Survey finds executive cybersecurity decisions are evolving from compliance to proactive cyber-risk management

October 28 2015, by Kim Cobb

A new research study from SMU's Darwin Deason Institute for Cyber Security finds that executives are changing the way they manage and invest in cybersecurity, moving away from limited, reactive approaches and adopting systemic risk management frameworks that combine hardware, software and operations protocols to mitigate cyber risk.

The study, Identifying How Firms Manage Cybersecurity Investment, was sponsored by IBM Security and based on a semi-structured survey of 40 executives across financial, retail, healthcare and government sectors. Participants, most of whom were chief information security officers (CISOs), were selected primarily from large firms.

The study revealed several signs of increasing support for cybersecurity programs, including:

- More than 80 percent of those interviewed reported broad and increasing support among senior-level management and corporate boards for their cybersecurity efforts.
- Eighty-eight percent of respondents reported that their security budgets have increased.
- The majority of respondents cited news coverage of large and harmful security breaches as the driver of that support.
- In an interesting twist of perception, while 46 percent of interview subjects believe their organization is spending the right

amount of money on cybersecurity, 64 percent reported that their peers were spending too little.

While most of those surveyed said getting funding for their cybersecurity efforts is not a hurdle, many executives talked about the difficulty they experience in finding and hiring skilled cybersecurity personnel. And while findings were similar across most of those interviewed from the private sector, the relatively small number of government executives surveyed noted that the lengthy budgeting processes they must work through make it difficult to react quickly to the emergence of new threats.

"Cybersecurity is more than a technology challenge," said Fred Chang, director of the Deason Institute in SMU's Bobby B. Lyle School of Engineering. "Dealing with the landscape as it exists today means making decisions within specific management cultures and understanding what drives the decision-making process. By explaining the move from compliance to risk-based cybersecurity programs we see in many C-suites, this report connects the dots for people making important decisions about what it takes to maintain privacy, financial security and operating capability—all of which are vulnerable."

The widespread use of security frameworks shows a general maturation of cyber risk management, the study notes.

"Companies are realizing that simply checking the box for compliance requirements is no longer a sufficient security strategy," said Bob Kalka, Vice President, IBM Security. "Hackers are becoming increasingly sophisticated in the battle for corporate data, and the survey results show that companies are evolving their security to keep pace. The increasing use of strategic, risk-based frameworks is a huge step forward in protecting these organizations' most critical assets."

"This report is powerful information for anyone guiding cybersecurity decisions today," Chang said. "And it's a good example of the kind of interdisciplinary focus the Deason Institute brings to the table."

Chang joined SMU's Lyle School of Engineering in September 2013 with the goal of creating a cybersecurity program that takes an interdisciplinary approach to what is frequently perceived as a strictly technical issue. The Deason Institute, launched in January 2014, provides SMU and the Lyle School with the critical resources to advance that goal. Chang's career spans service in the private sector and in government, including as the former Director of Research at the National Security Agency.

The research team for this study also included Deason Institute Principal Investigator Tyler Moore and Scott Dynes, a visiting scholar at the Institute. Moore's research focuses on the economics of information security, the study of electronic crime and the development of policy for strengthening security. Dynes' research addresses how firms identify and manage cyber risks at the firm and sector levels, and he is well published on topics related to incentives for firms to invest in information security, as well as the economic consequences of information security failures.

Interviews with the 40 executives cited in the survey were conducted in person or by phone with one or two researchers, and lasted from 30 minutes to an hour. The interviews were semi-structured in that researchers worked from a list of common questions in every interview, but allowed the answers to those questions to serve as a launching point for follow-ups. Of the participants, 33 represented U.S. organizations and the remaining seven were international.

Interview questions included:

- What methods and inputs do you use to prioritize cyber

investment?
- Do you feel you have adequate information in managing overall cyber risk?
- Is your management supportive? Do you have sufficient budget?
- What factors are driving cybersecurity investment at your firm?
- How do you decide among offerings in the marketplace?

A key study finding was the central role that frameworks now play in defining how executives perceive risk, and how much money they are willing to spend to mitigate that risk. "Using these frameworks provides a platform for CISOs to make an understandable, compelling case for specific cybersecurity products and operations," Moore said. Or as one interviewed executive put it, "Security has to be able to have a basis to argue its point of view in a compelling story with some thought behind it, rather than 'I want to get these things because it's the next cool security thing that's out there.'"

Worth noting, Moore added, is that the lack of qualified, available cybersecurity professionals creates its own set of problems. "In some cases, CISOs say their senior management wants to fund cybersecurity measures more quickly than they can staff them," Moore said. "In other cases, senior management is hesitant to fully fund proposed cybersecurity projects because they fear the CISO doesn't have the personnel available to implement them."

The interviews were conducted between February and October 2015 and participants were assured anonymity for themselves and their firms. The authors note that the advantage of the semi-structured interview methodology is that it enables the researcher to glean detailed contextual information that would not be possible under a more structured interview scenario. The disadvantage, they note, is that the contextual findings do not generalize to the profession as a whole.

The findings described in the report, Identifying How Firms Manage Cybersecurity Investment, are not to be construed as an endorsement of any person, product or company by the Darwin Deason Institute for Cyber Security at SMU. Note that the respondent opinions presented in the report do not necessarily reflect the opinions of the study authors or the study sponsor, IBM. The study's objective is to relay as accurately as possible the statements of the interview subjects.

More information: Identifying How Firms Manage Cybersecurity Investment, blog.smu.edu/research/files/2015/10/SMU-IBM.pdf

Provided by Southern Methodist University

Citation: Survey finds executive cybersecurity decisions are evolving from compliance to proactive cyber-risk management (2015, October 28) retrieved 9 April 2024 from https://phys.org/news/2015-10-survey-cybersecurity-decisions-evolving-compliance.html