CPA
Practice Advisor

FIRM MANAGEMENT

9 Tips to Minimize Risk of Cyber Attacks on Your Firm

Nov. 28, 2020

By Pete Schile.

In the world of accounting and finance, it's not if we will reconcile accounts, it's when we will reconcile accounts. Likewise, it's not if we will experience a cyber attack, it's when we will experience a cyber attack. It's bound to happen. As accountants, one of our key responsibilities is to highlight business risks. Because

cyber-based systems and activities are here to stay, our understanding of cyber risk implications to the business is paramount. Below we outline essential measures for the accounting and finance community's adoption to protect and recover from cyber attacks.

- **Gain a strong cultural understanding of the cyber threat landscape as it blends with business operations.** In addition, maintain awareness of current events and the implications to business and the assurance provided to clients and customers. This knowledge will help identify and prioritize potential risks and remedies to inform the development of a risk response that also reflects the risk appetite of the business. Implementing relevant protective measures should help secure the business, but not hinder nor obstruct it. Continued awareness and knowledge gathering are critical to the ongoing strengthening of an organization's security posture.
- **Educate ourselves and our team members on risks and threats.** Human error and negligence are the most common reasons viruses and hackers enter an environment. Complacency cannot exist. The more employees are aware that a cyber attack is not 100% avoidable, the more cautious they can be when working with data, whether from the office, from their home or the local coffee shop. Ownership of a security practice as custodianship of data should be discussed to increase that vigilance. Employees often have a lower level of awareness when working remotely due to distractions and environments not experienced in the office. Cyberattacks can place a business at risk of closing, especially if the organization does not have a response plan and cannot recover. Therefore, employees' jobs are placed at risk as well.
- **Enforce a review process** (whether formal, automated, or manual) for any critical financial changes. When parties request an urgent ACH, account change, etc. that modifies an established process of financial activity, a verification process should be completed to validate the change/request. This acts as an added level of security should a false request slip by other means of protection.
- **Develop, implement, and regularly improve** upon an incident response plan, which is a playbook for when a security incident occurs. These actions will help to limit exposure and ensure timely recovery from a data breach. Processes must include the roles and responsibilities, and immediate steps for communicating to all potential stakeholders during a breach. Therefore, the list of potential stakeholders must be kept current.
- **Restrict user access.** Advanced permissions within networks, systems and buildings can prevent or enable access based on role, level of permissions, time,

and/or status. Organizations may not be fully leveraging all permission settings that will provide heightened security. Connect with system vendors, IT teams, and facilities management to understand the options available and if best-in-breed capabilities are enabled.

- **Prioritize assets.** Identify and map the data that is most sensitive or critical and that requires the greatest protection according to the impact if compromised, or any mandates. Safety and recovery measures should be tailored for these assets.
- **Assess systems and data classification levels**. These systems include those on-prem, hosted by others, and by vendors' systems. System owners are responsible for ensuring patches and upgrades are completed in a timely manner according to patch criticality. Scanning and monitoring should be regularly performed to identify vulnerabilities. Firewall security configurations should be continuously reviewed, updated and adjusted on a regular basis. The landscape of systems includes printers, scanners, telephony, and those that traditionally support business processes (e.g., ERP, CPM, CRM, ATS).
- **Move to the cloud**. Cloud systems are continuously updated to address and correct security issues. Modernizing systems increases the 'hardening' of architecture. Budgeting for cloud migration should include security such as a Cloud Access Security Broker (CASB) for heightened protection appropriate for cloud environments and specific business operations. This is especially important if a cloud provider does not offer one as an add-on service. In addition, consider outsourcing certain cybersecurity aspects, such as monitoring, to allow more focus on business growth. 24/7 monitoring by a Managed Security Service Provider (MSSP) is almost a must for businesses that do not have their own Security Operations Center (SOC). Additional services may also include data redaction in platforms where sensitive information is not necessary for processing.
- **Enforce a password strength policy.** Use Multi-Factor Authentication (MFA) anywhere it is available. The best policies require passwords (combination of letters, numbers, and special characters) different than those used by employees for their personal accounts and, furthermore, encourage the use of a company-approved password manager tool for each employee.

Ultimately, we need to stay vigilant of the potential cyber threats to our business and the training, technology and best-in-class processes that are available to heighten our ability to safeguard information and our business' operations. Whether we own a company or work within an organization, we, as finance and accounting professionals, are in a strong position to question the practices and systems used by our internal and external security experts to protect our business.

==========

Pete Schile 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 • Article

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.