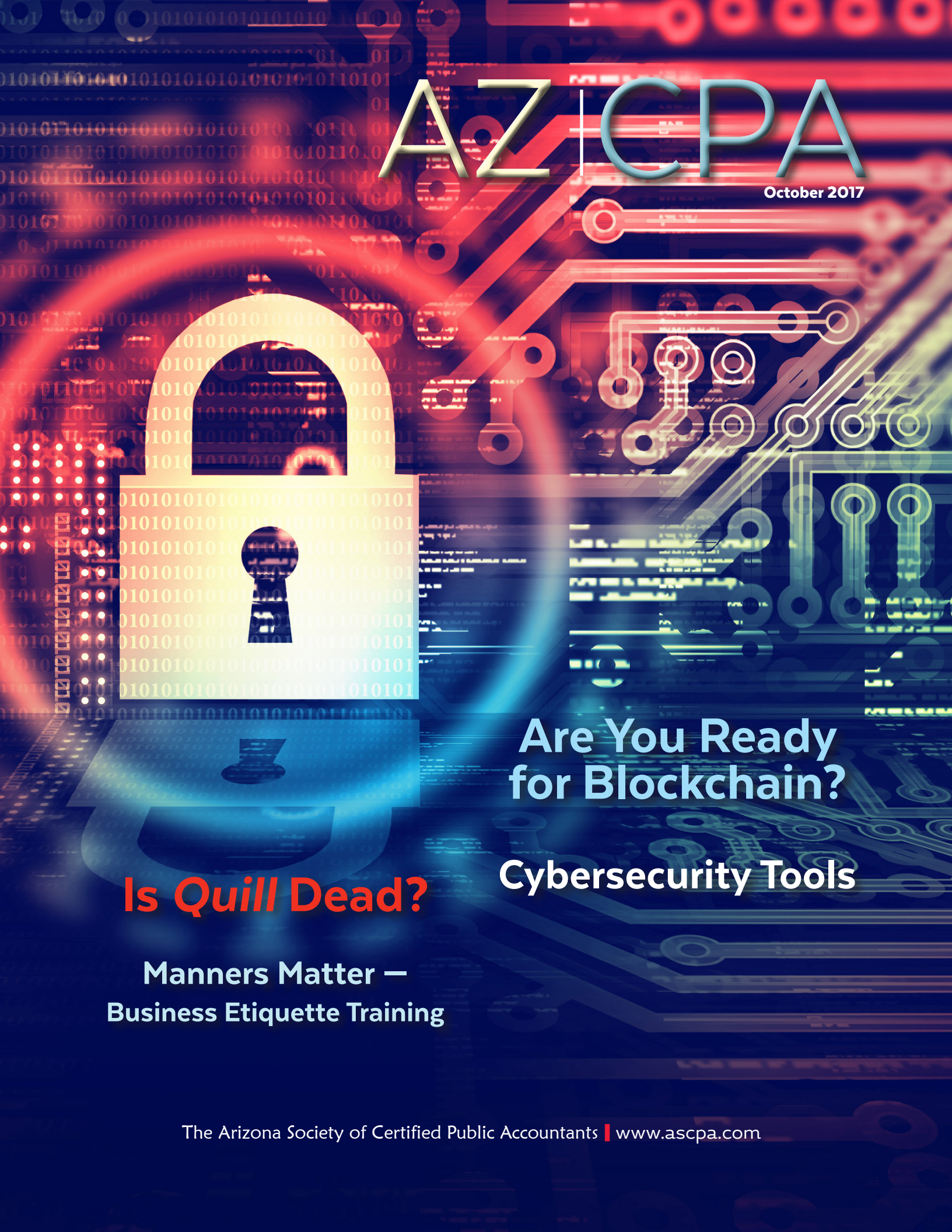

AZ CPA

October 2017

Are You Ready for Blockchain?

Cybersecurity Tools

Is *Quill* Dead?

Manners Matter — Business Etiquette Training

The Arizona Society of Certified Public Accountants | www.ascpa.com

Happy Cybersecurity Awareness Month! Are you Safe?

by Patrick X. Fowler

Since it was first announced by Presidential Proclamation in 2013, we mark each October as National Cybersecurity Awareness Month. The Department of Homeland Security explains that, in 2017, designation is "designed to engage and educate public and private sector partners through events and initiatives to raise awareness about the importance of cybersecurity, provide them with tools and resources needed to stay safe online and increase the resiliency of the nation in the event of a cyber incident." To that end, let's briefly address cybersecurity in 2017.

The Cyber Threat Environment: You and Your Clients Are Targets

As grimly noted by the IRS in its "Protect Your Clients; Protect Yourself" cybersecurity campaign:

> Every tax practitioner in the United States – whether a member of a major accounting firm or an owner of a one-person storefront – is a potential target for highly sophisticated, well-funded and technologically adept cybercriminals around the world. Their objective: to steal your clients' data so they can file fraudulent tax returns that better impersonate their victims. Their tactics are: to trick you into giving up computer passwords, e-Services passwords, to steal your EFINs or CAF numbers or even to take remote control of your entire computer system.

The IRS, state tax agencies and tax industries – working in partnership with the Security Summit – currently are conducting an awareness campaign called, "Don't Take the Bait," that includes warning tax professionals about the various types of phishing scams, including ransomware.

In late August, the IRS issued an "urgent warning" about a new phishing scheme that uses IRS and FBI emblems on emails to impersonate those agencies in order to get unsuspecting victims to click on a link and download ransomware onto their computers. The IRS also re-published an earlier alert for payroll and human resource personnel regarding the renewed threat of "email spoofing" attacks designed to steal W-2 information. Clearly, the threat from hackers and other bad actors on the Internet is not going away anytime soon.

Ransomware attacks, often facilitated through email phishing, remain the malware *du jour* of many hackers in 2017. As described by the FBI, "hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses—these are just some of the entities impacted by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them."

Cybersecurity Regulations Continue to Emerge and Evolve

Despite the rising threat, regulating cybersecurity remains a relatively new and evolving area. There is no single, uniform, all-encompassing set of mandatory cybersecurity regulations to govern all industries and organizations in the United States. In February 2014, the federal government released an initial, voluntary "framework" for how to improve cybersecurity for critical infrastructure in our country; a draft update to that framework was released in January 2017 and is still under review. Organizations can use the framework as a reference point to evaluate and improve their current cybersecurity posture.

In the last several years, different industries and governmental agencies have taken different approaches in developing more specific cybersecurity policies, recommended practices and even some mandatory regulations. In some industries, there are hints of an early, still-developing standard of care.

Earlier this year, the AICPA unveiled its "Cybersecurity Risk Management Reporting Framework." As described by the AICPA, "the framework is a key component of a new System and Organization Controls for Cybersecurity engagement, through which a CPA reports on an organization's enterprise-wide cybersecurity risk management program."

In the financial and banking areas, there have been significant regulatory developments. For example, at the end of August, the first set of state-enacted cybersecurity regulations for financial institutions took effect in New York, promulgated by the New York Department of Financial Services.

The state of Colorado's Division of Securities also recently adopted new rules that add cybersecurity requirements for certain entities with Colorado securities licenses.

On the federal level, a veritable cornucopia of agencies has issued policy statements, guidance and recommendations dealing with cybersecurity.

In April 2015, the U.S. Securities and Exchange Commission's Division of Investment Management (the "Division") issued a Guidance Update to investment and fund advisers on the topic of improving cybersecurity. The Update includes the following measures, all of which are applicable today, and are part of an emerging cybersecurity "standard of care" for organizations to meet:

Companies should create a strategy that is designed to prevent, detect and respond to cyber-security threats.

Conduct Periodic Assessments to Identify Threats and Vulnerabilities

Businesses should conduct a periodic assessment of:

1. The nature, sensitivity and location of information that the firm collects, processes and/or stores, and the technology systems it uses;
2. Internal and external cybersecurity threats to and vulnerabilities of the firm's information and technology systems;
3. Security controls and processes currently in place;
4. The impact, should the information or technology systems become compromised; and
5. The effectiveness of the governance structure for the management of cybersecurity risk.

The point of these assessments is to identify potential threats and vulnerabilities to allow a firm to better prioritize and mitigate those risks.

Develop a Cybersecurity Strategy to Prevent, Detect and Respond to Threats

Companies should create a strategy that is designed to prevent, detect and respond to cybersecurity threats. Such a strategy could include:

1. Controlling access to various systems and data via user credentials, authentication and authorization methods, firewalls and/or perimeter defenses, tiered access to sensitive information and network resources, network segregation and system hardening;
2. Data encryption;
3. Protecting against the loss or exfiltration of sensitive data by restricting the use of removable storage media and deploying software that monitors technology systems for unauthorized intrusions, the loss or exfiltration of sensitive data, or other unusual events;
4. Data backup and retrieval; and
5. Development of an incident response plan.

As with any strategies or plans, regular testing can enhance their effectiveness.

Implement the Strategy Through Written Policies and Procedures and Training

Businesses should implement the strategy through written policies and procedures and training that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cybersecurity policies and procedures.

The FDIC has issued its own set of cybersecurity recommendations, as has the Federal Financial Institutions Examination Council (which includes the Federal Reserve Board and the Comptroller of the Currency).

Non-governmental entities, such as FINRA, have also published guidance on cybersecurity.

Consequences

Cyberattacks can be costly, if not terminal events for organizations unprepared to quickly discover, defend and recover from them. According to the Ponemon Institute's 2017 Cost of Data Breach Study, the average per record cost of a data breach was $225 in the United States, with the overall organizational cost (cost per record x the number of records breached) was $7.35 million. Some key takeaways from the Ponemon Study include the following:

- The faster the data breach can be discovered and contained, the lower the costs;
- Incident response teams and the extensive use of encryption reduce costs;
- Hackers and malicious insiders cause the most data breaches;
- The inability to retain customers has serious financial consequences.

Hackers and other bad actors are persistent and creative, and they cannot be ignored. Maintaining proper cybersecurity controls is essential to the viability of any organization that touches protected personal, financial or health data. Keeping track of, and complying with voluntary standards and recommended practices, as well as any applicable mandatory regulations is now part of the cost of doing business. Companies that invest the time to enhance their cybersecurity competence can find that it creates a competitive advantage. ■

Patrick X. Fowler *is an attorney with Snell &Wilmer, LLP. He will be presenting the program, Cybersecurity and Data Privacy Regulations: Adapting to the New Normal, at the ASCPA Technology Conference on Dec. 6.*

Patrick Fowler will present the program, Cybersecurity and Data Privacy Regulations: Adapting to the New Normal, at the ASCPA Technology Conference on Dec. 6.