Simple & Cost Effective Ways to Reduce Your Cyber Risk

Why?

- Taking these precautions will not only lower your cyber risk, but also lower insurance costs and improve the coverage and capacity offered to you.

1) Dual Authorization

- Always have multiple people signing off on checks, ACH transactions, and wires. .
- Call the vendor directly with a number you have on file or a number you can find publicly.
- **DON'T:**
  - Call the number on an invoice - you could be calling the hackers directly.
  - Email to confirm payment details - you could be emailing the hackers directly.

2) Domain Keys Identified Mail and Domain-based Message Authentication, Reporting, and Conformance (DKIM & DMARC/SPF)

- These are standards that authenticate your email server and help provide even more protection against being compromised.

3) Adding in MDR Services/Endpoint Protection (Also Called EDM)

- Managed detection and response (MDR) services are a great way to maintain a dedicated cyber risk management program through a third-party service without an extensive budget.

- Many MDR services provide 24/7 real-time cyber incident response (IR) and security consulting services.

4) Cloud-Based Backups That Can Be Quickly Restored

- Keeping data stored on a remote server allows users to instantly access that data in the event of an outage, failure, or cyber attack.

5) Add a Secure Email Gateway (SEG)

- What is an SEG?

  - SEG is a type of software that monitors emails, both sent and received.

  - They defend against spam, malicious attacks, and fraudulent content while ensuring that legitimate emails still make their way to the intended recipient.

  - Popular vendors include Proofpoint, Mimecast, and Barracuda. The cost is usually less than $5 per month.

6) Multi-Factor Authentication (MFA) on Email and Remote Access to Networks

- MFA is a security measure that requires more than one method of authentication in order to confirm who a user is and grant access. This is generally free and should be implemented for email, network access, and privileged users.

  Examples:
  - Chip and pin on debit cards

  - Answering a security question to log into your bank account

  - Entering a specific code that has been sent to your cell phone (this is typically used for personal bank accounts)

- This feature is included and free for most email software, but the email provider does not default you to the most secure settings. Instead, they default your settings to the easiest setup.

7) Remote Desktop Protocol (RDP) Ports

- RDP is a Microsoft proprietary protocol that enables remote connections to other computers. It provides network access for a remote user over an encrypted channel.

- Criminals can easily scan and use open RDP ports to get into networks.

- Many Cyber Insurance carriers will scan for open ports and deny coverage if this is the case. Make sure RDP ports are constantly checked and fixed if there is an issue.

8) Patch Management

• It's common for software to become out of date and have security vulnerabilities. When vulnerabilities are announced, move quickly and patch them as soon as possible to avoid additional risk.

9) Use a Password Manager

• Password managers assist in generating and retrieving complex, strong, unique passwords.

10) Employee Training

• Employees are the weakest link, accounting for 90% of claims. Make sure to provide training and build a culture of awareness around cyber security.

• Recommended employee training: KnowBe4.

11) Incident Response Plan

• An incident response plan (IRP) for cybersecurity is a set of pre-made instructions that tell IT and cyber-security professionals how to respond in the event of a cyber attack.

• Without an IRP in place, management will scramble to understand what happened and respond quickly–exposing the company to potentially expensive missteps. Depending on where the business operates, an IRP may even be required by law.

• Businesses like NetDiligence can help companies to create plans for and respond to cyber attacks. Some insurance carriers will also offer IRP templates that are part of their own cyber risk management services after you buy a policy.

• IRPs are so essential to cyber risk mitigation that some cyber insurance companies require them before insuring a business.

12) Cyber Insurance Policy

• No matter how diligent you are in reducing your cyber risk, no business is 100% safe from a cyber attack.

• In the event of a cyber attack, your business needs an extra layer of assurance to transfer your cyber risk. In other words, you need a way to protect your business from costs associated with business disruption, equipment damage, revenue loss, public relations, legal fees, forensic analysis, and much more.

• We are here to help protect your business from the disastrous consequences of a cyber attack. Contact us today to learn more about your cyber insurance options.