MAY 2014
McKinsey Quarterly

The rising strategic risks of cyberattacks

Tucker Bailey, Andrea Del Miglio, and Wolf Richter

Research by McKinsey and the World Economic Forum points to a widening range of technology vulnerabilities and potentially huge losses in value tied to innovation.

More and more business value and personal information worldwide are rapidly migrating into digital form on open and globally interconnected technology platforms. As that happens, the risks from cyberattacks become increasingly daunting. Criminals pursue financial gain through fraud and identity theft; competitors steal intellectual property or disrupt business to grab advantage; "hacktivists" pierce online firewalls to make political statements.

Research McKinsey conducted in partnership with the World Economic Forum suggests that companies are struggling with their capabilities in cyberrisk management.[1] As highly visible breaches occur with growing regularity, most technology executives believe that they are losing ground to attackers. Organizations large and small lack the facts to make effective decisions, and traditional "protect the perimeter" technology strategies are proving insufficient. Most companies also have difficulty quantifying the impact of risks and mitigation plans. Much of the damage results from an inadequate response to a breach rather than the breach itself.

Complicating matters further for executives, mitigating the effect of attacks often requires making complicated trade-offs between reducing risk and keeping pace with business demands (see sidebar "Seizing the initiative on cybersecurity: A top-team checklist"). Only a few CEOs realize that the real cost of cybercrime stems from delayed or lost technological innovation—problems resulting in part from how thoroughly companies are screening technology investments for their potential impact on the cyberrisk profile.

These findings emerged from interviews with more than 200 chief information officers, chief information-security officers, regulators, policy makers, technology vendors, law-enforcement officials, and other kinds of practitioners in seven sectors across the Americas, Europe, the Middle East and Africa, and Asia.[2] We also drew on a separate McKinsey executive survey on cyberrisk, supplementing this research with an analysis of McKinsey Global Institute (MGI) data on the value-creation potential of innovative technologies. It showed that the eco-

Seizing the initiative on cybersecurity:
A top-team checklist

With trillions of dollars in play and cyberresiliency affecting a growing range of business issues—business continuity, customer privacy, and the pace of innovation, to name just a few—it's clear that current operating models for combatting attacks aren't up to the task. Often, they are compliance driven and technology centric. Instead, they must be grounded in collaboration across business functions. That requires active engagement by the CEO and other senior leaders who understand the broad strategic risks of inaction—and can catalyze change. We have developed a checklist of practices that can help top teams as they remap the boundaries of their cybersecurity operating models:

1. Prioritize information assets by business risks. Most companies lack sufficient insight into the precise information assets they need to protect—for example, the damage that might result from losing the intellectual property behind a new manufacturing process. Business leaders need to work with cybersecurity teams to assess and rank business risks across the value chain.

2. Differentiate protection by the importance of assets. Assigning levels of controls, such as encryption and more rigorous passwords for lower-value assets, will allow management to invest time and resources in protecting the most strategic information.

3. Integrate security deeply into the technology environment to achieve scale. Executives need to instill the mind-set that security isn't something bolted onto projects. Instead, every facet of the growing technology environment—from developing social-network applications to replacing hardware—needs to be shaped by the awareness of new vulnerabilities.

nomic costs of cybercrimes could run into the trillions of dollars.

Areas of business concern

From our interviews and survey research, four areas of concern emerged on how executives perceive cyberrisks, their business impact, and the readiness of companies to respond:

More than half of all respondents, and 70 percent of executives from financial institutions, believe that cybersecurity is a strategic risk for their companies. European companies are slightly more concerned than American ones. Notably,

4. Deploy active defenses to uncover attacks proactively. Massive intelligence is available about potential attacks. Much as top teams are organizing strategy around big data analytics, they must ensure that their companies can aggregate and model new information to establish robust defenses.

5. Test continuously to improve response plans. Teams responsible for diverse functions, such as public affairs and customer service, where technology isn't the core focus, must sharpen their ability to meet breaches. Running realistic cyberwar games on an ongoing basis can rally teams from across functions and build organizational "muscle memory."

6. Engage frontline personnel to aid their understanding of valuable information assets. The biggest vulnerabilities often stem from everyday use of e-mail and Internet technology. Segment the risks and then train employees, targeting behavior that undermines security.

7. Incorporate cyberresistance into enterprise-wide risk-management and governance processes. Assessments of risks from cyberattacks must be integrated with other kinds of risk analysis and presented in relevant management and board discussions. Moreover, cybersecurity must dovetail with broader enterprise-governance functions, such as human resources, regulatory compliance, and vendor management.

some executives think internal threats (from employees) are as big a risk as external attacks.

Equally worrisome, a large majority of executives believe that attackers will continue to increase their lead over corporate defenses. Sixty percent of the executives interviewed think the sophistication or pace of attacks will increase somewhat more quickly than the ability of institutions to defend themselves. Product companies, such as high-tech firms, are most concerned about industrial espionage. The leaking of proprietary knowledge about production processes may be more damaging than leaks of product specifications, given the

pervasiveness of “teardown” techniques and the legal protections afforded to product designs. Service companies are more concerned about the loss and release of identifiable information on customers and about service disruptions.

According to McKinsey’s ongoing cyberrisk-maturity survey research, large companies reported cross-sector gaps in their risk-management capabilities. Ninety percent of those most recently surveyed had “nascent” or “developing” ones. Only 5 percent were rated “mature” overall across the practice areas studied (exhibit). Notably, we found no correlation between spending levels and risk-management maturity. Some companies spend little but do a comparatively good job of making risk-management decisions. Others spend vigorously, but without much sophistication. Even the largest firms had substantial room for improvement. In finance, for instance, senior nontechnical executives struggled to incorporate cyberrisk management into discussions on enterprise risk management and often couldn’t make informed decisions, because they lacked data.

Concerns about cyberattacks are starting to have measurable negative business implications in some areas. In high tech, fully half of the survey respondents said they would have to change the nature of their R&D efforts over time. There is noticeable concern, as well, that cyberattacks could slow down the capture of value from cloud computing, mobile technologies, and health-care technologies. Some 70 percent of the respondents said that security concerns had delayed the adoption of public cloud computing by a year or more, and 40 percent said such concerns delayed enterprise-mobility capabilities by a year or more.

Cybersecurity controls are having a significant impact on frontline productivity, too. About 90 percent of the respondents overall said that controls had at least a moderate impact on it. Half of the high-tech executives cited existing controls as “a major pain point” that limited the ability of employees to collaborate.

While there is broad agreement among executives that concerted efforts by policy makers, companies, and industry associations will be needed to reduce threats, there is considerable disagreement about how a consensus might take shape. And executives worry that new regulations may be grounded in outdated techniques and that regulators’ skills and capabilities may be insufficient.

A global economic penalty

Looking forward, if the pace and intensity of attacks increase and are not met with improved defenses, a backlash against digitization could occur, with large negative economic implications. Using MGI data on the technologies that will truly matter to business strategy during the coming decade, we estimate that over the next five to seven years, $9 trillion to $21 trillion of economic-value creation, worldwide, depends on the robustness of the cybersecurity environment (see sidebar “About the research”).

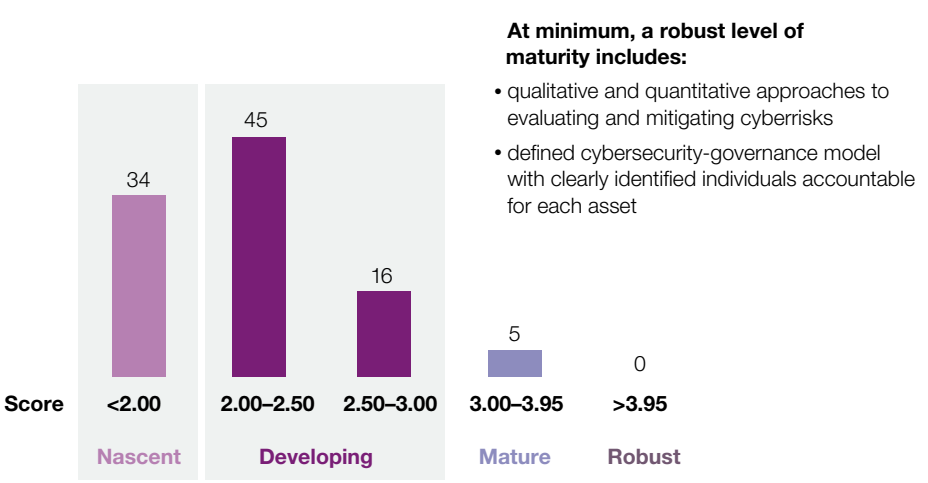
About the research

We modeled alternative scenarios for 2020, starting with estimates of the economic value that could be achieved in an environment where organizations and governments adopt robust cyberresilience strategies. We then estimated how that value might diminish, first, if institutions muddle through and make no substantive changes to current approaches, allowing cyberattackers to retain an advantage over defenders and, second, if a step-change increase in attacks prompts severe regulatory responses that constrict the use of technologies and produce a backlash against digitization. The basis of our economic analysis was a 2013 McKinsey Global Institute (MGI) report that focused on the speed and scope of, and the economic value at stake from, a dozen economically disruptive technologies, among them cloud technology, the mobile Internet, and the Internet of Things. For more, see the full MGI report, *Disruptive technologies: Advances that will transform life, business, and the global economy* (May 2013), on mckinsey.com.

Exhibit

A large majority of surveyed companies had nascent or developing cyberrisk-management capabilities.

Maturity level of companies' overall cyberrisk management, on a scale of 1 to 4, where 4 is strongest, % of companies



Source: 2013 McKinsey Global Survey on cyberrisk-management maturity, including nearly 100 institutions across Africa, the Americas, Europe, and the Middle East

Consider, for example, cloud computing. In an environment where a solid cyberresilience ecosystem accelerates digitization, the private and government sectors would increase their use of *public* cloud technologies,[3] with enhanced security capabilities allowing widespread deployment for noncritical workloads. Private clouds would handle more sensitive workloads. In this case, we estimate that cloud computing could create $3.72 trillion in value by 2020. However, in an environment of stepped-up cyberattacks, public clouds would be underutilized, given increased fear of vulnerabilities and higher costs from compliance with stricter policies on third-party access to data and systems. Such problems would delay the adoption of many systems and reduce the potential value from cloud computing by as much as $1.4 trillion.

These dynamics could play out in many areas, with the proliferation of attackers' weapons leading to widespread and highly visible incidents that trigger a public backlash and push governments to enforce tighter controls, which could dramatically decelerate the pace of digitization. Indeed, our interviews and workshops with executives from a variety of sectors reinforce the view that the cybersecurity environment may be getting more difficult and that early elements of a backlash are already beginning to materialize.

[1] For more, download the full report, *Risk and Responsibility in a Hyperconnected World*, in the online version of this article, on mckinsey.com.

[2] The Risk and Responsibility in a Hyperconnected World initiative was launched at the World Economic Forum's annual meeting in 2012. Over the past year, the Forum, in partnership with McKinsey, has continued a dialogue with executives and policy makers through interviews and workshops and through surveys exploring strategies for building a vigorous cyberresilience capability at the institutional level. We augmented our research with parallel McKinsey cyberrisk-maturity survey data on cyberresiliency.

[3] Where cloud-computing resources are offered by third-party service providers rather than hosted in-house.

The authors would like to acknowledge David Chinn, James Kaplan, Chris Rezek, Roshan Vora, and Allen Weinberg for their contributions to the development of this article.

Tucker Bailey is a principal in McKinsey's Washington, DC, office; **Andrea Del Miglio** is a principal in the Milan office; and **Wolf Richter** is a principal in the Berlin office.