Than Regulators

As pressure to develop more effective corporate cybersecurity programs continues to mount, 62.7 percent of C-suite and other executives in a recent Deloitte poll expect board of director requests for reporting on cybersecurity program effectiveness to ...

Jun. 07, 2018

As pressure to develop more effective corporate cybersecurity programs continues to

feeling obliged to provide greater transparency and uniformity when it comes to cybersecurity reporting—alone or as part of an enterprise-wide risk management program."

Industries expecting higher than average board requests on cybersecurity program effectiveness are life sciences and health care (71.8 percent); financial services institutions (69.9 percent); and technology, media and telecoms (66.3 percent). Financial services also expects higher than average cybersecurity regulatory scrutiny (69.5 percent).

Poll results point to one possible explanation: Just 16.7 percent of executives say they are highly confident in the effectiveness of their organization's current cyber program. The vote of high confidence drops even lower in industries such as financial services (14.3 percent); technology, media and telecoms (11.8 percent); and energy and resources (5.6 percent).

Further, as reporting structures for chief information security officers (CISOs) vary by organization, ownership of cybersecurity effectiveness measures can often be unclear. In fact, 28.5 percent of responding executives say their CISOs report to the CIO, 25.4 percent say CISOs report to CEOs, 9.7 percent say CISOs report to chief compliance officers or chief risk officers and 3 percent say CISOs report to chief legal officers. Some (12.9 percent) of executives don't know to whom CISOs report at all.

One-third plan to adopt AICPA SOC Cybersecurity framework

According to poll data, one-third (32.3 percent) of executives plan to adopt the American Institute for Certified Public Accountants (AICPA) System and Organization Controls (SOC) for Cybersecurity framework, with 19.2 percent reporting plans to do so within the next 12 months.

The AICPA SOC for Cybersecurity attestation framework was finalized in April

reporting framework.

"Whether organizations leverage the AICPA SOC for Cybersecurity alone or in concert with other industry-specific frameworks or standards, it offers another mechanism that can provide a higher degree of assurance around the effectiveness of an entity's cybersecurity risk management program," said Gaurav Kumar, a Deloitte Risk and Financial Advisory principal, Deloitte & Touche LLP. "An independent cybersecurity attestation can also serve to enhance stakeholder trust with readiness efforts that: focus on the appropriate level of risk and control assessment needed to protect the business's 'crown jewel' assets, monitor program strength continuously, and chart a measurable path toward ongoing improvements."

Organizations interested in implementing the AICPA SOC for Cybersecurity framework should first consider a readiness assessment including the following activities:

- **Perform a risk assessment** to identify the highest criticality assets (e.g., intellectual property, customer data, etc.) and update existing IT risk and control catalogs.
- **Define the company's cyber risk management program** and **conduct an IT risk and controls assessment** for critical assets and underlying infrastructure.
- **Conduct a gap analysis** of identified control deficiencies.
- **Develop a remediation roadmap** with prioritized activities and defined due dates.
- **Execute remediation activities** to address the control deficiencies identified.

Accounting • Advisory • Auditing • Technology

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