

# **CYBER-SECURITY... WHEN IS IT ENOUGH?**

**LIVE SEMINAR AT DSBA WITH ZOOM OPTION**

SPONSORED BY DORSET CONNECTS

---

**WEDNESDAY, OCTOBER 26, 2022 | 9:00 A.M. – 10:00 A.M.**

**1.0 Hour CLE credits in Enhanced Ethics for Delaware and Pennsylvania Attorneys**

## **ABOUT THE PROGRAM**

Join us to hear how you can protect your firm from online threats and ways to help avoid disasters! In this seminar we will review basics, compliance requirements, tips to office staff, and answer any questions!

## **PRESENTER**

Robert Sparre  
*CEO of Dorset Connects*

Visit <https://www.dsba.org/event/cyber-security-when-is-it-enough/>  
for all the DSBA CLE seminar policies.

# Presenter

---

Robert Sparre  
*CEO of Dorset Connects*

# Robert Sparre

## **Robert Sparre, CEO Dorset Connects**

Robert and his partner Jeffrey Rosenberg founded Dorset Connects, an IT consulting and Managed Service Provider serving Chester County and the Brandywine Valley area since 1997. Robert became a PC and networking expert at Delmarva Power in the early 1980's when the IBM PC was first introduced. Robert traveled the country in the 1990's setting up networking events with temporary Internet connections before hotels had their own Internet service. Dorset Connects is located in Kennett Square, PA, providing specialized security products and consulting as well as monthly support plans and projects.



Today we will talk about cyber security – BO-RING!!

We are going to leave time at the end for Q&A, but please don't hesitate to ask questions as we go

For several decades, antivirus and related software, installed on every computer, has been the norm for protecting your machines and the information stored on them. But is this enough?

The dept of Homeland Security recommends ALL organizations, regardless of size, adopt a heightened security posture.

No one can guarantee to keep you 100% protected from a cyber attack. Let's talk about things you can do to protect yourself

The Basics:  
Level of protection that all businesses need

Antivirus

Firewall

Unique, secure passwords and multi-factor authentication (MFA)


But is this enough?  
...probably not

dorset connects  
digital | innovation | growth

2

There is a basic level of protection that all businesses, no matter how small, should have in place.

- Anti-virus and anti-malware protects against known threats, but this is the bare minimum.
- Firewalls protect your network from direct attacks from the outside.
  - DOES EVERYONE KNOW WHAT A FIREWALL IS?
- Secure passwords and MFA are increasingly important to stop hackers from accessing your accounts
  - DOES EVERYONE KNOW WHAT MFA MEANS?



## Risk & Cost vs. Reward & Mandates

- No one size solution fits all
- Risk vs. Reward – nothing new here
  - Risk to reputation – can you afford to be associated with a breach?
  - Risk to business operations
  - Risk to finances
- Mandates – not-negotiable
  - PCI, HIPAA, government or industry compliance
  - Insurer requirement
  - Client or vendor requirement

dorset connects  
3

### **no one size solution fits all.**

You may have to sign in with a security building guard 24x7, while others of you might only have to do so during business hours.

Some may only have to swipe a keycard to enter the office  
others may have an old fashioned key.

The decision as to what level of cyber security is appropriate for you, like the decisions re physical security is enough, is a matter of balancing risks and costs against rewards. Then we add in items that might be mandated and over which you have little control.

### **Risk vs Reward**

Focus on reputation

Cyber Insurance protects you financially, but not your reputation – what would happen to your practice if you were associated with a breach?

Many businesses do not recover from a breach – most due to the reputation hit

### **Mandates**

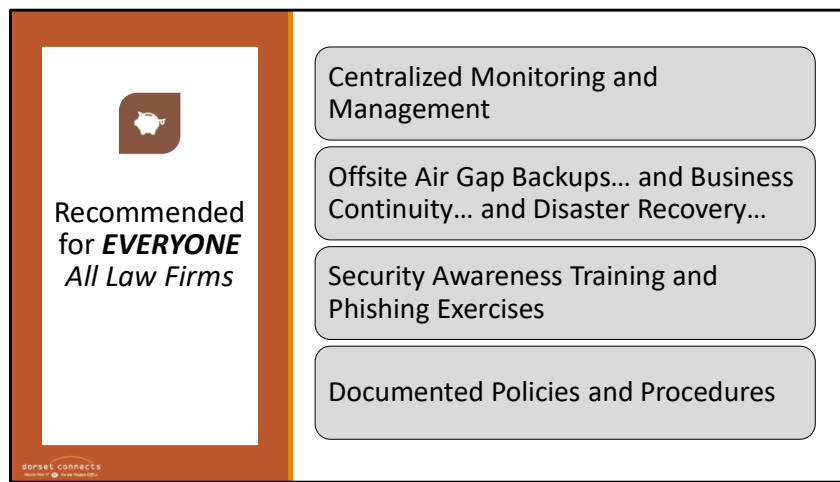
The primary motivating factor that that drives our clients to increase their security is when they are forced to.

Their industry mandates that everyone in their field must do something.

Or an insurer or client or vendor requires it in order to continue to do business or receive a favorable rate.

Or the government makes it a requirement to do business.

These requirements are usually not negotiable, but how strictly and fully a company complies can vary and can have repercussions when/if there is an incident.



Monitoring and management – for patches and security updates – who is making sure?

Offsite backups – the bad guys usually come in and make sure your backups are disabled or encrypted before they attack

An Air Gap backup is the best way to recover.

SAT – (Security Awareness Training) end users are the most common source of breach

Policies and procedures





**Cyber insurance** is a must today, either as an add-on to your current liability or as a standalone policy. This will provide the resources needed if a breach occurs. You still need backups that were not compromised.

**Encryption** helps ensure that if a device is misplaced or stolen, the data stored on it can not be retrieved. Encryption all laptops, cellphones and other devices that contain sensitive information

### **Auditing and Alerts**

Your IT team needs to be notified when certain events take place. These may be changes in user privileges, such as your mailroom clerk suddenly becoming a super user. Or they may be indications of unusual activity, such as someone starting a search of all email for the term “salary” or deleting thousands of files.

### **Security Score Review**

Similar to a credit score, a security score is a score given to your company by one of

several private companies who collect information on you, your company, your computers and your staff's behavior.

Is your website configured with a questionable certificate or security policies? That will affect your score.

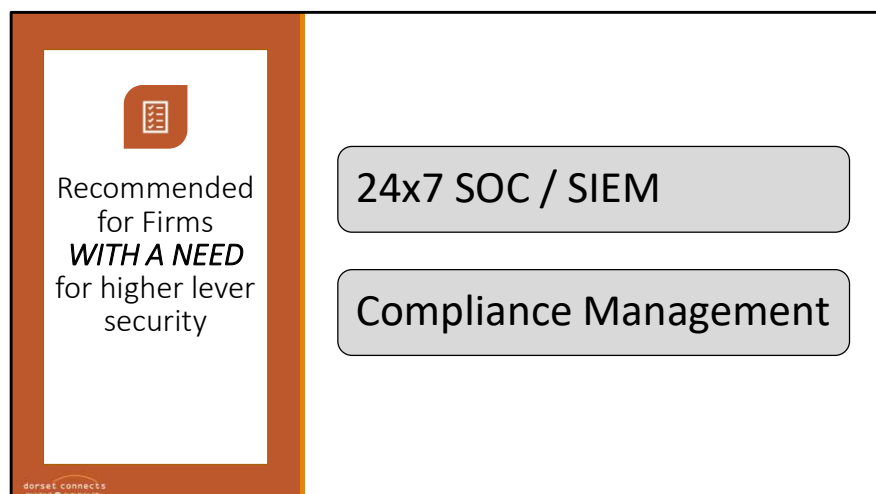
Is your staff appearing in lists of compromised passwords on the dark web, or are your computers appearing in botnet armies?

Are your machines involved in file sharing networks?

Has your email been considered spam?

Have your staff been to websites using unpatched or unsupported computers or browsers?

These types of information, and many more, are used to assign you a security score that may be used by insurers, clients, and vendors to help decide if they will do business with you and, in some cases, how much of a risk you represent and, therefore, how much to charge you.



### **24x7 SOC / SIEM**

A Security Operations Center (SOC) is a group employing people, technology, AI to continuously monitor your events taking place on your network.

A security information and event management system (SIEM) helps provide real-time analysis and monitoring as well as logging of information.

Together, these provide you with advanced detection and response to security incidents, especially those that are not easily detected from a single machine or data feed.

They weed through the millions of data points from the many sources and figure out what constitutes an actual security incident.

They may then take immediate action to minimize the impact or bring in your IT staff to respond to the incident.

If you have an active ransomware attack in progress and it got past your antivirus systems, you want a SOC that will stop that process, isolate that machine, and begin threat hunting for other potentially infected machines. You do not want one that will try to track down an engineer at Dorset or someone from your IT department at 3am

on a Sunday morning and tell them what to do, all while ransomware is spreading and destroying your systems and data. You want someone who will take action immediately.

## Compliance Management



- ☐ NIST CSF, 800-171 or 800-53 for almost everyone
- ☐ PCI-DSS if you accept credit cards or store credit card information
- ☐ HIPAA & HITECH if you are a health care provider or provide certain services to one.
- ☐ HITRUST CSF if you want to be certified.
- ☐ CMMC if you work with some parts of the government
- ☐ GDPR if you collect data related to people in the EU
- ☐ Banking, Financial Services or Insurance in New York? Anything for the State of Delaware? Other states?

Do you happen to do business in DE and maintain, store or manage data that includes personal information of DE residents?

-----

**NOTE: The goal of this slide is to show that there are a LOT of compliance requirements and (almost) everyone needs to be prepared. Even just doing business in DE means that you have to safeguard PII and make public reports when PII is compromised. There is no detail on what to do to protect the info, but the reporting requirement is codified in law. Everyone should get their act together.**

**Compliance management** is a complex subject and I could give an entire presentation on this one topic.

- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and other related standards. Often the base for security questionnaires that might come your way from insurers, vendors, clients.
  - 800-53 for federal information systems, but used by lots of others
  - 800-171 for non-federal information systems, but used by lots of others
- Payment Card Industry (PCI) Data Security Standard (DSS) covers security and

- standards for those who handle credit cards and credit card information
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Title II addresses protection of health and medical records... Protected Health Information (PHI)
    - Health Information Technology for Economic and Clinical Health (HITECH) Act made HIPAA stronger, increased penalties and addressed business associates (subcontractors) among other things.
    - Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) which rolls in HIPAA with others and provides specifics and can be certified
  - Cybersecurity Maturity Model Certification (CMMC) if you work with the DoD or other government agencies, especially if you handle any type of classified information. Currently mostly used at federal level.
  - European Union General Data Protection Regulation (GDPR) if you target or collect data related to EU residents
  - State and industry specific rules in New York. Government agency rules in Delaware.
  - And of course, state of DE public reporting requirements if you ever happen to lose or disclose DE residents' personal information.

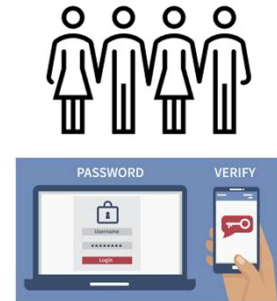
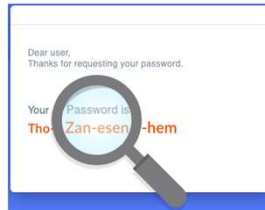
# Tips for Staff



- People are the weakest link
- MFA is the first, and by far the best, line of defense
- Do NOT email passwords!
- Phishing email - example

**From:** Rob Sparre <Rob@companydomain.pk>  
**Sent:** Monday, June 13, 2022 20:09  
**To:** Your Name <Your Name@companydomain.com>  
**Subject:** Picture of rick when he had hair

<https://mypictures.com/rickhair.jpg>



MFA - Multi-Factor Authentication



**dorset connects**  
Hassle-Free IT For the Modern Office

Robert.Sparre@dorsetconnects.com

# Summary



CONSIDER RISK VS.  
REWARD WITH  
REGULATORY AND  
OTHER REQUIREMENTS  
ADDED



VERY EASY INEXPENSIVE  
STEPS WITH HUGE  
RETURNS



ADD SECURITY TOOLS  
AND FEATURES TO MEET  
YOUR SPECIFIC  
SITUATION



KNOW WHERE YOUR  
SYSTEMS NEED  
IMPROVEMENT



GET OUTSIDE HELP  
WHEN NEEDED



BE AWARE OF YOUR  
COMPLIANCE AND  
REPORTING  
REQUIREMENTS

**IMPROVE YOUR BUSINESS AND PROCESSES,  
GAIN CREDIBILITY AND REPUTATION,  
AND POSSIBLY LOWER SOME INSURANCE COSTS**


9

Security is a matter of balancing risk and reward while taking into account regulatory or other requirements.

There are some very easy and inexpensive steps that you should take if you have not done so already. They have huge returns in terms of protecting your business and your clients.

Your needs will likely differ from others, as will your budget and your tolerance for risk. Add the tools and security features that are appropriate for your situation.

Take steps to test your systems so you actually know where you are strong and where you may have room for improvement.

Get outside help when needed. This may be an attorney or other specialist in a particular certification, or a company such as Dorset Connects to help you implement new security or document the systems you already have in place.

Be aware of your compliance and reporting requirements and be prepared to address them if you are even unfortunate enough to find yourself the victim of a cyber crime.



In this day and age, with the ever expanding risks, and ever increasing regulatory compliance requirements, it might be time to revisit your security.

As a benefit, you can improve your business and processes, gain credibility and reputation, and possibly lower some of your insurance costs.