difficult to develop an appropriate response to those risks. What kind of data is being protected? What cyber threats will the client face? Every dollar spent on ...

Feb. 14, 2018

CPAs have a great opportunity to solidify their role as the trusted advisor for the next generation of businesses by adding cybersecurity as a core competency. The AICPA is increasingly recognizing the need for CPAs to evolve and assist their clients with mitigating cyber risks. The AICPA has introduced a new System and Organization Controls (SOC) for Cybersecurity engagement, through which a CPA provides assurance regarding a company's cybersecurity program to board members, senior

executives and external stakeholders. CPAs should get educated about cyber risks and

Pitfall #2: Focusing solely on protection

The mindset of many IT professionals is still focused on protecting the external perimeter, where it is impossible to stay 100% protected. Today's middle market companies are simply outgunned, so a critical step is shifting attention from protecting to responding. The National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF) classifies the major functions of an information security program into five categories: (1) identify, (2) protect, (3) detect, (4) respond and (5) recover. CPAs should make sure their clients are not focused solely on (2) protect but also building the capability to (3) detect when their organization has been breached, and thus can (4) respond and (5) recover.

Pitfall #3: Not testing company backups

A foundational strategy for dealing with ransomware is using backups. When ransomware hits, a company can simply revert to the most recent backup. While restoring a single data file with backups is easy, restoring a complex system of interconnected applications with numerous data sets is difficult – and sometimes impossible. CPAs should work to develop strategies for responding to various ransomware scenarios and then practice those strategies. CPAs should also encourage tests of their client's ability to restore from backups.

Pitfall #4: Not educating staff regarding cyber risks

CPAs should encourage formal training regarding cyber risks. Business Email Compromise (CEO impersonation) scams focused on W-2 and wire transfer fraud have resulted in billions of losses. Despite repeated warnings, companies still unknowingly fall for these scams. Every finance, accounting and HR professional needs to know they will someday be the target of a cyber criminal. A good

cybersecurity training program will combine educating employees on cyber risks

Service Providers) who can bring world-class cybersecurity talent and expertise to a company no matter the size.

Pitfall #6: Not using a framework

Many small and midsize companies have limited structure to their cybersecurity programs, with their IT teams doing the best they can to keep cyber criminals at bay. CPAs need to encourage their clients to adopt a common language or framework for cybersecurity. Public companies are rapidly adopting the aforementioned NIST CSF as a set of standards, leading practices and recommendations for organizing and communicating with their boards and stakeholders. While originally intended for government critical infrastructure, the NIST CSF can be scaled down to fit smaller companies.

***

Cybersecurity is dramatically changing the environment in which CPAs and their clients operate. Clients will start to rely more on CPAs to provide advice, rather than just for accounting functions. Skill sets need to change, and the best first step is for CPAs to be versed in these pitfalls and how to avoid them.

———————

David Hartley is a Principal for UHY Advisors MO, Inc. where he focuses on delivering "Virtual CIO" technology consulting services to primarily middle market companies. He assists companies with everything from digital transformation and IT strategy to assessing cyber risks and implementing cybersecurity programs. David is a CPA and Certified Information Systems Auditor (CISA) with experience in technology, consulting, audit and C-suite business leadership roles. Prior to joining

UHY in 2015, David was VP & Chief Information Officer at Arch Coal, Inc.,

(NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.