IBM Study Reveals Critical Shift in the Role of Chief Information Security Executives Globally
Thursday, May 03, 2012 12:00:00 PM (GMT)

Analysis of 130+ interviews presents a new class of security chiefs; CISO role follows the evolution of CIO and CFO with more strategic organizational responsibilities

ARMONK, N.Y., May 3, 2012 /PRNewswire/ -- A new IBM (NYSE: IBM) study reveals a clear evolution in information security organizations and their leaders with 25 percent of security chiefs surveyed shifting from a technology focus to strategic business leadership role.

(Logo: http://photos.prnewswire.com/prnh/20090416/IBMLOGO)
(Photo: http://photos.prnewswire.com/prnh/20120503/NY00157-a)
(Photo: http://photos.prnewswire.com/prnh/20120503/NY00157-b)

In IBM's first study of senior security executives, its Center for Applied Insights interviewed more than 130 security leaders globally and discovered three types of leaders based on breach preparedness and overall security maturity. Representing about a quarter of those interviewed, the "Influencer" senior security executives typically influenced business strategies of their firms and were more confident and prepared than their peers—the "Protectors" and "Responders."

Overall, all security leaders today are under intense pressure, charged with protecting some of their firm's most valuable assets – money, customer data, intellectual property and brand. Nearly two-thirds of Chief Information Security Executives (CISOs) surveyed say their senior executives are paying more attention to security today than they were two years ago, with a series of high-profile hacking and data breaches convincing them of the key role that security has to play in the modern enterprise. More than half of respondents cited mobile security as a primary technology concern over the next two years. Nearly two-thirds of respondents expect information security spend to increase over the next two years and of those, 87 percent expect double-digit increases.

Rather than just reactively responding to security incidents, the CISO's role is shifting more towards intelligent and holistic risk management– from fire-fighting to anticipating and mitigating fires before they start. Several characteristics emerged as notable features among the mature security practices of "Influencers" in a variety of organizations:

- ***Security seen as a business (versus technology) imperative*:** One of the chief attributes of a leading organization is having the attention of business leaders and their boards. Security is not an *ad hoc* topic, but rather a regular part of business discussions and, increasingly, the culture. In fact, 60 percent of the advanced organizations named security as a regular boardroom topic, compared to only 22 percent of the least advanced organizations. These leaders understand the need for more pervasive risk awareness – and are far more focused on enterprise-wide education, collaboration and communications. Forward-thinking security organizations are more likely to establish a security steering committee to encourage systemic approaches to security issues that span legal, business operations, finance, and human resources. Sixty-eight percent of advanced organizations had a risk committee, versus only 26 percent in the least advanced group.
- ***Use of data-driven decision making and measurement:*** Leading organizations are twice as likely to use metrics to monitor progress, the assessment showed (59 percent v. 26 percent). Tracking user awareness, employee education, the ability to deal with future threats, and the integration of new technologies can help create a risk-aware culture. And automated monitoring of standardized metrics allows CISOs to dedicate more time to focusing on broader, more systemic risks.
- ***Shared budgetary responsibility with the C-suite*:** The assessment showed that within most organizations, CIOs typically have control over the information security budget. However, among highly ranked organizations, investment authority lies with business leaders more often. In the most advanced organizations, CEOs were just as likely as CIOs to be steering information security budgets. Lower ranking organizations often lacked a dedicated budget line item altogether, indicating a more tactical, fragmented approach to security. Seventy-one percent of advanced organizations had a dedicated security budget line item compared to 27 percent of the least mature group.

"This data painted a profile of a new class of CISO leaders who are developing a strategic voice, and paving the way to a more proactive and integrated stance on information security," said David Jarvis, author of the

report and senior consultant at the IBM Center for Applied Insights. "We see the path of the CISO is now maturing in a similar pattern to the CFO from the 1970s, the CIO from the 1980s – from a technical one to a strategic business enabler. This demonstrates how integral IT security has become to organizations."

Recommendations to Evolve the Security Role in an Enterprise
To create a more confident and capable security organization, IBM recognizes that security leaders must construct an action plan based on their current capabilities and most pressing needs. The report offers prescriptive advice from its findings on how organizations can move forward based on their current maturity level.

For example, those "Responders" in the earliest stage of security maturity can move beyond their tactical focus by establishing a dedicated security leadership role (like a CISO); assembling a security and risk committee measuring progress; and automating routine security processes to devote more time and resources to security innovation.

"Security in a hyper-connected era presents a new set of challenges, but these can be greatly eased by implementing innovative practices and adopting a more integrated, holistic approach," said Marc van Zadelhoff, an author of the report and vice president of Strategy, IBM Security Systems. "CISOs that prioritize these factors can help their organizations significantly improve business processes and achieve measurable success in their progress toward building a risk-aware culture that is agile and well-equipped to deal with future threats."

About the Assessment
The IBM Center for Applied Insights study, "Finding a strategic voice: Insights from the 2012 IBM Chief Information Security Officer Assessment," included organizations spanning a broad range of industries and seven countries. During the first quarter of 2012, the Center conducted double-blind interviews with 138 senior business and IT executives responsible for information security in their enterprises. Nearly 20 percent of the respondents lead information security in enterprises with more than 10,000 employees; 55 percent are in enterprises with 1,000 to 9,999 employees.

To access the full study, visit ibm.com/smarter/cai/security.

About IBM Security
IBM's security portfolio 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, network security and more. IBM operates the world's broadest security research and development organization and delivery organization. This comprises nine security operations centers, nine IBM Research centers, 11 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM monitors 13 billion security events per day in more than 130 countries and holds more than 3,000 security patents.

For more information on IBM security, please visit: www.ibm.com/security.

Contact:

Tod Freeman
IBM Media Relations
415-320-5893
tefreema@us.ibm.com

Colleen Haikes
IBM Media Relations
415-545-4003
chaikes@us.ibm.com

SOURCE IBM

Countries: United States

Industries: Computer Electronics, Hardware & Software, High Tech Security, Multimedia, Internet & Wireless Technology
Languages: English
Primary Identifiers: IBM-US
Related Identifiers: IBM-US