Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025

Board Directors Rate Cybersecurity Second-Highest Source of Risk for the Enterprise

By 2025, 40% of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member, up from less than 10% today, according to Gartner, Inc.

This is one of several organisational changes Gartner expects to see at the board, management and security team level, in response to greater risk created by the expanded digital footprint of organisations during the pandemic.

According to the Gartner 2020 Board of Directors Survey*, cybersecurity-related risk is rated as the second-highest source of risk for the enterprise, following regulatory compliance risk. However, relatively few directors feel confident that their company is properly secured against a cyberattack.

“To ensure that cyber risk receives the attention it deserves, many boards of directors are forming dedicated committees that allow for discussion of cybersecurity matters in a confidential environment, led by someone deemed suitably qualified,” said Sam Olyaei, research director at Gartner. “This change in governance and oversight is likely to impact the relationship between the board and the chief information security officer (CISO).”

While CISOs should experience more scrutiny as a result, they are also likely to receive more support and resources, according to Gartner. CISOs must expect executive conversations to shift away from performance and health-related discussions to risk-oriented and value-driven exercises.

Gartner also predicts that by 2024, 60% of CISOs will establish critical partnerships with key executives in sales, finance and marketing, up from less than 20% today.

“Effective CISOs realize that heads of sales, marketing and business unit leaders are now key partners as the use of technology and, subsequently, the incurrence of risk happens outside of IT,” said Mr. Olyaei.

According to the Gartner CISO Effectiveness Index, top-performing CISOs regularly meet with three times as many non-IT stakeholders as they do IT stakeholders; and they meet with them more frequently than bottom performers.

Cyber, physical and supply chain security converge

For asset-intensive enterprises such as utilities, manufacturers and transportation networks, security threats targeting cyber-physical systems present an increasing risk to the organisation.

Bad actors increasingly target weaknesses wherever they are, as demonstrated by the surge in ransomware affecting organisations’ operational systems and recent supply chain attacks.

The siloed nature of today’s security disciplines then becomes its own risk and a liability to the organisation, and the IT-centric focus of most security teams needs to expand to include threats in the physical world.

Gartner predicts that by 2025, 50% of asset-intensive organisations will converge their cyber, physical and supply chain security teams under one chief security officer role that reports directly to the CEO.

Remote work can improve access to IT security talent

Gartner research conducted pre-COVID-19 found that 61% of organisations surveyed were struggling to find and hire security professionals.

“As organisations shifted to remote working in response to the pandemic, it proved that some, if not all, security capabilities could be delivered remotely,” said Richard Addiscott, senior research director at Gartner. “This includes security monitoring/operations, policy development, security governance and reporting, security awareness, and incident response via dispersed teams. Cybersecurity teams can work remotely and still provide effective capabilities.”

As a result, Gartner predicts that by 2022, 30% of all security teams will have increased the number of employees working remotely on a permanent basis.

Gartner recommends that security and risk leaders consider adapting their operating models and expand their job advertising to gain access to candidates residing outside of their organisation’s traditional recruitment geographies.

*For Editors: The 2021 Gartner Board of Directors Survey was conducted via an online survey from May through June 2020 with 265 respondents in the U.S., EMEA and APAC in a board of director role or a member of the corporate board of directors.

Gartner clients can read more in the report “Predicts 2021: Cybersecurity Program Management and IT Risk Management.”

Gartner Security & Risk Management Summits

Gartner analysts will provide the latest research and advice for security and risk management leaders at the Gartner Security & Risk Management Summit 2021, taking place February 22-23 in the Middle East, March 17-18 in India, March 23-24 in APAC, September 13-15 in London, September 20-22 in Orlando, FL. and October 6-8 in Tokyo. Follow news and updates from the conferences on Twitter using #GartnerSEC.

About Gartner

Gartner, Inc. (NYSE: IT) is the world’s leading research and advisory company and a member of the S&P 500. We equip business leaders with

indispensable insights, advice and tools to achieve their mission-critical priorities and build the successful organisations of tomorrow.

Our unmatched combination of expert-led, practitioner-sourced and data-driven research steers clients toward the right decisions on the issues that matter most. We are a trusted advisor and an objective resource for more than 14,000 organisations in more than 100 countries — across all major functions, in every industry and organisation size.

To learn more about how we help decision makers fuel the future of business, visit www.gartner.com.

Contacts

Susan Moore
+61 2 9459 4692
mailto: susan.moore@gartner.com