Cybersecurity Risk Reviews:

A Practical Approach to Protecting Your Organization

By Jarrett Meiers, Director, Strategic IT Services, Blueprint Essential, a Division of Reynolds + Rowella

CPAs have always had a duty to maintain data confidentiality. In the digital age, this duty has taken on a completely new set of risks and threats. Sensitive information no longer exists solely on sheets of paper on desks or in filing cabinets; it is now in multiple locations (many of those digital in the cloud and on servers) across the organization.

Modern technology has made accessing and transferring information so simple that we may be inclined to forget how easy it has become for the wrong people to get their hands on it. All too often files are moved around in an unsafe manner through unencrypted email, flash drives, smartphones, or laptops. These seemingly innocent and convenient data storage and transfer methods can result in major risks for your organization.

Because large company cybersecurity breaches often make news headlines, it is easy to think they are the only ones being targeted. Many global companies do house a tremendous amount of sensitive data (and sometimes still leave much to be desired in their protection practices), but they are certainly not always the ideal target.

Hackers aren't usually looking for a major challenge; they are interested in low-effort, high-reward targets. CPAs and other financial professionals often fit this description because their data is a treasure trove of confidential information that is highly lucrative on the black market. Couple that with the fact that many small to medium-sized businesses have not instituted advanced data-theft prevention methods, and there is a perfect storm of easy prey and high value.

In fact, 43 percent of cyber attacks target small businesses, according to Symantic's *Internet Security Threat Report*.

While there are myriad professional development programs and articles focused on cybersecurity, developing a course of action can be overwhelming. It's easy to let cybersecurity and business continuity plans fall to the back burner while you focus on seemingly more pressing day-to-day business needs.

One thing is certain: there will be more and more cyber attacks in the coming days, weeks, and years. Organizations who face a breach will face harsh consequences.

No business wants to have to inform its customers or clients that their personal

information is for sale on the dark web because of a breach. The U.S. National Cyber Security Alliance estimates that 60 percent of small companies go out of business within six months of a cyber attack.

The good news is there's a simple step you can take to lay a solid foundation for your cybersecurity strategy: get a cybersecurity risk review. A cybersecurity risk review assesses your organization's current ability to safeguard confidential information and provides you with practical ways to reduce risk and protect sensitive data in the future.

These reviews are relatively inexpensive, help demystify cybersecurity, and will provide you with a list of actionable steps to perform as you move forward. A risk review should not focus solely on IT systems and infrastructure. Rather, it should take a holistic approach, examining elements such as regulatory compliance, asset protection, user awareness, liability insurance, business resiliency, policies, procedures, systems, funding and spending levels, and incident response.

> Hackers aren't usually looking for a major challenge; they are interested in low-effort, high-reward targets. CPAs and other financial professionals often fit this description because their data is a treasure trove of confidential information that is highly lucrative on the black market.

At the end of the risk review you will be presented with the findings and a framework that will be used to address the most important cybersecurity planning and protection needs going forward.

If you haven't had an expert review your cybersecurity risks, I encourage you to do so as soon as possible. If you have in the past, I recommend having an updated review at least once a year to ensure you maintain adequate protection in today's fast-changing security environment.

In the meantime, the next page provides you with a practical list of nine cybersecurity steps you can start to implement today to make sure your organization is protected. ▶

(continued)

9 Practical **Cybersecurity Steps** to Help **Protect Your Organization**

1 Identify critical data.

CPAs are accustomed to working with confidential data. It is important to identify all the areas where critical data exists. This includes confidential client data, employee data, and company financial information.

2 Map the flow of data.

After critical data has been identified, the organization must review all the places that data resides and how it moves through various locations – both inside and outside the organization. Chances are good that critical data flows through multiple storage sites that could be subject to cyberattacks. Also pay special attention to how customer and client communication is handled, including what information is being shared and how.

3 Determine responsibility.

Even if your company is not large enough to employ a full-time security officer, responsibility must rest somewhere. It is important to determine who in the organization will take the lead on protecting assets and implementing security measures. Include any internal and external parties, such as software vendors, support companies, and outside consultants.

4 Assess your information security policies.

Clear, well-written security policies must be in place to set the ground rules for the business and its employees. These policies are dynamic, living documents that must be reviewed and updated frequently. If ambiguities exist, those responsible for security inside the organization must be responsible for clarification of the policy.

5 Increase employee awareness and training.

Your company may have excellent policies, but unless you actively get buy-in from staff, the policies will be ineffective. Implementing an ongoing security awareness program can help educate employees on policies, safeguards, and vulnerabilities, increasing the effectiveness of cybersecurity measures.

6 Have an incident response plan.

The company should have a specific process in place for staff to report potential threats or breaches. This should include the detailed chain of response in place to immediately address security incidents. Conduct drills to verify readiness. Often, this is where disaster recovery/business continuity plans and cybersecurity plans overlap.

7 Have regular cybersecurity reports.

Hold meetings throughout the year to discuss ongoing security efforts within the organization. The agenda should include security incidents, emerging threats, proposed security changes, project updates, and vendor issues. Keeping security top of mind increases the entire organization's vigilance.

8 Control your physical assets.

Critical data exists both in physical and digital form, so best practices should be put in place to secure printed copies of sensitive data as well as devices such as laptops, tablets, and flash drives. Keep a strong inventory of your assets. Don't overlook building security safeguards, including locks on server rooms and network closets, visitor controls, and cameras.

9 Stay active.

Continue to keep cybersecurity high on your agenda and provide cybersecurity teams with the resources needed to protect both digital assets and your most valuable assets – your employees and customers. Keep an eye on regulatory developments and breaking news.

In conclusion, having a cybersecurity risk review is one practical approach to protecting your business and will help guide you in the right direction. Even still, cybersecurity isn't a "set it and forget it" project that you can complete and cross off your list. Today's ever-changing environment demands ongoing maintenance, monitoring, patch management, penetration testing, and assessment.

This high level of consistent vigilance requires time, money, and effort. It may sometimes seem easier to direct these resources at more tangible and seemingly urgent needs. Unfortunately, this could easily prove to be a costly mistake. The stakes are high. Companies that take these threats seriously may survive where others may not. Be sure you're doing everything you can to protect your customers and clients, your employees, and your business.

Jarrett Meiers leads Reynolds + Rowella's IT consulting division, Blueprint Essential. He advises accounting firms and businesses on technology, security, and practice management. He can be reached at jarrettm@reynoldsrowella.com.