Employee Owned
SCOTT
Est. 1864

Cybersecurity Best Practices

How to Address Today's Cyber Threat

High-profile cyber attacks like the Microsoft Exchange server hack, the SolarWinds Orion software compromise and the Colonial Pipeline ransomware attack have highlighted increasing cyber risk for nearly every type of business. Furthermore, 2020 brought a massive shift to working from home for many companies due to the COVID-19 pandemic, further exacerbating the increase in frequency and severity of cyber attacks. As a result, the cyber liability insurance market is seeing increased premiums and deductibles and lower coverage limits. Businesses across all industry segments are subject to these trends.

Top Cyber Risks Facing Businesses Today

1. **RANSOMWARE:** businesses in all industries have suffered from the increased prevalence of ransomware attacks. These attacks are often very costly due to operations and communications disruptions resulting from information and operations technology systems being held for ransom.
2. **WIRE TRANSFER FRAUD:** hackers often deceive employees into wiring large sums of money into the wrong hands. The orchestration of these events is generally conducted via email, either by impersonating a business parter or employee or by taking over an internal email account.
3. **PHISHING:** phishing emails are overwhelmingly the most common attack vectors for most companies. A single successful phishing email can open a company up to a variety of different types of major cyber attacks.

To address today's cyber threat, businesses should perform three major functions:

Assess Your True Cyber Risk ▶ *Build Strong Defenses to Improve Your Odds* ▶ *Develop & Practice a Thorough Incident Response Plan*

Assess Your Cyber Risk

The first step to managing your organization's cyber exposures is to thoroughly assess the risk inherent in your business operations and the adequacy of your defenses to prevent a bad actor from compromising your network. Some questions to consider:

- How much sensitive data do we store on our network?
- How frequently do we wire large sums of money?
- What are we doing currently to block phishing attacks?
- How strong is our overall network security posture?
- Do we conduct cyber risk awareness training with our employees?
- What is our business continuity plan for when our network is shut down?

Once you've assessed your exposures, it's also important to assess the potential impact to your business:

- What's your estimated cost or lost revenue per day of downtime due to a ransomware attack?
- How many individual PII, PHI, and PCI records do we have stored on our network and what's the average cost per record if they were to be leaked in a data breach?
- How much money do we wire on a monthly or annual basis? Do we wire sums large enough to exceed our financial ability (liquidity, insurance policy limits, etc.) to cover the loss?

Build Defenses

Building strong cyber defenses improves your organization's odds of protecting your employees, partners and customers and ensuring business continuity. You should consider the following categories of defenses when assessing your cybersecurity posture:

> **EMPLOYEE TRAINING** – conduct cyber risk awareness training, particularly focusing on phishing, as well as simulated phishing attacks to identify susceptible individuals in your organization.
>
> **ACCESS CONTROLS** – consider instituting more complex password policies and regular expiration intervals, implementing multi-factor authentication (MFA) to protect against compromised credentials, and setting up user accounts using the principle of least privilege.
>
> **BACKUPS** – the industry standard for redundant backups is the 3-2-1 strategy, which dictates having three copies of your data, on at least two different media (cloud, air-gapped disk, etc.), and one off-site copy for disaster recovery.
>
> **THIRD-PARTY REVIEW** – consider hiring a cybersecurity firm to perform a thorough risk assessment and penetration test to reveal vulnerabilities in your network.
>
> **CALLBACK PROCEDURES** – verify the validity of all wire transfers and their destination before initiation.
>
> **INCIDENT RESPONSE PLANNING AND PRACTICE** – develop a written incident response plan and test it with simulated attacks and tabletop exercises.
>
> **NETWORK MONITORING** – consider solutions that give you greater oversight of your network activity to catch potentially malicious behavior before it becomes a problem. This includes solutions like endpoint detection and response (EDR) software and security information and event management (SIEM) services.
>
> **PATCHING** – ensure your IT team is regularly patching software with the latest version and replacing outdated hardware.
>
> **FIREWALL** – develop a strategy to monitor and filter inbound and outbound network traffic to stop malicious activity.
>
> **POLICIES AND PROCEDURES** – develop written policies and procedures to set clear expectations with employees on what is expected of them while using company network resources.

Write and Practice Your Incident Response Plan

Shift your mindset from if we face a cyber attack to when we get attacked, what will we do? Your written incident response plan (IRP) is your guide to a fast, efficient and effective response to a cyber attack when minutes count. A thorough IRP will help minimize the cost and downtime associated with a cyber attack. According to IBM, companies with an incident response team that tested their IRP effectively, saved an average of $2 million when they faced an actual data breach.

Your IRP should define who is on the IR team (including third-party resources), how to contact them and what their responsibilities are during each phase of the IR process. It should also include technical and disaster recovery considerations, levels of escalation and communication plans.

Lastly, you should practice the plan. There are many third-party cybersecurity firms and data privacy attorneys who can guide you through tabletop exercises or simulated cyber attacks.

Conclusion

Businesses that can regularly incorporate these three functions - assessing cyber risk, building defenses, and incident response planning – into their company's overall risk management program will be in a significantly improved position to effectively prevent and minimize the damage of cyber attacks.

About the Author

Bennett Whitehouse
Occurrence Prevention Specialist
Scott Insurance

Bennett joined Scott's Risk Performance Group in 2019 and is based in Scott's Raleigh office. Before joining Scott, he spent four years as a digital marketing consultant for Merkle, Inc., specializing in website content and code audits, code modifications, GDPR compliance, coordinating with software development teams, and business development. Bennett transferred this digital experience to his role as the team's cyber risk specialist. He helps clients mitigate the ever-increasing threats of cybersecurity by applying Risk Performance principles to cyber risk management and other operational risks organizations are facing. Bennett obtained his Bachelor of Arts degree in business economics from Wofford College.

About Scott Insurance

Scott Insurance is a regional, employee-owned, independent agency. Since 1864, Scott has been serving the needs of mid-market clients for risk management and insurance services. With nine offices throughout Virginia, North Carolina, South Carolina and Tennessee, and captive operations in Grand Cayman and the United States, Scott is one of the largest independent agencies in the Southeast. Scott's expertise and services include Property & Casualty, Employee Benefits, Bonds and Captives.