Harvard Business Review

REPRINT H032DZ
PUBLISHED ON HBR.ORG
SEPTEMBER 13, 2016

ARTICLE
INFORMATION & TECHNOLOGY

Cybersecurity Is Every Executive's Job

by Bill Sweeney

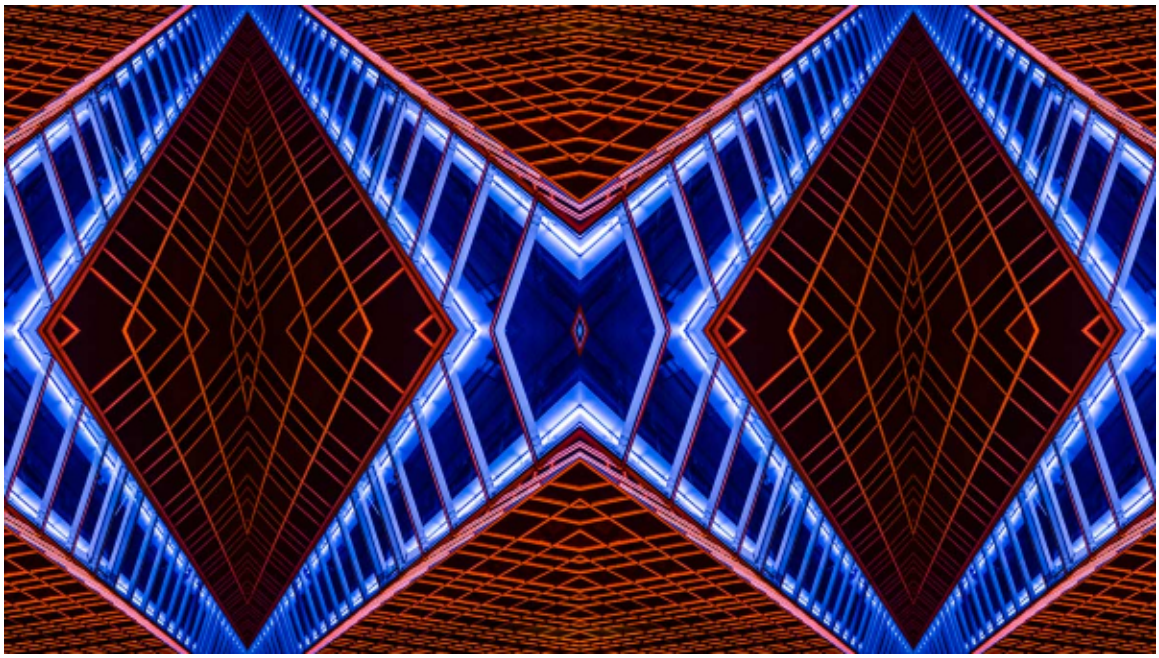
Harvard Business Review

INFORMATION & TECHNOLOGY

Cybersecurity Is Every Executive's Job

by Bill Sweeney

SEPTEMBER 13, 2016



All companies connected to the internet are vulnerable to cyber attacks. And the potential losses are significant. Retail giant Target, for example, estimated its losses from a 2013 data breach at more than $250 million. What's more, according to a recent survey conducted for BAE Systems of 300 managers in the financial services, insurance, and IT/tech industries in the U.S., 85% of respondents listed reputational damage as the most prominent result of a data breach, with 74% citing legal liability as the second largest concern.

Liability for data breaches that affect customers leads directly to the C-suite. Executives need to personally know how strong their company's cyber defenses are, as well as the expected responses

for attacks or breaches. But according to the survey, 40% admitted that they lacked a clear understanding of the cybersecurity protocols within their organizations. This should be an urgent wake-up call to executives that cybersecurity needs to be taken seriously throughout the organization.

Executives should start by understanding what protocols they currently have in place — and where they fall short. An annual security assessment is thought to be a best practice to prevent data breaches. If performed correctly, the security assessment reveals the residual risk — the number and scale of attacks that are likely to get through. If the residual risk is acceptable, then an annual review may be sufficient. However, if the residual risk is concerning, then a semiannual or even quarterly review may not be enough. This, of course, shifts the discussion to what level of residual risk is acceptable, depending on your company.

In many ways, this risk assessment reflects the new reality of cybersecurity. In a fast-moving, hyper-connected world, the approach needs to be dynamic rather than static. For example, a dynamic approach would be to schedule two annual reviews with two different vendors and stagger them by six months. In doing so, a company can cut in half the average time a successful attack goes undetected, rather than relying on annual reviews. Extending this model so that assessments are quarterly or "on demand" in response to predetermined events — or even random checks against known threats — are other alternatives.

But reviews and assessments aren't enough. The best and most effective means for senior executives to guarantee change is to establish a solid working relationship with the Chief Information Security Officer (CISO). CISOs today are called upon to help business executives understand cyber risk and to implement the right security controls while promoting a culture of defense. Our research found that nine out of 10 CISOs are now connected directly to their company's top leadership team, and half of them are directly on the team. Strengthening the role of the CISO to drive this initiative is an encouraging trend, but executives need to engage these CISOs proactively to see real results throughout the organization.

While the CISO will identify risks and prioritize security protocols, it is incumbent on senior executives to understand and carry out the procedures across the business — to the most-vulnerable points of entry for cyber criminals. Executives must sponsor the CISO's threat assessments and review the results together. The CISO should be included on new business initiatives early on so that security is baked in rather than bolted on afterward. In fact, the best practice is to have the CISO work with each team to determine ways to reach goals in the most secure fashion, and then executives must hold their people accountable for risks and flaws identified by the CISO.

What's more, executives should help promote the importance of security within the organization, starting with better education and training. Companies should train midlevel and junior staff on cybersecurity more frequently to reinforce defensive behaviors. Our research found that only 38% of companies conduct training on a quarterly or biannual basis; the rest train annually or even less

frequently. Additionally, most training only gives employees a 25% chance of successfully recognizing a cyber attack one month later. Executives should make it their prerogative to improve these training programs in order to reduce the likelihood of a successful penetration beyond the one-month mark. Training should include role playing, scripts that mimic real life attacks, and testing to assess effectiveness.

Defending against attacks is now a permanent part of senior executives' job descriptions. It's no longer enough to leave cybersecurity to annual reviews or a lone CISO. Senior executives must understand what procedures are in place and ensure that everyone in the organization understands protocol and takes accountability. But most of all, they need to establish the right partnership with the CISO so that security is a part of every company initiative, not an afterthought.

Bill Sweeney is CTO, Americas, at BAE Systems and is an experienced financial services CIO. His background includes seven years as CTO at HSBC's Investment Bank, seven years as CIO Risk, Compliance and Legal at Citibank's Investment Bank, and four years with Bridgewater Associates.