McKinsey&Company

JUNE 2011

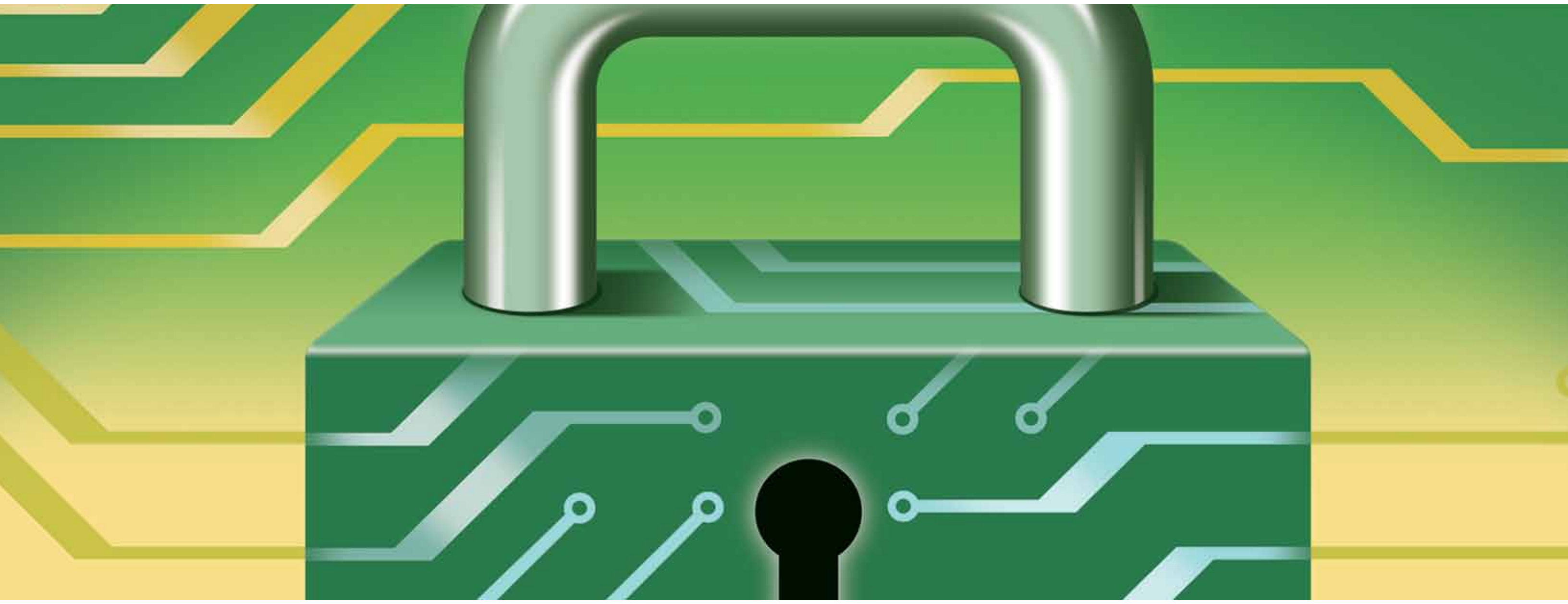
McKinsey Quarterly

BUSINESS TECHNOLOGY OFFICE

Meeting the cybersecurity challenge

Eliminating threats is impossible, so protecting against them without disrupting business innovation and growth is a top management issue.

James Kaplan, Shantnu Sharma, and Allen Weinberg



Cybersecurity—the protection of valuable intellectual property and business information in digital form against theft and misuse—is an increasingly critical management issue. The US government has identified cybersecurity as “one of the most serious economic and national security challenges we face as a nation.”[1]

Companies must now fend off ever-present cyberattacks—the threat of cybercriminals or even disgruntled employees releasing sensitive information, taking intellectual property to competitors, or engaging in online fraud. While sophisticated companies have recently endured highly public breaches to their technology environments, many incidents go unreported. Indeed, businesses are not eager to advertise that they have had to “pay ransom” to cybercriminals or to describe the vulnerabilities that the attack exposed.

Given the increasing pace and complexity of the threats, corporations must adopt approaches to cybersecurity that will require much more engagement from the CEO and other senior executives to protect critical business information without constraining innovation and growth.

Why cybersecurity is a bigger issue now

Most large companies have dramatically strengthened their cybersecurity capabilities over the past five years. Formal processes have been implemented to identify and prioritize IT security risks and develop mitigation strategies, and hundreds of millions of dollars have been dedicated to execute these strategies. Desktop environments are far less “wide open” than they were even five years ago, as USB ports have been disabled and Web mail services blocked. Robust technologies and initiatives have been put in place to address attacks on the perimeter.

However, we recently conducted in-depth interviews and problem-solving sessions with information security leaders at 25 top global companies, and the results revealed widespread—and growing—concern. The combination of advances in enterprise technology and more effective malevolent actors is complicating the task of protecting business processes and information.

Our interviews reinforced that changes in how enterprises use technology have simultaneously made corporate environments harder to protect while increasing the importance of protecting them. Four common trends emerged:

- Value continues to migrate online, and digital data have become more pervasive. Why are some institutions experiencing more online attacks per hour than they did in a month just a few years ago? With apologies to Willie Sutton, because that’s where the money is. Quite simply, more online transactions create bigger incentives for cybercriminals. Moreover, corporations looking to mine data—for instance, transaction and customer

[1] Barack Obama, “Remarks by the president on securing our nation’s cyber infrastructure,” The White House, Washington, DC, May 29, 2009.

information, results of product launches, and market information—create valuable intellectual property that is in itself an attractive target.

- Corporations are expected to be more 'open' than ever before. Increasingly, people working in business units are demanding access to corporate networks through the same mobile devices that they use in their personal lives. While smartphones and tablets increase connectivity, they also present new types of security threats: when hackers "crack" a device, it creates an easy point of entry into corporate networks for malware.[2]

- Supply chains are increasingly interconnected. To strengthen ties to customers and optimize supply chains, companies are encouraging vendors and customers to join their networks. However, this engagement makes walling off a company's technology environment all but impossible. Tighter integration with business partners, of course, can deliver clear benefits, but it also means that a company's defense against attacks rests in part on the security policies of partners and customers. As one executive told us, "The whole network is now at risk from the weakest link." One large company, for example, barred its employees from sharing sensitive company documents over Web networks using peer-to-peer software, only to discover that on-site contractors routinely used this software to review the same documents.

- Malevolent actors are becoming more sophisticated. Professional cybercrime organizations, political "hacktivists," and state-sponsored groups have become more technologically advanced, in some cases outpacing the skills and resources of corporate security teams. Hackers provide "cybercrime as a service"—receiving payment for each end user device they infect with malware. As a result, the past five years have seen more complex, targeted attacks. Malware today is much more difficult to trace and often customized to steal data that can be used for financial gain. Some executives joke that organized crime seems to have better funding than their own security operations. National intelligence agencies appear to undertake some of the most advanced cyberattacks as part of industrial espionage efforts.[3]

The most challenging attacks exploit human vulnerabilities rather than technological ones, which are easier to remediate. Increasingly, cybercrime organizations use information gleaned from social-networking sites to craft highly targeted "phishing" attacks that entice senior executives or systems administrators to click on links that will install spyware on their laptop. Just as retailers seek to create a "multichannel" experience across e-commerce and in-person interactions, some cybercrime organizations combine on- and offline tactics. One institution was the target of a concerted effort to steal inadequately

[2] Software, including viruses and spyware, that are created with the intent of damaging a computer or network, sometimes by taking partial control of applications.

[3] In response to the threat of cyberattacks, the US government has signaled it would view a computer attack from a foreign nation as justification for military action. See Elisabeth Bumiller and David E. Sanger, "Pentagon to consider cyberattacks acts of war," *New York Times*, May 31, 2011.

secured devices from senior executives to facilitate access to sensitive data through the corporate network.

Getting to a new business-driven cybersecurity model

Now more than ever, protecting a corporation's technology assets from malicious damage and inappropriate use requires intelligent constraints on how employees, customers, and partners access corporate applications and data. Insufficient safeguards will result in the loss of critical data, but overly stringent controls can get in the way of doing business or have other adverse effects. At an investment bank, for instance, deathly slow security software caused its M&A specialists to abandon corporate laptops and e-mail services for personal devices and Web mail.

As a result, a business-driven cybersecurity model—one that can provide resiliency to increasingly flexible, open enterprises even in the face of highly capable and determined malevolent actors—is starting to emerge.

Cybersecurity must be addressed at the most senior levels

In many organizations, cybersecurity has been treated primarily as a technology issue. Most respondents believe that senior corporate leaders have too little understanding of the IT security risks and business implications to discuss the trade-offs for investment, risk, and user behavior.

A few institutions have started to make cybersecurity a key part of business strategy rather than technology governance. At one company, the CEO signaled the importance of cybersecurity by his direct involvement with senior security executives in making key decisions. Some organizations have placed divisional chief information security officers in business units, pairing them closely with senior executives there. Others report on cybersecurity issues to the board's risk committee rather than the technology committee.

Cybersecurity must be 'business back' rather than 'technology forward'

Increasingly, companies will have to reverse their thinking to address cyberrisks. Rather than starting with technological vulnerabilities (say, the insufficient patching of servers or routers), they should first protect the most critical business assets or processes (such as customer credit card information)—what we call a "business-back" approach. Already, many large institutions have implemented multiyear programs to classify corporate data so they can focus cybersecurity efforts and policies on their most critical information assets. Corporations have begun to evaluate their cyberrisk profile across the full value chain, clarifying expectations with vendors and enhancing collaboration with key business partners. Some institutions have made cybersecurity a core part of the customer value proposition, establishing an ongoing dialogue on the right balance between collecting enough data to verify identity without forcing customers to spend too much time setting up or signing on to their online accounts. For these companies, cybersecurity could represent a business opportunity, as they create end-to-end customer experiences that are both convenient and secure.

Move from protecting the perimeter to protecting data

Most organizations have approached cybersecurity by trying to put increasingly sophisticated defenses around their perimeter. The reality is that a motivated attacker will likely find a vulnerability—or an employee may inadvertently create an opening (for example, by accidentally e-mailing sensitive customer information).

Progressive corporations are reorienting security architectures from devices and locations to roles and data. Ultimately, plugging your laptop into the network at a corporate location may enable you to do no more than reach publicly available Web sites. Accessing corporate data or applications, however, would require authentication of your identity.

Security will soon become a fundamental design decision in underlying technology architectures. If customer credit card information resides in a single database, for example, a cybercriminal would only have to breach security once to engage in fraudulent transactions. Separating credit card numbers and expiration dates vastly complicates the task. Since a malicious systems or database administrator can be much more dangerous than even the most careless end user, some IT organizations have started to limit the number of people who can access production systems and data, preventing not only application developers but also infrastructure architects and engineers from touching "live machinery."

Refresh cybersecurity strategies to address rapidly evolving business needs and threats

We heard many respondents say that CEOs and other senior executives inquire how to "solve" cybersecurity. Corporations need to acknowledge that it is an ongoing battle. New digital assets and mechanisms for accessing them simply mean new types of attacks.

Already, many corporations are conducting simulated cyberattacks to identify unexpected vulnerabilities and develop organizational muscles for managing breaches. Some have built sophisticated capabilities to aggregate and analyze massive amounts of operational data (such as e-mail headers and IP traffic) to uncover emerging threats. In addition, corporations must make cybersecurity, such as the information security measures that need to be implemented before entering new geographies, a key part of the business case for major initiatives or new-product introductions.

What should senior executives do to ensure that cybersecurity is sufficiently addressed?

At leading organizations, cybersecurity should be a constant item on the agendas of CEOs and boards. To stay ahead of the threats, executives must engage in an ongoing dialogue to ensure their strategy continually evolves and makes the appropriate trade-offs between

Related thinking

Reshaping IT management for turbulent times”

“How IT is managing new demands: McKinsey Global Survey results”

business opportunity and risks. We believe this dialogue should start with a number of critical questions:

- Who is responsible for developing and maintaining our cross-functional approach to cybersecurity? To what extent are business leaders (as opposed to IT or risk executives) owning this issue?

- Which information assets are most critical, and what is the “value at stake” in the event of a breach? What promises—implicit or explicit—have we made to our customers and partners to protect their information?

- What roles do cybersecurity and trust play in our customer value proposition—and how do we take steps to keep data secure and support the end-to-end customer experience?

- How are we using technology, business processes, and other efforts to protect our critical information assets? How does our approach compare with that of our peers and best practices?

- Is our approach continuing to evolve, and are we changing our business processes accordingly?

- Are we managing our vendor and partner relationships to ensure the mutual protection of information?

- As an industry, are we working effectively together and with appropriate government entities to reduce cybersecurity threats?

● ● ●

As more value migrates online and corporations adopt more innovative ways of interacting with customers and other partners, the cybersecurity challenge will only increase.

Since the virulence and sophistication of assaults and complexity of IT environments have risen rapidly, addressing this challenge requires solutions that cut across strategy, operations, risk management, and legal and technology functions. Companies need to make this a broad management initiative with a mandate from senior leaders in order to protect critical information assets without placing constraints on business innovation and growth. ○

James Kaplan is a principal in McKinsey’s New York office, where **Allen Weinberg** is a director; **Shantnu Sharma** is a consultant in the Boston office.