Contrary to popular belief, privacy events and their associated risks do not exclusively arise from external, malicious sources. As the chart, “2018 Privacy Event Claims, by Incident Type,” indicates, external attacks were the most frequent cause of privacy event claims asserted against CPA firms in the AICPA Professional Liability Insurance Program in 2018. However, internal human error, whether it is the direct cause of a privacy event or an inadvertent action that assists an external bad actor, also contributes to a firm’s data security risk.

While the fences you build to help protect your firm from external attacks are important, the housekeeping you do within your firm is equally important in managing information security risks facing your practice. Here are some housekeeping reminders to consider.

**WAKE UP AND SMELL THE PHISHY EMAILS**

Phishing is a form of social engineering in which a bad actor uses various technological channels, typically an email, to solicit personal information from a targeted individual or company by posing as a credible source. According to Verizon’s 2018 Data Breach Investigations Report, phishing and pretexting represented 93% of breaches, of which email was a common vector. This demonstrates the need to be vigilant and alert when opening and reacting to email.

To address risks associated with phishing attempts, CPA firms should consider using anti-phishing tools that commonly provide the following types of capabilities:

- Preventive means to scan for and block malicious links, attachments, or accounts;
- Simulation of phishing attacks on users to test and raise their phishing attack awareness and detection savvy; and
- Post-delivery capabilities to intercept and neutralize malware and/or ransomware when a phishing message is opened.

**PREPARE FOR THE UNEXPECTED**

Author Radhika Mundra said, “Nothing inspires cleanliness more than an unexpected guest.” Preparing and training your employees with the information and tools to raise their security awareness can be one of the most effective, and efficient, preventive measures to mitigate data security risks.

According to the Ponemon Institute and IBM’s 2018 Cost of Data Breach Study, employee training is one of the highest cost-saving contributors to the per-capita cost of a data breach. To select the most relevant training topics, firms should stay informed about the latest information security threats facing the professional services industry, and, if applicable, analyze their own prior security events, thus turning a painful memory into a learning opportunity.

**LOOK INSIDE BEFORE YOU LOOK OUT**

Strong passwords are basic, yet paramount, in controlling how internal system users are authenticated and allowed to access a firm’s systems. The more critical an application is to your organization, the more robust the authentication requirements should be. Many types of authentication methods are available, including system-level password configurations, multifactor authentication, single sign-on, and password managers, which are tools that generate and store complex passwords.

With the increased use of cloud applications to enable business functions, CPA firms also should understand the authentication requirements controlled by the cloud application vendor versus those that can be configured or controlled by the firm in order to achieve the most appropriate level of control over authentication.

When researching to determine what authentication and configurations to apply, firms should reference best practices or guidelines set by organizations such as the National Institute of Standards and Technology. Keep in mind that best practices can and do evolve, and that firms should be proactive in referencing best practices to achieve an appropriate balance between the “unnecessarily complex” versus the “appropriately secure.”

**REMOVE THE CLUTTER**

Your home is not a storage space, so why should your firm be different? Don’t risk being a hoarder when it comes to stale data, users and accounts, and sensitive files.
Data is at risk, whether it’s in transit, in use, or at rest. According to Varonis’s 2018 Global Data Risk Report, more than 54% of data is stale, meaning it’s neither required nor used during daily operations. Firms should balance the benefits of retaining data versus its associated costs and compliance risks. The regulatory implications of storing data are on the rise. Regulations such as the General Data Protection Regulation instituted by the European Union have applied conditions to erase personal data that is no longer necessary in relation to the purpose for which it was originally collected or processed. Similar data security laws, such as the California Consumer Privacy Act, have been adopted by some U.S. states, and the momentum for enacting comparable statutes in other states does not appear to be slowing anytime soon.

When it comes to users and accounts, apply the concept of “least privilege.” In other words, access to sensitive information should be restricted based upon whether certain users require that information or knowledge to execute their intended job functions. According to Varonis’s report, 41% of companies have more than 1,000 sensitive files open to all employees, while 34% of users and/or accounts are active but not in use. Doesn’t that sound messy? Firms should consider how access to key applications is provisioned to ensure the access granted to users is commensurate with their job functions. Also, consider reviewing access to key applications at least once a year, and more frequently for privileged accounts, to determine whether stale accounts that are neither used nor needed are removed or disabled and that user access for appropriate accounts is assigned appropriate privileges.

**A FINAL NOTE**

Addressing the risks associated with the increased use of technology in your practice may seem daunting to tackle, much like a pile of laundry or a sink full of dishes. Just as your clothes or dishes won’t wash themselves, information security risk facing your practice won’t go away overnight. Start with the aspects that appear most manageable for you and your firm, and seek the advice of experts in complex areas.

Jamie Yoo, CISA, is a risk control consultant at CNA. For more information about this article, contact specialtyriskcontrol@cna.com.

Continental Casualty Company, one of the CNA insurance companies, is the underwriter of the AICPA Professional Liability Insurance Program. Aon Insurance Services, the National Program Administrator for the AICPA Professional Liability Program, is available at 800-221-3023 or visit cpai.com.

This article provides information, rather than advice or opinion. It is accurate to the best of the author’s knowledge as of the article date. This article should not be viewed as a substitute for recommendations of a retained professional. Such consultation is recommended in applying this material in any particular factual situations.

Examples are for illustrative purposes only and not intended to establish any standards of care, serve as legal advice, or acknowledge any given factual situation is covered under any CNA insurance policy. The relevant insurance policy provides actual terms, coverages, amounts, conditions, and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice.

To learn more, please visit cpai.com or call 800.221.3023