Key to Risk Reduction: The Cybersecurity Roadmap

Setting a course for building a resilient and mature enterprise starts with devising a workable plan of action.

The damage caused by cyber crime is predicted to reach $6 trillion annually by 2021 — double the 2015 figure.[1] This alarming increase in the cybersecurity threat level demands a new approach to risk management.

Most organizations realize that their defenses may be inadequate, but attacking vulnerabilities one at a time as they become visible is neither efficient nor cost-effective. A better strategy exists, based on the same methodology that companies regularly use to get new products out the door on time and in budget: the cybersecurity roadmap.

A roadmap brings a level of clarity, discipline and cohesion to IT risk management that is all too often absent. It also brings concepts that are familiar to senior management and boards, such as schedules, capability targets and budgets to achieve them. However, many organizations fail to develop a roadmap because they are too busy putting out fires to step back and consider the bigger picture.

Creating a Roadmap to Safety

A cybersecurity roadmap is the ideal foundation for a comprehensive, organization-wide risk management strategy within the IT domain. Its three components can be described in very simple terms: the starting point, the destination and the path to get there. All three, however, involve significant complexity.

The starting point. Given the distributed nature of data in today's IT infrastructure and the constantly evolving nature of the threat landscape, determining "where we are" is no easy task. Two key questions can bring clarity:

- What is the business risk associated with the data to be protected?
- What is the maturity level of the current defenses?

Budgets for cybersecurity are always limited, which means that resources must be carefully allocated so that vulnerabilities posing the greatest business risk receive the highest levels of protection. Sometimes, the level of risk can be

quantified; fines for regulatory non-compliance are an example. In other cases, security decisions will involve strategic determinations made at the board level. An example would be determining the importance of the harm to a brand's image that would result from a data breach.

Once risk levels are established, the next step is determining the maturity level of the defenses currently deployed against those risks. As part of CMMI's total strategic security assessment offering, the CMMI Cybermaturity Platform defines five levels of maturity that range from a fragmented and reactive approach to one that is coordinated across the organization and proactive. Importantly, these levels apply not only to technology but to people and processes as well.

The destination. A fully implemented cybersecurity strategy — the destination — has three important characteristics:

- Proactive. The organization is prepared to deal with the attacks that are now inevitable and focused on constant improvement rather than operating in a catch-up mode.

- Cost-Effective. The security measures in place work, are efficient and have resource allocations (including budget) in line with the value of the data they protect.

- Resilient. The organization has measures in place to "fight back" should a successful attack occur and ensure continuity of operations.

The path. The path from "where we are" to "where we want to be" should be formalized via the same project management techniques as any other complex endeavor. Beyond the basics of task identification, technology acquisition, milestones and resource allocation, the issues that require particular attention are:

- Priorities. The vulnerabilities that present the highest risk should obviously be addressed first, assuming there are gaps between the actual cybersecurity maturity levels and the desired levels. Among vulnerabilities that present equal risk, those with the greatest gap between actual and desired maturity levels should move to the front of the timetable.

- Dependencies. Sometimes, specific technologies serve as a foundation for other, higher-level technologies that support multiple cybersecurity goals. These dependencies should be taken into account in planning the roadmap.

- Budget. Funders of strategic cybersecurity initiatives should be made aware that there is a direct relationship between budget and speed of implementation.

The value of putting a cybersecurity strategy into effect is enormous. Prevention of data breaches is the obvious benefit. The average cost of a large enterprise data breach in 2017 was $3.62 million,[2] and in many cases, the figure was much higher. A less obvious benefit lies in the cost-effectiveness of a comprehensive and integrated approach to IT risk management. Controlling security costs by ensuring that the level of spending is appropriate to the level of risk can have a significant effect on the bottom line. Finally, the peace of mind that comes from knowing that a cybersecurity strategy is in place is not insignificant to your board, to your co-workers or to your customers too.

Sources

[1] https://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html
[2] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN