Harvard Business Review

REPRINT H036JQ
PUBLISHED ON HBR.ORG
OCTOBER 25, 2016

ARTICLE
RISK MANAGEMENT

Good Cybersecurity Doesn't Try to Prevent Every Attack

by Greg Bell

Harvard Business Review

RISK MANAGEMENT

Good Cybersecurity Doesn't Try to Prevent Every Attack

by Greg Bell

OCTOBER 25, 2016

I discuss cybersecurity with hundreds of executives every year. The biggest mistake I see is companies treating cybersecurity solely as a technology matter for IT departments to solve. But it's not. It's an enterprise-wide opportunity that's critically important.

If the end game is preventing something bad from happening, companies typically waste time and money on futile attempts to build an impenetrable wall of systems. Even if it were possible to build a

wall that's 100% secure, it wouldn't begin to protect the rapidly growing amount of sensitive data that flows outside the firewall through devices and systems beyond the company's direct control.

It's far more important to focus on two things: identifying and protecting the company's strategically important cyber assets and figuring out in advance how to mitigate damage when attacks occur.

Choose Which Areas to Protect

We live in a world where more and more products are connected to the internet — not just computers and phones, but home appliances, alarm systems, and garage door openers. Whether they know it or not, customers are sharing vast amounts of device usage and personal data whenever they turn on a product or use a service.

The companies entrusted with this data must recognize that cybersecurity and data protection are no longer just IT risks; they're strategic business risks of the highest order. Reputations, brands, and revenue are all at stake. On some level, CEOs know this. According to our "CEO Outlook" study, cybersecurity is the most important risk concern on chief executives' minds right now. But although executives seem to understand that strategy itself is a series of choices — about what your company will excel at and where competing doesn't make sense — they take a peanut butter approach to cybersecurity, spreading it evenly across the entire business.

That's why I stress the value of a cyber risk management framework that begins by focusing on the business factors driving growth and profitability and ends with the technology infrastructure. This is the opposite of the traditional approach, but it's much more effective. Cybersecurity investments cannot be treated equally; some are simply more important than others.

For example, I recently learned that the chief security officer (CSO) of a large insurance company was spending much of his time, and millions of dollars, securing the company's dealer network, a disparate group of thousands of brokers who have a direct relationship with policy holders. The brokers are not employees of the insurance company, and the systems these brokers use are not controlled by the company, even though they collect and process customer data. This is a real dilemma faced by many IT security specialists: How do I protect something that's not in my environment but could impact the brand and the trust that our customers have in us?

What the CSO did not know at the time was that his company was planning to change its business model and expected to dismantle its dealer network within the next couple of years, meaning much of what he had been doing could soon be irrelevant. Companies that can talk about upcoming changes and plan for them in advance can build adaptive, agile, and effective cybersecurity strategies.

Although nearly one in five CEOs reported in KPMG's survey that they're uncomfortable with the degree to which mitigating cyber risk has become part of their responsibilities, one of their top

priorities should be driving greater alignment between their business units and IT than typically exists today.

As in any risk management strategy, executives must look across the entire organization and assess the company's cybersecurity assets, including investments in technology systems and highly skilled professionals to run them. Make sure these investments are aligned with both the company's needs today and how its business model may evolve in the next three to five years.

Prepare to Be Breached

Once the key risks to the organization's "crown jewels" and business processes are identified, it's important to make informed, fiscally responsible judgments about which can be fixed and which can be monitored closely on a continuous basis. While it's painful to think about, chances are your defenses will be breached at some point, and it's best to have a plan in place for when such breaches are discovered.

Cybersecurity training that continuously evolves based on changing circumstances and evolving personnel roles is absolutely essential. Every employee should be informed about cybersecurity best practices and how to identify malicious software or phishing attempts. Too many companies have failed to recognize the importance of ongoing employee training.

Conduct regular cyber risk assessments, focusing on the most-important corporate data and business priorities, and conduct controlled breach scenarios to see how the company and its employees respond. What is the corporate chain of command in the event of a cybersecurity attack? How will you communicate with the news media and your customers?

A survey we recently conducted suggests that this kind of contingency planning is not taking place in many companies. In fact, it's not even being funded: Nearly one-third (31%) of the executives reported that their companies had no designated leader whose sole focus is on cybersecurity, while 49% reported that they had not invested funds in information security during the past year.

The fact that we see so many companies not investing in cyber protections and not designating a cybersecurity leader suggests that even though cybersecurity concerns are top of mind, in many instances they aren't being addressed appropriately.

Consumers see value in companies providing more transparency, education, and communication about their cybersecurity efforts and their effectiveness. Companies that do this successfully not only are more likely to win in the marketplace but also are able to withstand a security breach if it occurs.

Greg Bell, who is based in Atlanta, is the U.S. leader of KPMG's cybersecurity practice.