IBM UK Newsroom

IBM Study Finds C-Suite and CISOs Not Aligned on How to Combat Cybercriminals

Education and Engagement Needed to Empower C-Suite for New Security Landscape

ARMONK, N.Y. - 17 Feb 2016: IBM (NYSE: IBM) Security and IBM's Institute for Business Value (IBV) today released a survey of more than 700 C-level executives, which found many leaders across the C-suite are confused about who the true cybersecurity adversary is and how to effectively combat them.

The new study, *Securing the C-Suite, Cybersecurity Perspectives from the Boardroom and C-Suite,* is based on interviews with CxOs, from 28 countries, across 18 industries, on cybersecurity in the enterprise. The research excluded the CISO to get a true picture of what everyone else in C-Suite thinks about cybersecurity. While on paper, cybersecurity is viewed as a top concern of 68 percent of CxOs1, and 75 percent believe a comprehensive security plan is important, the study found key executives need to be more engaged with CISOs beyond planning for security, and take more active role.

A major finding of the study was that 70 percent of CxOs think rogue individuals make up the largest threat to their organizations. The reality is that 80 percent of cyberattacks are driven by highly organized crime rings in which data, tools and expertise are widely shared according to a United Nations report2. The study found that a broad set of adversaries concerned the C-Suite including 54 percent who acknowledged crime rings were a concern, but they gave nearly equal weight of concern to competitors at 50 percent.

Over 50 percent of CEOs agree collaboration is necessary to combat cybercrime. Ironically, only one-third of CEOs expressed willingness to share their organization's cybersecurity incident information externally. This exposes a resistance to widespread and coordinated industry collaboration, while hacking groups continue to perfect their ability to share information in near real-time on the Dark Web. CEOs also emphasize that external parties need to do more; stronger government oversight, increased industry collaboration and cross-border information sharing – a dichotomy that needs to be resolved.

“The world of cybercrime is evolving rapidly but many C-Suite executives have not updated their understanding of the threats,” said Caleb Barlow, Vice President, IBM Security. “While CISOs and the Board can help provide the appropriate guidance and tools, CxOs in Marketing, Human Resources, and Finance, some of the most sensitive and data-heavy departments, should be more proactively involved in security decisions with the CISO.”

In fact, Marketing, Human Resources, and Finance departments represent prime targets for cybercriminals as they manage some of the most sensitive customer and employee data, manage corporate financials and have access to banking details. In the study, roughly 60 percent of CFOs, CHROs, and CMOs readily acknowledge they, and by extension their divisions, are not actively engaged in cybersecurity strategy and execution. For example, only 57 percent of CHRO's report they have rolled out employee training that addresses cybersecurity, a first step in getting employees engaged on cybersecurity.

What Organizations Can Do

An overwhelming number of the CxOs surveyed, 94 percent, believe there is some probability that their company will experience a significant cybersecurity incident in the next two years. According to IBM's analysis, 17 percent of the respondents feel prepared and capable to respond to these threats. IBM identified standout respondents to the survey, classifying 17 percent as "Cyber-Secure" respondents, the most prepared and capable CxOs. "Cyber Secure" leaders are two times more likely to have incorporated C-Suite collaboration into the cybersecurity program and two times more likely to have elevated cybersecurity to a regular agenda item at the Board level.

"Cyber-Secure" Tips for Organizations:

- **Understand the Risk**: Evaluate your ecosystem for risks, conduct security risk assessments, develop education and training for employees and incorporate security into the enterprise risk plan.
- **Collaborate, Educate & Empower**: Establish a security governance program, empower the CISO, elevate and regularly discuss cybersecurity at C-Suite meetings, include the C-suite in developing an incident response plan.
- **Manage Risk with Vigilance & Speed**: Implement continuous security monitoring, leverage incident forensics, share and utilize threat intelligence to secure the environment, understand where the organization's digital assets reside and develop mitigation plans accordingly, develop and enforce cybersecurity policies.

To download the full report and infographic, go to **ibm.com/security/ciso**.

About IBM Security

IBM's security platform provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

- *"Redefining Boundaries: Insights from the Global C-suite Study." IBM Institute for Business Value. November 2015. http://www-935.ibm.com/services/c-suite/study/study/*
- *UNODC Comprehensive Study on Cybercrime 2013*

---

https://uk.newsroom.ibm.com/2016-Feb-17-IBM-Study-Finds-C-Suite-and-CISOs-Not-Aligned-on-How-to-Combat-Cybercriminals