

A new posture for cybersecurity in a networked world

As the dangers mount, current approaches aren't working. Cyberrisk management needs a root-and-branch overhaul.

Thomas Poppensieker and Rolf Riemenschitter



Until recently, financial firms and governments were the primary targets of cyberattacks. Today, with every company hooking up more and more of their business to the Internet, the threat is now universal. Consider the havoc wreaked by three recent events. From 2011 to 2014, energy companies in Canada, Europe, and the United States were attacked by the cyberespionage group Dragonfly. In May 2017, WannaCry ransomware held hostage public and private organizations in telecommunications, healthcare, and logistics. Also in 2017, NotPetya ransomware attacked major European companies in a wide variety of industries. And in 2018, Meltdown and Spectre were exposed as perhaps the biggest cyberthreat of all, showing that vulnerabilities are not just in software but hardware too.

Little wonder, then, that risk managers now consider cyberrisk to be the biggest threat to their business. According to a recent McKinsey survey, 75 percent of experts consider cybersecurity to be a top priority. That's true even of industries like banking and automotive, which one might think would be preoccupied with other enormous risks that have emerged in recent years.

But while awareness is building, so is confusion. Executives are overwhelmed by the challenge. Only 16 percent say their companies are well prepared to deal with cyberrisk. The threat is only getting worse, as growth in most industries depends on new technology, such as artificial intelligence, advanced analytics, and the Internet of Things (IoT), that will bring all kinds of benefits but also expose companies and their customers to new kinds of cyberrisk, arriving in new ways.

So what should executives do? Keep calm and carry on? That's not an option. The threat is too substantial, and the underlying vectors on which they are borne are changing too quickly. To increase and sustain their resilience to cyberattacks, companies must adopt a new posture—comprehensive, strategic, and persistent. In our work with leading companies across industries, and in our conversations with leading experts, we have seen a new approach take root that

can protect companies against cyberrisk without imposing undue restrictions on their business.

A global insurance company's experience indicates the potential. It budgeted \$70 million for a comprehensive cybersecurity program. One year later, only a fraction of the planned measures had been implemented. Business units had put pressure on the IT department to prioritize changes they favored, such as a sales campaign and some new reports, at the expense of security measures, such as email encryption and multifactor authentication. The business units also took issue with the restrictions that came with cybersecurity measures, such as the extra efforts that went into data-loss prevention, and limitations on the use of third-party vendors in critical areas.

To get its cybersecurity program back on track, the company took a step back to identify the biggest business risks and the IT assets that business continuity depends upon. It then streamlined its cybersecurity investment portfolio to focus on these "crown jewels." It also established a new model of governance for cybersecurity that empowered the central team to oversee all cyberrisk efforts across the enterprise. Because business owners were involved in the analysis, they warmly welcomed the required initiatives. Not only did the crown-jewels program increase buy-in and speed up implementation, it also led to a substantial cost savings on the original plan.

Spinning their wheels

Even after years of discussion and debate, the attacks continue and even escalate. Most companies don't fully understand the threat and don't always prepare as well as they might. We don't claim to have all the answers, either, but we hope that this recap of the problems and the pitfalls will help companies calibrate their current posture on cyberrisk.

More threats, more intense

The US government has identified cybersecurity as "one of the most serious economic and national security challenges we face as a nation."¹ Worldwide, the threat

from cyberattacks is growing both in numbers and intensity. Consider these figures: some companies are investing up to \$500 million on cybersecurity; worldwide, more than 100 billion lines of code are created annually. Many companies report thousands of attacks every month, ranging from the trivial to the extremely serious. Several billion data sets are breached annually. Every year, hackers produce some 120 million new variants of malware. At some companies, 2,000 people now report to the chief information security officer (CISO)—and he or she in turn reports to the chief security officer (CSO), who has an even larger team.

Paradoxically, most of the companies that fell prey to the likes of NotPetya and WannaCry would probably have said that they were well protected at the time of the attacks. Even when a company is not a primary target, it's at risk of collateral damage from untargeted malware and attacks on widely used software and critical infrastructure. And despite all the new defenses, companies still need about 99 days on average to detect a covert attack. Imagine the damage an undetected attacker could do in that time.

Growing complexity makes companies more vulnerable

While hackers are honing their skills, business is going digital—and that makes companies more vulnerable to cyberattacks. Assets ranging from new product designs to distribution networks and customer data are now at risk. Digital value chains are also growing more complex, using the simplicity of a digital connection to tie together thousands of people, countless applications, and myriad servers, workstations, and other devices.

Companies may well have a state-of-the-art firewall and the latest malware-detection software. And they might have well-tuned security operations and incident-response processes. But what about third-party suppliers, which might be the weakest link of a company's value chain? Or the hotshot

design studio that has access to the company's intellectual property (IP)? They may have signed a nondisclosure agreement, but can companies be sure their cybersecurity is up to snuff? The entry point for cyberattackers can be as trivial as a Wi-Fi-enabled camera used to take pictures at a corporate retreat. Some prominent recent cases of IP theft at media companies targeted third-party postproduction services with inferior cybersecurity.

Billions of new entry points to defend

In the past, cyberrisk has primarily affected IT. But as the IoT grows and more companies hook their production systems up to the Internet, operating technology (OT) is coming under threat as well. The number of vulnerable devices is increasing dramatically. In the past, a large corporate network might have had between 50,000 and 500,000 end points; with the IoT, the system expands to millions or tens of millions of end points. Unfortunately, many of these are older devices with inadequate security or no security at all, and some are not even supported anymore by their maker. By 2020, the IoT may comprise as many as 30 billion devices, many of them outside corporate control. Already, smart cars, smart homes, and smart apparel are prone to malware that can conscript them for distributed denial-of-service attacks. By 2020, 46 percent of all Internet connections will be machine-to-machine, without human operators, and this number will keep growing. And of course, billions of chips have been shown to be vulnerable to Meltdown and Spectre attacks, weaknesses that must be addressed.

Common pitfalls

Corporate cybersecurity is struggling to keep up with the blistering pace of change in cyberrisk. We've seen the following three typical problems:

- *Delegating the problem to IT.* Many top executives treat cyberrisk as a technical issue and delegate it to the IT department. This is a natural reaction, given that cybersecurity presents many

technical problems. But defending a business is different from protecting servers. Defending a business requires a sense of the value at risk, derived from business priorities; the business model and value chain; and the company's risk culture, roles, responsibilities, and governance. IT alone cannot tackle cybersecurity.

- **Throwing resources at the problem.** Other companies try to spend their way to success, assuming that the threat will go away if they persuade enough high-profile hackers to join the company's ranks. But even the finest hackers don't stand a chance at anticipating and fending off tens of thousands of attacks on millions of devices in a complex network.
- **Treating the problem as a compliance issue.** Some companies introduce new cybersecurity protocols and checklists seemingly every other day. But these efforts often bring about an undue focus on formal compliance rather than real resilience. Even when all boxes on the CISO's checklist are ticked, the company may be no less vulnerable to cyberattacks than before.

A new posture

To ready global companies for an age of all-encompassing connectivity, executives need a more adaptive, more thorough, and more collaborative approach to cyberrisk (Exhibit 1). We have observed the following principles used by some of the world's leading cybersecurity teams at global companies:

- **Cyberrisk needs to be treated as a risk-management issue, not an IT problem.** Cyberrisk is much like any other complex, critical, nonfinancial risk. Key elements of its management include the prioritization of relevant threats, the determination of a company's risk appetite (its willingness to accept some risk), and the definition of initiatives to minimize risk. Additionally, companies need to put in place an organizational structure and a governance

approach that bring transparency and enable real-time risk management.

- **Companies must address cyberrisk in a business context.** Technical experts cannot solve the problem without understanding the underlying commercial and organizational requirements. Companies tend to overinvest in technical gadgets and underinvest in complexity reduction and consistent coverage of their whole value chain, such as vendor risk management. The result is an inefficient system.
- **Companies must seek out and mitigate cyberrisk on many levels.** Data, infrastructure, applications, and people are exposed to different threat types and levels. Creating a comprehensive register of all these assets is tedious and time-consuming. Companies should take advantage of automated tools to catalog their assets, the better to focus on those at most risk.
- **Adaptation is essential.** Sooner or later, every organization will be affected by a cyberattack. A company's organization, processes, IT, OT, and products need to be reviewed and adjusted as cyberthreats evolve. In particular, companies must fine-tune business-continuity and crisis-management structures and processes to meet changes in the threat level.
- **Cyberrisk calls for comprehensive, collaborative governance.** Traditionally, many companies distinguish between physical and information security, between IT and OT, between business-continuity management and data protection, and between in-house and external security. In the digital age, these splits are obsolete. Scattered responsibility can put the entire organization at risk. To reduce redundancies, speed up responses, and boost overall resilience, companies need to address all parts of the business affected by cyberthreats—which is to say, all parts of the business, and

suppliers and customers too. While it may be hard—or even impossible—to protect a company against the most advanced attacks, systematic governance is the best insurance against the bulk of everyday attacks.

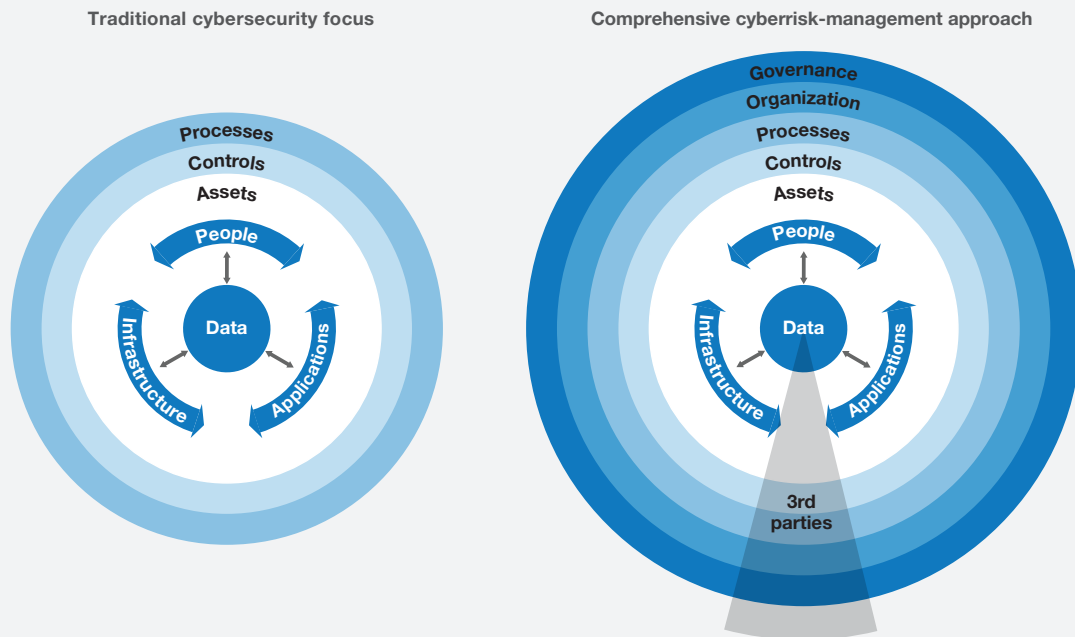
Companies that adhere to these principles tend to be much more resilient to most attacks than their peers. A defense ministry set out to ramp up cyberresilience across its entire organization. Scenario exercises helped increase cyberrisk awareness and instill a sense of urgency, by focusing on the mind-set of potential attackers and the concept of the weakest link in the chain of defense. Through an extensive training program, this kind of thinking was rolled out to the entire agency, making sure skills were passed on from

expert to expert. Throughout, the intelligence unit acted as the stronghold of cybersecurity expertise and the catalyst of change. In parallel, the institution reviewed and adjusted its IT architecture to increase resilience against destructive attacks, such as those that corrupt current data and backups, leading to a nonrecoverable situation.

The new approach also makes better use of cybersecurity resources and funds. Just refocusing investment on truly crucial assets can save up to 20 percent of cybersecurity cost. In our experience, up to 50 percent of a company’s systems are not critical from a cybersecurity perspective. We’ve also seen that the cost of implementing a given security solution can vary by a factor of five between comparable companies,

Exhibit 1

In a world where everything is connected, cybersecurity must be comprehensive, adaptive, and collaborative.



Source: NIST; McKinsey analysis

suggesting that many companies are missing out on considerable efficiencies.

Other benefits include less disruption of operations, which cybersecurity initiatives often bring about. And by involving business owners from the beginning, companies can speed up significantly the design and implementation of their cybersecurity architecture.

Building resilience, step by step

Successful cyberstrategies are built one step at a time, drawing on a comprehensive understanding of relevant business processes and the mind-set of prospective attackers. Three key steps are to prioritize assets and risks, improve controls and processes, and establish effective governance.





Prioritize assets and risks by criticality

Companies can start by taking stock of their cyber risk capabilities and comparing them with industry benchmarks. With that knowledge, they can set realistic aspirations for their resilience level. Generic visions to become world-class are usually not productive. Rather, the aspiration should be tailored to the industry and the current threat level.

Almost all companies are exposed to automated attacks and, indirectly, to industry-wide attacks. Beyond these unspecified threats, the relevance of other attack categories differs significantly, depending on the industry and the company's size and structure. Before investing in cyberdefenses, executives should strive to clarify the most relevant risks (Exhibit 2).

Exhibit 2

Companies should assess threats and develop controls to the most critical.

Assets	Threats	Controls
 Data	<ul style="list-style-type: none"> • Data breach • Misuse or manipulation of information • Corruption of data 	<ul style="list-style-type: none"> • Data protection (eg, encryption) • Data-recovery capability • Boundary defense
 People	<ul style="list-style-type: none"> • Identity theft • "Man in the middle" • Social engineering • Abuse of authorization 	<ul style="list-style-type: none"> • Controlled access • Account monitoring • Security skills and training • Background screening • Awareness and social control
 Infrastructure	<ul style="list-style-type: none"> • Denial of service • Manipulation of hardware • Botnets • Network intrusion, malware 	<ul style="list-style-type: none"> • Control of privileged access • Monitoring of audit logs • Malware defenses • Network controls (configuration, ports) • Inventory • Secure configuration • Continuous vulnerability assessment
 Applications	<ul style="list-style-type: none"> • Manipulation of software • Unauthorized installation of software • Misuse of information systems • Denial of service 	<ul style="list-style-type: none"> • Email, web-browser protections • Application-software security • Inventory • Secure configuration • Continuous vulnerability assessment

Source: European Union Agency for Network and Information Security; The SANS Institute

Turning to assets, companies need to know what to secure. Automated tools can help executives inventory all assets connected to the corporate network (that is, IT, OT, and the IoT). With some extra work, they can even catalog all the people that have access to the network, regardless of whether they are on the company payroll or work for a supplier, customer, or service provider. The asset inventory and people registry can be studied to help companies prioritize their security initiatives as well as their response to attacks and recovery afterward.

Establish differentiated controls and effective processes

Blunt implementation of controls across all assets is a key factor behind cybersecurity waste and productivity loss. Not all assets need the same controls. The more critical the asset, the stronger the control should be. Examples of strong controls include two-factor authentication and background checks of employees who have access to critical assets.

Similarly, processes can be made more effective. The traditional focus on compliance—adhering to protocols, ticking boxes on checklists, and filing documentation—is no longer suited to the quickly evolving cyberthreat landscape, if it ever was. Companies need to embrace and adopt automation, big data solutions, and artificial intelligence to cope with the ever-increasing number of alerts and incidents. And in a world where digital and analytical talent is scarce, and cybersecurity skills even more so, they should build a network of partners to fill gaps in their capabilities. Companies should keep reviewing their partner strategy, checking which processes can be outsourced and which should be handled in-house to protect intellectual property or fend off high risk.

Consolidate the organization and establish universal governance

Most current security organizations are still driven by analog dangers. The resulting structures, decision rights, and processes are inadequate to deal with

cyberrisk. A state-of-the-art cybersecurity function (Exhibit 3) should bridge the historical splits of responsibility among physical security, information security, business continuity, and crisis management to minimize conflicts of interest and duplication of processes. It should align its cybersecurity work with relevant industry standards so that it can more effectively work with others to manage incidents. The organizational structure should clearly define responsibilities and relationships among corporate headquarters, regional teams, and subsidiaries. And it should establish strong architectures for data, systems, and security to ensure “security by design” and build long-term digital resilience.

To be effective, though, the organization needs a company-wide governance structure, built on a strong cyberrisk culture. Governance of IT, OT, the IoT, and products should be consolidated into one operating model, and the entire business system should be covered, including third parties. Ten elements characterize the ideal governance structure. The cybersecurity unit should hold responsibility for cybersecurity company-wide, and:

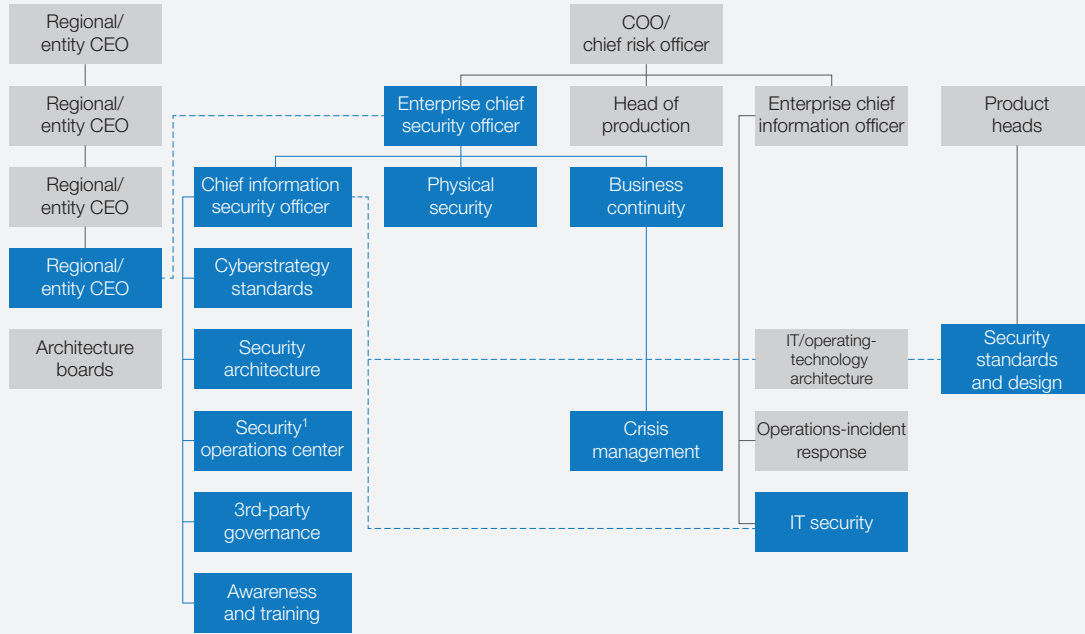
- be led by a senior, experienced CSO with a direct reporting line to the board
- own the overall cyberrisk budget
- be accountable for implementation of a portfolio of initiatives
- report regularly on the progress of risk remediation to the board and other stakeholders (this task might be handled by the chief risk officer (CRO))
- maintain a veto on all cyberrisk-related decisions, such as outsourcing, vendor selection, and exceptions from security controls
- establish an effective committee structure from the board down, ensuring coverage of all

Exhibit 3

Companies should assess threats and develop controls to the most critical.

Example of consolidated structure

■ Cybersecurity team



¹ Including forensics, intelligence, and response.

Source: McKinsey analysis

cyberrisk-related activities (such as outsourcing, vendor management, and third-party management) across all businesses and legal entities

- build awareness campaigns and training programs, and adjust these regularly to cover the latest threats (this task might be handled by the CRO)
- set clear and effective communication and incentive structures to enforce cybersecurity controls
- stage frequent and realistic attack and crisis simulations within the organization, with partners, and with other players in the industry

- set up efficient interfaces with law enforcement and regulators

How one company built resilience

A global industrial company suffered substantial damages from a cyberattack, surprising its leaders, who had believed that its IT security processes and a highly standardized software architecture would not be so easily breached. Its IT organization had regularly issued patches and updates to cope with new threats and had a strong protocol of automated backups. However, IT was managed regionally, and it took some time before the attacked region discovered the breach and reported it. It also turned out that there were gaps in business-continuity management, vendor-risk

management, and stakeholder communication along the value chain.

Based on a thorough postmortem, the company designed a number of initiatives to increase resilience, including the following:

- creating an empowered CSO function to increase cyberrisk awareness and establish a cybersecurity culture at all levels of the organization
- implementing state-of-the-art global business-continuity-management processes across the organization
- building redundancy of critical systems (for example, Linux backups for Windows-based production systems) to reduce risk concentration
- improving processes to manage vendor risk

The company now thinks its resilience is improved, as it can now monitor the concentration of risks, reduce them systematically, and have confidence that the gaps in governance have been plugged.



As companies shift to this new posture, special thought must be given to the people who will make it happen. Ultimately, winning the war against cyberrisk is tantamount to winning the war for cybertalent. Cybersecurity functions need to attract, retain, and develop people who are nimble, innovative, and open-minded. No matter how refined the technology, it is the human factor that will win the war. ■

¹ “The Comprehensive National Cybersecurity Initiative,” May 2009, obamawhitehouse.archives.gov.

Thomas Poppensieker is a senior partner in McKinsey’s Munich office, and **Rolf Riemenschitter** is a partner in McKinsey’s Frankfurt office.

Copyright © 2018 McKinsey & Company.
All rights reserved.