pandemic on the usage, storage, and discovery of ESI
 - Client Impact
 - Outside Counsel Impact
 - Vendor Impact
- Unique Challenges
 - Conducting discovery whose relevant period occurs on or after March, 2020.
 - Ephemeral Data and Proliferation of Chat Applications



Case Law Outside of Delaware

- *In Re Skanska*, No. 3:20-CV-05980-LC/HTC (N.D. Fla Aug. 23, 2021)
- *Benebone LLC v. Pet Qwerks, Inc.*, 2021 WL 831025 (C.D. Cal. Feb. 18, 2021)
- *FTC v. Noland*, Case No. 20-cv-00047 DWL (D. Ariz. Aug 30, 2021)
- *Tigi Linea Corp. v. Professional Products Group*, Case No. 4:19-cv-00840-RWS-KPJ (E.D. Texas, Sherman Division, May 14, 2021)



eDiscovery in the News

- Alex Jones/Sandy Hook
 - Discovery Orders
 - Ultimate sanction
- Arnold and Porter Issue
 - Slipping of document into litigation database
- Jon Gruden Investigation
 - Control Issues
 - Retention Issues
 - Expectation of Privacy Issues



Questions?

