McKinsey&Company

JULY 2015

McKinsey Quarterly

Repelling the cyberattackers

Tucker Bailey, James M. Kaplan, and Chris Rezek

Organizations must build digital resilience to protect their most valuable information assets.

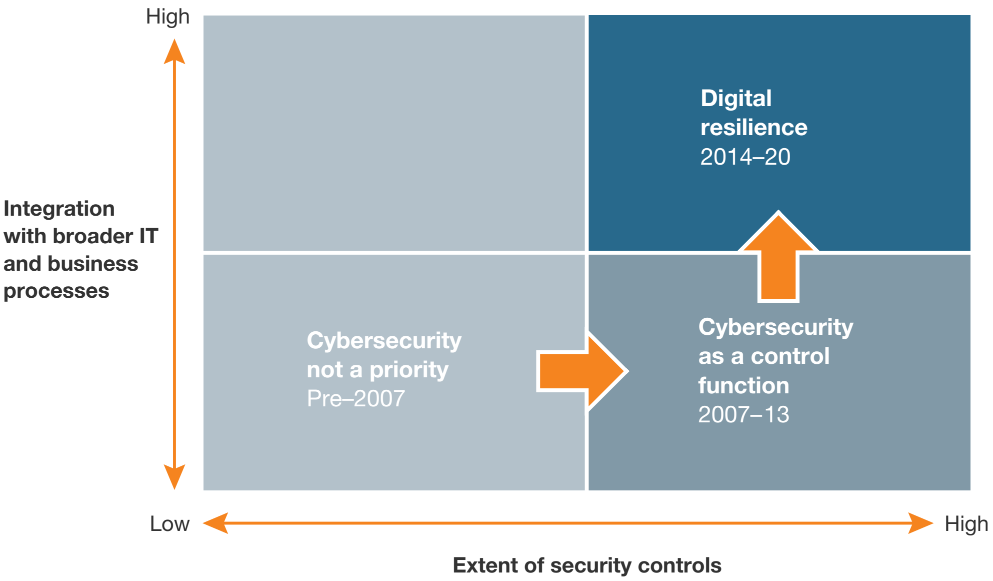
For many businesses, the next wave of innovation and growth will likely involve intelligent analytics, rich mobile experiences, and "one touch" processes that require no further manual intervention. Success will depend on maintaining trust: consumers and business customers alike will accept nothing less than a complete assurance that the companies they engage with protect their highly sensitive data carefully in the hyperconnected information systems powering the digital economy.

When companies think about cybersecurity in such a world, most ask, "How can we protect ourselves and comply with standards or regulations?" instead of "How do we make confident, intelligent investments given the risks we face?" Many also treat cybersecurity primarily as a technology function rather than integrating it into business operations. As a result, they get the wrong answer about how to construct a cybersecurity program. The consequences are painfully clear: nearly 80 percent of technology executives surveyed report that their organizations cannot keep up with the attackers' increasing sophistication.

The solution, we're convinced based on years of research and experience on the front lines, is to move beyond models that make cybersecurity a control function and toward what we call digital resilience: the ability to design customer applications, business processes, technology architectures, and cybersecurity defenses with the protection of critical information assets in mind (Exhibit 1). Digital resilience is the subject of our new book, *Beyond Cybersecurity: Protecting Your Digital Business*, and the focus of this article.

Exhibit 1

Companies need to move beyond cybersecurity as a control function toward a more integrated and resilient approach.


High
Integration with broader IT and business processes
Low
Digital resilience
2014–20
Cybersecurity not a priority
Pre–2007
Cybersecurity as a control function
2007–13
High
Extent of security controls

Source: Tucker Bailey, James Kaplan, and Chris Rezek, *Beyond Cybersecurity: Protecting Your Digital Business*, April 2015

Given the size of the stakes and the solution's cross-functional nature, progress requires senior-level participation and input. Unfortunately, top management often doesn't engage. At roughly two-thirds of the companies we evaluated, the managers in charge of cybersecurity have no regular interaction with the CEO. So the launch—or relaunch—of a digital-resilience program gives the senior-management team an ideal opportunity to set and clarify expectations for how each of its members will help to identify and protect important information assets.

This article describes six critical actions for any organization planning to achieve digital resilience. Reflecting on them will stimulate a dialogue among members of the top team about how they can work together to safeguard their company.

1. Identify all the issues

It's nearly impossible to have an intelligent perspective on how well a cybersecurity function performs without first understanding which information assets are at risk. When companies fail to do so, they can make the wrong downstream choices. One financial institution started its program by assessing regulatory requirements. Two years later, it had made some technical progress but had spent a lot of money and devoted almost all of its efforts to protecting consumers' personal data, to the exclusion of other important information assets.

Companies must assess the risks in an integrated way. An attacker doesn't just have to defeat their processes for identity and access management (I&AM) or for detecting intrusions; it must defeat a *system* of defenses spanning different types of controls. The attacker will have a much harder time if those defenses interlock. Unfortunately, many companies assess each element—intrusion detection, I&AM, data protection, incident response, and the like—separately. They neglect to evaluate how these controls *combine* to protect important information.

Finally, companies must go beyond traditional protections of the perimeter. We often hear executives say that they want to have a security-control assessment. Unfortunately, that starting point frames the exercise around tactical issues, such as the efficacy of the intrusion-detection tool kit or of the antimalware environment. The result, too often, is that any change occurs within an extremely limited security framework. To accomplish something real, companies must typically make substantive business-process changes in the context of broader strategic and operational considerations. Effective cybercapability assessments not only address existing protocols, personnel, and tools but also governance, controls, the security architecture, and delivery systems.

2. Aim high but toward a well-defined target

A cybersecurity plan should be aspirational but attainable—and simple enough to explain so that its leaders can build organizational support. After companies identify the priority business risks, they can then target three types of mechanisms to step up the security of their information assets: business-process controls (changes to end-user behavior and business processes beyond IT), broader IT controls (changes to the IT architecture as a whole), and cybersecurity controls (the discrete technological changes designed to protect information, such as encryption, I&AM, and security analytics). Many companies focus too much on cybersecurity controls and thus create unnecessarily expensive and intrusive systems. Ideally, they should draw on all three types of controls. Actions should be prioritized by the number and nature of the business risks they address and the extent to which they require the organization to change.

Any plan should synthesize the broad set of improvements, initiatives, and actions into a short list of major strategic themes. Those of one healthcare provider included the following:

- The protection of personal health information as it moves through the entire business system, from patients to doctors to hospitals and, when relevant, to supporting vendors.

- Detecting and responding to cyberevents to minimize harm to the business and the disruption of care for patients.

- Scrutiny of insider activities, both accidental and intentional, at the same level that external activity receives. This final point particularly deserves attention. Many companies focus their resiliency programs on external attackers, not threats from insiders.

The themes the healthcare provider identified, taken together, enabled managers to describe this change program to senior managers, to rally the staff around it, and, ultimately, to track and measure progress.

3. Work out how best to deliver the new cybersecurity system

Once a company has identified its cybersecurity goals, turning aspirations into realities requires an array of operational processes, such as updating access rights for accounts, assessing the vendors' security capabilities, and reviewing the security architectures of applications. Historically, business and IT managers alike have often viewed such controls as a brake on the organization's ability to get things done. And, frankly, many aspects of cyberprotection do act as constraints. For example, new safeguards to protect vital information assets will require much more granular policies on passwords and access rights. That can strain existing processes, make the business less agile, and frustrate employees and customers.

Bear in mind, however, that no implementation can be expected to proceed without some turbulence. The leading cybersecurity organizations learn by doing. They push themselves aggressively—drilling, iterating, and refining the construction of ready and flexible defenses. This approach may also reveal processes that can be radically enhanced. One insurance company, for example, dramatically upgraded its operations by segmenting requests according to their complexity. Making this change helped the business eliminate rework and allowed it to run its core security processes in parallel, improving both productivity and response times by 30 percent.

Determining the cybersecurity organization's roles and reporting relationships will be critical, as well. Building resilience requires seniority and visibility. In our experience, it's valuable for one executive—often called the chief information security officer—to have sole organizational ownership for all aspects of cybersecurity. Typically, this executive reports to the CIO, but, increasingly, he or she will also have a solid or dotted reporting line to the chief risk officer or to another business executive. This sort of structure shows that cybersecurity is as much a business issue as a technology one and helps cut through complexity when companies must implement changes quickly.

Improving skills and resources may be one of the most demanding and important aspects of a digital-resilience program. Given the tightness of the cybersecurity labor market, it may help companies to focus on their retention efforts. They also ought to draw from nontraditional talent pools, such as young professionals in the military or the intelligence communities, or from strong problem solvers elsewhere in the organization—or competitors.

4. Establish the risk–resource trade-offs

Different companies have different degrees of tolerance for risk, depending on their sectors, cultures, and overall business strategies. There is no simple metric for quantifying an organization's risk profile, including with respect to cyberattacks. Rather than trying to formulate some highly abstract (and therefore largely meaningless) statement of a company's appetite for risk, the executives responsible for cybersecurity should present senior leaders with three or four pragmatic options representing different levels of risk reduction and resource commitments.

For example, a North American bank's cybersecurity team laid out an ambitious program that represented an enormous change for it. The team noted that some of the proposed security measures were essential to achieve a minimum level of responsible practice. Others were standard at the bank's peers and provided additional protection for the bank's most important information assets. A final set of actions deemed more cutting-edge was directed at sophisticated attackers. The team used this framework to develop three security options (with progressive levels of protection and resource commitment) and to describe which types of business risks each would address.

Although the effort was time consuming, it gave senior managers a practicable set of options. It sparked a robust discussion about how much additional capital investment, operating expense, and management attention the company could devote to its cybersecurity program and how much each option would reduce risk. Perhaps predictably, the bank's senior management decided that it had a responsibility to go beyond the bare minimum. However, because the institution lacked the global footprint (and resources) of the largest financial players, its leaders also decided that investing in relatively cutting-edge protections against the most sophisticated attackers did not make business sense. Instead, the bank settled on a middle option: making sure it had appropriate protection for its most important information assets.

5. Develop a plan that aligns business and technology

Once a company has assessed its cybersecurity capabilities, defined its appetite for risk, and agreed on an organizational model, it must develop a plan that aligns the business with the technology. Regulatory requirements, while important, should not be the sole foundation of the new, technology-driven controls. One insurer, for example, started down this path and found that its program didn't create change in its business units. Indeed, most senior executives barely knew what the program did. The insurer was able to right itself only after it took time to rethink its most important assets and business risks and then tailored its cybersecurity protections to meet them specifically. To do so, it had to comb through the portfolio of each business to assess its information assets, identify business-process changes needed to protect critical data, and implement leading-edge technology controls. And the company had to tackle these actions, as much as possible, in order of greatest impact.

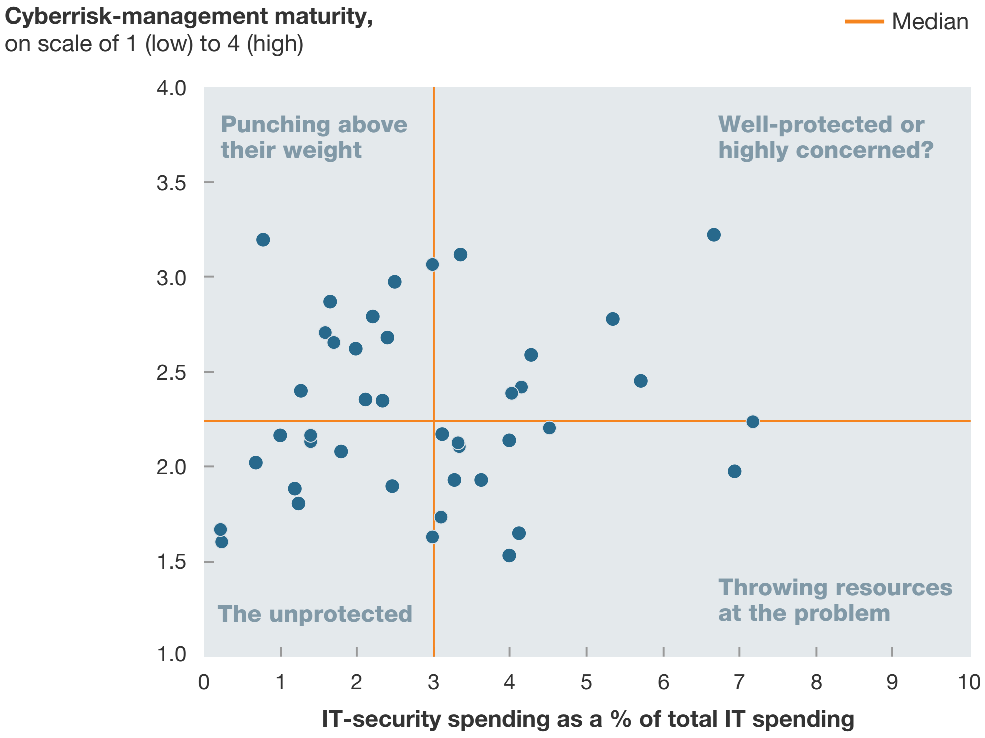
Companies can reduce their vulnerabilities and increase their overall security significantly by implementing many IT improvements, such as the private cloud, desktop virtualization, software-defined networking, and enhanced application development. An integrated cybersecurity plan must take these elements into account. What's more, its leaders must spend lots of time with the leaders of other internal technology programs to understand existing initiatives, see that they have the greatest and best possible impact on security, and ensure that they are in line with the company's broader cybersecurity program.

6. Ensure sustained business engagement

Cybersecurity is a high-stakes topic, so it is a CEO-level one. Attaining digital resilience also requires more than just throwing resources at the problem. Indeed, we've found that additional cybersecurity spending doesn't necessarily bring the management of cyberrisks to maturity (Exhibit 2). Because cybersecurity demands hard decisions that affect many functions across a business, digital resilience requires an actively engaged senior-management team. The company's leaders must signal—with their time and attention—

Exhibit 2

Big spending cannot buy mature cyberrisk management.



Source: Tucker Bailey, James Kaplan, and Chris Rezek, *Beyond Cybersecurity: Protecting Your Digital Business*, April 2015

the importance they attach to protecting information assets. That engagement must not only be sustained but also reinforced through clear actions and the inclusion of cybersecurity objectives (such as the achievement of major program milestones) in the senior team's evaluations and incentives. Of course, this approach means additional work for the executives involved. But the result is a more nimble and better-prepared organization.

The resiliency levers described in this article represent a fundamental change in how most business organizations interact with IT, how IT addresses security, and how a robust portfolio of interconnected long-term safeguards can emerge and evolve. There are no shortcuts or pat solutions. Indeed, any cybersecurity program for a sizable institution will involve hundreds of individual design and implementation decisions. Senior, cross-functional oversight is essential to avoid a mere patchwork of compromises that will undermine digital resilience. Given the stakes, nothing else will do. ○

The authors wish to thank Alan Marcus and Derek O'Halloran for their contributions to this article.

Tucker Bailey is a principal in McKinsey's Washington, DC, office; **James Kaplan** is a principal in the New York office; and **Chris Rezek** is a senior expert in the Boston office. This article is adapted from *Beyond Cybersecurity: Protecting Your Digital Business* (Wiley, April 2015), by Tucker Bailey, James Kaplan, Alan Marcus, Derek O'Halloran, and Chris Rezek.