

DELAWARE STATE BAR ASSOCIATION

PRESENTS

# CYBER SECURITY FOR THE NEW NORMAL IN LAW PRACTICE 2021

**LIVE SEMINAR AT DSBA WITH ZOOM OPTION**

---

SPONSORED BY THE DELAWARE STATE BAR ASSOCIATION

**THURSDAY, SEPTEMBER 9, 2021 | 11:00 A.M. TO 12:00 P.M.**

**1.0 Hour 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.*

# CYBER SECURITY FOR THE NEW NORMAL IN LAW PRACTICE 2021

## ABOUT THE PROGRAM

Law firms, in particular, are currently under siege from clever cybercriminals on the hunt for a variety of enticing and lucrative data. The often-costly consequences of cyberattacks, both financially and to a firm's reputation, are inevitable and in many cases can put a firm out of business.

This webinar presentation will discuss:

- Covid-19 Effects on Cyber Threats
- Why Law Firms are Being Threatened
- Cyber Losses
- Risk Management
- Cyber Insurance

## PRESENTER

Michael Mooney, Senior Vice President  
*USI Affinity*

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 12/31/2021.

### REGISTRATION INFORMATION AND RATES

This CLE will be conducted live and via Zoom. To register, visit [www.dsba.org/cle](http://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](mailto: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.

# CYBER SECURITY FOR THE NEW NORMAL IN LAW PRACTICE 2021



---

Michael Mooney, Senior Vice President  
*USI Affinity*



# Real World Cyber Risks for Attorneys





Mike Mooney  
Senior Vice President  
Professional Liability Practice Leader  
USI Affinity

---

# AGENDA

Covid-19 Effects on Cyber Threats

Why Law Firms

Cyber Losses

Cyber Insurance

Risk Management

Live Question & Answer Session

# Covid-19 Effects

## Increased Attacks

Up to a 700% increase in phishing emails, including BEC – Theft of Funds

Attacks on devices and remote network vulnerabilities

- Network/Device Mapping, Inventory, Security and Patching

Business Associate, Software Supply Chain and Cloud Attacks – Theft of Data

- Data Mapping, Vendor Risk Management Program, BAA, Cyber Insurance

Ransomware Attacks – Patient Care and Safety Issue. Encryption of Data

- Redundant Offline Backups, Patching, Incident Response Plan and Exercise

Theft of COVID Related Research, Treatment Protocols and Vaccine Research

- Risk Management Program to Identify Risk and Protect Research and Preserve Government Funding

# Target Rich Environment

National Security

Intellectual Property

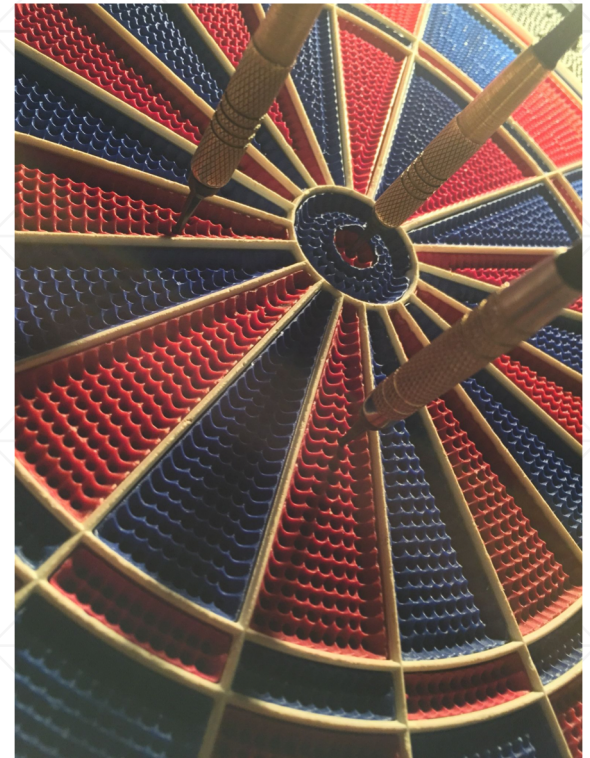
Business Intelligence

Protected Health Information

Bank Account and Credit Card Information

Personally Identifiable Information

Attorney IOLA/escrow account funds





# CYBER EXPOSURES – LAW FIRMS ARE PRIME TARGETS

## Rich Collection of Data

- Sensitive Information
- Bank Information
- PII

## Poor Safeguards

- Lack of internal training and controls
- Lack of IT resources
- Wireless access
- Vendor Management
- Lost or stolen devices

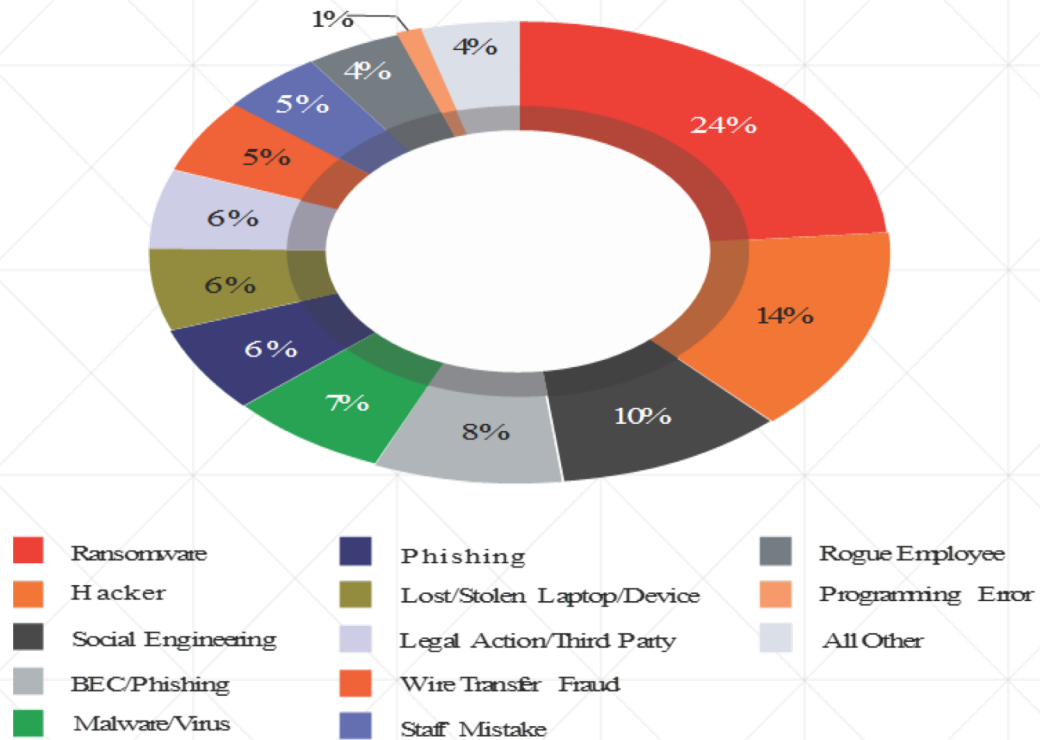
## Internal Exposures

- Rogue employees
- Careless staff

## External Exposures

- Business associates, vendors and suppliers
- Organized crime
- Hackers

# CLAIM STATISTICS – BY CAUSE OF LOSS



Source: NetDiligence Cyber Claims Study

## High Cost of Data Breach

### IBM Security: Cost of a Data Breach Report 2021

- \$4.24 Million → Global Average (highest average in 17 history of report)
- \$180 average cost for lost or stolen record for PII data
- \$9.05 Million → United States Average
- Average cost was \$1.07 Million higher where remote work was a factor in breach
- Compromised credentials responsible for 20% of breaches
- Security AI and automation provided the biggest cost mitigation. Organizations with security AI and automation had breach costs \$3.81 million less than organizations without it.

# CYBER EXPOSURES – CYBER LOSS

- Loss or damage to data/information
- Loss of revenue due to a computer attack
- Extra expense to recover/respond to a computer attack
- Legal liability to others for computer security breaches
- Legal liability to others for privacy breaches (not just computers!)
- Regulatory actions and scrutiny
- Loss or damage to reputation
- Cyber-extortion
- Cyber-terrorism
- Management time expended on breach response

# COMPETENCE AND DILIGENCE

## Model Rule 1.1

- Duty of competence includes knowing benefits and risks associated with technology

## Model Rule 1.3

- A lawyer shall act with reasonable diligence and promptness in representing a client.

## Model Rule 1.4

- Must keep clients "reasonably informed" about the status "to the extent reasonably necessary to permit a client to make an informed decision regarding representation."

## Model Rule 1.6 "Confidentiality of Information"

- Attorney must "make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to" confidential information.

## Model Rules 5.1 and 5.3

- Requiring supervision of law firm staff to conform with the rules

# COMPETENCE AND DILIGENCE

## ABA Opinions

### Opinion 477R (5/11/17) -Securing communication of protected client information

- A lawyer may transmit information relating to a client over the internet where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access.
- A lawyer may be required to take special security precautions when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

### ABA Opinion 483 (10/17/18) – Obligations to Clients after a Data Breach

- After detection of the breach, a lawyer must “act reasonably and promptly to stop the breach and mitigate damage resulting from the breach.”
- a lawyer "must make reasonable attempts to determine whether electronic files were accessed, and if so, which ones...[and] determine what occurred during the breach."

# COMPETENCE AND DILIGENCE

## ABA Opinion 498 (3/10/21) – Virtual Practice

- Attorneys permitted to practice virtually
- lawyers must make reasonable efforts to prevent inadvertent or unauthorized disclosures of information relating to the representation and take reasonable precautions when transmitting such information.

# SOCIAL ENGINEERING

- Social Engineering is the psychological manipulation of legitimate users into performing actions, breaking security procedures, divulging confidential information and parting with tangible assets
- Social Engineering scams take advantage of the “human factor” to perpetrate a fraud



# SOCIAL ENGINEERING - NOT AN ISSUE FOR MY LAW FIRM

- **WRONG!**
- Roughly 26% of all law firms already victim of a data breach
- Roughly 51% of law firms have taken no measures to prevent data breach
- Roughly 50% have no data breach response plan
- Ransomware attacks occur every 10 seconds

# TYPES OF SOCIAL ENGINEERING SCAMS

- Email/fax from “client” to law firm with change in payment instructions
- Email/fax from “law firm” to client with change in payment instructions
- “Internal” email directed payment or turn over of personal information from partner/management level employee
- Email impersonating third party vendor

# EXAMPLES OF SOCIAL ENGINEERING SCAMS INVOLVING LAW FIRMS

- Misdirection of Escrow Funds
- Fraudulent court notices
- Fake job posting/resumes for review
- Bank account/LinkedIn/Netflix password reset/purported “unauthorized access”
- Email with incoming fax notification
- Misdirection of real estate closing costs
- Recent Examples of Ransomware Attacks:
  - 3 small SD Law Firms were subject to ransomware and threatened to expose confidential data
  - TX boutique firm client data was released because of a ransomware attack

# RANSOMWARE TRENDS 2020-2021

- Attacks are highly targeted against specific entities
- Phishing emails is still the primary “attack vector” – because it’s simple and it works
- Increasing in sophistication and severity. Ryuk, Conti and DoppelPaymer, Mamba, Nefilim
- Network and data backups may be targeted first
- Ransomware may now execute within hours or minutes upon initial compromise leaving very little reaction time to identify and contain
- Ransom demands are increasing and scaled based upon size of organization targeted, multi-million-dollar requests common, reports of ransom demands exceeding \$60,000,000 in 2020
- High volume/disruptive telephone calls to executives and staff demanding ransom payment.
- Ransomware attack combined with other cyber crimes - data extortion. Criminals threaten to sell /publish stolen data

# INSURANCE COVERAGE GAPS

|   | Property | General Liability | Crime/Bond | K&R | E&O | Cyber/Privacy |
|---|----------|-------------------|------------|-----|-----|---------------|
| <b>1st Party Privacy / Network Risks</b>    |          |                   |            |     |     |               |
| <i>Physical Damage to Data</i>              |          |                   |            |     |     |               |
| <i>Virus/Hacker Damage to Data</i>          |          |                   |            |     |     |               |
| <i>Denial of Service attack</i>             |          |                   |            |     |     |               |
| <i>B.I. Loss from Security Event</i>        |          |                   |            |     |     |               |
| <i>Extortion or Threat</i>                  |          |                   |            |     |     |               |
| <i>Employee Sabotage</i>                    |          |                   |            |     |     |               |
| <b>3rd Party Privacy/Network Risks</b>      |          |                   |            |     |     |               |
| <i>Theft/Disclosure of private Info</i>     |          |                   |            |     |     |               |
| <i>Confidential Corporate Breach</i>        |          |                   |            |     |     |               |
| <i>Technology E&amp;O</i>                   |          |                   |            |     |     |               |
| <i>Media Liability (electronic content)</i> |          |                   |            |     |     |               |
| <i>Privacy Breach Expense</i>               |          |                   |            |     |     |               |
| <i>Damage to 3rd Party's Data</i>           |          |                   |            |     |     |               |
| <i>Regulatory Privacy Defense/Fines</i>     |          |                   |            |     |     |               |
| <i>Virus/ Malicious Code Transmission</i>   |          |                   |            |     |     |               |

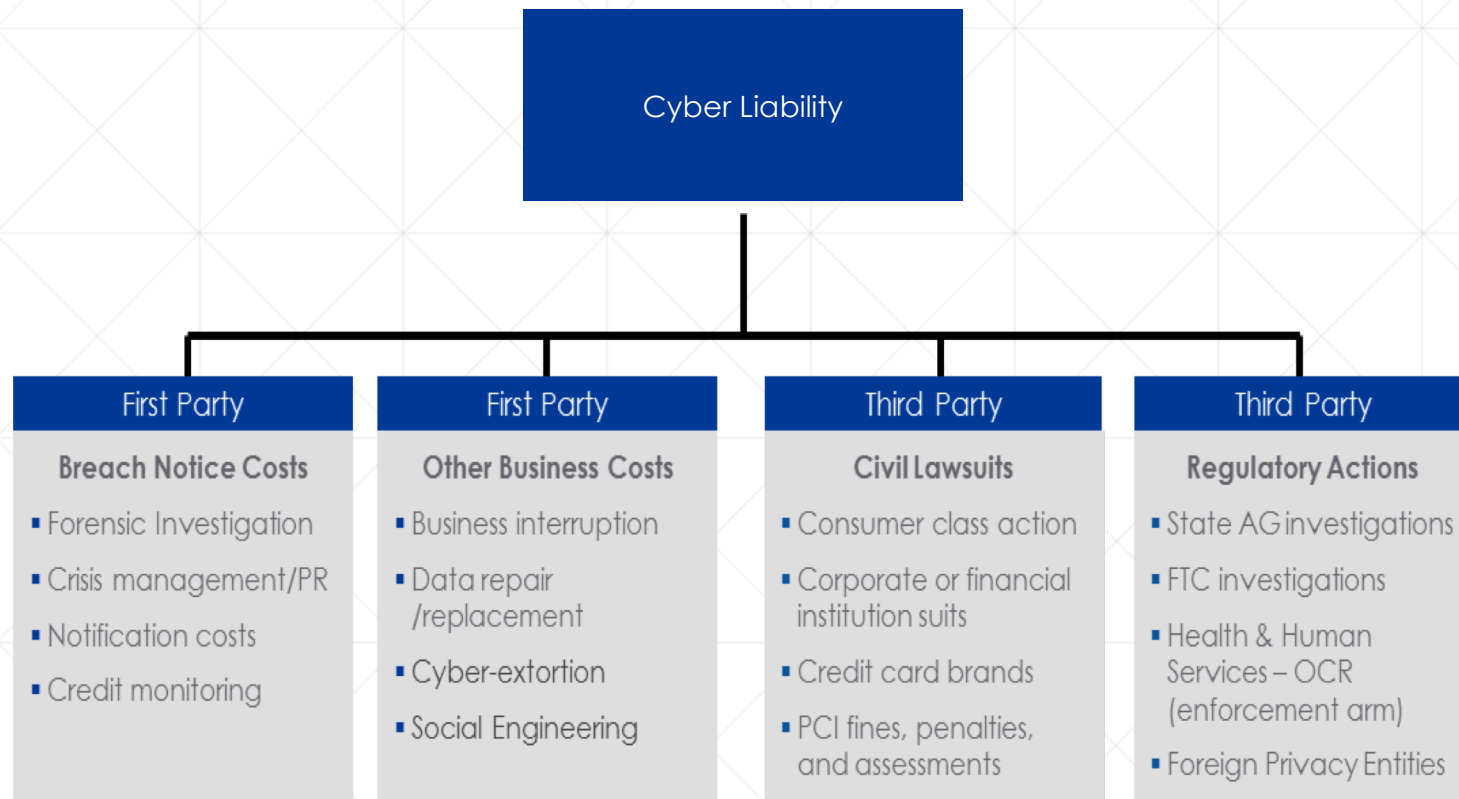
|                    |  |
|--------------------|--|
| Coverage Provided: |  |
| Limited Coverage:  |  |
| No Coverage:       |  |

## Traditional Insurance Gaps to name a few:

- Theft or disclosure of Third Party Information - GL
- Security & Privacy - "intentional act" exclusion - GL
- Data is not tangible Property - GL, Prop. and Crime
- Bi/PD Triggers - GL
- Value of Data if corrupted, destroyed or disclosed - Prop & GL
- Contingent Risks from external hosting, etc .

- Commercial Crime policies require "intent" and only cover "money securities and other Tangible Property"
- Territorial Restrictions
- Sublimits or long waiting periods applicable to any virus coverage available - Prop.

# WHAT DOES CYBER INSURANCE COVER?



# WHAT IS NOT COVERED BY CYBER INSURANCE?

- Theft of Corporate Intellectual Property or Trade Secrets
- Brand Damage
- Loss of Future Revenue
  - As in the case of Target, for example, if sales were down due to customers staying away after data breach
- Negligence/Induced Incidents
- Nation State Attacks (excluded)
- Improved IT Security Measures (Starting to be covered by endorsement – Betterment Coverage)
- Hardware Damage – (Starting to be covered by endorsement – Bricking Coverage)
- Physical Damage

# CRITICAL COVERAGE ISSUES

- Choice of counsel
- Betterment Coverage
- Bricking Coverage
- Choice of third-party vendors
- Delete exclusions
  - Lack of patch upgrades/unencrypted data/devices
- Incident caused by a third-party vendor
- Allocation of coverage between necessary remediation costs and relative upgrades
- Extra costs incurred due to complying with a government order to take (or not take) certain actions to stop the incident
- “GDPR Endorsements”
- Definitions: Privacy Regulation/Law; Personal Information; Privacy Regulatory Proceeding (just proceeding or investigation/inquiry)
- Wrongful Collection Exclusions (“Spam” Exclusions) need to be addressed.



# CYBER EXPOSURES – HOW A LAW FIRM CAN PROTECT ITSELF

- Buy Cyber Coverage!
- Incident Response Planning
- Employee Training
- Risk Analysis
- Encryption
- Two-factor Authentication
- Back-ups
- Document Retention Policy
- Penetration Testing
- Anti-virus and Patching
- Intrusion Prevention and Detection
- Vendor Risk Management

# RISK MANAGEMENT

- Use common sense
- Avoid clicking on links in emails
- Utilize SPAM filters, malware detectors and anti-virus software
- Click on “details” for email address of sender
- Verify with a phone call to client/law firm
- Secure and frequent backups
- Changing password on frequent basis, complex passwords
- Continuous maintenance of operating systems and software programs
- Inform clients that wire instructions will not be sent over email, do not accept instructions over email



**Mike Mooney**

[Mike.Mooney@usi.com](mailto:Mike.Mooney@usi.com)

610-537-1441