requirements, including planning for cyber incident response and recovery. From an accounting and finance perspective, outlining key considerations for acting upon ...

Dec. 08, 2020

Part 2 of 2. Read part 1: 9 tips to reducing cyber threats in accounting firms.

Every organization and department must take responsibility for its own security requirements, including planning for cyber incident response and recovery. From an accounting and finance perspective, outlining key considerations for acting upon

cyberattacks – and doing so with speed and finesse – will better position finance

Because the risk of a cyberattack occurring to any individual or company is incredibly high, here are the key elements of a response plan for consideration and adoption:

1. **Determine incident scope:** Many cyberattack campaigns are designed to target multiple individuals and systems within an organization at once. It is important to identify affected systems quickly to enable rapid incident response and remediation.
2. **Quarantine infected computers:** During a cyberattack, the intruder rarely gains immediate access to their intended target. Often, attackers compromise one system and need to move laterally through the network to achieve their final objectives. Quarantining infected systems helps to restrict this lateral movement, making it more difficult for an attacker to achieve their eventual goals.
3. **Collect relevant evidence:** Computer systems have mutable storage, and many malware variants attempt to cover their tracks after an attack. Making a copy of infected devices' current state as quickly as possible is essential to ensuring that vital evidence is not deleted or overwritten.
4. **Secure expert assistance:** Effective incident response often requires access to specialized skill sets, such as digital forensics experts, malware analysts, and a legal team. If this expertise is not available in house, partner with a provider that can offer it quickly when needed.
5. **Remediate and eradicate:** Many malware variants have built-in persistence mechanisms designed to make them difficult to remove from infected machines. After identifying the scope of the incident, ensure that the infection is completely eradicated, which may include completely wiping infected machines.
6. **Restore from clean backups:** Remediation efforts or a ransomware attack may render a system and its data unusable. If this is the case, affected systems should be restored from the most recent backup that is known to not be affected by the attack.

7. **Determine reporting requirements:** Data breaches and other cybersecurity

compromised by the attack. This is especially important for high-value accounts such as online bank account pages, databases containing internal financial data, etc.

9. **Manage customer relationships:** A cyberattack against an organization can significantly impact its customers. Account for the damage caused to customers, assume full responsibility, and attend to their needs in the aftermath. It is important to consider that an attack may have internal impacts as well, such as delaying employee payroll, and to take steps to mitigate these impacts.
0. **Evaluate partner impacts:** A cybersecurity incident can impact an organization's ability to meet commitments to customers and third-party partners. Evaluate these impacts, inform stakeholders, and identify methods for minimizing these impacts. For example, an attack may cause delays in paying vendor invoices.
11. **Learn and improve:** An old proverb says, "Fool me once, shame on you. Fool me twice, shame on me." A cybersecurity incident highlights exploitable vulnerabilities within your organization's cybersecurity. Based on the incident response experience, take steps to improve cyber defenses to make the organization more difficult to attack in the future. For example, requiring approval by multiple parties for high-value financial transfers can reduce an organization's risk of business email compromise ("BEC") attacks.
2. **Review and revise procedures:** A cybersecurity incident is an opportunity to test what does and doesn't work in your organization's incident response procedures. Take the time to perform a retrospective and take steps to improve and streamline responses to future cybersecurity incidents.

Responding to a cyberattack is time consuming, a major disruption to business operations, and can impact ongoing reputation if not comprehensive and effective. What's more, overcoming the loss in trust from customers, employees, and investors is difficult. Legal ramifications also exist if personally identifiable information (PII)

is compromised. Breaches can trigger regulatory inquiries that consume more

Pete Schiff is the Managing Director of the Global Cybersecurity Professional Services practice at MorganFranklin. Pete has 25 years of experience in technology and cybersecurity, and has been with Vaco, and now MorganFranklin, since 2012.

Firm Management • Technology