McKinsey&Company

JANUARY 2014

Risk and responsibility in a hyperconnected world: Implications for enterprises

David Chinn, James Kaplan, and Allen Weinberg

For the world's economy to get full value from technological innovation, it must have a robust, coordinated approach to cybersecurity. A new report from the World Economic Forum and McKinsey & Company looks at how that could happen.

When "everything is becoming digital," private, public, and civil institutions become more dependent on information systems and more vulnerable to attack by sophisticated cybercriminals, political "hacktivists," nation-states, and even their own employees. As a result, all of our institutions will have to make increasingly thoughtful trade-offs between the value inherent in a hyperconnected world and the risk of operational disruption, intellectual property loss, public embarrassment, and fraud that cyberattacks create.

Over the past year, McKinsey and the World Economic Forum undertook joint research to develop a fact-based view of cyberrisks, assess their economic and strategic implications, and lay out a path forward. Interviews with executives and data from more than 200 enterprises, technology vendors, and public agencies contributed to the three main findings for enterprises:

- Despite years of effort, and tens of billions of dollars spent annually, the global economy is still not sufficiently protected against cyberattacks—and it is getting worse. The risk of cyberattacks could materially slow the pace of technology and business innovation with as much as $3 trillion in aggregate impact.

- Enterprise-technology executives agree on the seven practices they must put in place to improve their resilience in the face of cyberattacks; even so, most technology executives gave their institutions low scores in making the required changes.

- Given the cross-functional, high-stakes nature of cybersecurity, it is a CEO-level issue, and progress toward cyberresiliency can only be achieved with active engagement from the senior leaders of public and private institutions.

A critical social and business issue

The theft of information assets and the intentional disruption of online processes are the most important technology risks that major institutions face. Nearly two-thirds of companies across sectors and regions described the risk of cyberattack as a "significant issue that could have major strategic implications."

The defenders are losing ground to the attackers. Nearly 80 percent of technology executives said that they cannot keep up with attackers' increasing sophistication. Many frontline practitioners said they are seeing the dissemination of sophisticated attack strategies from major nation-states to a broader array of criminals and hacktivists who have much more destructive ambitions.

Large institutions lack the facts and processes to make effective decisions about cybersecurity. Of the more than 60 institutions whose practices we surveyed in detail, 34 percent had a "nascent" level of maturity and another 60 percent were "developing." Larger expenditures have not translated into an increased maturity, and many institutions appear to be throwing money at the problem.

Controls required to protect against cyberattacks are already having a negative business impact. For example, security concerns are delaying mobile functionality in enterprises by an average of six months—and are dramatically limiting the extent to which many companies are using public-cloud services. For nearly three-quarters of companies, security controls reduce frontline productivity by slowing employees' ability to share information. And even though direct cybersecurity spend is small, it can have a much larger indirect-cost impact on the IT organization. Some chief information officers said that security requirements could drive as much as 20 to 30 percent of their overall activity.

There are multiple scenarios for how the cybersecurity environment could evolve over the next five to seven years. However, if attackers continue to get better more quickly than defenders, this could result in a world where a "cyberbacklash" decelerates digitization. In this scenario, a relatively small number of destructive attacks reduces trust in the economy, causing governments to impose new regulations and institutions to slow down the pace of technology innovation. As a result, the world would capture less of the $10 trillion to $20 trillion available from big data, mobility, and other innovations by 2020—the ultimate impact could be as much as $3 trillion in lost productivity and growth.

Making institutions cyberresilient

Current models for protecting institutions from cyberattacks are becoming less and less effective. They are technology-centric and compliance-driven. They do not effectively involve senior business leaders. They are highly manual and require specialized talent. As a result, they do not scale, given an increasing volume of attacks, and they place too high a burden on the business. All too often security is the choke point for any innovative business initiative.

As a result, not only do practitioners agree they need to build very different cybersecurity operating models but there is also emerging consensus on what these models need to look like. Here are the key tenets:

1. Prioritize information assets based on business risks. Most institutions do not have enough insight into what information assets they need to protect with what priority. Going forward, cybersecurity teams need to work with business leaders to understand business risks (for example, loss of proprietary information about a new manufacturing process) across the entire value chain and prioritize the underlying information assets accordingly.

2. Provide differentiated protection based on importance of assets. As Frederick the Great said, "To protect everything is to protect nothing." Employing differentiated controls (for example, encryption, more rigorous passwords) allows institutions to focus time and resources on protecting information assets that matter the most.

3. Deeply integrate security into the technology environment to drive scalability. Almost every part of the broader technology environment impacts an institution's ability to protect itself, from application-development practices to policies for replacing outdated hardware. Institutions must move from simply bolting on security to training their entire staff to incorporate it from day one into technology projects.

4. Deploy active defenses to uncover attacks proactively. There is a massive amount of information available about potential attacks, both from external intelligence sources and from an institution's own technology environment. Increasingly, companies will need to develop capabilities to aggregate relevant information and analyze and tune their defense systems accordingly (for example, firewalls).

5. Test continuously to improve incident response. An inadequate response to a breach—not only by the technology team but also from marketing, public affairs, or customer-service functions—can be as damaging as the breach itself. Taking a page from the military, institutions should run cross-functional cyberwar games to improve their ability to respond effectively in real time.

6. Enlist frontline personnel to help them understand the value of information assets. Users are often the biggest vulnerability an institution has—they click on links they should not, select insecure passwords, and e-mail sensitive files to broad distribution lists. Institutions need to segment users and help each group understand the business risks of the information assets they touch every day.

7. Integrate cyberresistance into enterprise-wide risk-management and governance processes. Cybersecurity is an enterprise risk and has to be managed like one. Assessments of possible cyberattacks must be integrated with other risk analysis and presented in relevant management and board discussions. Moreover, cybersecurity implications should be integrated into the broad set of enterprise-governance functions like HR, vendor management, and regulatory compliance.

While enterprises must upgrade their own capabilities, technology executives said that individual institutions could not be left to fend for themselves. However, there was a high degree of disagreement about the most effective roles for law enforcement, regulators, policy makers, industry associations, and technology vendors.

There is much less consensus on many public issues in cybersecurity. For example, technology executives were closely split on the value of cybersecurity regulation. Interestingly, health-care and insurance technologists were most likely to say that even if regulation might be clumsy, it forced top management to devote required time and resources to cybersecurity. In contrast, a clear majority of banking technologists said regulation has little value: nearly one-fifth of them said current regulations were actively harmful and made their institutions less secure.

A CEO-level issue

Given the trillions of dollars in play, the stakes are high. And given the range of social and business issues that cyberresiliency affects—for example, intellectual property, regulatory compliance, privacy, customer experience, product development, business continuity, legal jurisdiction—it can only be addressed effectively with active engagement from the most senior business and public leaders.

Even improving cybersecurity capabilities within a single institution requires collaboration across a host of business functions. Operational managers must assess which information assets are most valuable. Privacy and compliance functions have to evaluate the impact of losing customer data. Decisions about how much to monitor employee access to sensitive data have major HR implications. And procurement must negotiate security requirements into vendor contracts.

Given the scale of impact and the degree of coordination and cultural change required, progress toward cyberresilience requires active engagement from the CEO and other senior leaders. They have to make clear they expect the following:

- an honest, granular assessment of existing capabilities and risks, given their business model

- alignment on the most important information assets and a clear approach for providing them with required protection

- a road map for getting to a scalable, business-driven cybersecurity operating model

- a well-practiced set of skills for responding to breaches across business functions

Sustaining the pace of innovation and growth in the global economy will require resiliency in the face of determined cyberattacks. Only CEOs and senior public leaders can solve the problem, because of the strategic and organizational-change issues that need to be resolved.

For more on this research, download the full report, *Risk and Responsibility in a Hyperconnected World*, on mckinsey.com. □

The authors would like to thank Roshan Vora for his contribution to the development of this article.

David Chinn is a director in McKinsey's London office; **James Kaplan** is a principal in the New York office, where **Allen Weinberg** is a director.