Top Cybersecurity Tactics for CPAs in the Digital Age

BY STACEY HOWARD

While navigating digital transformation, the world positions the accounting profession in its crosshairs. Many CPAs and accounting firms are sitting on a treasure trove of sensitive data and are becoming prime targets for cybercriminals.

Technology has introduced innovative measures for streamlining processes and enhancing the efficiency of CPA firms. However, everything that glitters is not gold.

According to IBM's Cost of a Data Breach report, firms investing in cybersecurity now are saving an average cost of $4.45 million/data breach, a 15% increase over the past three years.

These advancements also open up the accounting profession to novel risks. Consequently, cybersecurity solutions have become imperative for CPAs to safeguard their businesses and clients.

THE RISE OF DIGITAL TRANSFORMATION IN ACCOUNTING

CPAs and accounting firms are actively reshaping themselves through digital transformation. They are embracing advanced tools and technologies such as artificial intelligence (AI), machine learning and automation. These innovative measures enhance efficiency and empower CPAs and accountants to transition their focus from mere data crunching to high-value services. This shift includes strategic financial planning and risk management, even business advisory services.

Technology has revolutionized the accounting profession; however, it introduces new challenges – notably cybersecurity threats – that demand immediate attention.

WHY HACKERS ARE TARGETING CPAS

In recent years, we have witnessed a shift in focus among hackers. They no longer concentrate solely on the prominent, headline-making targets associated with previous breaches. Instead, their attention extends to smaller and less conspicuous victims.

Emerging patterns suggest that certain financial cybersecurity criminals might even circumvent launching ransomware attacks against larger organizations. This will help to prevent national political or law enforcement responses – as Sherry Bambrick, Senior Underwriter for the AICPA Member Insurance Programs, asserts. This is an evolving strategy carrying significant implications for CPAs.

Bambrick stated: "Hackers find CPA firms particularly attractive because these entities essentially aggregate financial and personal identifiable information (PII) data. The escalating emphasis on smaller organizations, along with the vast amount of PII potentially held by a firm, significantly amplifies the risk they encounter."

Hackers target CPA firms not only for their access to client funds but also due to the assumption that mid-size and smaller firms lack robust information security strategies. These assumptions are born from a misguided belief held by their leaders that they're too small to be targeted.

WHAT ARE THE BEST CYBER-SECURITY PRACTICES FOR CPAS?

Let's tap into some of the cybersecurity practices to stay ahead in the competitive market.

Continued on page 23

1 Proactively Detect Risks

CPAs must proactively detect risks and vulnerabilities and protect against breaches or "active" concerns such as phishing and ransomware. They need to put measures in place for this.

Moreover, these protective strategies should address the technology involved and its users. Comprehensive security is a shared responsibility where both digital systems and human factors intersect in all their complex intricacies. How you can go about it:

- Use risk assessments for a health check of your business;
- Implement zero trust factor that aims to protect the network and security infrastructure;
- Watch for advanced persistent threats (APTs) and monitor end-points by using tools such as end-point detection response (EDR); and
- Use software like MetricStream IT and cyber risk management software for risk identification.

2 Conduct Training and Build a Secure Culture

CPA firm owners should conduct security awareness training that includes real-world exercises. In particular, realistic and challenging phishing simulations should be implemented. To reinforce best practices, adeptly blend teaching with engaging activities.

Construct a firm emphasizing a "culture of security," focusing on data governance and management. Remember that the business side – not just the IT and risk management divisions – must provide robust input for this initiative. CPAs can run cybersecurity governance and risk management programs using voluntary framework, which can include the risk assessment.

For instance, the National Institute of Standards and Technology (NSIT) includes the following five continuous functions.

Identify: Develop an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities.

Protect: Proactively implement appropriate safeguards to ensure the delivery of critical services. By doing so, you can take control of your cybersecurity landscape.

Detect: Identify the occurrence of a cybersecurity event.

Respond: Take action regarding a detected cybersecurity incident.

Recover: Maintain resilience plans and restore any capabilities or services that were impaired by a cybersecurity incident.

3 Emphasize Self-Awareness Practice

Remind your employees to cultivate self-awareness, a crucial practice in today's digital landscape. Taking a moment before responding or acting upon suspicious emails can often mark the turning point; it is usually half the battle won.

To illustrate this concept, urge them to evaluate dubious URLs for anomalies and validate the sender's identity through another trusted method – perhaps by placing an essential phone call.

4 Implement Multi-Factor Authentication and Restrict Online Sharing

All access points require more than just a password to join the network, so utilize multi-factor authentication. Implementing confirmation via text messages, phone calls or fingerprints, despite its minimal effort, can significantly enhance a firm's security.

You should push employees to restrict the online sharing of work-related information, as potential attackers can leverage this practice for social engineering schemes. It will effectively mitigate cyber criminals' ammunition by refraining from incorporating details such as client or colleague names in personal social media posts.

5 Use VPN

A virtual private network (VPN) masks employees' identities, safeguarding their communications from potential attackers, a measure particularly crucial when they utilize public WiFi.

To scan and block malicious links, attachments or accounts – thus potentially intercepting and neutralizing malware from a corrupt link or attachment – requires the active tasks of installing and maintaining regular updates. Anti-virus/anti-phishing software is our tool for such critical operations.

6 Ensure Strict Control Over Data Sharing

When engaging with third-party providers, exercise stringent control measures like incorporating indemnification clauses or stipulating that the provider maintains cyber insurance in its service agreement for potential breaches on a third-party platform.

7 Plan Ahead for Any Data Breach

You must create a robust security and breach response plan that can be quickly implemented in the event of an issue. Furthermore, it is imperative to revisit and update this plan regularly. This practice helps ensure its effectiveness against the ever-evolving risk landscape.

BOTTOM LINE

Integrating AI in accounting services not only augments cybersecurity defenses but also empowers firms to navigate the complexities of modern digital landscapes with confidence. See how at this link.

The evolution of digital transformation in accounting necessitates a paramount focus on cybersecurity. As cyber threats continue to advance, CPA firms must actively enhance their security measures. This is crucial for both protecting sensitive data and ensuring compliance with industry regulations.

STACEY HOWARD is an accomplished blogger with over a decade of experience in the field of accounting and bookkeeping. With her extensive knowledge and expertise, she has been working as an accountant at a leading business process management firm Accounting To Taxes. Throughout her career, she has developed a passion for sharing valuable insights and information on various accounting industries through her engaging and informative write-ups. Her contributions to the accounting community have been widely recognized, making her a sought-after expert in the field.