Published in

Bio·IT World
Next-Gen Technology • Big Data • Personalized Medicine

Certified Public Accountants Launch Framework For Cybersecurity Audits

Contributed Commentary by Christian Leitner, OUM & Co.

July 20, 2017 | WannaCry and Petya ransomware have made headlines all over the world recently with cybercriminals beginning to target healthcare data. In February 2016, the Department of Health and Human Services (HHS) reported nearly 112 million individuals have been affected by protected health information breaches—more than 60 times the 1.8 million impacted in 2014.

Cybercriminals are stealing healthcare data by targeting vendors and third parties, both of which often have weaker security in place. In fact, 30% of breaches reported to HHS in 2016 were attributed to third party vendors. The Office for Civil Rights (OCR) has extended their reach further downstream, looking not only at Health Insurance Portability and Accountability Act (HIPAA) covered entities, but also at the practices of their business associates and their third party oversight. The new OCR approach is leading to a deeper evaluation of third party practices that go beyond self-assessments and self-monitored compliance. In addition to healthcare regulations issued by the OCR, certain states (e.g., New York) have implemented additional cybersecurity control requirements and third-party oversight covering healthcare insurers registered in their states. A lack of vigilance in ensuring that partners and other third parties are protecting patient information is a key concern of covered entities and business associates.

Cybersecurity is no longer just a topic discussed during IT meetings; it has now become a business conversation. More and more board and audit committee members at major healthcare companies view cybersecurity and loss of company reputation as a major risk to which more attention must be paid.

Board members should get involved and ask security professionals within their organizations the following questions:

- What is our real risk and exposure?
- How much risk is acceptable to our organization considering research and development or client and patient data we collect?
- How do we compare to our industry peers?
- How would we respond to an incident or breach? Do we have an incident response plan? Is it documented?
- When was it last tested?

Executive agendas will also need to address some or all of these key cybersecurity topics in committee meetings: business dependencies on technology regarding operations and growth, end-to-end data

security throughout the supply chain, the increasing number of cyber threats and increased press attention, domestic and international legislation, as well as an increased number of vulnerabilities due to more pervasive use of technology.

In May 2017, The American Institute of CPAs (AICPA) released their Cybersecurity Attestation Framework (CAF). Also known as Service Organization Control (SOC) for cybersecurity, this framework builds on top of the long-established Trust Services Principles (TSPs) reporting. TSPs are the underlying criteria for SOC reports, but were usually limited to one or more systems delivering services to an organization's customers. The newly released CAF uses these TSPs, but applies them across an entire organization instead of just a specific system or department. In what could be seen as "SOC reporting on steroids," the scope is much larger and covers all aspects of an organization's cybersecurity program.

The purpose of such an attestation is to deliver an independent evaluation by a Certified Public Accountant (CPA) registered and in good standing with the AICPA. CPAs are in the unique position to perform these audits given the AICPA standards, which are available to the public and whose scope is the same for every organization. Many CPAs are currently promoting this as a separate service line to be performed annually or semi-annually.

The reports could be a vital tool as you deal with cybersecurity questions related to your own organization, your customers, and other third parties identified during your risk assessment. The independence factor will move this approach above the existing self-monitoring and self-assessment reports given to stakeholders. For example, a customer will get the report addressing the effectiveness of its cybersecurity program according to the TSPs and can then use it to show internal (e.g., board members, audit committees) or external (e.g., customers, third-party contractors) stakeholders that their program can be relied upon.

Before its public release in May, the CAF received positive feedback from early adopters and professionals in the cybersecurity field. Our hope is that the CAF will open new ways for organizations across the U.S. to deal with cybersecurity questions and help evaluate internal and external cybersecurity risks from a business perspective.

Christian Leitner, Director of IT/IS Assurance at OUM & Co., is a Certified Information Systems Auditor (CISA) with more than 10 years of experience in all aspects of technology infrastructure and compliance. He has been leading Sarbanes-Oxley IT audits, SSAE16 SOC1/SOC2/SOC3 engagements and other IS compliance consulting projects since 2004. He also has in-depth knowledge of hardware and software implementations, business process analysis and redesign, IT project management, IT risk advisory services, disaster recovery and business continuity planning. He can be reached at cleitner@oumcpa.com.

San Francisco, CA
415.434.3744

Carlsbad, CA
800.208.3367

oumcpa.com