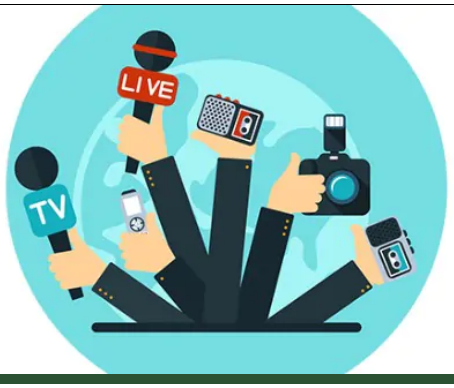
Deloitte.



Press releases

Corporate Boards May Be More Likely Than Regulators to Scrutinize Cybersecurity Program Effectiveness This Year

New Deloitte poll shows one third of executives plan to adopt AICPA's SOC for Cybersecurity framework.

New York, June 06, 2018 — 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 increase in the next 12 months. A slightly lower 57.3 percent of executives expect increased cybersecurity regulatory scrutiny during the same period.

"Boards want to gain a higher level of confidence in their organizations' cyber risk management program effectiveness, so an expectation of more robust and consistent reporting is not surprising," said Andrew Morrison, Deloitte Risk and Financial Advisory principal, Deloitte & Touche LLP. "Corporate executives in all sectors are 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 2017 and serves as a voluntary market-driven solution intended to provide companies with a common language reporting mechanism to communicate with key stakeholders on how they are effectively managing cybersecurity risk. Improving stakeholder visibility, including boards and audit committees, regulators, customers, business partners and investors, is an underlying tenet of the framework. Boards planning to have a robust assurance reporting process to effectively challenge management's assertions with respect to company-wide cybersecurity risk management program effectiveness can leverage the AICPA's SOC for Cybersecurity 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

Media contacts:

Lauren Hallman
Public Relations
Deloitte Services LP
+1 215 282 1213

Shelley Pfaendler
Public Relations
Deloitte Services LP
+1 212 492 4484

- **Develop a remediation roadmap** with prioritized activities and defined due dates.
- **Execute remediation activities** to address the control deficiencies identified.

About the online poll
On Feb. 22, 2018, a Deloitte Dbriefs webcast titled "Fight the good fight: Three lines of cyber defense working arm-in-arm" polled more than 1,130 C-suite and other executives about the role of any organization's three lines of defense in cybersecurity. Respondents largely work in the financial services (29.1 percent); consumer and industrial products (26.9 percent); and technology, media and telecommunications (16.6 percent) industries. Answer rates differed by question.

About Deloitte
Deloitte provides industry-leading audit, consulting, tax and advisory services to many of the world's most admired brands, including more than 85 percent of the Fortune 500 and more than 6,000 private and middle market companies. Our people work across more than 20 industry sectors to make an impact that matters — delivering measurable and lasting results that help reinforce public trust in our capital markets, inspire clients to see challenges as opportunities to transform and thrive, and help lead the way toward a stronger economy and a healthy society. Deloitte is proud to be part of the largest global professional services network serving our clients in the markets that are most important to them.

Get in touch

Andrew Morrison
Principal | Cyber Risk Services
anmorrison@deloitte.com
+1 404 220 1170

Andrew is a principal in Deloitte & Touche LLP's Cyber Risk Services practice and specializes in assisting clients with the risk associated with cyber threats. Andrew currently serves as the US leader... More

Gaurav Kumar
Principal | Deloitte Risk and Financial Advisory
gukumar@deloitte.com
+1 212 436 2745

Gaurav is a principal in Deloitte & Touche LLP. He advises clients on managing risk and internal controls, including those focused information technology risk management, identity access management, a... More

Jeff Schaeffer
Managing Director | Risk and Financial Advisory
jschaeffer@deloitte.com
+1 973 223 4864

Jeff is a managing director in Deloitte's Risk and Financial Advisory practice with more than 15 years of experience specializing in risk management, corporate governance and compliance, and controls ... More

Recommendations

Deloitte: Upstream Oil & Gas Companies Face Portfolio Predicament

Deloitte wins six prestigious Oracle Excellence Awards for the second consecutive year

Organization recognized for experience in delivering specialized services and solutions across multiple industries

Cyber risk management oversight and reporting

Proactive steps to protecting and advancing your brand

Related topics

Board of Directors | Risk Assurance | Cyber Risk | Press Releases

Contact us	Search jobs	Submit RFP

https://www.facebook.com/DeloitteUS

https://www.twitter.com/deloitteus

https://www.linkedin.com/company/1038

https://www.youtube.com/user/DeloitteLLP

http://www.glassdoor.com/Overview/Working-at-Deloitte-EI_IE2763.11,19.htm

https://www.instagram.com/lifeatdeloitteus/

Professional Services means audit, tax, consulting, and advisory.

36 USC 220506