Making Sound Investments in Cybersecurity

With annual losses from cyberattacks averaging $4.7 million per company in fiscal 2018 and more than one in 10 companies losing over $10 million, businesses worldwide are expected to boost their cybersecurity investments during fiscal 2019 by a healthy 34 percent.[1] Moreover, around 12 percent of the organizations in that survey, conducted in early 2019 year by ESI Thought Lab and Willis Towers Watson, plan to bolster their cybersecurity investments by an even healthier 50 percent or more.

While significant, these increases may still be less than what's needed. Current industry research suggests that a robust cybersecurity budget should comprise 9 to 14 percent of an IT department's annual budget.[2] Yet most businesses are still spending less than 6 percent of their IT budgets on security and risk management.

A potentially worse issue, though, is that many of the investments being made may be missing the mark.

A recent study by McKinsey & Co.[3] finds that even though an overwhelming majority of corporate board members now consider cybersecurity a top concern, they remain anxious that their companies are not adequately prepared to manage cyber threats. This, despite a spate of new investments in personnel, training and technology.

The McKinsey report blames this on the absence of a comprehensive approach to cybersecurity. "A holistic approach," the authors state, "proceeds from an accurate overview of the risk landscape. [The goal] is to empower organizations to focus their defenses on the most likely and most threatening cyber risk scenarios, achieving a balance between effective cyber resilience and efficient operations."

A Lack of Board-Level Confidence

McKinsey is not alone in this assessment. "If I had to point to what is the single biggest challenge that's out there, I would say that most C-level executives—and specifically 87 percent of all corporate boards—lack confidence in their cyber security readiness and their cybersecurity program," agrees Doug Grindstaff, senior vice president of cybersecurity solutions for the CMMI Institute. "A key reason for this," he adds, "is that the information they receive about the state of their program does not provide the evidence they need to support sound investment decisions. It's not surprising, therefore, that these board members are not confident in the outcomes."

To help C-Suite and board members sort out their cyber risks and determine their cybersecurity investment priorities, Grindstaff initiated the development of the CMMI Cybermaturity Platform. It's now used by hundreds of businesses and government agencies to systematically assess their cybersecurity preparedness. Grindstaff says the framework's chief benefit is how it can help security teams reassure their boards that the steps taken—and investments made—by their organizations are indeed the right ones to address the key threats to the business.

This is crucial because rather than mitigate the threats posed by cybercrime, one-sided or misplaced investments in cybersecurity can actually heighten the risks facing an enterprise. The reasoning behind this is simple, Grindstaff explains. Because all organizations, no matter how large and successful, have limits on their resources, over-investment in one area can deplete the resources available to safeguard against other, potentially graver threats. This in turn can increase the company's risk overall.

"[Executives] have to figure out what really matters," concurs Kevin Mandia, CEO of FireEye, a provider of cybersecurity solutions. "What are the critical assets to protect and [which] threats are intolerable."[4]

When asked, many executives will often say that they want their company to be as secure as a bank. But while that sounds quite reasonable, since banks are among the best protected institutions when it comes to cybersecurity, most companies outside the financial services industry face very different types of threats and expect very different outcomes.

Overcoming Investment Disconnects

To determine whether or not a company's cybersecurity investments will support the outcomes it wants, the organization needs to consider the nature of the threats that it faces in the context of its business goals. It also needs to take into account any technical and regulatory constraints, as well as the limitations on the resources it can devote to security. Maturity assessments like the CMMI platform help identify any disconnects that may exist, so that the company's security investments can be brought in line with its risk tolerances and business priorities.

"If you aren't taking your cybersecurity investment decisions seriously enough, then you are undermining yourself in more ways than you know," Grindstaff declares. "Investing your cyber dollars in the wrong areas can significantly increase your risk exposure. Spending your cyber budget on the wrong thing means you haven't spent properly on the right things, leaving you exposed in ways that could be disastrous for your business."

The framework developed by CMMI requires an organization to prioritize its data assets—encouraging it to concentrate its security resources where they will have the greatest impact, instead of squandering them on secondary concerns. And by helping security teams provide board-level executives with the information they need to make informed investments, the CMMI platform builds confidence in those decisions over time.

"We're demonstrating and communicating information in a consistent fashion," Grindstaff says. "And if I'm closing the gaps in my security framework; if I'm investing in capabilities that are strategic for my business—then those are the type of investments that a board recognizes will generate ROI over time."

[1] 'Organizations expect to boost their cybersecurity investments by 34%,' Help Net Security, https://www.helpnetsecurity.com/2019/07/15/boost-cybersecurity-investments/

[2] 'How Much Should Your Company Invest in Cybersecurity?' Cybershark, https://www.blackstratus.com/how-much-should-your-company-invest-in-cybersecurity/

[3] 'Cyber risk measurement and the holistic cybersecurity approach,' McKinsey & Co., https://www.mckinsey.com/business-functions/risk/our-insights/cyber-risk-measurement-and-the-holistic-cybersecurity-approach

[4] 'The Executive's Cybersecurity Playbook,' Fire Eye, https://www2.fireeye.com/rs/848-DID-242/images/executive-cyber-security-playbook-NEW.pdf?mkt_tok=%3D%3DeyJpIjoiTXpOa1pUY3lNVFUwWVdJMyIsInQiOiJpSjdDemdidHpsRWVJTCtUTDRUVGQzQVwvWHVkUXorUXZ0UXN1aUhKR2NtTXM4OFozTlZWS29LR0tEc1dGWjZrQXE4ZmZldDNuM0NITHZQTnZsMVJoTG8xOFpueDlVNThlaGVublhiYTAyK0pXTW03RXBXTzRTTlVLbm5IblRram4ifQ