slowdown in cyber threats, the Deloitte poll taken during a webcast on cyber preparedness and wargaming exposes a still siloed approach to cybersecurity that can be ...

Oct. 30, 2018

Nearly half (46 percent) of executive-level respondents to a Deloitte poll say their organizations have experienced a cybersecurity incident over the past year, with

more than 1,500 surveyed professionals feeling only “somewhat confident” in their

response plan, with 20 percent reporting a lack of resources such as funding, tools, and skills as the biggest challenge.

“We used to say it’s ‘not if, but when’ an organization will experience a cyber incident. That message has evolved well beyond a single incident to ‘how often’ or ‘how to respond to and withstand persistent attacks,’” said Andrew Morrison, principal, Deloitte Risk and Financial Advisory Cyber Risk Services, Deloitte & Touche LLP. “Improving internal processes and providing employees with the knowledge, practice and skills needed to succeed can help organizations mitigate risk through preparedness, as well as increase overall business resilience to future attacks.”

Forty-nine percent of executive and C-level respondents to the poll admitted that their organization does not conduct cyber wargaming exercises, with more than one-third (34 percent) indicating that they do not know their individual role within their organization’s cyber incident response plan. These findings are consistent with Deloitte’s recently released CEO and Board Risk Management Survey, which identified cybersecurity as the biggest threat to organizations —and yet only 25 percent of the 400 CEOs and board members surveyed said their organizations are actively wargaming or scenario planning for cyber incidents.

“Cyber wargames are an important way to raise awareness of the latest cyber risks and attack types, as well as cyber risk management and adaptive response capabilities an organization needs during, after, and preparing for the next cyber incident,” said Daniel Soo, cyber wargaming leader for Deloitte cyber risk services, and Deloitte Risk and Financial Advisory principal, Deloitte & Touche LLP. “The most impactful wargames are those that use live knowledge of an organization’s current threat environment to support the decision-making process across operations, finance, regulatory, marketing, and beyond.”

A typical wargame allows participants to hone organizational reflexes and

exercises amongst specific executive and functional teams is important, identifying intersections between different teams and mixing siloes creates a more realistic dynamic.

- Keep it simple at the start. The minutia of daily work environments won't disappear during a cyber incident, but can distract and detract from the lessons learned during a wargaming exercise. When your organization is just getting started with wargaming, gathering participants in one place can be valuable to set the stage.
- Plausibility is crucial. Identifying a realistic scenario with realistic vulnerabilities drives real actionable results.

Deloitte Cyber Risk Services has conducted hundreds of cyber wargaming exercises over the past several years, with organizations now repeating exercises and testing new scenarios as often as six to eight times per year. This shift in cyber preparedness is consistent with the number of companies that are aligned across industry organizations that practice their collective cyber response and information sharing procedures. Examples include: simulations such as the financial industry's SIFMA Quantum Dawn exercises; Cyber RX in the healthcare industry; as well as Cyber Storm, a biennial cyber exercise sponsored by the Department of Homeland Security that spans industries.

Accounting • Advisory