McKinsey & Company

Perspectives on transforming cybersecurity

Digital McKinsey and Global Risk Practice March 2019

Perspectives on transforming cybersecurity

Introduction

It wasn't too long ago that sophisticated executives could have long, thoughtful discussions on technology strategy without even mentioning security. Today, companies have substantial assets and value manifested in digital form, and they are deeply connected to global technology networks – even as cyberattackers become ever more sophisticated and adaptable to defenses.

At most companies, boards and senior executives acknowledge the serious threats that cyberattacks pose to their business. What they are not sure of is how to create a strategy that helps them understand and address the threats, in all their forms, today and in the years ahead. And they're asking for such a strategy every day.

Our experience working to protect some of the world's largest and most sophisticated companies, and our proprietary research, have revealed three broad mandates that can help organizations transform their cyber-security efforts. In this compendium, we offer a comprehensive series of articles that describe how companies can make these mandates a reality, and help their leaders sleep more soundly.

1. Go beyond technical controls to build a holistic program that protects the enterprise

- **"Hit or myth? Understanding the true costs and impact of cybersecurity programs"** shows that more spending doesn't necessarily lead to better protection.
- **"A new posture for cybersecurity in a networked world"** explains how companies can use organizational structure and governance to enhance cybersecurity protections.
- **"Protecting your critical digital assets: not all systems are created equal"** shows that companies must focus their strongest protections on their most important systems and assets.
- **"Insider threat: The human element of cyberrisk"** discusses how to use targeted analytics to eliminate threats from the adversaries within the organization.
- **"To survive in the age of advanced cyberthreats, use 'active defense'"** explains how to respond to emerging attacks by applying threat intelligence and analytics.
- **"Making a secure transition to public cloud"** reveals how leading-edge companies are exploiting the opportunities of public cloud infrastructure while they build the processes, architectures, and operating models necessary to protect sensitive data.
- **"Cyberrisk measurement and the holistic cybersecurity approach".** Comprehensive dashboards can accurately identify, size, and prioritize cyberthreats for treatment.
- **"Cybersecurity and the risk function".** Information technology, cybersecurity, and risk professionals need to work together to protect their organizations from cyberthreats.

2. Engage the full set of stakeholders to ensure appropriate support and decision-making

- **"A framework for improving cybersecurity discussions within organizations"** explains tangible mechanisms the chief information security officer can use to gain buy-in throughout the company, and improve decision-making.

- **"The board's role in managing cybersecurity risks"** lays out what cybersecurity data the board of directors should expect, and the questions it should ask.

- **"Asking the right questions to define government's role in cybersecurity"** provides a framework for how public policy makers can think about engaging constructively on cybersecurity.

3. Integrate cybersecurity with business strategy to build trust and create value

- **"How CEOs can tackle the challenge of cybersecurity in the age of the Internet of Things"** shows how companies can engineer security into IoT products.

- **"Shifting gears in cybersecurity for connected cars"** makes the case for automakers to start investing in security design, to protect themselves and the people who drive their vehicles.

- **"Critical resilience: Adapting infrastructure to repel cyberthreats"** highlights the mindset shifts required for managers in physical infrastructure companies.

David Chinn
Senior Partner, London

James M. Kaplan
Partner, New York

Thomas Poppensieker
Senior Partner, Munich

Table of contents

1. Go beyond technical controls to build a holistic program that protects the enterprise

Hit or myth? Understanding the true costs and impact of cybersecurity programs

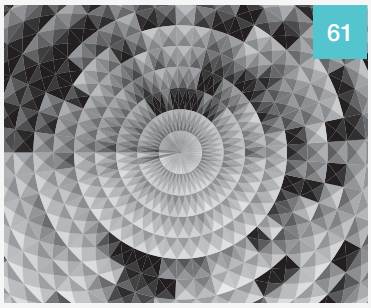
A new posture for cyber-security in a networked world

Protecting your critical digital assets: Not all systems and data are created equal

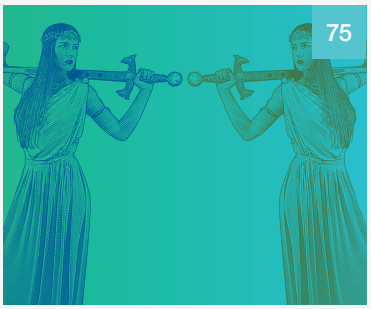
Insider threat: The human element of cyberrisk

To survice in the age of advanced cyberthreats, use ‘active defense’

Making a secure transition to the public cloud



Cyberrisk measurement and the holistic cybersecurity approach

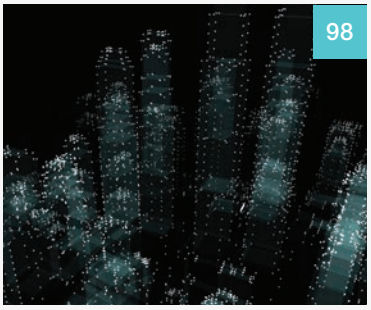


Cybersecurity and the risk function

2. Engage the full set of stakeholders to ensure appropriate support and decision-making

A framework for improving cybersecurity discussions within organizations

The board's role in managing cybersecurity risks



Asking the right questions to define government's role in cybersecurity

3. Integrate cybersecurity with business strategy to build trust and create value

How CEOs can tackle the challenge of cybersecurity in the age of the Internet of Things

Shifting gears in cybersecurity for connected cars

Critital resilience: Adapting infrastructure to repel cyber theats

fotomay/Getty Images

Hit or myth? Understanding the true costs and impact of cybersecurity programs

Jason Choi, James Kaplan, Chandru Krishnamurthy, and Harrison Lung

Cybersecurity is a critical but often misunderstood aspect of companies' technology infrastructures. Here's how business and technology leaders can ensure that important corporate assets remain safe.

Companies are using all kinds of sophisticated technologies and techniques to protect critical business assets. But the most important factor in any cybersecurity program is trust. It undergirds all the decisions executives make about tools, talent, and processes. Based on our observations, however, trust is generally lacking in many organizations' cybersecurity initiatives—in part, because of competing agendas. Senior business leaders and the board may see cybersecurity as a priority only when an intrusion occurs, for instance, while the chief security officer and his team view security as an everyday priority, as even the most routine website transactions present potential holes to be exploited.

This lack of trust gives rise to common myths about cybersecurity—for instance, about the

types of threats that are most relevant, the amount of spending required to protect critical data, and even about which data sets are most at risk. Perceptions become facts, trust erodes further, and cybersecurity programs end up being less successful than they could be. If incidence of breaches has been light, for instance, business leaders may tighten the reins on the cybersecurity budget until the CIO or other cybersecurity leaders prove the need for further investment in controls—perhaps opening themselves up to attack. Conversely, if threats have been documented frequently, business leaders may reflexively decide to overspend on new technologies without understanding that there are other, nontechnical remedies to keep data and other corporate assets safe.

In our experience, when there is greater transparency about companies' cybersecurity programs, and trust among the various stakeholders, companies reap significant benefits. Businesses can make better decisions about their security priorities and response plans, as well as the training and investments required to hold attackers at bay. In this article, we explore four common myths executives tend to believe about cybersecurity, and we suggest joint actions business and IT executives can take to create more transparency and understanding company-wide about the technologies and processes that are most effective for protecting critical business information.

Separating myths from facts

Based on our work with companies across industries and geographies, we've observed that business and cybersecurity leaders fall under the sway of four core myths when discussing or developing protection programs for corporate assets.

Myth 1: All assets in the organization must be protected the same way

Not all data are created with equal value. The customer data associated with a bank's credit-card program or a retailer's loyalty-card program are of greater value than the generic invoice numbers and policy documents that companies generate in-house. Companies don't have endless resources to protect all data at any cost, and yet most deploy one-size-fits-all cybersecurity strategies. When faced with a request from the IT organization for more funding for cybersecurity, C-suite leaders tend to approve it reflexively (particularly in the wake of a recent security breach) without a more detailed discussion of trade-offs—for instance, how much is "too much" to spend on protecting one set of critical data versus another? Or if the company protects all external-facing systems, what kind of opportunities is it missing by not bringing suppliers into the fold (using appropriate policies and governance approaches)? Indeed, most business executives we've spoken with acknowledge a blind spot when it comes to understanding the return they are getting on their security investments and associated trade-offs.

In our experience, a strong cybersecurity strategy provides differentiated protection of the company's most important assets, utilizing a tiered collection of security measures. Business and cybersecurity leaders must work together to identify and protect the "crown jewels"—those corporate assets that generate the most value for a company. They can inventory and prioritize assets and then determine the strength of cybersecurity protection required at each level. By introducing more transparency into the process, the business value at risk and potential trade-offs to be made on cost would

then be more obvious to all parties. A global mining company, for example, realized it was focusing a lot of resources on protecting production and exploration data, but it had failed to separate proprietary information from that which could be reconstructed from public sources. After recognizing the flaw, the company reallocated its resources accordingly.

Myth 2: The more we spend, the more secure we will be

According to our research, there is no direct correlation between spending on cybersecurity (as a proportion of total IT spending) and success of a company's cybersecurity program. Some companies that spend quite a bit on cybersecurity are actually underperforming the rest of the market with respect to developing digital resilience[1] (Exhibit 1). In part, this is because those companies were not necessarily protecting the right assets. As we mentioned earlier, companies often default to a blanket approach (protecting all assets rather than the crown jewels). Throwing money at the problem may seem like a good idea in the short term—particularly when an intrusion occurs—but an ad hoc approach to funding likely will not be effective in the long term. Business and cybersecurity leaders instead must come to a shared understanding of costs and impact and develop a clear strategy for funding cybersecurity programs. The business and cybersecurity teams at a healthcare provider, for example, might agree that protecting patient data is the first priority but that confidential financial data must also be secured so as not to compromise partner relationships and service negotiations. They could allocate resources accordingly. Without this shared understanding, business leaders may balk when a data breach occurs after they've funded significant changes in the security infrastructure. The lack of transparency and trust between the C-suite and the IT organization will only get worse.

Myth 3: External hackers are the only threat to corporate assets

It is true that threats from outside the company are a huge concern for cybersecurity teams, but there are significant threats inside corporate walls as well. The very people who are closest to the data or other corporate assets can often be a weak link in a company's cybersecurity program—particularly when they share passwords or files over unprotected networks, click on malicious hyperlinks sent from unknown email addresses, or otherwise act in ways that open up corporate networks to attack. Indeed, threats from inside the company account for about 43 percent of data breaches.[2]

Business and cybersecurity leaders must therefore collaborate on ways to improve internal risk culture. They must educate employees at all levels about the realities of cyberattacks and best practices for fending them off—for instance, holding town meetings, mounting phishing campaigns, or staging war-game presentations to familiarize employees with potential threats and raise awareness. Many of these activities will need to be led by the CIO, the chief security officer, or other technology professionals charged with managing cybersecurity programs. But none will be fruitful if the company's business leaders are not fully engaged in a dialogue with the cybersecurity function and if companies don't build explicit mechanisms for ensuring that the dialogue continues over the long term.

[1] Unless otherwise indicated, statistics relating to the composition and effectiveness of companies' cybersecurity programs are from the 2015 McKinsey Cyber Risk Maturity Survey.

[2] *Grand theft data*, Intel Security, 2015, mcafee.com.

Exhibit 1

Companies' spending on cybersecurity does not necessarily correlate with level of protection.

Note: Reflects responses from 45 companies in the Global 500 about their cybersecurity spending and capabilities.

[1]Companies' cybersecurity maturity is rated on a scale of 1 to 4, with 4 being the most mature (highest-level talent and capabilities).
[2]Spending is rated on a scale of 1 to 10; no companies allocated more than 10% of their budget on security.

Source: 2015 McKinsey Cyber Risk Maturity Survey

Business leaders at all levels must realize that they are actually the first line of defense against cyberthreats, and cybersecurity is never the sole responsibility of the IT department.

Myth 4: The more advanced our technology, the more secure we are

It is true that cybersecurity teams often use powerful, cutting-edge technologies to protect data and other corporate assets. But it is also true that many threats can be mitigated using less-advanced methods. After all, most companies are not dealing with military-grade hackers. According to research, more than 70 percent of global cyberattacks come from financially motivated criminals who are using technically simple tactics, such as phishing emails.[3]

When companies invest in advanced technologies, but do not understand how best to use them or cannot find properly skilled administrators to manage them, they end up creating significant inefficiencies within the cybersecurity team, thereby compromising the cybersecurity program overall.

Companies must, of course, explore the latest and greatest technologies, but it is also critical that companies establish and maintain good security protocols and practices to supplement emerging technologies—for instance, developing a robust patch-management program[4] and phasing out software for which vendors no longer provide security updates. This sort of foundation can help companies mitigate many of the biggest threats they may face. Consider the following example: a patch covering the vulnerabilities that could be exploited by the WannaCry cryptoworm was released March 14, 2017—some two months before the ransomware worked its way into more than 230,000 computers across more than 150 companies.

Building a culture of resilience

Rather than perpetuate myths, business and cybersecurity leaders should focus on bridging the trust gaps that exist between them. We believe most companies can do that when technology and business leaders jointly train their attention on two main issues of control: how to manage trade-offs associated with cybersecurity, and how to discuss cybersecurity issues and protocols more effectively.

How do we manage trade-offs?

Technology professionals have a role to play in reeducating the C-suite about best practices in cybersecurity spending—specifically, illustrating for them why a tiered approach to cybersecurity may be more effective than blanket coverage for all. The budget cannot grow and shrink depending on whether the company recently suffered a system intrusion. Cybersecurity must be considered a permanent capital expenditure, and allocations should be prioritized based on a review of the entire portfolio of initiatives under way. Business and technology professionals must work together to manage the trade-offs associated with cybersecurity.

When discussing which initiatives to invest in and which to discontinue, business and cybersecurity professionals can use a risk-categorization model with four threat levels denoted, from minor to severe. The cybersecurity team can then engage the

[3] *2017 Data breach investigations report*, Verizon, 2017, verizonenterprise.com.

[4] Patch management is the structured process of acquiring, testing, and installing code changes to an administered computer system.

C-suite in discussions about the most important data assets associated with each part of the business value chain, the systems they reside in, the controls being applied, and the trade-offs associated with protecting higher-priority assets versus lower-priority ones.

At a broader level, technology professionals can help the C-suite create benchmarks for cross-company and multiyear expenditures on cybersecurity initiatives that can be reviewed regularly—for instance, cybersecurity spending as a percentage of overall IT expenditures. The CIO and his team could create a capital-expenditure index for security investments to help the C-suite justify cost per risk-adjusted losses or cost per percentage of infrastructure protected Or, technology and business professionals could jointly develop a formula for quantifying the upside of making improvements to the cybersecurity program. In this way, they can make clear decisions about which tools to buy and add to the existing cybersecurity architecture, which systems to upgrade, and which to retire.

Regardless of the metrics used, it is important to have a comprehensive, formal approval process for planning and reviewing capital expenditures associated with cybersecurity. Priorities must be set from a business perspective rather than a systems perspective. CIOs and chief security officers must collaborate with the business to identify those assets with the potential to generate the greatest amount of value for the business and develop a cybersecurity road map accordingly. The road map would illustrate the distribution of crown jewels across the organization and the greatest surface areas of exposure. It would outline current controls and the sequence for launching new security initiatives, looking two to three years out. Of course, business and cybersecurity executives would need to revisit these plans quarterly or annually to ensure that they are still relevant given changes to the environment. The road map would also define roles and responsibilities, as well as mechanisms by which the C-suite and the leaders in the cybersecurity function could monitor progress made against the plan and revise it accordingly.

How do we talk about cybersecurity?

Weak communication accounts for much of the lack of trust between business leaders and members of the cybersecurity function. Our research indicates that in most companies, cybersecurity professionals are at least two layers from the CEO in the corporate hierarchy, with few opportunities for direct discussion about protection issues and priorities (Exhibit 2). What's more, in about half of the companies we studied, there was little to no formal documentation shared by the cyber function with the C-suite about the status of their defense systems; many companies relied instead on occasional emails, memos, and notes (Exhibit 3).

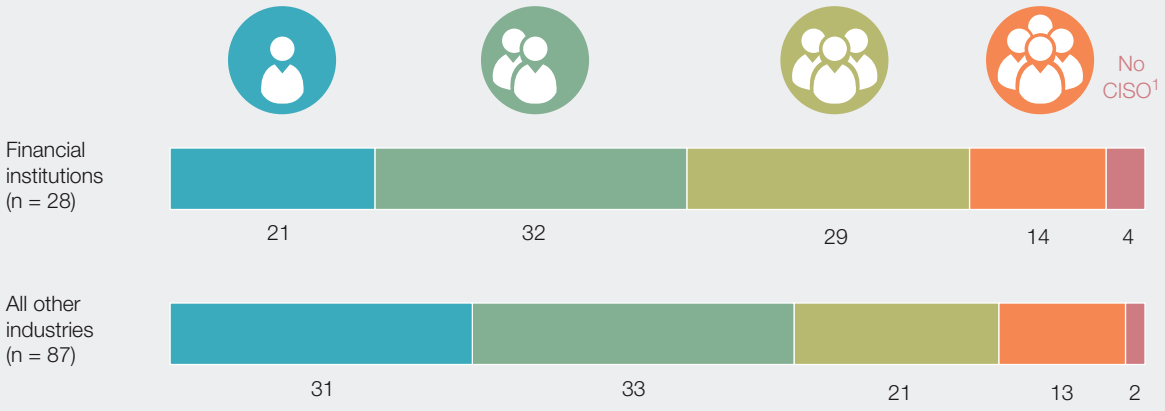
Furthermore, when business and technology professionals do get in a room together, cybersecurity is usually discussed using highly technical language—for instance, "We already have measures to cover all CVE, however APT is something we need to watch out for. With our current SVM and SIEM infrastructure, there is no way we can defend these advanced attacks."[5] Jargon notwithstanding, the technology and business professionals in the room all understand how critical it is to build

[5] CVE stands for common vulnerabilities and exposures, APT stands for advanced persistent threat, SVM stands for security and vulnerability management, and SIEM stands for security information and event management.

Exhibit 2

Cybersecurity teams' access to the C-suite is limited.

How many direct reports away is the senior-most cybersecurity executive from the CEO?, % of survey respondents



Note: Executives polled included chief information security officers and other C-suite executives charged with making decisions about cybersecurity investments.

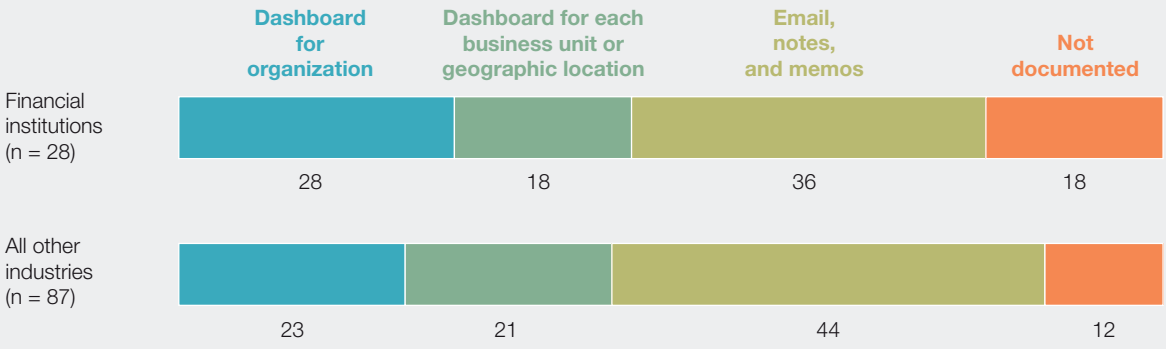
[1]Chief information security officer.

Source: 2015 McKinsey Cyber Risk Maturity Survey

Exhibit 3

Many cybersecurity teams use informal means to communicate with business leaders.

How do you summarize the status of defense systems to the chief information security officer and business-level executives?, %



Note: Executives polled included chief information security officers and other C-suite executives charged with making decisions about cybersecurity investments.

Source: 2015 McKinsey Cyber Risk Maturity Survey

a robust cybersecurity program given the potential effects on the bottom line if corporate assets are compromised. But each side is typically only getting half the story.

Instead of reporting that "ten vulnerabilities were remediated," for example, technology professionals can use visual aids and outcomes-oriented language to help business leaders understand potential security threats and ways to address them. A status update might be better phrased in the following manner: "Our cybersecurity team has patched a security hole in our customer-relationship-management system that could have given hackers access to millions of packets of our retail customers' data, creating $100 million in financial damage." Cybersecurity professionals could also clearly delineate and communicate levels of systems access for intended and unintended users—a database administrator would have greater privileges than frontline employees, for instance.

Finding a common vocabulary is important not just for ensuring clear communication between the C-suite and the cybersecurity function but also for raising awareness about potential cyberthreats and risks among employees throughout the company. Members of the cybersecurity function should schedule frequent, regular check-ins with staff at all levels to educate them about relevant cybersecurity topics—how to recognize a phishing email, for example—and to showcase the company's security capabilities. The cybersecurity team at one technology firm conducts "road shows" to demonstrate which systems are being scanned and how they are being monitored. One online retailer, meanwhile, includes details about its cybersecurity efforts in existing financial reports—for instance, reporting on its development of an antimalware scanner to protect the integrity of its recommendation engine, which helps drive advertising. It does this to illustrate that cybersecurity is part of the business process and can help drive revenue.

These discussions should take place regardless of whether the company is facing an imminent threat or not. The cybersecurity team at one company we observed shared with top leadership a simple breakdown of a typical security-event drill (Exhibit 4). The team wanted to give members of the board and the C-suite a step-by-step overview of what would happen in a typical attack—not just to prove the effectiveness of the company's security capabilities but also to familiarize individuals with potential threats so they might recognize them when they encounter deviations from the norm.

◆◆◆

As we mentioned earlier, technology leaders may have to lead the charge in forging direct communications, creating cost transparency, and identifying business priorities. But the tasks suggested will require experience in C-suite-level communication, budgeting, and strategy planning—some of which may be beyond the core skill set of those on the cybersecurity team. To come up to speed more quickly, cyber leaders may want to reach out to others with relevant expertise—for example, vendors and partners who can share best practices. In the spirit of agile development, cybersecurity teams may also want to take on these activities in "launch-review-adjust" mode. They could update threat and risk profiles in one- to six-month sprints, thereby ensuring they are responsive to the latest trends and technologies.

Exhibit 3

A cybersecurity data theft has a pattern of event and response.

1

Insider takes sensitive data via flash drive

A disgruntled employee installs indexing malware in corporate systems and transfers files from servers to USB drive.

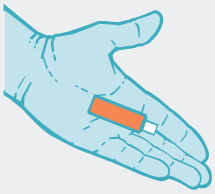
Visible hints

- Inquiry is made to senior executives about temp file being created and deleted.
- Slow laptops are reported to IT department and chief information officer.
- Help-desk ticket is sent to IT security lead.

Typical response

- Initially, the IT-security team does not realize that data are being threatened.
- Once the data are breached, the security team tries to determine best way to inform senior executives; the process is ad hoc, because protocols are not clear.

2



Insider gives or sells employee data to a cybercriminal

Cybercriminal uses old but valid credentials to access company servers and download employee records containing personally identifiable information (PII).

Visible hints

- Data-loss alerts are sent to the security lead in the IT organization.

Typical response

- Team focuses on the forensics of the alert but is not able to connect it to previous notifications.

3

Cybercriminal sells PII data to identity thieves on the black market

Identity thieves buy and use the employee data for fraudulent transactions.

Visible hints

- Based on individuals' and organization's complaints, the FBI detects the data breach and files a report with government affairs.

Typical response

- IT security reactively investigates employee data leak, trying to determine the scope of the breach.
- Team escalates event to privacy team.

4

Sensitive data is published on social media

Online bloggers publish video with references to the sensitive data stolen.

Visible hints

- An online video, found by employees, is sent to the head of communications.

Typical response

- The security team engages the communications group.

Source: 2015 McKinsey Cyber Risk Maturity Survey

Make no mistake, the time to foster greater transparency about cybersecurity is now. The board must have trust in the C-suite and its ability to handle security breaches without dramatically affecting the company's value and brand. The C-suite needs to trust the chief information security officer's claims that every penny spent on improving the security of IT infrastructure is worth it. The company needs to trust that vendors can properly protect shared data or ensure service stability if breaches occur. And, of course, customers need to trust that their personal data is being carefully safeguarded behind corporate walls.

The C-suite and the cybersecurity function can no longer talk past one another; security must be a shared responsibility across the business units. It must be embedded in various business processes, with the overarching goal of building a culture of resilience. The companies that take steps now to build greater trust between the business and the IT organization will find it easier to foster a resilient environment and withstand cyberthreats over the long term. ◆

Jason Choi is a consultant in McKinsey's Hong Kong office, where **Harrison Lung** is an associate partner; **James Kaplan** is a partner in the New York office, and **Chandru Krishnamurthy** is a senior partner in the Atlanta office.

The authors wish to thank Suneet Pahwa and Chris Rezek for their contributions to this article.

Designed by Global Editorial Services.

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 Riemenschnitter

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

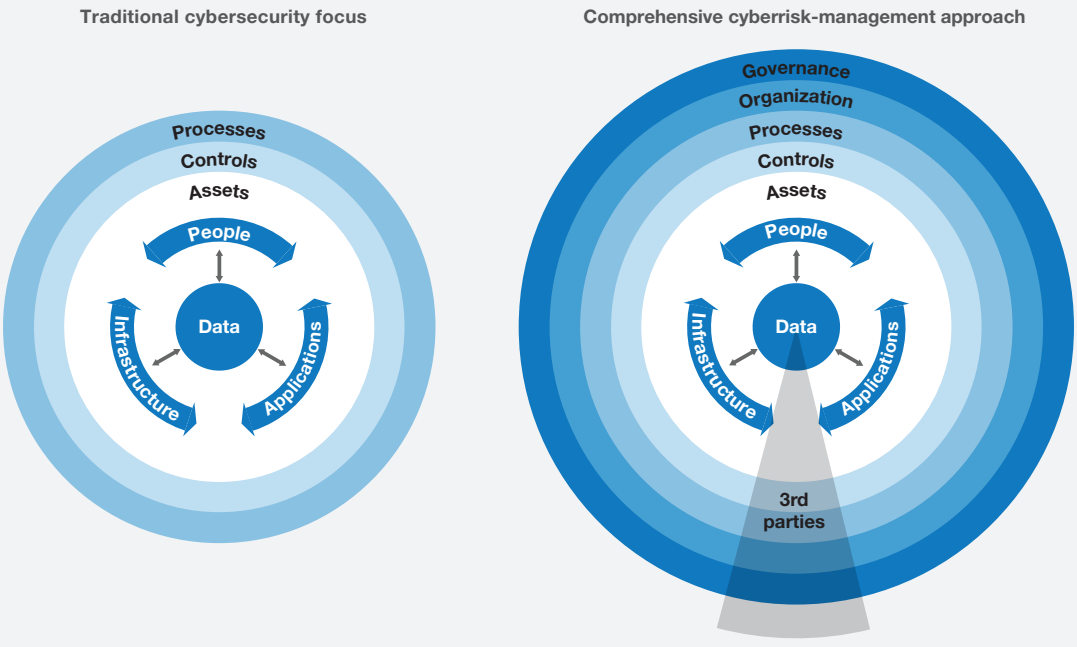
suppliers and customers too. While it may be hard—or even impossible—to protect a company against the most advanced attacks, systematic governance is the best insurance against the bulk of everyday attacks.

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 cyberrisk 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	• Data breach • Misuse or manipulation of information • Corruption of data	• Data protection (eg, encryption) • Data-recovery capability • Boundary defense
People	• Identity theft • "Man in the middle" • Social engineering • Abuse of authorization	• Controlled access • Account monitoring • Security skills and training • Background screening • Awareness and social control
Infrastructure	• Denial of service • Manipulation of hardware • Botnets • Network intrusion, malware	• Control of privileged access • Monitoring of audit logs • Malware defenses • Network controls (configuration, ports) • Inventory • Secure configuration • Continuous vulnerability assessment
Applications	• Manipulation of software • Unauthorized installation of software • Misuse of information systems • Denial of service	• 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 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

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 Riemenschnitter** is a partner in McKinsey's Frankfurt office.

Risk

Protecting your critical digital assets: Not all systems and data are created equal

Top management must lead an enterprise-wide effort to find and protect critically important data, software, and systems as part of an integrated strategy to achieve digital resilience.

Piotr Kaminski, Chris Rezek, Wolf Richter, and Marc Sorel

The idea that some assets are extraordinary—of critical importance to a company—must be at the heart of an effective strategy to protect against cyber threats. Because in an increasingly digitized world, protecting everything equally is not an option. The digital business model is, however, entirely dependent on trust. If the customer interface is not secure, the risk can become existential. Systems breaches great and small have more than doubled in the past five years, and the attacks have grown in sophistication and complexity. Most large enterprises now recognize the severity of the issue but still treat it as a technical and control problem—even while acknowledging that their defenses will not likely keep pace with future attacks. These defenses, furthermore, are often designed to protect the perimeter of business operations and are applied disjointedly across different parts of the organization.

Our research and experience suggest that the next wave of innovation—customer applications, business processes, technology structures, and cybersecurity defenses—must be based on a business and technical approach that prioritizes the protection of critical information assets. We call the approach "digital resilience," a cross-functional strategy that identifies and assesses all vulnerabilities, defines goals on an enterprise-wide basis, and works out how best

to deliver them. A primary dimension of digital resilience is the identification and protection of the organization's digital crown jewels—the data, systems, and software applications that are essential to operations.

Burgeoning vulnerabilities, finite resources, fragmented priorities

In determining the priority assets to protect, organizations will confront external and internal challenges. Businesses, IT groups, and risk functions often have conflicting agendas and unclear working relationships. As a result, many organizations attempt to apply the same cyber-risk controls everywhere and equally, often wasting time and money but in some places not spending enough. Others apply sectional protections that leave some vital information assets vulnerable while focusing too closely on less critical ones. Cybersecurity budgets, meanwhile, compete for limited funds with technology investments intended to make the organization more competitive. The new tech investments, furthermore, can bring additional vulnerabilities.

The work to prioritize assets and risks, evaluate controls, and develop remediation plans can be a tedious, labor-intensive affair. Specialists must review thousands of risks and controls, and then make ratings based on individual judgment. Some organizations mistakenly approach this work as a compliance exercise rather than a crucial business process. Without prioritization, however, the organization will struggle to deploy resources effectively to reduce information-security risk. Dangers, meanwhile, will mount, and boards of directors will be unable to evaluate the security of the enterprise or whether the additional investment is paying off.

All data and systems are not created equal

In any given enterprise, some of the data, systems, and applications are more critical than others. Some are more exposed to risk, and some are more likely to be targeted. Critical assets and sensitivity levels also vary widely across sectors. For hospital systems, for example, the most sensitive asset is typically patient information; other data such as how the emergency room is functioning may even be publically available. Risks to priority data include breach, theft, and even ransom—recall that a Los Angeles hospital paid a $17,000 Bitcoin ransom to a hacker that had seized control of its systems. An aerospace-systems manufacturer, on the other hand, needs to protect intellectual property first and foremost, from systems designs to process methodologies. A financial-services company requires few controls for its marketing materials but is vulnerable to fraudulent transactions; its M&A database, furthermore, will need the best protection money can buy. Attackers can be individuals or organizations, such as criminal syndicates or governments with significant resources at their command. The attacks can be simple or sophisticated, the objectives varying from immediate financial reward to competitive or even geopolitical advantage.

Cybersecurity spending: When more is less

In the face of such diverse threats, companies often decide to spend more on cybersecurity, but they are not sure how they should go about it.

- A global financial-services company left cybersecurity investments mainly to the discretion of the chief information-security officer (CISO), within certain budget constraints. The security team was isolated from business leaders, and resulting controls were not focused on the information that the business felt was most important to protect.

- A healthcare provider made patient data its *only* priority. Other areas were neglected, such as confidential financial data relevant to big-dollar negotiations and protections against other risks such as alterations to internal data.

- A global mining concern focused on protecting its production and exploration data but failed to separate proprietary information from information that could be reconstructed from public sources. Thus, broadly available information was being protected using resources that could have been shifted to high-value data like internal communications on business negotiations.

These typical examples illustrate the need for a unified, enterprise-wide approach to cyber risk, involving the business and the risk, IT, and cybersecurity groups. The leaders of these groups must begin to work together, identifying and protecting the organization's critical digital assets as a priority. The process of addressing cyber risk will also have to become technologically enabled, through the implementation of workflow-management systems. Cybersecurity investment must be a key part of the business budget cycle and investment decisions must be more evidence-based and sensitive to changes.

The business-back, enterprise-wide approach

The key point is to start with the business problem, which requires a consideration of the whole enterprise, and then to prioritize critical risks. This work should be conducted by an enterprise-wide team composed of key individuals from the business, including those in product development, and the cybersecurity, IT, and risk functions. The team's main tasks are to determine which information assets are priorities for protection, how likely it is that they will be attacked, and how to protect them. In order to function, the team must successfully engage the leaders of several domains. They need to work together to discover what is most important—no mean challenge in itself. The best way to get started is to found the team on the agreement that cyber risks will be determined and prioritized on an enterprise-wide "business back" basis. In other words, the team will first of all serve the enterprise. Critical risks, including the impact of various threats and the likelihood of occurrence, will be evaluated according to the dangers they pose to the business as a whole.

Guiding principles

The following principles can help keep companies on track as they take the unified approach to prioritizing digital assets and risk:

- *Start with the business and its value chain.* The effort should be grounded in a view of the business and its value chain. The CISO's team, particularly when it is part of the IT organization, tends to begin with a list of applications, systems, and databases, and then develop a view of risks. There are two major flaws to this approach. First, it often misses key risks because these can emerge as systems work in combination. Second, the context is too technical to engage the business in decision making on changes and investments. By beginning with the business, the team encourages stakeholder engagement naturally, increasing the likelihood that systemic exposures will be identified.

- *The CISO must actively lead.* In addition to being a facilitator for the business's point of view, the CISO should bring his or her own view of the company's most important assets and risks. By actively engaging the business leaders and other stakeholders as full thought partners, the CISO will help establish the important relationships for fully informed decision making on investments and resource allocation. The role of the CISO may thus change dramatically, and the role description and skill profile should be adjusted accordingly.

- *Focus on how an information asset can be compromised.* If an information asset is exposed by a system being breached, the

vulnerability of this system should be considered, even if the system's primary purpose does not relate to this information asset.

- *Focus on prioritization, not perfect quantification.* The team needs only enough information to make decisions on priority assets. It does not need highly precise risk quantifications—these would be difficult to produce and would not make a difference in deciding between investment options.

- *Go deeper where needed.* The same level of analysis is not needed to quantify all risks. Only for particularly high-impact or complex risks should the team invest in deeper analyses. It should then decide on and acquire the information needed to make more informed investment decisions.

- *Take the attacker's view.* Risk reviews and vulnerability analyses must not focus solely on the value of the information to the company and the ascertainable gaps in its defenses. The profiles of potential attackers are also important: Who wants the organization's information? What skills do they possess? Thinking about likely attackers can help identify new gaps and direct investment to protect the information that is most valuable to the most capable foes.

A flexible systematic process with a designed platform

The object of the enterprise-wide approach is to identify and remediate gaps in existing control and security systems affecting critical assets. The solution, in our experience, will be an end-to-end process, likely requiring multiple development iterations, including a detailed account of hundreds of assets. A workflow system and asset database would be an ideal tool for supporting this complex process, allowing focus on prioritizing risks. A flexible, scalable, and secure online application can be easy to use while managing all the inventory and mapping data, the rigorous risk and control evaluations, sector-specific methodologies, and rationales for each risk level. The platform can also support detailed data to be used when needed as the team undertakes analysis of the priority assets and gaps and makes the recommendations that will shape remediation initiatives.

In developing this approach for clients, McKinsey experts defined the following five key steps:

1. *Identify and map digital assets, including data, systems, and applications, across the business value chain.* This can be accelerated by applying a generalized-sector value chain and a common taxonomy for information assets and then customizing these to the organization.

2. *Assess risks for each asset, using surveys and executive workshops.* By basing this analysis on the business importance of the asset, the organization will have identified its crown jewels.

3. *Identify potential attackers, the availability of assets to users, and current controls and security measures protecting the systems through which access can be gained to the assets,* using similar surveys and workshops as in step two.

4. *Locate where security is weakest around crown-jewel assets and identify the controls that should be in place* to protect them, by comparing the results of these assessments using dashboards.

5. *Create a set of initiatives to address the high-priority risks and control gaps.* Implementation will involve a multiyear plan, including

timelines for follow-up reviews. Once the initial assessment is complete, this plan becomes a living document, regularly refreshed to reflect new data, systems, applications, risks, and mapping, as well as progress to remediate known vulnerabilities (see sidebar, "An institution's progress").

The process promotes cyber-risk transparency, answering key stakeholder questions: What are our inherent information risks? Where is our organization vulnerable? How big (and where) is the residual exposure? What remediation actions should we prioritize? How do we know if what we did is working? Information-risk trade-offs can be defined based on a perspective on value at risk across the company. This helps the C-suite and board discuss information-security risk in terms of enterprise value, providing transparency on what risks they are willing to accept and why.

Results inform budget and investment decisions, helping to satisfy both regulatory and shareholder expectations. With investments targeted to best protect the most sensitive digital assets, costs are held down as the digital resilience of the organization is elevated. To build digital resilience

An institution's progress

One financial institution that used our approach was able to identify and remediate gaps in its control and security systems affecting critical assets. The change program began with a risk assessment that had highlighted several issues. Business and IT priorities on cybersecurity spending were found to be somewhat out of alignment, while communication on risks and risk appetite between risk management and businesses was less than optimal. The lack of agreement among stakeholder groups consequently stalled progress on a mitigation plan for cyber risk.

In response, the company established a unified group which together developed a work plan to protect critical data. The team inventoried all systems and applications in all business units, validating the results with key stakeholders to ensure completeness. They then identified critical data and performed a risk assessment with input from the stakeholders. The team was now able to identify the critical information assets based on potential risk impact. The level of control in each system was also evaluated, as the team mapped information assets to the systems and applications where they reside and isolated gaps between current and needed controls.

The critical data assets requiring additional protection were identified globally and by business unit. The systems and applications holding critical data that needed remediation could then be addressed. The team developed a series of detailed scenarios to reveal system vulnerabilities and help stakeholders understand what could happen in a breach. A comprehensive set of prioritized initiatives and a multiyear implementation plan was then created. The data resulting from this process are continually updated and provide guidance in budgeting decisions and board reviews on an ongoing basis.

into their operations, furthermore, the process can help organizations create periodic assessments to highlight trends and new gaps. Risk managers can then develop new initiatives prioritized to the enterprise's global needs.

■ ■ ■

Organizations in sectors with higher digital maturity will benefit the most from this approach, including financial services, manufacturing, and healthcare. They face the tough task of fully protecting their most important assets, while not stifling business innovation. To achieve this balance, the business, IT, risk, and other functions will have to work together toward the same, enterprise-wide end—to secure the crown jewels so that the senior leaders can confidently focus on innovation and growth. ■

Piotr Kaminski is a senior partner in McKinsey's New York office, **Chris Rezek** is a senior expert in the Boston office, **Wolf Richter** is a partner in the Berlin office, and **Marc Sorel** is a consultant in the Washington, DC, office.

The authors wish to thank Oliver Bevan and Rich Cracknell for their contributions to this article.

Insider threat: The human element of cyberrisk

Cyber programs often miss the significant portion of risk generated by employees, and current tools are blunt instruments. A new method can yield better results.

Tucker Bailey, Brian Kolo, Karthik Rajagopalan, and David Ware

Insider threat via a company's own employees (and contractors and vendors) is one of the largest unsolved issues in cybersecurity. It's present in 50 percent of breaches reported in a recent study. Companies are certainly aware of the problem, but they rarely dedicate the resources or executive attention required to solve it. Most prevention programs fall short either by focusing exclusively on monitoring behavior or by failing to consider cultural and privacy norms.

Some leading companies are now testing a microsegmentation approach that can target potential problems more precisely. Others are adopting in-depth cultural change and predictive analytics. These new approaches can yield more accurate results than traditional monitoring and can also help companies navigate the tricky business of safeguarding assets while also respecting employees' rights.

Understanding the threat

Organizations sometimes struggle to clearly define insider threat. In this article, we use the term to mean the cyberrisk posed to an organization due to the behavior of its employees, rather than other kinds of insider threat, such as harassment, workplace violence, or misconduct. For these purposes, contractors and vendors are also considered employees; many of the largest cases in recent memory have trusted third parties at their center.

Briefly, inside threats arise from two kinds of employees: those who are negligent and those with malicious intent (see sidebar, "Double trouble"). Negligent or co-opted insiders are easy for companies to understand; through poor training, middling morale, or pure carelessness, usually reliable workers can expose the company to external risks. However, organizations often misunderstand malicious insiders in two ways.

Double trouble

Two types of workers can create cyberrisk:

Malicious insiders are those who purposefully seek to benefit themselves at the organization's expense or to harm the organization directly. They might steal valuable data, commit fraud for financial gain, publicly expose sensitive information to attract attention, or sabotage IT systems in disgruntlement. Most organizations focus their attention on malicious insiders, using activity-monitoring software and small investigative teams.

Negligent or error-prone insiders may not harm an organization intentionally but expose the organization to risk through their mistakes or carelessness. This can happen in two ways. First, an employee can carelessly create a vulnerability, which can be exploited by attackers directly. For example, a developer might misconfigure a company's Simple Storage Service (S3) buckets, or someone might lose a hard drive carrying sensitive data. Employees can also make themselves personally vulnerable to attack and co-option. For example, by sharing too much personal information online, employees may make themselves easy targets for spear-phishing attacks, in which attackers co-opt a user's account and use it to conduct further nefarious activities.

First, malicious insiders do not always seek to harm the organization. Often, they are motivated by self-interest. For example, an employee might use client information to commit fraud or identity theft, but the motive is self-enrichment rather than harm to the employer. In other cases, employees may be seeking attention, or have a "hero complex" that leads them to divulge confidential information. They might even think they are acting for the public good, but in reality they are acting for their own benefit. Understanding motive can help companies shape their mitigation strategy.

Second, malicious insiders rarely develop overnight or join the company intending to do it harm. In most recent examples of malicious insider events, normal employees became malicious insiders gradually, with months or years of warning signs leading up to a culminating insider event.

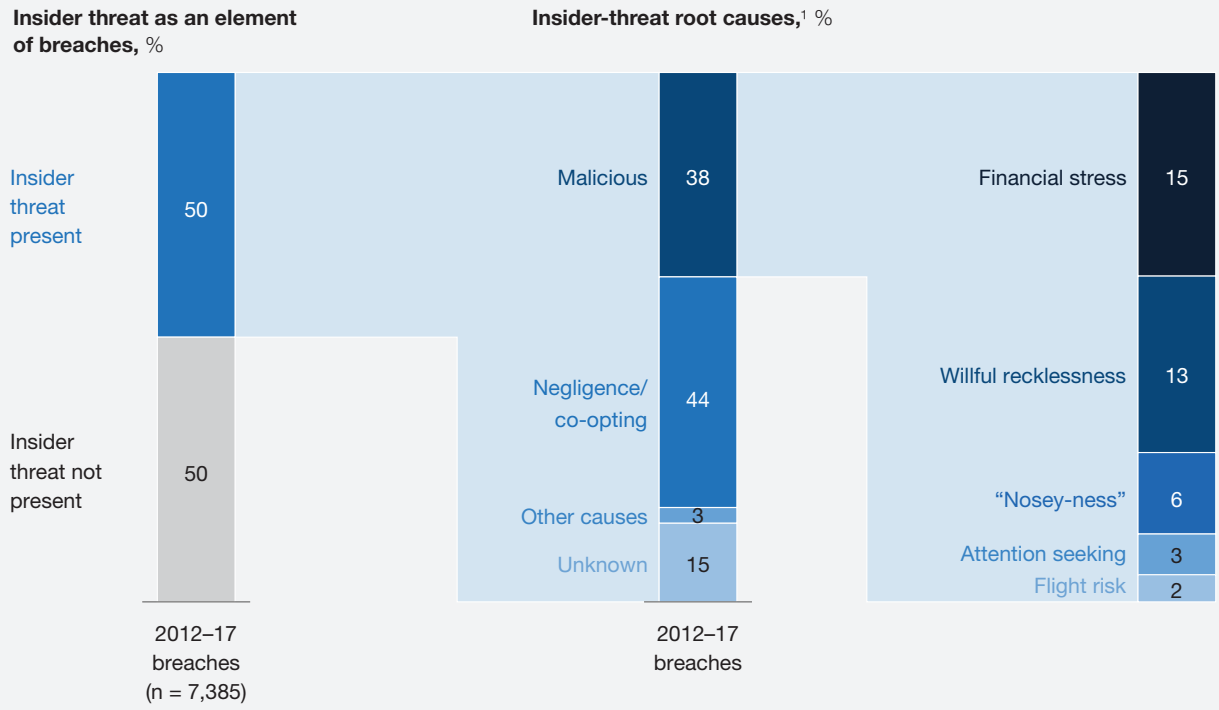
How big an issue is it, really?

In a world of competing cyber-priorities, where needs always seem to outpace budgets, it can be tempting to underinvest in combating insider threat. The risk is not well understood, and the solution feels less tangible than in other cyber areas. Many executives have asked us, "Is this actually an important issue? How much risk does it represent?"

We recently reviewed the VERIS Community Database, which contains about 7,800 publicly reported breaches from 2012 to 2017, to identify the prevalence of insider threat as a core element of cyberattacks. We found that 50 percent of the breaches we studied had a substantial insider component (Exhibit 1). What's more, it was not mostly malicious behavior, the focus of so many companies' mitigation efforts. Negligence and co-opting

Exhibit 1

Insider threat is present in 50 percent of cyberbreaches.



[1] Figures are approximate and may not sum, because of rounding.

Source: VERIS Community Database

accounted for 44 percent of insider-related breaches, making these issues all the more important.

In addition to being frequent, insider-threat breaches often create substantial damage. We have seen high-value events in which customer information was stolen by both negligent and malicious insiders in financial services, healthcare, retail, and telecom in recent years. Some companies lost hundreds of millions of dollars. Pharmaceutical and medical-products companies, as well as governments, have seen a significant rise in intellectual-property theft by malicious insiders.

Why current solutions fall short

To combat the risks of malicious insiders, most companies rely on user-behavior monitoring software (Exhibit 2). These rules-based or machine-learning-based applications ingest troves of data about employee actions, especially their use of IT systems. Generally, they attempt to identify divergence from what is considered "normal" behavior for that employee. When the software spots an anomaly, a small team investigates.

While this method can be helpful, we find that it usually falls short, for four reasons:

- By the time negative behaviors are detected, the breach has often already occurred. The organization is already at a disadvantage, and it cannot deploy an active defense.
- Monitoring for "divergence from normal behavior" creates a huge number of false positives, wasting much of the investigation team's time.

Exhibit 2

Current methods of management fall short.

Typical approach	Prevention and monitoring	Event detection: Behavior-variability analysis	Investigation	HR/business-unit action
	• "Dragnet" monitoring of all employee actions, all the time • General controls and preventions	• Analyze divergence from "normal" behavior	• Manually investigate numerous cases	• Take actions on a case-by-case basis
Pain points/risks	• Massive number of signals • High risk of misuse of data • Perception of privacy invasion • Preventions not customized to risks, actors, and actions	• Bad behaviors can be built into baseline • Huge volume of false positives (>30% in some cases)	• Often a long backlog of cases • Little ability to prioritize investigations	• Uncertainty about how to manage between investigation and action • Actions not well defined or tailored to individual incidents

- Serial bad actors may not be caught; malicious activity may be built into the baseline of "normal" activity.

- Collecting massive amounts of employee data creates privacy concerns and significant potential for abuse.

Beyond these issues, some organizations take this type of monitoring to an extreme, deploying military-grade software and conducting full-blown intelligence operations against their employees. Several recent news stories have highlighted the risks of overstepping the organization's cultural and privacy norms. Best practices and necessary precautions in the defense industry may be seen as invasive at a bank or insurer.

Finally, to the extent that companies pursue insider threat, they often focus on malicious actors. While most cyber organizations know that negligence is an issue, many start and end their prevention efforts with half-hearted employee education and anti-phishing campaigns.

A better way

Some leading cybersecurity teams are using a different approach, built on three pillars:

- *Microsegmentation* allows the organization to home in on the "hot spots" of risk and take a targeted rather than blanket approach to threat monitoring and mitigation.

- *Culture change* makes malicious, co-opted, or negligent risk events less likely, and puts the company in a preventive rather than reactive posture.

- *Prediction* allows an organization to identify and disrupt insider activities much earlier in the threat life cycle.

Microsegmentation

Rather than going immediately to wholesale monitoring, we believe that organizations should take a much more nuanced approach, tailored to their information assets, potential risk impacts, and workforce. The key to this approach is microsegmentation, which identifies particular groups of employees that are capable of doing the most damage, and then develops focused interventions specific to those groups.

To create a microsegmentation, the first step is to understand the business capabilities or information most important to protect. Next, companies can use identity-and-access-management (IAM) records, as well as organizational and HR information, to determine which groups and individual employees have access to those assets. These groups form the microsegments that are most important for the program to focus on. For each segment, a company can then determine which types of insider threats are most likely to cause damage, and it can create differentiated strategies to monitor and mitigate insider events.

Imagine that a pharmaceutical company wants to protect the intellectual property created in new drug development. An analysis of IAM and HR data reveals that specific portions of its product-development and its R&D organizations represent the highest risk. The company knows that sabotage of this kind of IP is relatively rare (other researchers would easily catch mistakes), but that flight risks—scientists who take IP with them when hired by competitors—are very probable. The company designs strategies to identify flight risks in the R&D team (such as people who missed promotions, poor workforce satisfaction, and low pay relative to peers), and then monitors the group for these characteristics. The company could then design interventions, such as retention programs, specifically for its flight risks.

Microsegmentation offers three key benefits. First, it creates a clearer understanding of risk; not all insider-threat events are created equal. Second, it allows organizations to identify a clear set of remediation actions, tailored to a particular group of employees. This helps them to move from reacting to insider-threat events to preventing them. Finally, the analysis allows the organization to monitor groups rather than individuals, using metrics such as employee attrition and workforce satisfaction of a team rather than individual behaviors. This provides significant privacy benefits.

Exhibit 3 shows an illustrative microsegmentation analysis for several kinds of information assets.

Culture change

While many programs focus on catching and responding to negative behaviors, it's also vitally important to directly and assertively address the cultural issues that drive negligence and malicious behavior.

To combat negligence and co-opting, companies often conduct rudimentary cybersecurity trainings, as well as phishing testing. Too often these focus only on behavior—educating employees on proper cyber-procedures—and miss the attitudes-and-beliefs part of the equation. Targeted interventions (such as periodic communications on cyber-impact) help employees see and feel the importance of "cyber-hygiene," and

Exhibit 3

Microsegmentation can reveal groups at risk, the actions they might commit, and their likely personas.

Threat assessment, illustrative example

Very likely Somewhat likely Not likely

Top assets	Employee populations with access	Insider-threat actions they might take			Likely personas involved
		Fraud/theft	Exposure	Destruction	
Intellectual property for new products	• R&D team • Business-unit (BU) exec				• Flight risk • Disgruntled
Financial forecasts	• Finance/investor-relations team • BU execs				• Financially stressed • Negligent
PII/PHI[1]	• HR team • Sales team				• Negligent • Reckless • Snooper
High-net-worth customer information	• High-net-worth sales and delivery team				• Flight risk • Financially stressed
Core financial platform	• IT team • BU execs				• Saboteur • Disgruntled
Records of corporate conduct	• HR/legal				• Attention seeker

[1] PII = personally identifiable information, PHI = protected health information.

purposeful reinforcement from senior executives is critical to achieving workforce buy-in. Best-in-class organizations rigorously measure both behaviors and attitudes and develop comprehensive change plans to beat cyber-negligence, complete with targets and clear owners within the organization.

Addressing the drivers of malicious behavior is an even more personal task. The drivers vary for each organization, and often for each microsegment. For instance, they might include personal financial stress, disgruntlement over lack of promotion, or flight risk due to poor management. Organizations that successfully address drivers of malicious behavior often begin by analyzing workforce trends (using satisfaction surveys, for example) to determine potential hot spots. They then design changes in process, governance, hiring, compensation, and so on, specific to the identified risk areas aligned to their microsegmentation strategy. For example, if an employee group has a high prevalence of "flight risks" due to disgruntlement over a manager, the organization may require leadership coaching or even rotating the manager out of the group. If financial stress seems to be an issue, the organization may choose to provide free financial-planning help or to reevaluate its compensation model.

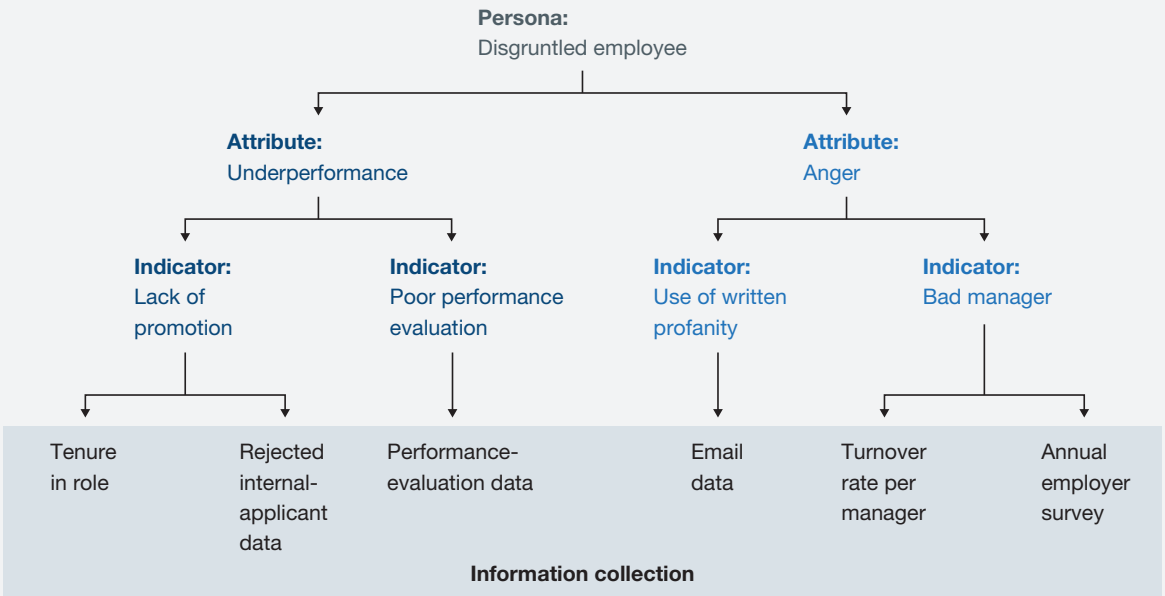
Prediction

Advanced organizations are taking one further step to identify groups or individuals early in the threat life cycle: predictive insider-persona analytics. The main personas that present a risk are well established and have been studied at length. High-performing organizations have identified the markers of these personas and actively monitor these markers for specific personas, rather than looking for divergence from normal. This analysis can identify a group or individual likely to represent a threat well before the event takes place; companies can then take steps to mitigate the threat. Exhibit 4 outlines the predictive analysis for identifying disgruntled employees, one of the established personas.

Exhibit 4

The markers of risky personas can give companies a head start on intervention.

Example risky persona



While powerful, these analytics require careful consideration about their use in the context of an organization's culture, its privacy norms, and the evolving standards of privacy in society at large. Failing to think it through often results in employee complaints about invasion of privacy.

A few words on privacy

Privacy is an inherently personal and intangible subject—its meaning and importance varies by geography, by industry, by company, and often by individual. Many individuals are fiercely protective of their privacy, even when at work and even in their use of corporate assets. This is never more true than when it comes to monitoring their use of communications systems such as email—even corporate email. As standards on individual and corporate privacy rights evolve (for example, through the European Union's General Data Protection Regulation), organizations need to design their insider-threat programs based on what will work within their own cultural and regulatory environments. In all cases, organizations need to tailor their insider-threat program by respecting what data may be gathered, how it may be collected and used lawfully, and how best to create awareness of the program, both generally and specifically, with potentially affected staff.

While each organization must make its own trade-offs between privacy and risk, we believe our approach will make such trade-offs easier to navigate than traditional programs. First, the microsegmentation approach does not require a baseline of individual activity (by which traditional programs judge "normalcy"), which some organizations could perceive as a privacy concern. Second, microsegmentation presents natural groups of employees for analysis, which improves the anonymity of the analysis. Microsegmented groups can be analyzed for potential threats with reasonable precision of results. Investigations of specific individuals can be conducted only when there is reasonable suspicion of a threat and must be done in line with applicable law.

■ ■ ■

Insider threat is one of the largest problems in cybersecurity, representing a massive share of attacks and financial damages. Monitoring technologies have their place in organizations' cyber-arsenal. But their effectiveness increases significantly when combined with more nuanced approaches, like microsegmentation, prediction, and direct cultural engagement. ■

Tucker Bailey is a partner in McKinsey's Washington, DC, office, where **Brian Kolo** is a digital expert and **David Ware** is an associate partner; **Karthik Rajagopalan** is a consultant in the Dallas office.

solarseven/Getty Images

To survive in the age of advanced cyberthreats, use 'active defense'

Brad Brown, Daniel Ennis, James Kaplan, and Jim Rosenthal

Anticipating attacks, responding to them in real time, setting traps to contain them, and protecting assets according to their value can help companies stop sophisticated cybercriminals.

For all the resources devoted to improving cybersecurity, threat levels continue to rise faster than defense capabilities. The WannaCry ransomware attack in May 2017 offers a case in point. Hackers helped themselves to tools stolen from intelligence agencies and others and created havoc around the world, forcing systems off-line at the Chernobyl nuclear power station, affecting several parts of Britain's National Health Service, and interrupting scores of computer systems.

The relatively unsophisticated nature of the attack limited the overall take. Yet, it reveals just how vulnerable organizations are to even rudimentary hacks done at scale. Imagine if the attackers actually had their acts together.

Some do. Several of the world's best-protected organizations have been attacked over the past few years, including a number of preeminent government agencies and technology companies. Hackers who may

are acquiring a deeper understanding of who they're targeting and how to get inside. Thanks to a proliferation of botnets[1] and the easy sharing of tools on the dark web, the expense of mounting cyberattacks is also plunging. Put it all together, and criminals, some of whom are state sponsored, have ready access to cash, technologies, and resources. Over the coming years, crimes in the cyberrealm are predicted to cost the global economy $445 billion annually.[2]

Perversely, the high-profile hacks may have done us a favor. For a long time, cybersecurity experts have proselytized about the evolving threat landscape. But like doctors who caution their patients to avoid sedentary lifestyles, the risks these experts describe seem important but distant. The WannaCry attack—its brazenness, the speed at which it scaled, and how effortlessly it derailed business as usual—took cyberthreat activity from a slow-moving abstraction and made it real.

Businesses must consider themselves warned. Rather than continue in a passive stance, organizations must adopt an "active defense" model: they should assume their firewalls will be penetrated. They should assume that encryption keys will be compromised, and that hackers will stay a step ahead of them in deploying malware in their infrastructure. Active defense requires organizations to anticipate attacks before they happen, detect alarms to contain attacks, and adopt a tiered approach to protecting critical assets.[3]

Understanding the challenges

The threat environment is constantly changing, but how businesses have responded to those threats has remained largely the same. That's not going to work anymore. Here's why:

- **A significant number of breaches are still caused by employee lapses:** Despite years of training employees on good data data-hygiene practices and continued investment in malware and virus detection, the majority of corporate data breaches are caused by simple human error: clicking on an innocent-seeming email, downloading a legitimate-looking attachment, or revealing identifying information to a seemingly trustworthy source.[4] Even if two-thirds of employees avoid these traps, about one-third will still fall prey (and about 15 percent of this group will go on to become repeat victims).[5] That means an automated barrage like a phishing campaign that blasts messages to thousands of employees is assured a reliable percentage of hits—and this is just by using basic techniques. More devious attackers can do extensive damage. All it takes is one or two employees to expose their credentials, and an attacker can decrypt them and make their way inside. Most organizations are not set up to thwart this behavior.

[1] A network of private computers infected with malicious software and controlled as a group without the owners' knowledge.

[2] *The global risks report 2016*, World Economic Forum, 2016, weforum.org.

[3] In this article, we define "active defense" as all actions aimed at anticipating, detecting, diverting, and isolating cyberattacks. We specifically exclude potentially illegal actions, such as hacking back.

[4] *2017 data breach investigations report*, Verizon, 2017, verizonenterprise.com.

[5] *Data breach digest: Perspective is reality*, Verizon, 2017, verizonenterprise.com.

- **Perimeter and encryption defenses aren't enough:** Large organizations have spent millions on firewalls and encryption. But the strongest perimeter defenses won't keep a company safe if intruders are already inside—and given the earlier point regarding internal threats, businesses must assume some are. Once there, intruders can stay for months, acquiring information and using that information to enter the systems of other companies. Criminals know that the best targets are well defended, so rather than trying to penetrate a heavily secured front door, they can go around to the back, to the company's supply chain. Data show that 63 percent of data breaches come from exploiting weak points in a company's customer and vendor network.[6] One major consumer-goods chain, for instance, suffered a major loss when attackers climbed in through the proverbial ducts—by hacking the company's air-conditioning vendor and working their way in. Companies need to do more than bar the gates; they need to monitor their entire network (and, in some cases, their network's network) to anticipate where attacks will come from. But most organizations don't have that capability.

- **IT organizations are overwhelmed and under-resourced:** Challenging the IT and security organization to keep up with the latest attacker moves is unfeasible. After all, hackers may only need a blunt tool and a few resources to exact a toll on one target. IT organizations meanwhile have to stay alert to thousands of external threats from a variety of sources. They need to be able to filter out the most pertinent intelligence, and have a sufficiently detailed understanding of where their most critical data assets are stored, and as well as what could put those assets at risk to secure them properly—all the while continuing to support the IT needs of the entire business. Trying to manage all these demands can lead to indecision and conflicting priorities. An effective response requires expertise and capabilities to detect, deter, and defend against these risks. But while some companies, such as large banks and telecommunications organizations, have been able to build credible defenses at that scale, the spending level required can stretch to the hundreds of millions. Few organizations can match that.

We are likely to have more malicious actors entering the field, more attacks that take advantage of basic loopholes, and more players capable of launching sustained, pernicious insider-based attacks. New strategies and partnerships are required.

Shifting to an active-defense model

Active defense allows organizations to engage and deflect attackers in real time by combining threat intelligence and analytics resources within the IT function. The approach draws upon lessons the military community learned in defending itself in fluid attack environments like Afghanistan and Iraq. To ferret out and respond to risks faster, commanders began positioning operators, planners, and intelligence analysts in the same tent where they could feed special operations teams with ongoing, real-time information. Integrated and more accurate intelligence made it easier for units to track chatter, identify targets, and increase the

[6] *2016 data breach investigations report*, Verizon, 2016, verizonenterprise.com.

number of missions they could conduct over the course of an evening.

In recent years, some large organizations have applied that thinking to bolster their own defenses. A major financial-services institution, for instance, greatly enhanced its cybersecurity capabilities by convening a team dedicated to providing active defense. The team established state-of-the-art threat-monitoring capabilities so it could continually scan the company's ecosystem—its own network as well as the broader supply chain—for unusual patterns and activity, sniff out potential threats, and thwart attacks, often within minutes of detection. It has impeded thousands of attacks as a result.

Few organizations have the budget to build dedicated centers of this scale. But there are other ways to access needed capabilities. By realigning the existing budget, engaging outside resources, and forging information-sharing partnerships, businesses can still mount a strong active defense. Success in doing so starts with understanding what's involved. Here are the central elements of an active-defense posture:

- **Anticipate attacks before they happen.** If the old model was all about defending the organization with layers of perimeter protection, the new model is far more proactive. Businesses need to scour the threat environment to find out if someone is talking about them or someone in their chain, pinpoint software and network vulnerabilities, and spot potential hacks before they occur. This is an intelligence-heavy, data-driven process—and it's critical. Bringing cybersecurity experts into the tent can help organizations gain the insights needed. Third parties that specialize in threat intelligence monitor a wide range of sources. That includes following threads and conversations in places like the dark web—websites that require special software to access and provide user anonymity—to gauge evolving threats to the company or its vendors.

- **Detect and respond to attacks in real time.** Early detection depends on an organization's ability to track network patterns and user behavior that deviate from the norm. The challenge is to figure out what normal is, given that businesses are constantly changing and human behavior is unpredictable. Intrusion detection and anomaly detection are two widely used approaches. Intrusion-detection systems (IDS) look for misuse based on known attack patterns. However, because these systems are trained to spot defined-threat signatures, they may miss emerging ones. They may also have a hard time distinguishing problematic activity from legitimate activity, such as innocuous internal communications that contain flagged language or Internet addresses (for example, malware warnings), ongoing network-security-vulnerability scans, or attacks against systems that have already been patched. Anomaly-detection models work the other way around. Instead of looking for known attack signatures, they look for behavior that deviates from typical network patterns, such as an unusual spike in volume. Companies with an active-defense posture use both IDS and anomaly-defense systems to provide more comprehensive threat detection.

- **Establish traps and alarms to contain attacks.** Decoy servers and systems, known as deceptions, are another tool that companies can deploy as part of their active defense. Deceptions lure attackers into a dummy environment where they can

be studied to gain additional intelligence. Entrance into the trap sets off an alarm, alerting the threat-operations center and triggering software agents and other deterrents to be placed in the network to close off access and prevent damage to the business. Some businesses also salt these environments with false information to confuse attackers. Once intruders breach a system, they usually return through the same gateway. Deceptions and other traps need to be convincing enough facsimiles to keep intruders inside long enough for the company to gather useful insights. Companies can then use those repeat visits to record the methods attackers are using to gain file, system, or server access and update their defenses accordingly.

- **Use ring architectures to protect critical assets.** Over the longer term, businesses need to construct layers of defense to keep the company's most critical assets deeply buried. Ring architectures, for instance, allow organizations to store data in different layers depending on the value and sensitivity of those assets. Each layer requires a specific key and authorization protocol to manage access. Penetration in any one layer will set off alarms. Active defense also requires an IT plan that organizes and prioritizes security-related technology spending. Otherwise, it can be tempting to try to protect everything and in the end create vulnerabilities when spending and systems prove too difficult to maintain.

Taken together, these measures can make a profound difference. At one financial institution, for instance, intelligence gathered on the dark web revealed that an overseas criminal syndicate was seeking to access the credentials of the bank's high-net-worth clients. Analysts informed their IT counterparts, all of whom worked together in an integrated active-defense unit. Engineers spotted command-and-control-type traffic emanating from PCs associated with high-income zip codes and found a pattern of anomalous log-ins for some of their high-net-worth accounts. The threat center immediately activated a forced password reset for affected customer accounts and placed temporary holds on all wire transfers in excess of $100,000. In addition, it reimaged affected desktops and issued a communication to select high-net-worth customers, encouraging them to implement two-factor authentication. This quick, coordinated response prevented sensitive information from being compromised.

Getting started

Knowing the core elements of an active-defense model can help organizations realign their cybersecurity spending, integrate analytics with intelligence-gathering processes, and provide tighter ongoing coordination. By pinpointing the critical holes in their defense structures, businesses can then determine where it makes sense to acquire needed skills, tools, and expertise and where they can partner with others to fill those voids.

As with any new approach, making the case for change is critical. Shifting to an active-defense posture requires leaders to recognize that cybersecurity requires top-level oversight and commitment, backed with the right budget, authority, and performance incentives to make it real. Organizations looking to implement an active-defense model must also recognize that changes in traditional working practices are required. Some of those changes may be uncomfortable. Given the sophisticated

nature of some attacks and the prospect of state-sponsored intervention, companies accustomed to keeping intrusion activity closely guarded may need to open up and work more collaboratively with peers within and across their industries to share notes, best practices, and resources. Such collaboration can take place within industry associations like the Financial Services Information Sharing and Analysis Center, which shares threat intelligence and incident information across nearly 7,000 financial-services institutions.

Changes across the broader security ecosystem are also necessary. The best partnerships will bring together a mix of government, technology, and business leaders to create an open and ongoing exchange of information. The vendor community also must adapt. They need to evolve their offerings from chasing down alerts to providing a range of sophisticated services similar to those that major banks and telecommunications companies have built for themselves.

Collectively, better intelligence, smarter analytics, and stronger collaboration can help organizations build the active-defense capabilities they need to respond more effectively to pervasive, advanced cyberthreats. ◆

Brad Brown is a director emeritus in McKinsey's Boston office and an ongoing adviser to BlueVoyant, **Daniel Ennis** is the head of threat intelligence and operations at BlueVoyant and the former director of the National Security Agency's Threat Operations Center, **James Kaplan** is a partner in McKinsey's New York office, and **Jim Rosenthal** is the cofounder and chief executive officer of BlueVoyant.

Designed by Global Editorial Services.

Making a secure transition to the public cloud

Arul Elumalai, James Kaplan, Mike Newborn, and Roger Roberts

As enterprises scale up their use of the public cloud, they must rethink how they protect data and applications—and put in place four critical practices.

After a long period of experimentation, leading enterprises are getting serious about adopting the public cloud at scale. Over the last several years, many companies have altered their IT strategies to shift an increasing share of their applications and data to public-cloud infrastructure and platforms.[1] However, using the public cloud disrupts traditional cybersecurity[2] models that many companies have built up over years. As a result, as companies make use of the public cloud, they need to evolve their cybersecurity practices dramatically in order to consume public-cloud services in a way that enables them both to protect critical data and to fully exploit the speed and agility that these services provide.

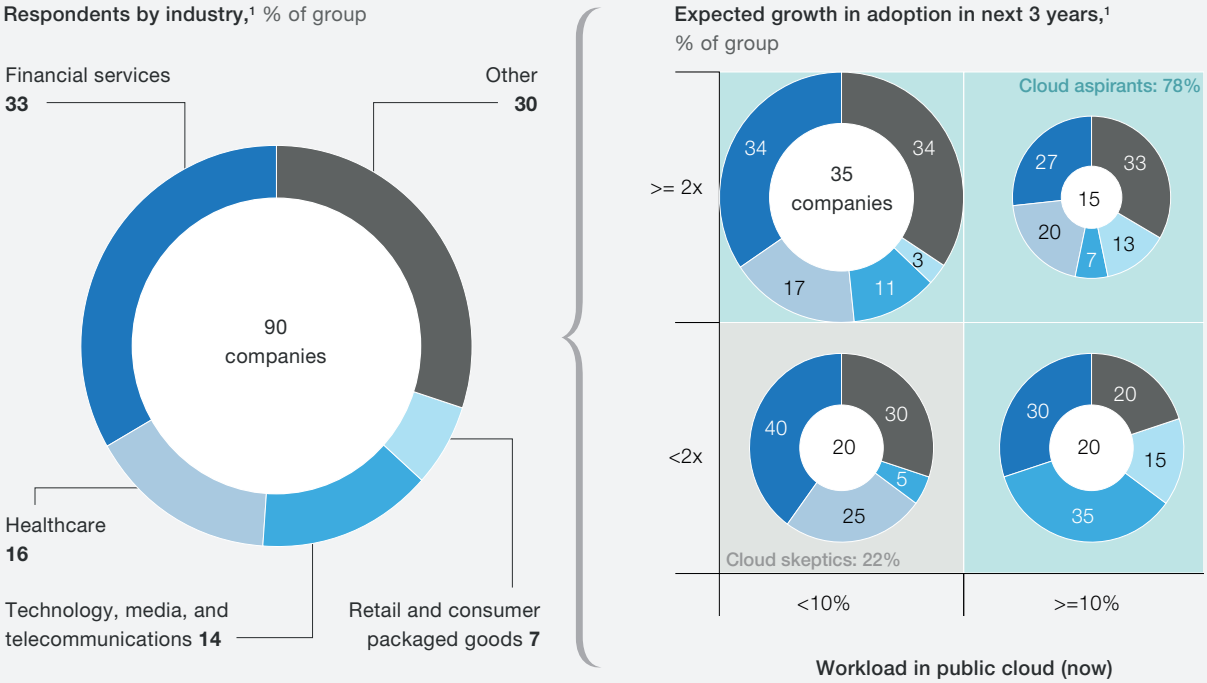
1 For more, see Nagendra Bommadevara, James Kaplan, and Irina Starikova, "Leaders and laggards in enterprise cloud infrastructure adoption," October 2016, McKinsey.com. Also see Arul Elumalai, Kara Sprague, Sid Tandon, and Lareina Yee, "Ten trends redefining enterprise IT infrastructure," November 2017, McKinsey.com, which primarily addresses the impact of infrastructure as a service (IaaS) and platform as a service (PaaS), rather than software as a service (SaaS).

2 By cybersecurity, this article means the full set of business and technology actions required to manage the risks associated with threats to the confidentiality, integrity, and availability of systems and information. Some organizations may refer to this function as information security or IT security.

While adoption of the public cloud has been limited to date, the outlook for the future is markedly different. Just 40 percent of the companies we studied have more than 10 percent of their workloads on public-cloud platforms; in contrast 80 percent plan to have more than 10 percent of their workloads in public-cloud platforms in three years, or plan to double their cloud penetration. We refer to these companies as "cloud aspirants" (Exhibit 1).[3] They have concluded that the public cloud offers more technical flexibility and simpler scaling for many workloads and implementation scenarios. In some cases, using the public cloud also reduces IT operating costs.

Exhibit 1

Cloud aspirants: Nearly 80 percent of companies plan to have 10 percent or more of their workloads in the public cloud or double their public-cloud use within three years.



[1]Percentages may not sum to 100% due to rounding.

McKinsey&Company | Source: McKinsey global cloud cybersecurity research, 2017

3 McKinsey conducted a global survey and in-depth discussions with IT security executives at 97 companies between August 2017 and November 2017, receiving 90 complete survey responses. Forty-one percent of these 97 companies generate annual revenues of less than $3 billion, 22 percent generate $4 billion to $10 billion, 20 percent generate $11 billion to $22 billion, and 17 percent generate more than $22 billion. Thirty-five percent of the 97 companies are in the financial-services industry; 15 percent are in the healthcare industry; 13 percent are in the technology, media, and telecommunications industry; 6 percent are in the retail or consumer packaged goods industries; and 30 percent are in other industries.

As a result, companies are both building new applications and analytics capabilities in the cloud and starting to migrate existing workloads and technology stacks onto public-cloud platforms.

Despite the benefits of public-cloud platforms, persistent concerns about cybersecurity for the public cloud have deterred companies from accelerating the migration of their workloads to the cloud. In our research on cloud adoption from 2016, executives cited security as one of the top barriers to cloud migration, along with the complexity of managing change and the difficulty of making a compelling business case for cloud adoption.[4]

Interestingly, our research with chief information security officers (CISOs) highlights that they have moved beyond the question, "Is the cloud secure?" In many cases they acknowledge that cloud-service providers' (CSPs) security resources dwarf their own, and are now asking how they can consume cloud services in a secure way, given that many of their existing security practices and architectures may be less effective in the cloud. Some on-premises controls (such as security logging) are unlikely to work for public-cloud platforms unless they are reconfigured. Adopting the public cloud can also magnify some types of risks. The speed and flexibility that cloud services provide to developers can also be used, without appropriate configuration governance, to create unprotected environments, as a number of companies have already found out to their embarrassment.

In short, companies need a proactive, systematic approach to adapting their cybersecurity capabilities for the public cloud. After years of working with large organizations on cloud cybersecurity programs and speaking with cybersecurity leaders, we believe the following four practices can help companies develop a consistent, effective approach to public-cloud cybersecurity:

- **Developing a cloud-centric cybersecurity model.** Companies need to make choices about how to manage their perimeter in the cloud and how much they will rearchitect applications in a way that aligns with their risk tolerance, existing application architecture, resources available, and overall cloud strategy.

- **Redesigning the full set of cybersecurity controls for the public cloud.** For each individual control, companies need to determine who should provide it and how rigorous they need to be.

- **Clarifying internal responsibilities for cybersecurity, compared to what providers will do.** Public cloud requires a shared security model, with providers and their customers each responsible for specific functions. Companies need to understand this split of responsibilities—it will look very different from a traditional outsourcing arrangement—and redesign internal processes accordingly.

4 For more, see Nagendra Bommadevara, James Kaplan, and Irina Starikova, "Leaders and laggards in enterprise cloud infrastructure adoption," October 2016, McKinsey.com.

- **Applying DevOps to cybersecurity.** If a developer can spin up a server in seconds, but has to wait two weeks for the security team to sign off on the configuration, that attenuates the value of the public cloud's agility. Companies need to make highly automated security services available to developers via APIs, just as they are doing for infrastructure services.

Developing a cloud-centric cybersecurity model

For a company that has only begun to use the public cloud, it can be tempting to build a public-cloud cybersecurity model using the controls it already has for on-premises systems. But this can lead to problems, because on-premises controls seldom work for public-cloud platforms without being reconfigured. And even after being reconfigured, these controls won't provide visibility and protection across all workloads and cloud platforms. Recognizing these limitations, cloud aspirants are experimenting with a range of security strategies and architectures, and a few archetypes are emerging.

The most effective approach is to reassess the company's cybersecurity model in terms of two considerations: how the network perimeter is defined and whether application architectures need to be altered for the public cloud. The definition of the perimeter determines the topology and the boundary for the cloud-cybersecurity model. And choices regarding application architecture can guide the incorporation of security controls within the applications. These two key choices also inform one another. A company might opt, for example, to make its applications highly secure by adding security features that minimize the exposure of sensitive data while the data are being processed and making no assumptions about the security controls that are applied to a given environment.

Choosing a model for perimeter security

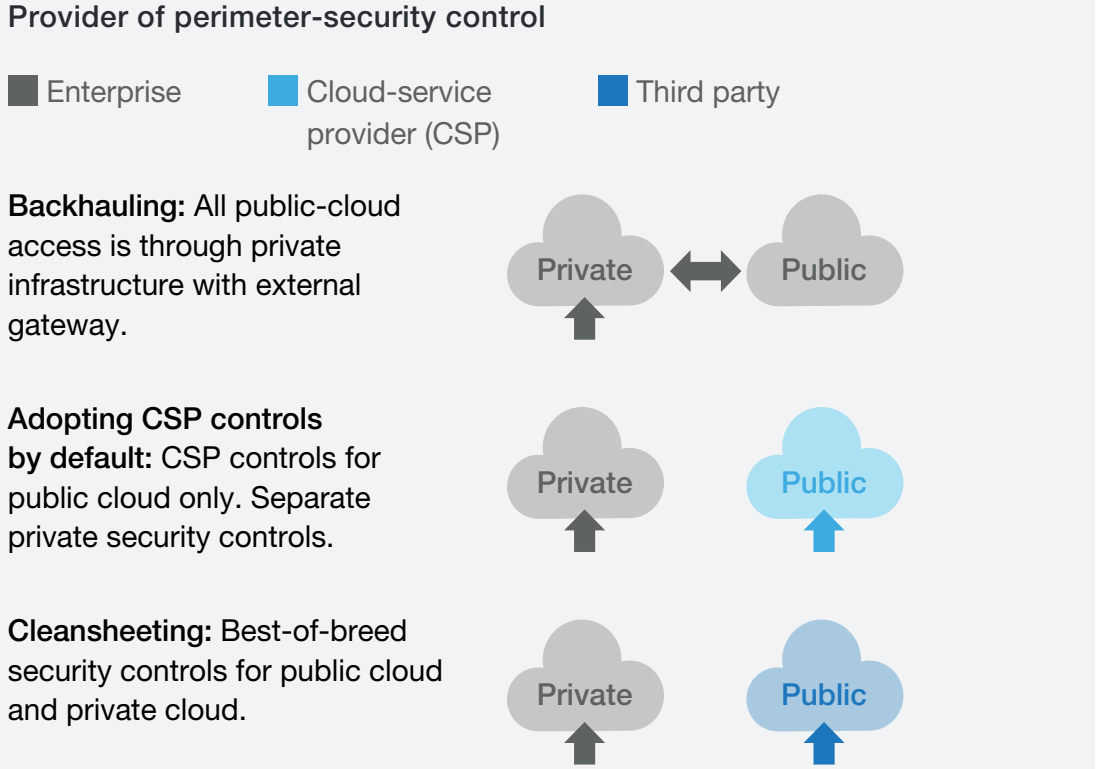
Among cloud aspirants, the following three models for perimeter design stand out (Exhibit 2):

- **Backhauling.** Backhauling, or routing traffic through on-premises networks, is how half of cloud aspirants manage perimeter security. This model appeals to companies that require internal access to the majority of their cloud workloads and wish to tailor their choices about migrating workloads to fit the architecture they have. Companies with limited cloud-security experience also benefit from backhauling because it allows them to continue using the on-premises security tools that they already know well. But backhauling might not remain popular for long: only 11 percent of cloud aspirants said they are likely to use this model three years from now.

- **Adopting CSP-provided controls by default.** This model is the choice of 36 percent of cloud-aspirant companies we studied. Using a CSP's security controls can cost less than either of the other perimeter models, but makes it more complex to secure a multicloud environment. For larger and more sophisticated organizations, using CSP-provided controls appears to be a temporary measure: 27 percent of cloud aspirants say they will use this model in three years (down from 36 percent today).

Exhibit 2

Architecture options: Three models for perimeter architecture stand out among cloud-aspirant companies.



- **Cleansheeting.** Cleansheeting involves designing a "virtual perimeter" and developing cloud-specific controls from solutions offered by various external providers. Used by around 15 percent of cloud-aspirant companies, this approach enables companies to apply the best perimeter-security solutions they can find, switching them in and out as needed. Since changing solutions creates technical demands, companies typically practice cleansheeting when they have enough in-house cybersecurity expertise to select vendors and integrate their solutions. Although those efforts can slow the migration of workloads into the cloud, cleansheeting appears to be on the rise, with 47 percent of cloud aspirants saying they will use cloud-specific controls in three years. Despite the high cost and complexity of cleansheeting, organizations choose this approach so they can support multicloud environments and replace point solutions more easily as their needs evolve.

Backhauling is now the most popular model for perimeter security among the cloud aspirants we researched. However, enterprises are moving toward a virtual-perimeter model, which they

develop through cleansheeting (see sidebar "A progressive outlook on perimeter-security design"). Cleansheeting is the least popular practice for managing perimeter security today, but more executives say they will use cleansheeting over the next three years than any other model.

A progressive outlook on perimeter-security design

A cybersecurity executive we interviewed at a large pharmaceutical company described a forward-looking view of perimeter-security design that is fairly typical of cloud aspirants. As the company increases its use of the public cloud, it is backhauling as a stepping stone but intends to move to a flexible architecture that leverages CSP controls where available and third-party controls for areas that CSPs do not support. Said the executive: "We lift and shift applications to the public cloud, and backhauling is an intermediate step. However, we see that CSPs and third-party tools provide more secure technology. We appreciate the shared responsibility with our CSP, but we require additional third-party tools to go beyond default CSP capabilities."

Deciding whether to rearchitect applications for the cloud

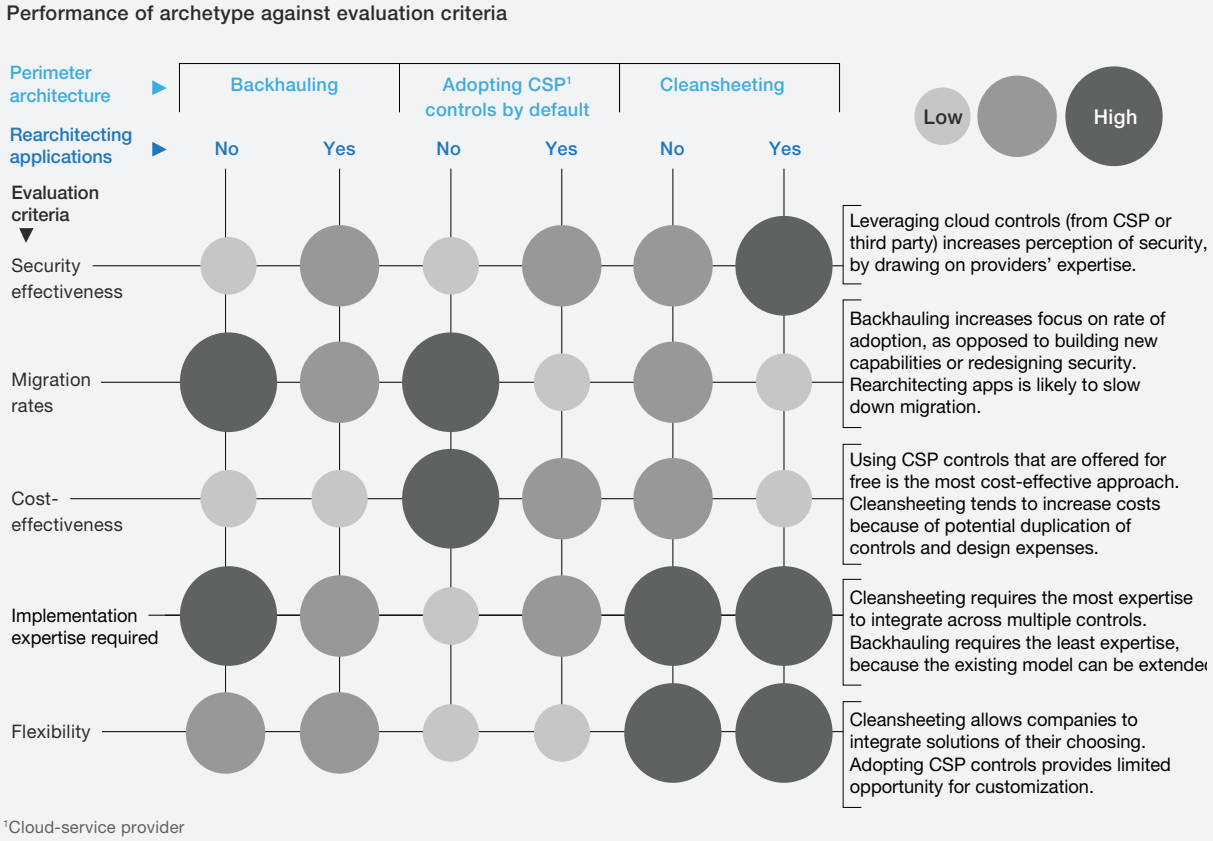
The second choice that defines a company's cloud-cybersecurity posture is whether to rearchitect applications in the public cloud, by rewriting code or altering application architectures (or both). Just 27 percent of the executives we interviewed said their companies do this. The benefits are compatibility with all CSPs (with container architectures, for example), stronger security (with changes like tamper detection using hash, memory deallocation, and encrypting data flows between calls), superior performance (for example, by allowing horizontal scaling in the public cloud), and lower operating costs (because app-level security protections reduce the need for a company to choose best-of-breed security solutions). However, rearchitecting applications for the cloud can slow a company's migration rate. Because of this, a large majority of enterprises in our survey, 78 percent, migrate applications without rearchitecting them for the public cloud.

The choice of perimeter-security design, along with the choice about whether to adapt applications to the public cloud, create six archetypes for cloud cybersecurity. In our experience, five primary criteria inform enterprises' decisions about their overall cloud-cybersecurity model: public-cloud security effectiveness, their desired cloud-migration rate, their willingness to pay additional security costs, their expertise implementing new security programs, and the flexibility they desire from their security architectures (Exhibit 3).

Rearchitecting applications for the public cloud improves security effectiveness but can slow down migration. Backhauling extends existing controls that companies are already familiar with to public-cloud implementations. Using default CSP controls is the simplest and most cost-effective approach. Cleansheeting controls calls for substantial security expertise but provides flexibility and support for multiple clouds. Organizations can use these criteria to choose the best methods. That said, companies need not apply the same archetype to their entire public-cloud profile. It's possible, even advantageous, to use different archetypes for applications

Exhibit 3

Assessing architectures: Cloud-cybersecurity models generally follow six archetypes, which are defined by their designs for perimeter and application architectures.



with different requirements: for example, backhauling with a single CSP for a core transaction system to enable faster migration and familiar controls, while using CSP-provided security controls for low-cost, accelerated deployment of new customer-facing applications.

Redesigning a full set of cybersecurity controls for the public cloud

Once enterprises have decided on a security archetype (or a mix of archetypes, with each archetype matched to a group of workloads with similar security requirements), they can design and implement cybersecurity controls. Understandably, companies are experimenting with a variety of designs for controls, and, given the pace of progress, cybersecurity executives anticipate considerable change to these controls over the next three years. Cybersecurity controls can be categorized into eight areas, which organizations need to think about in combination. The eight control areas are listed below, along with observations from our research.

- **Identity and access management.** IAM solutions for cloud-based applications and data are gradually shifting into the cloud (see sidebar "Moving into the next generation of IAM"). Sixty percent of interviewees reported that they employ on-premises IAM solutions today, but only half as many expect to be using on-premises IAM solutions in three years. By that time, 60 percent of interviewees anticipate that their enterprises will rely on a third-party IAM service that supports multiple public-cloud environments and unifies IAM controls across on-premises and public-cloud resources.

Moving into the next generation of IAM

A Fortune 500 healthcare company we spoke with has redesigned its IAM controls for the public cloud by using the automation and analytics features of its public-cloud platforms. Specifically, it has created automated authorization schemes, based on CSP-provided identity services, to eliminate human factors from provisioning and deprovisioning. The company has also developed a risk model that predicts each user's behavior based on monitoring data from the CSP and compares that behavior with what is observed to determine whether the user should gain access. As a company executive told us in an interview, "Passwords are obsolete. Even MFA [multifactor authentication] is a step backward. Behavioral authentication is the next generation. With the training data from CSPs, we are taking a risk-based approach and building continuous authentication."

- **Data.** Encryption of cloud data in motion and at rest should soon be standard practice. Eighty-four percent of cloud aspirants expect that within three years they will encrypt the data they store in the cloud. Over time CISOs would like to have more practical mechanisms for encrypting data in memory as well. However, interviewees have different approaches to managing encryption keys for cloud workloads: 33 percent prefer to have CSPs manage keys, 28 percent keep them on-premises, and 11 percent prefer to have third parties manage keys (see sidebar "Why companies manage keys differently").[5]

- **Perimeter.** Enterprises are moving toward a "virtual perimeter" model. Around 40 percent of enterprises are routing traffic via on-premises data centers today, using on-premises security controls with some form of virtual private network or direct connectivity between on-premises and public-cloud workloads as the only way to access applications or data on public-cloud platforms. But 49 percent of interviewees say they expect their companies to use third-party perimeter controls over the next three years. The transition to these perimeter-control models will typically involve developing cleansheet designs that draw on a combination of services, such as security web gateway, web application firewall, and network monitoring from different third parties that support multiple clouds.

5 Twenty-eight percent of interviewees declined to discuss key management.

Why companies manage keys differently

Companies determine their key-management practices based on various factors, such as regulatory compliance and security benefits. Two examples from our interviews show why approaches differ. An IT services company has opted to generate and manage keys using a localized private system so it can use key ownership as a mechanism to stay in the loop if CSPs are forced to hand over data. The executive explained, "We are holding the key ourselves because it gives us and our compliance people confidence that only local employees have access to keys, and data cannot be accessed without our knowledge. That control gives peace of mind."

A global pharmaceuticals and medical-products company takes a different approach, drawing on its CSP's key-management capabilities to improve cost-effectiveness and performance. The executive we interviewed said, "Our public-cloud application functionality is improved when keys are stored in the public cloud. Public-cloud applications need the keys to decrypt public-cloud data, and so we see less security benefit to storing keys privately. We get better performance having keys closer to apps, and encryption and decryption cost less with publicly stored keys."

- **Applications.** Most interviewees (84 percent) define security-configuration standards for cloud-based applications and depend on CSPs to implement them. But 85 percent said their companies are likely to drive more developer governance as workloads move to the cloud. This is likely to be soft governance, with only 20 percent of enterprises using application security tools or templates.

- **Operations monitoring.** Sixty-five percent of enterprises rely on their current security information and event management (SIEM) tools for monitoring cloud apps. This allows them to maintain a single view of their on-premises and cloud workloads. Another 30 percent use other native monitoring tools provided by their CSPs or request logs from CSPs to generate insights using proprietary data analytics solutions. Since CSPs can provide a wealth of monitoring data, it is critical for organizations to collaborate with them on selecting solutions that provide a unified view of on-premises and public-cloud workloads.

- **Server-side end points.** Interviewees are mostly confident in the server-side security offered by CSPs: 51 percent indicate that they have a "high" level of comfort with CSP-provided security for server-side end points. Many companies, especially ones that have less sophisticated security programs, believe that CSPs have insight into and control over their server fleet than they could ever achieve internally.

- **User end points.** Moving workloads onto the cloud ordinarily necessitates changes to controls for user devices, mainly for data-loss prevention and for protections against viruses and malware. Seventy percent of interviewees said using a public-cloud infrastructure requires their enterprises to change users' end-point controls.

- **Regulatory governance.** Most cybersecurity programs are governed by regulations on data protection (such as the European Union's General Data Protection Regulation), data location and sovereignty, and personally identifiable information. Financial institutions and healthcare organizations are also subject to industry-specific regulations. More than 50 percent of the executives we spoke with indicated that they would like their CSPs to be jointly responsible for compliance with regulatory mandates.

In selecting controls, organizations should consider all eight areas in conjunction and build a comprehensive cybersecurity architecture rather than following a piecemeal approach. Companies can start to design controls based on threat scenarios and levels of security required, and then apply an appropriate security model archetype (such as backhauling or cleansheeting) to determine the best security controls and their scope. Companies can also work with CSPs to determine which of their controls to use and which ones to procure from third parties. Finally, companies should shortlist and prioritize controls that can be standardized and automated, and implement them in agile iterations.

Clarifying internal responsibilities for cybersecurity, compared to what providers will do

When enterprises migrate applications and data to the public cloud, they must depend on CSPs and third-party providers for some security controls—but they should not depend on them to provide all of the necessary controls. Unless companies and CSPs clearly divide all the responsibilities for cybersecurity in public-cloud environments, some responsibilities could fall through the cracks. This makes it essential for companies to develop and maintain a clear understanding of what controls their CSPs provide, by having CSPs provide a comprehensive view of their security operating models, along with timely updates as those models change. (CSPs organize their cybersecurity responsibility models differently, and take various approaches to sharing them, so each situation needs to be handled carefully.) That way, companies can design and configure controls that work well in multiple cloud environments and integrate well with various tools, processing models, and operating models.

Based on our experience and research, we find that enterprises can benefit greatly from collaborating with CSPs across the full cybersecurity life cycle, from design to implementation and ongoing operations. However, four main areas emerged as top priorities for collaboration between companies and their CSPs.

- **Transparency on controls and procedures.** Companies should get CSPs to provide full visibility into their security controls and procedures, as well as any exposure incidents. Companies will also need to understand each CSP's ability to conduct security audits and penetration testing.

- **Regulatory compliance support.** Companies should ask their CSPs to provide detailed descriptions of the assurances they provide with regard to regulatory

compliance and inquire about how they stay abreast of regulatory changes for each industry, and update their compliance mechanisms accordingly.

- **Integrated operations monitoring and response.** Companies will likely have to collaborate with CSPs when it comes to integrating their SIEM tools in a way that supports centralized security administration. Companies should request that their CSPs provide them with comprehensive reporting, insights, and threat alerts on an ongoing basis. They can pass on insights to help CSPs develop new capabilities for all their tenants. They must also ensure that CSPs make their logs readily available in a format that companies can process using on-premises analytics tools.

- **Multicloud IAM capabilities.** Companies should insist that CSPs provide native multifactor authentication. Those that use identity as a service (IDaaS) or on-premises IAM solutions will need to work with CSPs to integrate them properly, so they have adequate support for multiple public-cloud environments. Companies should also have their CSPs share their IAM road maps so they can plan to take advantage of features such as behavioral authentication and role-based access.

Applying DevOps to cybersecurity

DevOps is an increasingly prevalent approach to integrating development and IT operations that supports continuous delivery of new software features, in part by providing developers with APIs to access operational services. Secure DevOps (sometimes called "SecDevOps" or "continuous security") integrates security reviews, implementation of security controls, and deployment of security technology with the DevOps approach that many teams have already adopted for movement into the cloud. Integration is achieved by automating security services across the full development cycle and making them available via APIs (Exhibit 4).

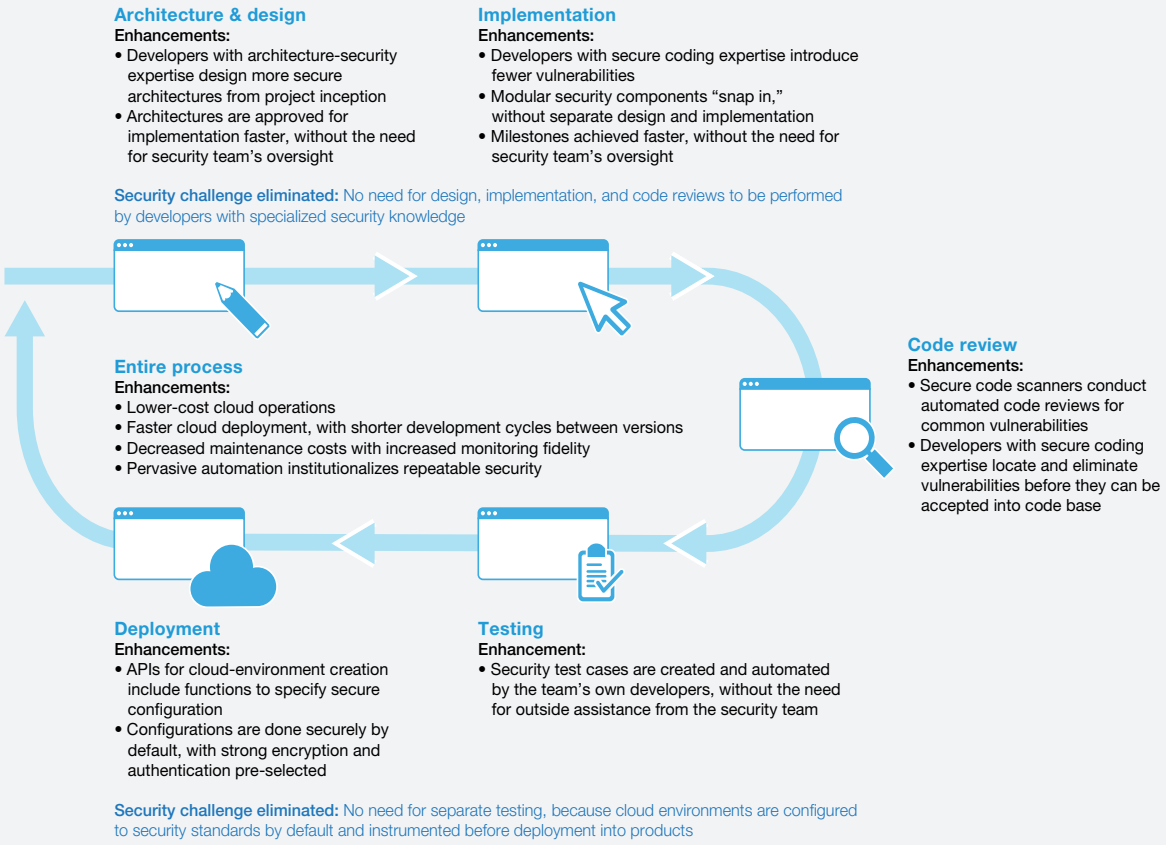
Secure DevOps enhances all categories of security controls for the cloud, by shortening deployment timelines and reducing risk. For example, some companies have policies requiring the classification of all data. But when data can only be classified manually, the necessary effort adds time to deployment schedules. With secure DevOps, mandatory data classification becomes much more practical, because all data receives a default classification based on preset rules. As a result of that improvement, and others provided by secure DevOps, organizations can decrease their risk of breaches in public-cloud environments, while reducing or removing delays that would have been caused by manually classifying data before they are stored.

Adopting secure DevOps methods requires companies to foster a culture in which security is a key element of every software project and a feature of every developer's work. Many developers will need additional security training to provide effective support during and after the public-cloud migration. Training also helps developers understand the security features of the tools they are using, so they can make better use of existing security APIs and orchestration technologies and build new ones.

Exhibit 4

Traditional security models make it harder to take advantage of cloud's speed and agility.

Cloud-deployment process with secure DevOps



Companies should streamline their security-governance procedures to make sure they do not cause delays for developers. As companies automate their security controls, they can make controls fully visible to developers. That way, developers can independently check whether controls are working properly in the background, rather than delaying work to consult with security specialists. Automating the processes of auditing security mechanisms is also helpful. For example, companies can require that code is automatically scanned every night for compliance with policy, and integrate build-time checks of security components into applications.

To implement secure DevOps, companies also change their IT operating model so security implementation becomes a part of the cloud development and deployment process. In such an operating model, a properly trained development team is the security team; no outside

engagement is needed to obtain the right security expertise. Embedding security expertise in the development team eliminates delays in the cloud-deployment process and permits the development team to iterate much faster than traditional security models allow.

How companies can begin strengthening cybersecurity in the cloud

The four practices we have described for structuring a public-cloud cybersecurity program should enable companies to take greater advantage of public-cloud platforms. Nevertheless, setting up the program can be a complicated task, because companies have multiple cloud workloads, CSPs, on-premises and private-cloud capabilities, locations, regulatory mandates, and security requirements to account for. This ten-step workplan will help companies stay coordinated as they move through design, development, and implementation of their public-cloud cybersecurity programs.

1. **Decide which workloads to move to the public cloud.** For example, many organizations choose to move customer-facing applications or analytical workloads to the public cloud initially, while keeping core transaction systems on-premises. Then they can determine security requirements for workloads that are migrated.

2. **Identify at least one CSP that is capable of meeting security requirements for the workloads.** Companies may choose multiple providers for different workloads, but these selections should be consistent with the objectives of the company's overall cloud strategy.

3. **Assign a security archetype to each workload based on the ease of migration, security posture, cost considerations, and internal expertise.** For example, companies can rearchitect applications and use default CSP controls for customer-facing workloads, and lift and shift internal core transaction apps without rearchitecting, while backhauling for data access.

4. **For each workload, determine the level of security to enforce for each of the eight controls.** For example, companies should determine whether IAM needs only single-factor authentication, requires multifactor authentication, or calls for a more advanced approach such as behavioral authentication.

5. **Decide which solutions to use for each workload's eight controls.** Given the capabilities of the CSP (or CSPs) identified for each workload, the company can determine whether to use existing on-premises security solutions, CSP-provided solutions, or third-party solutions.

6. **Implement the necessary controls and to integrate them with other existing solutions.** This requires the company to gain a full understanding of CSP's security capabilities and security enforcement processes. CSPs need to be transparent about these aspects of their offerings.

7. **Develop a view on whether each control can be standardized and automated.** This involves analyzing the full set of controls and making decisions on which controls to standardize across the organization and which ones to automate for implementation.

8. **Prioritize the first set of controls to implement.** Controls can be prioritized according to which applications a company migrates and which security model it chooses to apply.

9. **Implement the controls and governance model.** For controls that can be standardized but not automated, companies can develop checklists and train developers on how to follow them. For controls that can be standardized and automated, companies can create automated routines to implement the controls and to enforce standardization, using a secure DevOps approach.

10. **Use the experience gained during the first wave of implementation to pick the next group of controls to implement.** Drawing on this experience will also help to improve the implementation process for subsequent sets of controls.

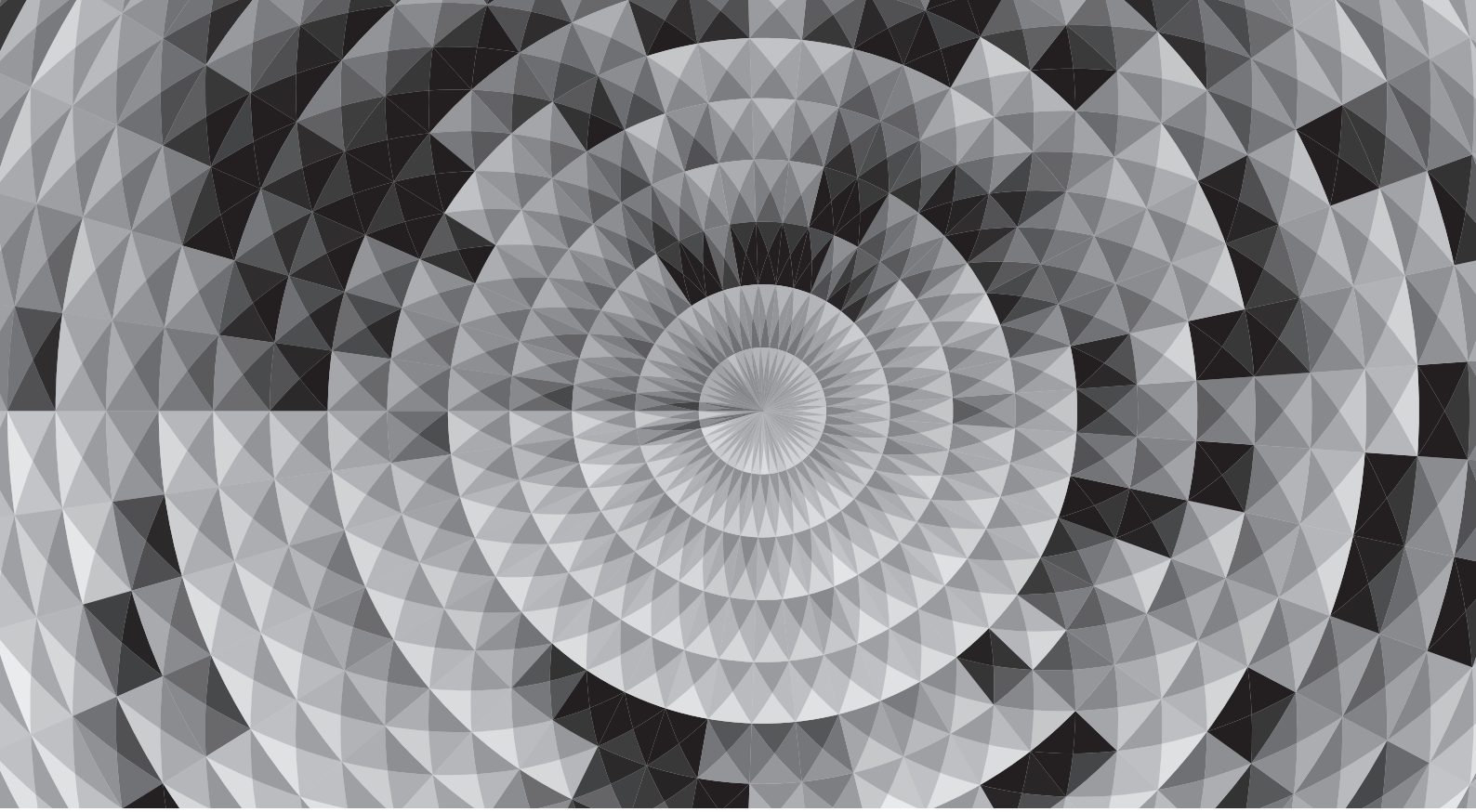
▼ ▼ ▼

Companies are steadily moving more of their applications from on-premises data centers and private-cloud platforms onto public-cloud platforms, which provide superior levels of cost-effectiveness, flexibility, and speed in many situations. But public-cloud migrations will only succeed if companies maintain the security of their applications and data—a task that some have struggled with.

Our experience and research suggest that public-cloud cybersecurity is achievable with the right approach. By developing cloud-centric cybersecurity models, designing strong controls in eight security areas, clarifying responsibilities with CSPs, and using secure DevOps, companies can shift workloads into the public cloud with greater certainty that their most critical information assets will be protected.

Arul Elumalai and **Roger Roberts** are partners in McKinsey's Silicon Valley office, **James Kaplan** is a partner in the New York office, and **Mike Newborn** is a specialist in the Washington, DC, office.

The authors wish to thank Yash Agrawal, Rich Cracknell, Srikanth Dola, Lisa Donchak, Dan Guo, James Manyika, Brent Smolinski, and Adam Tyra for their contributions to this article. They also wish to express their thanks to the security team at Google Cloud for their input and insights and to the more than 100 security executives who shared their practices and plans, without which this article would not have been possible.



Cyberrisk measurement and the holistic cybersecurity approach

Comprehensive dashboards can accurately identify, size, and prioritize cyberthreats for treatment. Here is how to build them.

Jim Boehm, Peter Merrath, Thomas Poppensieker, Rolf Riemenschnitter, and Tobias Stähle

Damaging cyberattacks and streams of suspicious digital communications have made cybersecurity a top concern of the world's business leaders. So say the overwhelming majority of responding board members in a recent McKinsey survey. Their answers are further evidence that cyberrisk is now as important a priority for the leaders of public and private institutions as financial and legal risks.[1] Facing the rising threat level and the magnitude of the potential impact, executives are insisting on full transparency around cyberrisk and ways to manage it actively to protect their organizations.

This evolved attitude was also expressed in the responses to our recent article, "A new posture for cyberrisk in a networked world."[2] Most of our readers agreed on the urgency of the issue, and many volunteered stories of rising cyberthreats, new types of attacks, and the increasing complexity of managing digital risk in large corporations. A board member for a multinational company in advanced industries admitted, "So far, we have not taken a big hit, but I can't help feeling that we have been lucky. We really need to ramp up our defenses." Another executive said: "Digital resilience is one of our top priorities. But we haven't agreed on what to do to achieve it." These concerns are widely held, as executives in all sectors and regions seek guidance on the path to a new cybersecure posture.

Board members and their discontents

Survey responses revealed that companies are rolling out a wide range of activities to counter cyberrisk. They are investing in capability building, new roles, external advisers, and control systems. What they lack, however, is an effective, integrated approach to cyberrisk management and reporting. As top executives attest, these tools are urgently needed to support fast, fact-based cyberrisk management. There are three specific gaps:

- *Lack of structure.* Boards and committees are swamped with reports, including dozens of key performance indicators and key risk indicators (KRIs). The reports are often poorly structured, however, with inconsistent and usually too-high levels of detail. Research indicates that most IT and security executives use manually compiled spreadsheets to report cyberrisk data to their boards; unsurprisingly, many board members are dissatisfied with the reports they receive.[3]

- *Lack of clarity.* Most reporting fails to convey the implications of risk levels for business processes. Board members find these reports off-putting—poorly written and overloaded with acronyms and technical shorthand. They consequently struggle to get a sense of the overall risk status of the organization. At a recent cybersecurity event, a top executive said: "I wish I had a handheld translator, the kind they use in *Star Trek*, to translate what CIOs [chief information officers] and CISOs [chief information security officers] tell me into understandable English." In a recent survey, 54 percent of executives said that risk reports are too technical.

- *Lack of consistent real-time data.* Different groups in the same organization often use different, potentially conflicting information to describe or evaluate the same aspects of cyberrisk. An executive remarked that one day he received a report listing an asset as sufficiently protected, but the next day a different department reported the same asset as under threat. "Which should I believe?" he asked, "and what should I do?" To compound the problem of conflicting reporting, underlying data are often too dated to be of use in managing quickly evolving cyberthreats.

A holistic strategy

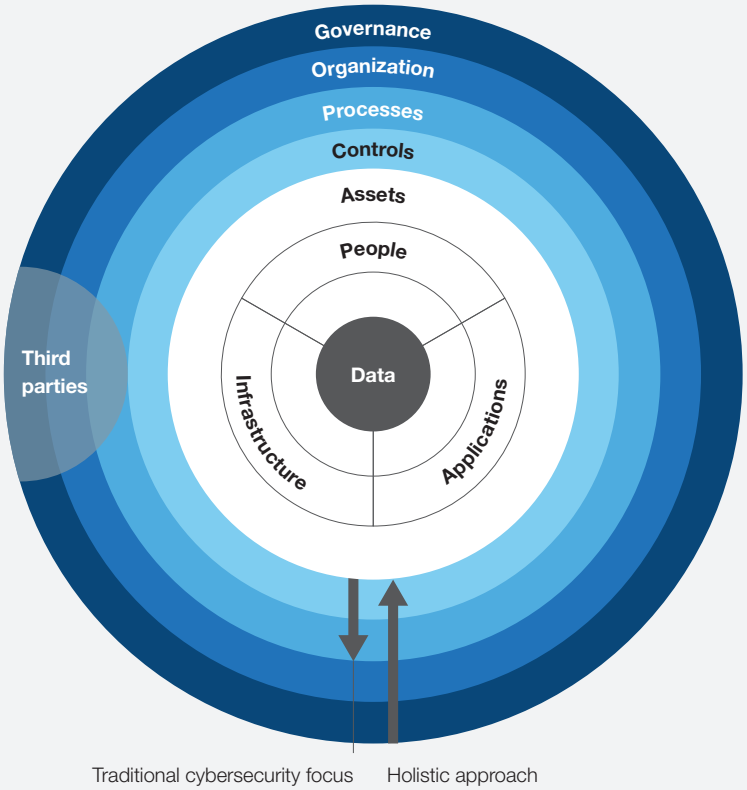
A holistic approach to cybersecurity can address these failings and their implications for governance, organizational structures, and processes (Exhibit 1).

A holistic approach proceeds from an accurate overview of the risk landscape—a governing principle that first of all requires accurate risk reporting. The goal is to empower organizations to focus their defenses on the most likely and most threatening cyberrisk scenarios, achieving a balance between effective resilience and efficient operations. Tight controls are applied only to the most crucial assets. The holistic approach lays out a path to root-cause mitigation in four phases (Exhibit 2).

1. Identify risks and risk appetite. Working with top management and drawing on internal and external resources, the chief risk and information security officers create a list of critical assets, known risks, and potential new risks. In conjunction with this effort, top management and the board establish the organization's appetite for the risks that have

Exhibit 1 **The holistic approach to managing cyberrisk proceeds from a top-management overview of the enterprise and its multilayered risk landscape.**

Holistic cyberrisk management approach



Assets. Clearly defined critical assets

Controls. Differentiated controls to balance security with agility

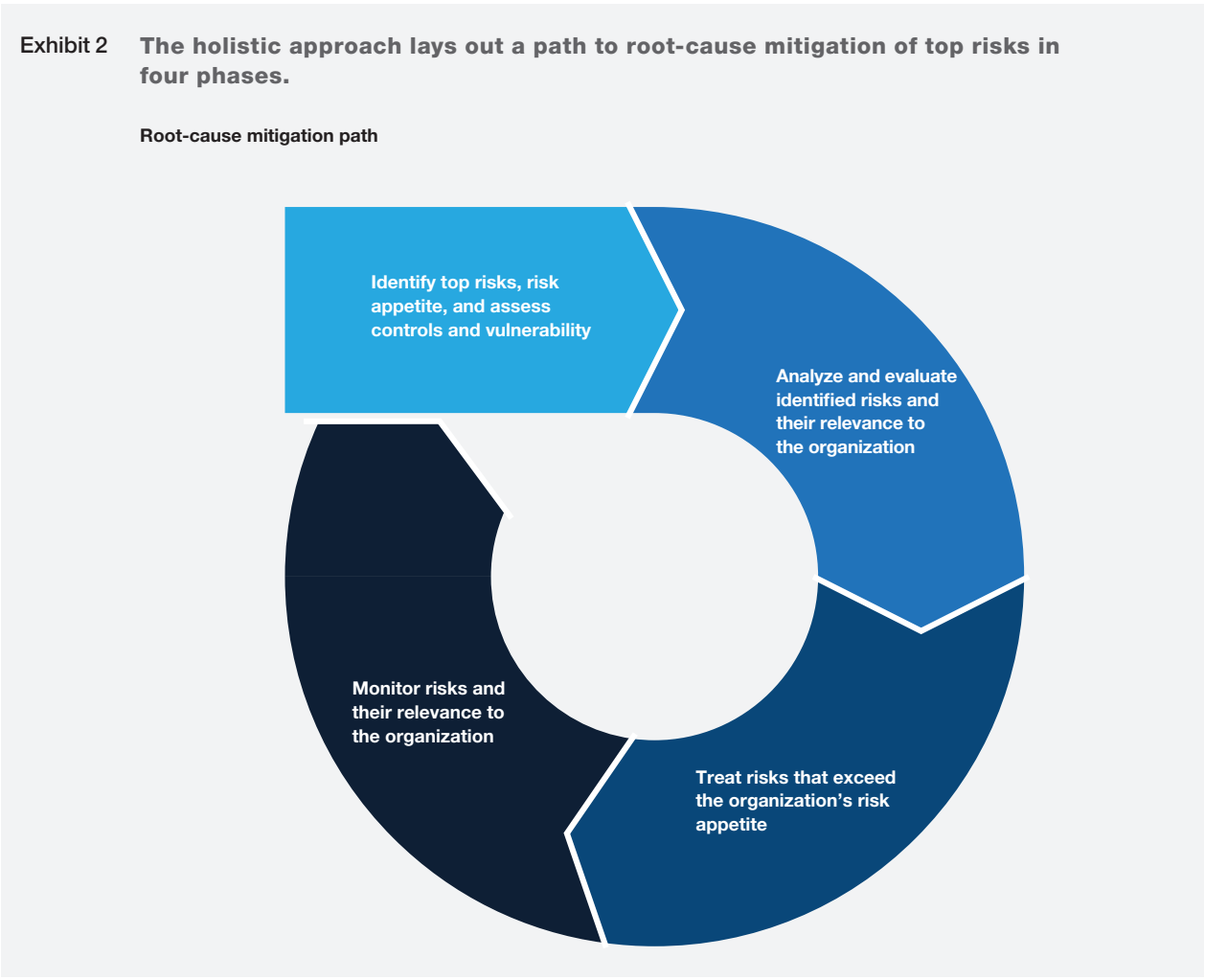
Processes. State-of-the-art cybersecurity processes focused on effective responses

Organization. Right skills, efficient decision making, and effective enterprise-wide cooperation

Governance. Investments in operational resilience prioritized based on deep transparency into cyberrisks

Third parties. Coverage of the whole value chain, including third-party services

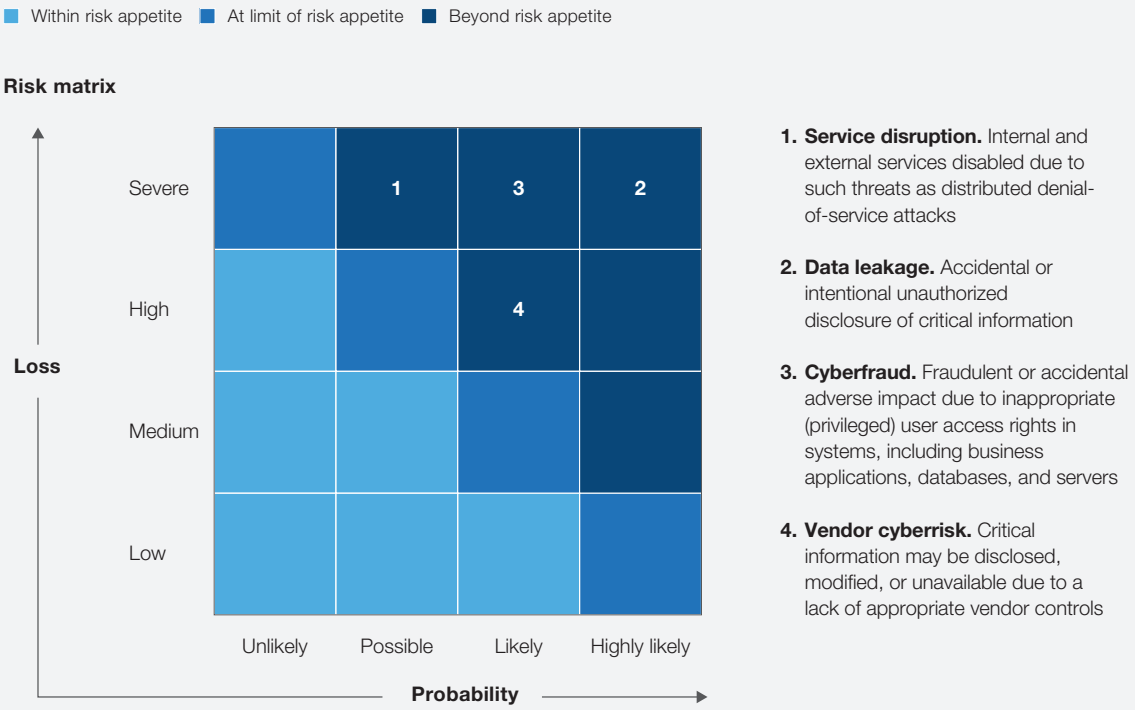
Exhibit 2 **The holistic approach lays out a path to root-cause mitigation of top risks in four phases.**



been identified. An assessment is also made in this phase of existing controls and vulnerabilities. The risk appetite will vary according to the value to the organization of the threatened asset. A leaked internal newsletter, for example, is less likely to pose a serious threat than the exposure of customer credit-card data. The chief measure of cyber-resilience is the security of the organization's most valuable assets. The prioritization of identified risks is therefore a task of utmost importance, which is why top management must be involved.

2. Analysis and evaluation. Once the risks and threats have been identified, internal and external experts need to evaluate each risk in terms of likelihood of occurrence and potential impact, including, as applicable, regulatory, reputational, operational, and financial impact (Exhibit 3).

Exhibit 3 **Each identified risk is evaluated in terms of potential loss and likelihood of occurrence; a matrix displays resulting prioritized threats.**



Based on this assessment, the risk function or risk owners can prioritize areas for mitigation, starting with the most likely scenarios that will have the biggest negative impact (top right-hand area of the map, marked in dark blue in the exhibit).

3. Treatment. Once risks have been identified and prioritized according to likelihood and impact, the risk owners and the risk function should work together to create an overview of all initiatives undertaken to mitigate the top cyberrisks. The initiatives should be evaluated on their effectiveness in reducing the probability of a risk event occurring and the impact of an event that does occur. Taking into account the effects of the mitigating initiatives, risk experts determine whether the residual risk for each top risk now falls within the parameters of the organization's risk appetite. Should the residual risk level exceed these considered limits, additional mitigation initiatives can then be developed and deployed.

4. Monitoring. Among the most important instruments for fostering discipline throughout the organization are scheduled status updates to senior management on top cyberrisks, treatment strategy, and remediation. Over time, the indicators and criteria used in such updates will become the basic

language in the organization's conversations about risk. The updates should be well written, concise, and free of mysterious acronyms and specialized jargon. For the board, a single well-composed page of text should suffice.

Focused risk mitigation

Cyberrisk managers in large organizations are often swamped with information on threats that exceeds their capacity to respond appropriately. Fortunately, not all the alerts are warranted. For example, most organizations are little threatened by a so-called advanced persistent attack. The low probability should become visible in risk analysis, freeing organizations from devoting resources to the highly sophisticated defenses needed to protect against such attacks. Instead, they will be able to focus on creating countermeasures for common kinds of attacks—such as, for example, a distributed denial of service induced by malware or malicious overload. The optimal strategy will include controls to prevent collateral damage and investment in state-of-the-art safeguards to ensure business continuity in case of an attack. The goal for cyberrisk managers is an efficient, adaptive, and sustainable regime. To attain it, fact-based prioritization is of central importance. Accurate risk-sizing is dependent on a few basic inputs:

- a business perspective of the institution's key assets and the top risks that could affect them
- realistic updated assessments of relevant threats and threat actors, formulated in detail as appropriate
- a consistent and accurate definition of risk appetite for the organization as a whole, prioritized and revised as appropriate

With an approach based on these factors, executives can give clear guidance on cyberrisk to all levels of the organization. The overall strategy includes a well-prioritized risk profile, efficiently focused on reducing disruption or slowdowns. For example, employee-related controls would be tailored by role—controls to avoid data leakage would apply only to those with access to key assets, rather than to all.

Resolving the data dilemma

Most companies are wary of their operational data sources and often assign risk, compliance, or control teams to build additional data sources or clean existing operational data. This response to one problem often creates a number of others. It expends substantial resources and leads to different, inconsistent reports as well as a growing reservoir of "stale" data from past risk assessment efforts. Yet when specific questions arise, needed data cannot be located and appropriate action cannot be taken. Risk teams must scramble to dig up the data manually, double-check facts, and conduct interviews to discover what is really going on. As the head of cyberrisk for an insurance company remarked, "We spend half our time looking for data and aggregating information from different sources."

Integrated data architecture and a consolidated data lake

Consistent cyberrisk reporting is an essential part of the response to the everyday demands of cybersecurity. To achieve a state of readiness against cyberattacks, companies need to build an integrated data architecture, including a consolidated data lake. To avoid conflicting, inconsistent information, the data lake should be filled directly from an organization's "golden sources" of data on vendors, people, applications, infrastructure, and databases.

All data corrections need to be made to these original sources in a consistent manner, covering all relevant assets.

By enforcing data consistency, companies will help foster cyberrisk consciousness. Those charged with gathering, cleaning, and processing data are actually contributing to a cybersecurity transformation. One financial-services executive explained:

> *Initially, we created a data lake with an off-the-shelf interface, assuming the organization would figure out what to use it for. We failed miserably. Very few people used it at all, and everybody else tried to prove the output wrong. Now we work with our most experienced people to outline the benefits and build our data regime one use case at a time. To want to work with data, people need to see how data can make their life easier and their business more resilient.*

To ensure continuous, consistent, accurate, and timely cyberrisk reporting, the level of automation in data gathering and processing should be increased gradually, step by step. Areas such as asset identification and compliance monitoring can be tackled in sequence. Automation can help improve data quality: advanced analytics and machine learning can find empty cells, missing pieces, and suspicious patterns in the underlying data. Automated pattern-hunting is especially effective in verifying the quality of external data sources, from partners along the value chain, for example, or from specialized providers of risk-related data.

Holistic cyberrisk reporting

When risk managers set out to implement holistic cyberrisk reporting, they are often surprised by how little they know about their organization. Many organizations have no reliable inventory of databases, applications, devices, people, buildings, third parties, and access rights. At many companies, vulnerable critical assets are managed locally, invisible to cyberrisk managers at company headquarters. At one financial-services firm, as many as 50 copies of the same data were being held, including for highly sensitive customer information. While some of the copies were well protected with state-of-the-art controls, others floated around and were frequently transferred using unencrypted email and even employees' personal thumb drives. Although strict controls had been defined, business units granted exceptions from the rules in a parallel process that was not aligned with the overall digital risk-management regime. This double standard was a major source of uncontrolled risk for the whole organization.

At a large manufacturer, critical industrial production environments were connected to the internet through unregistered interfaces. These had been installed by third-party providers for remote maintenance. In effect, they exposed the entire production environment to cyberattacks. The scope of such attacks has lately extended beyond IT systems to operational technology (OT). OT systems include industrial control systems and Internet of Things devices, from refrigeration units to pacemakers. Such equipment is often more vulnerable than IT systems because OT security standards are less developed. The lesson from the experience of OT vulnerability is that all critical assets must be part of the cybersecurity strategy. The strategy must cover the entire value chain, minimizing the blind spots of an organization's risk assessment.

Visualizing threat control: The cyberrisk dashboard

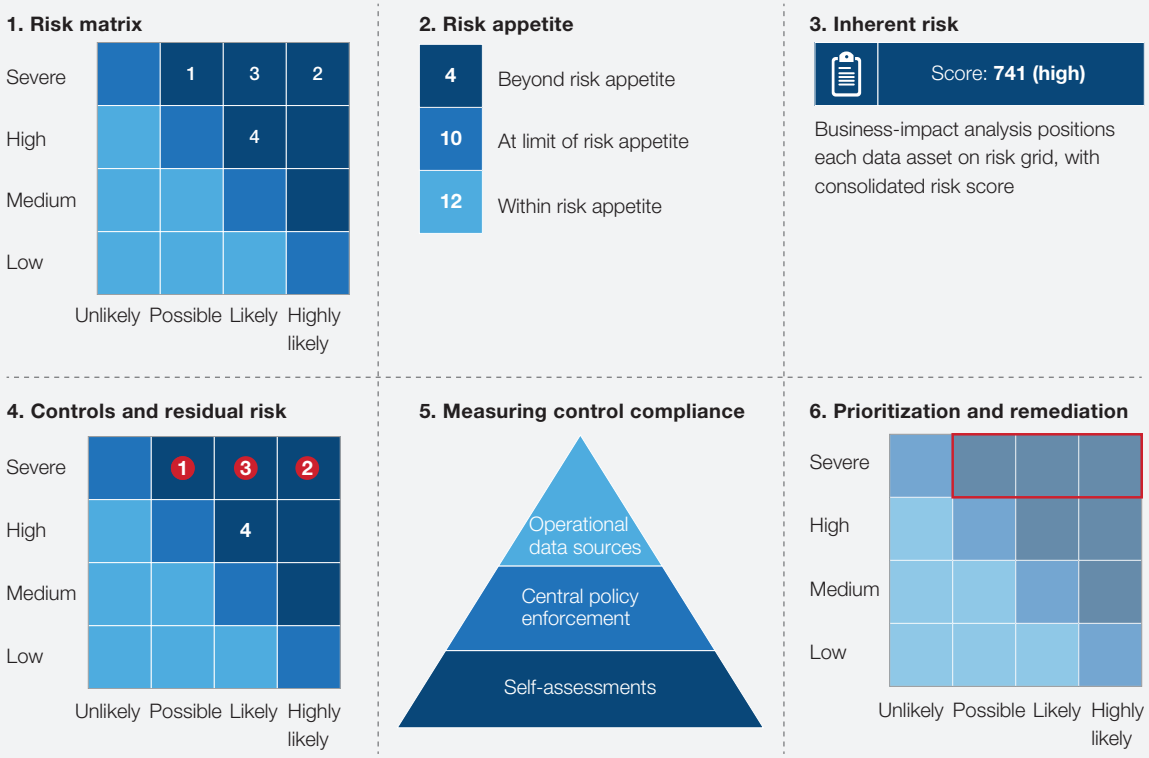
Leading companies include progress updates in their cyberrisk reporting. The updates provide information on the status of counter-risk initiatives and

the changing threat landscape. To make information most accessible to decision makers, dashboards for cyberrisk are needed. These instrument panels allow nonspecialists to readily scan the crucial data (Exhibit 4). A good dashboard can summarize the entire risk management terrain in a series of dynamic panels, presenting the following analyses:

- the evolution of the relevant threat landscape and its implications for the organization
- an overview of recent cyberrisk events, incident development, and key countermeasures taken
- the top cyberrisks as defined in cooperation with the business units and measured through clearly defined key risk indicators
- risk assessments in light of clearly defined risk appetites, with recommendations on the assets in need of prioritized attention (see sidebar "Prioritizing counter-risk initiatives according to the value at risk")
- a detailed plan of the counter-risk initiatives in place, with relevant accountabilities, implementation status, and actual impact on risk reduction

Exhibit 4 **The cyberrisk dashboard displays end-to-end risk monitoring and management in real time, enhancing executive control.**

Cyberrisk dashboard, illustrative



To support effective decision making, optimally designed dashboards allow users to drill down from the group-level risk status to individual businesses and legal entities—and finally to the vulnerable assets underlying particular threats. Experience with risk dashboards demonstrates that decision makers need to view all pertinent KRIs, for individual assets as well as the business unit as a whole. KRI views should be adapted to individual roles: business-unit managers should be able to view only KRIs related to their own business unit, while the chief information officer (CIO) or chief risk officer (CRO) should be able to aggregate the dashboard output across business units, functions, and entities.

The cyberrisk dashboard metrics must accurately measure actual risk levels. Their purpose is to enable better, faster decisions to avert threats and increase an organization's overall resilience. The dashboard must be built upon data that is relevant, up to date, vetted for quality, and aggregated in meaningful ways. Integrated data from trusted sources, frequent updates, and analytical capabilities allow decision makers to derive meaningful insights directly from a dashboard. They are provided with the facts they need to fight against digital attacks, fraud, and blackmail. It is best understood as the most visible part of an integrated data and analytics platform for holistic digital risk management (Exhibit 5).

How dashboards enable better decision making

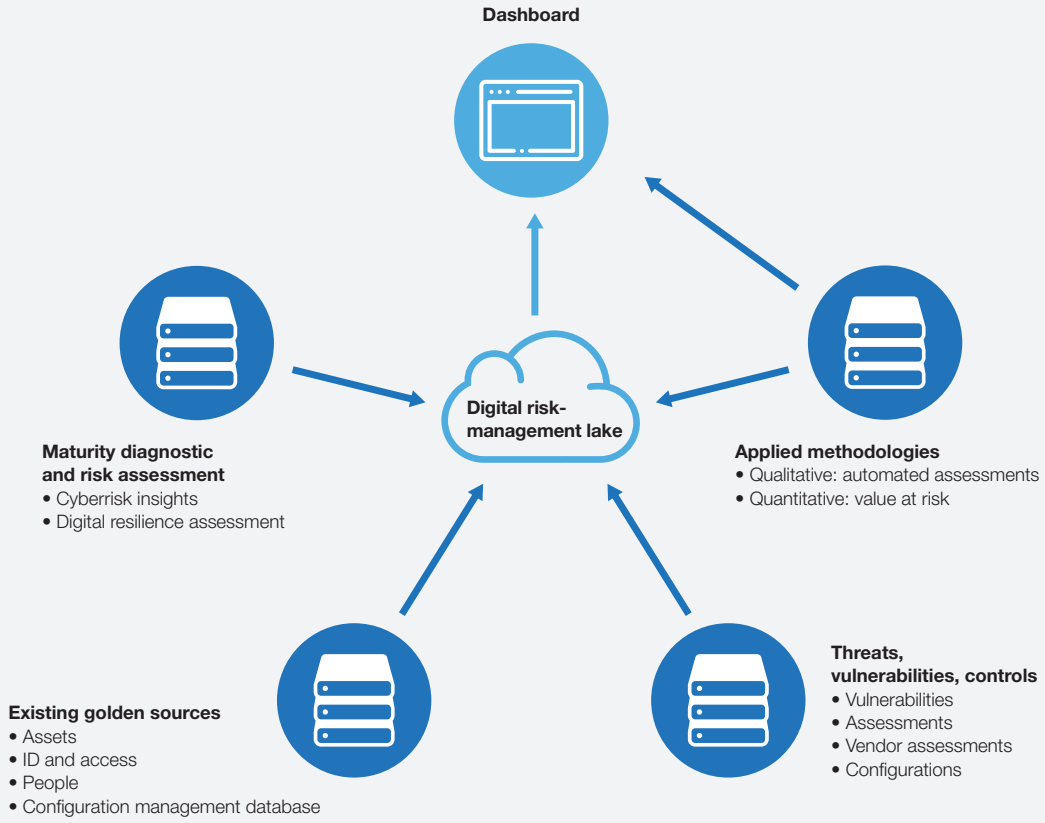
A good cyberrisk dashboard is one designed to promote good decision making. One way it does this is by simplifying details, intricate KRIs, and complicated visuals to communicate the most essential information—an essentially complete risk profile. An executive in the financial-services industry explained the advantages of a relatively simple dashboard:

> *Before we had a cyberrisk dashboard, we implemented cyberrisk controls more or less at random. Everything was important. We tried to protect all assets with middle-of-the-road controls. As a result, we were spread too thinly in some critical areas, such as private banking applications. At the same time, we were going overboard with cumbersome controls in other, less critical areas. What the dashboard helped us do was focus our efforts and our investments. We were able to limit the scope of the [heavy controls], such as advanced encryption and two-factor authentication, to crucial, high-risk assets. As a result, we are now better protected than before, while our operations run much more smoothly.*

Over the course of dozens of cybersecurity transformations, we have found that almost all companies systematically overinvest in the protection of virtually risk-free assets, while the

To support effective decision making, optimally designed dashboards allow users to drill down from the group-level risk status to individual businesses and legal entities.

Exhibit 5 **A digital risk dashboard is the most visible part of an integrated data and analytics platform for holistic digital risk management.**



protection of high-risk assets is often underfunded or undermanaged. A good cyberrisk dashboard provides the kind of information that will help risk managers rebalance the scales and focus their resources on averting the biggest threats to the organization's most critical assets. As another executive remarked:

> *Implementing controls for everything is the easy way, but it's ultimately too expensive, and it slows us down too much. You have to pick your battles, in line with your company's risk appetite. But you need a reliable fact base. Only then can you decide not only for but also against the implementation of controls and still sleep soundly.*

While the benefits of a cyberrisk dashboard may be obvious, the challenges only become apparent when companies begin to put holistic cyberrisk management into practice.

Overcoming blind activism

A good dashboard promotes resilience and efficiency; an unsuitable dashboard does the opposite. At worst, it might deceive decision makers about threats and controls, leaving the organization

Prioritizing counter-risk initiatives according to the value at risk

Consolidated information about threats, vulnerabilities, and an organization's cyber-resilience is a powerful lever in its own right. Consolidation creates transparency, awareness, and discipline around the ways an organization understands and manages risk. But this information becomes even more powerful when it is combined with information about critical business processes and the losses incurred under adverse scenarios—such as a temporary suspension in service. The combination of risk and business data allows risk managers to calculate the value at risk in a given area and accordingly prioritize counter-risk initiatives. This means that the organization is directing available resources toward its most pressing material risks. Prioritization is especially important as the scope of risk-management increases. In the financial-services industry, most risk managers we surveyed said that they expect to take on more comprehensive responsibilities in the future. Given the coming risk burdens, companies will need to invest in an integrated data and analytics platform that drives fast, fact-based decision making. For more details, see our recent report *The future of risk management in the digital era*, created in collaboration with the Institute of International Finance.

more vulnerable than it appears. Poorly performing dashboards can trigger blind activism, with red flags going up all the time. Misleading alarms can be set off by an inarticulate risk appetite, excessively cautious managerial self-assessments, poor data quality, undifferentiated controls across all assets, and inadequate alert thresholds.

When alarms are near constant, response teams are always in firefighting mode and risk managers and IT and OT security experts are always overloaded with work. Blind activism increases stress on entire organizations but rarely increases resilience. For that, the organization needs effective cyberrisk governance structures. These are best supported by a well-constructed dashboard reflecting the risk appetite and fed with consistent data from golden sources. These tools will bring transparency and resilience and also do wonders for efficiency and employee motivation. Fact-based prioritization will help focus an organization's efforts on fighting cyberrisks in the top right-hand quadrant of the risk heat map: those that are most serious and likely to occur.

Conversely, controls for risks nearer the bottom left-hand quadrant (less threatening, less likely) can be loosened or discontinued to free up resources. Before long, the organization will have moved from a blind, undifferentiated compliance focus to one in which controls and business continuity management processes are based on robust facts about actual risks.

Building a good dashboard is not, or at least not primarily, about coding. It is more the result of engaged conversations across roles in which acceptable risks are identified, the data needed to

understand the organization's true resilience are marshalled, and the focal points for risk-reducing investment are established, along with the most effective ways to monitor progress.

Breaking down silos

In our experience, silos—isolated functional units and the disconnected thinking they foster—are one of the biggest obstacles to cyberrisk transformations. At many institutions, data owners and line managers confine themselves to only that part of the data pool, organization, or value chain for which they are responsible. They are not required to look left or right and by design cannot see the big picture. They are therefore unable to make the choices needed to balance resilience with smooth operations. Data

Application examples and voices from the C-suite

ROI-based cyberrisk management and advanced control implementation in healthcare

Healthcare is among the most risk-sensitive industries because of the trove of patient data and financial information it generates, stores, and processes on a daily basis. The chief information officer (CIO) of a health-insurance provider sought to put the company's cybersecurity funds to optimal use. The governing objective was to reduce overall risk and implement advanced capabilities to counter evolving threats. Historically, the company had been focused on compliance with high-level regulatory requirements. Existing controls were undifferentiated, and the CIO was concerned that her investments were not effectively prioritized from a return-on-investment (ROI) perspective. In response, the board members, relying upon a customized probability–loss matrix, determined the most critical assets as well as the acceptable risk levels for each (risk appetite). In a second step, the company was able to reallocate 20 percent of its total investment in a multiyear cybersecurity program (exceeding $100 million) from routine activities, such as penetration testing, to advanced controls for highly critical assets.

We now have the financial leeway to build out our next-generation security operations center and an insider-threat program. Thanks to the new approach, we are definitely getting more value for our money than before.
—Healthcare CIO

Reducing the value at risk with improved business-continuity management in consumer goods

Alerted by the proliferation of computer viruses, untargeted malware, and attacks on production systems, a consumer-goods manufacturer decided to ramp up its cyberrisk reporting and management regime. The company took a holistic risk-monitoring and management approach. Specifically, the CIO enhanced the company's business-continuity management. The primary objectives were to reduce the value at risk in core processes and to assign the company's cybersecurity resources according to a risk-based approach, leveraging operational data. In effect, the company put its limited resources and maintenance windows to much better use than under the previous regime. Investments in controls and responses are now focused on the most critical,

owners often hesitate to share what they own, and line managers often feel burdened by the need to comply with risk-management guidelines. As one data owner put it, "If I give up my data, what do I have left? The data is what makes me relevant to the company." A line manager said, "All these controls slow me down. Why should I cooperate with the cyberrisk team if all they do is make my life more difficult?" The reports emanating from an organization of siloed thinkers will frustrate decision makers, one of whom complained, "Why do I need to look at all these moon phases and traffic lights? How do all these indicators relate to our business? What I need to know is whether our top assets are protected, and what I should do if they are not."

most vulnerable applications, such as the system that steers the supply chain and the browser-based interface to distribution partners. To increase resilience even further, the company's IT and HR departments set up an online training program that helps employees handling critical systems spot signs of cyberattacks at an early stage. The company's key informational and operational assets are now much better protected than before.

The new reporting has significantly reduced our risk of becoming the victim of an untargeted attack.
—Consumer goods CIO

Enhanced risk-appetite setting and streamlined cyberrisk reporting in financial services

The chief risk officer (CRO) of a global bank complained that the company's cyberrisk reporting was outdated and inconsistent across the different lines of defense. Frequently, the board and regulators were presented with conflicting messages about threats and increasingly impatient requests for responses from multiple stakeholders. "We have had complaints from regulators in three different countries. The supervisory board is breathing down my neck," the CRO remarked. The bank in fact held no common understanding of cyberrisk nor consensus about acceptable risk levels. The CRO, the chief operating officer, and business-unit leaders decided to develop a consistent cyberrisk scorecard focused on the top 15 cyberrisks, a consolidated set of key risk indicators, an enterprise-wide definition of risk appetite, and selected key performance indicators to measure the success of the bank's investments in cybersecurity. An additional benefit of these enhancements was that the digitization they required also freed up significant team resources that had been assigned to report generation.

For the first time, we have real transparency and consistency in how we manage cyberrisk. The scorecard is fully digitized. I can bring it up on my tablet any time. When nervous members of the supervisory board or regulators call me, I have all the information I need to answer their questions. In most cases, I can tell them right away what we are doing to fight the threat they have read about in the paper. And instead of wasting time debating inconsistencies, my direct reports now have the time to develop recommendations for better controls.
—Financial-services CRO

A good dashboard can help break down the silos, by bringing together different kinds of people—from detail-oriented database managers to top executives with short attention spans. To create a good dashboard the group needs to collaborate, as all will eventually benefit from its output. The dashboard forces all to adopt a common language, one that harmonizes definitions of KRIs, criticality, threat levels, and compliance (for further insight, see sidebar "Application examples and voices from the C-suite").

Neither groups of technical wizards nor of business specialists could accomplish the needed transformation on their own. For that, the diverse group of interested parties—business owners, programmers, data scientists, designers, change managers, and privacy lawyers—must be made to relate to each other regularly. Only then will the business implications of the technology, as well as the technological requirements of the business goals, be reciprocally understood. The culture will transform itself once these many roles, with their rich collective expertise, rediscover their common purpose.

Establishing holistic cyberrisk reporting and governance is as much about people as it is about processes and dashboards. In the most successful transformations, consistent reporting acted as a catalyst of cultural change. At first sight, a dashboard may appear to be a piece of software with a fancy front end. In truth, it is the material expression of the agreed-upon KRIs, aggregation levels, and reporting cycles. The discussions that lead to these agreements are change agents in their own right. Two further lessons of successful transformations are worth underlining: involve business owners from day one and be willing to make trade-offs to find the right balance between protection and productivity. Executives will find experienced managers to help them with these decisions, who will then become the abiding advocates of the new holistic approach.

[1] McKinsey global survey of 1,125 board members of leading companies in all industries, April 2017. Seventy-five percent of respondents included cybersecurity among the top five board concerns.

[2] *McKinsey on Risk* Number 5, June 2018, McKinsey.com.

[3] Osterman research.

Jim Boehm is an associate partner in McKinsey's Washington, DC, office; **Peter Merrath** is an associate partner in the Frankfurt office, where **Rolf Riemenschnitter** is a partner and **Tobias Stähle** is a senior expert; **Thomas Poppensieker** is a senior partner in the Munich office.

Cybersecurity and the risk function

Are your information technology, cybersecurity, and risk professionals working together as a championship team to neutralize cyberthreats and protect business value?

Oliver Bevan, Jim Boehm, Merlina Manocaran, and Rolf Riemenschnitter

Most CEOs of large organizations are convinced of the existential dimensions of cyberrisk. The most savvy have begun to approach cybersecurity with an enterprise-wide perspective, involving the teams of the chief information security officer (CISO), the chief information officer (CIO), and the chief risk officer (CRO), as well as the business units. A true partnership between these teams is the optimal approach, having emerged from a recognition that no single leader or team can gain the complete perspective needed to be effective in the cyberdomain. No one group within a company could manage the number and types of internal and external threats, the complex technological landscape, and the many actions needed to address vulnerabilities associated with people and technology. They rather need to work together.

The status quo: CISO-only control

A collaborative, enterprise-wide approach has not yet been widely adopted, however. For many companies, de facto responsibility for cybersecurity has devolved almost exclusively on the chief information security officer. The CISO may work with teams led by the CRO and the CIO, but collaboration usually occurs on an ad-hoc basis rather than within a coordinated strategy. As such, the risk function will not participate to the extent needed to embed business-risk awareness in a company's cybersecurity posture and planning nor to align the strategy with the company's business-risk appetite. Without a risk-based focus on cybersecurity, companies often overlook the true drivers of risk, an error that can magnify a crisis and lead to unnecessarily large business losses. One of the challenges to collaboration has been the technical nature of the cybersecurity environment, an abiding condition that must be addressed when organizations embed the risk function and risk thinking in cybersecurity strategy. Risk organizations can find it difficult to contribute meaningfully to tech-based discussions. Conversely, cybersecurity teams can be reluctant to add risk processes—such as risk and control self-assessments—to their agendas, overfull as they are with complex technical tasks. A further complication is the tendency of executives and board members to rely exclusively on the CISO and the CISO team whenever they face a cybersecurity issue. This usually adds pressure on an already overtaxed team while reinforcing the notion that the CISO has the only point of view on the topic.

The urgency of a risk lens

In theory, the risk function is charged with managing all operational risk across the organization, but under the CISO-centered arrangement for cybersecurity, the risk function is often sidelined in the area of cyberrisk. The absence of the essential risk perspective can skew the cybersecurity stance irrationally: either toward issues of the most immediate concern to senior leaders or toward the security scare du jour. Such biases potentially magnify the danger of the actual vulnerabilities being ignored. Risk oversight of cybersecurity practices can ensure that the strategy protects the most valuable assets, where a breach would pose the greatest potential business damage, whether in terms of reputation, regulatory intervention, or the bottom line. A simultaneous benefit is that this risk lens helps to control costs. The inevitability and proliferation of cyberattacks make mitigation of every risk financially impossible. Companies must therefore review all risks across the organization, locating and mitigating the most significant ones, applying protection, detection, and response interventions in a prioritized way.

Fulfilling this obvious requirement, to prioritize the most important risks to the enterprise, is practically difficult within the CISO-centered approach. The task can be especially hard for CISOs and other security professionals whose training and experience has centered on designing and implementing strong security protections, or running a security-operations workflow. Risk management—the identification, quantitative evaluation, and prioritization of risks—is outside their main focus. Of course, these are exactly the purposes of the risk organization. In nearly every other area of the business, the risk group is constantly identifying, evaluating, and remediating risks. Risk should be doing this for cyberrisk as well. The question is, how best to integrate risk into the cybersecurity environment?

Barriers to CISO–Risk collaboration

While organizational models for handling cyberrisk vary across institutions, several shortcomings are commonly observed. The most basic has been a lack of clarity in how the lines-of-defense concept should be applied. This concept, as developed by financial institutions to manage risk in the regulatory environment, clearly delineates three lines—business and operations managers, risk and compliance functions, and internal auditors.

For cyberrisk, the lines-of-defense concept can be seen in the roles of the cybersecurity function as the first line of defense and the risk function as the second. That is, the cybersecurity function, usually as an integral part of IT, initiates the risk-mitigating interventions that protect against, detect, and respond to threats generated in business and IT operations. As the second line of defense, the risk function works with the first line to identify and prioritize cyberrisks.

In practice, some blurring of these boundaries occurs (and a healthy exchange of perspectives is recommended), as organizations work collectively across the lines to identify risks and mitigate vulnerabilities. The "blurring" does not, however, diminish the importance of the challenge responsibilities of the second line of defense. It rather provides the second line with the opportunity to challenge the first line more often in open dialogue. As will be seen, this relationship benefits both the first and second lines. The first line becomes more aware of how cyberrisk fits into enterprise risk management and better prepared for arising risk challenges once interventions are under way. The second line, meanwhile, becomes more familiar with the capabilities and plans of the first line.

The lines-of-defense concept can be seen in the roles of the cybersecurity function as the first line of defense and the risk function as the second.

In CISO-centered approaches to cybersecurity, the CISO team can be responsible for all roles across the lines of defense. The team might identify the cyberrisks, decide on the investments in mitigation, design the technical and nontechnical security controls, manage the resources needed to implement controls and operational initiatives, and determine how risk-reduction efforts should be measured and reported. The same function (and sometimes the same person) will thus perform or direct all risk-identifying and risk-reducing activities and then certify whether the activities are working. (Not surprisingly, under such an arrangement, the reporting usually shows that progress has been good.)

At some companies using a CISO-led approach, the risk function theoretically plays an oversight role as the second line of defense. Yet meaningful insight into cybersecurity activities cannot be obtained without deeper engagement. Often the CRO will have no clear mandate for this kind of involvement and will find it organizationally difficult to challenge CISO-controlled activities. Other obstacles include a lack of cybersecurity skills within the risk function and an insufficient view on the unit of risk (the information asset) and the corresponding value at stake. In short, if the risk function is not integral to risk assessment and remediation in the cybersecurity space, it will be unable to play a meaningful challenger role. Instead, for reports and additional information, CRO and team will be dependent on voluntary cooperation, often initiated after events—too late, that is, to do much good.

Organizational friction

As when the CISO controls all aspects of the cybersecurity strategy, issues can also arise when cyberrisk responsibilities are formally divided among two or more teams. If the operating model for the division of responsibilities is inadequate or has not been fully implemented, silos can develop, generating organizational friction.

At one company, the CRO and experts within the risk organization crafted all cyberrisk policies in accordance with the company's risk appetite and then assessed adherence by the CISO, CIO, and business units. The CRO also informed executives and the board of the top risks, advising on a course of action and reporting on progress. The CISO was responsible for designing the technical and manual controls, and for executing risk-mitigating initiatives. Detailed implementation was the responsibility of the CIO. Despite the clear delineation of roles, significant organizational friction arose.

At this company, the risk function was rightly trying to take on a more integrated role, based on its knowledge of adjacent relevant risks, including fraud and vendor risk. Yet because risk and security were so heavily siloed, the risk function proceeded without much collaboration. The CISO and CIO teams were given little opportunity to provide input before being presented with finished requirements. Unsurprisingly, they reacted negatively, tending to regard the policies and targets as unreasonable, unattainable, and therefore irrelevant. At this point, the chances of gaining the cooperation needed to improve outcomes were much reduced. And things regressed from there, as the CISO and CIO teams mostly ignored the risk function. Eventually the executive team supported the CISO and the risk function was deprived of its deeper role in cybersecurity.

Friction between different parts of an organization drives up costs, wastes resources, and impairs alignment—in this case, alignment around an enterprise-wide strategy to reduce cyberrisk. When this happens, a kind of risk blindness can afflict everyone involved. The situation will eventually become apparent to top management and the board, after they receive piecemeal reports on cyberrisk outcomes from different groups in a variety of formats and frequencies. These leaders must be forgiven if they wonder whether the right hand knows what the left hand is doing.

A strategic security partnership

Many CISOs and CIOs would like to integrate their vantage points more deeply into the enterprise risk process, and the risk function can and should be better involved in cybersecurity. However, best practices for achieving risk's optimal role in identifying, prioritizing, and managing cyberrisk have only begun to emerge. Many companies have struggled to define and distinguish the duties of all relevant parties clearly and logically, so that they can interact effectively and in the right sequence to actually reduce risk. But some companies are finding a better way.

We see emerging best practice in an approach we call a "strategic security partnership." Motivated by an explicit mandate from executive leadership, the approach involves the full commitment and cooperation of the CISO, CIO, and CRO teams in the cybersecurity space. To implement the approach, an integrated operating model needs to be carefully plotted and tested, starting with the key processes around which an organization and culture are designed. What follows is a sketch of this method as successfully implemented by one large corporation.

1. The role of the chief risk officer and the risk team

- In partnership with the CISO and the security specialists, the risk team forms an early view of the cyberrisks across the enterprise, including such adjacent risks as fraud and vendor risk. This early challenge of potential first-line interventions helps foster the collaboration needed for a more effective and efficient process to prioritize risks for remediation.
- The CRO helps the CISO and the CIO design the principles of cyberinvestment for the company.
- The risk team works with the CISO and the CIO to develop and present the overall portfolio of initiatives to executive management.
- Risk independently monitors the progress and status of initiatives as well as the outcomes of cyberinvestments and mitigation. The team also collaborates with the CISO and CIO to work out reasonable mitigations and timelines when agreed-upon guidelines are violated.

2. The role of the chief information security officer

- With the guidance of the chief risk officer, the CISO and team translate the cyberrisk recommendations into technical and nontechnical initiatives. The CISO vets and aligns them with the CIO team, since initiative design, architecture, and implementation will require CIO resources. The teams of the CISO, CIO, and CRO jointly approve the program of work. The CISO team works with the CIO team to design the solutions to fulfill each initiative.

- Together with the CRO, the CISO aligns the format, content, and cadence of cyberrisk reporting, so that cyberrisk is reported with all other risks. The CISO and the CIO implement reporting initiatives and jointly report on progress and status to the CRO, who then reports to the executive leadership and the board.

- Either alone or together with the CIO, the CISO directs a security operations center (SOC). In a successful case, the operations center is jointly run, with the CIO team focusing on the operational workflow and the CISO team providing security-specific support, including threat intelligence, forensics, and red team–blue team exercise planning. Even if the CISO team has full control of the SOC, however, it will need to work closely with the CIO teams running IT operations such as network or production monitoring.

3. The role of the chief information officer

- As indicated in the foregoing discussion of the CRO and CISO roles, the CIO team has an equal stake in addressing cyberrisk throughout the processes. Their equality is absolutely essential, since CIO and team are primarily responsible for implementation and will have to balance security-driven demands for their capacity with their other IT "run" and "change" requirements.

The advantages of a strategic security partnership

The advantages of a strategic security partnership will usually outweigh the challenges of adopting it. First, this approach ensures that risk-based thinking is embedded in the CISO's program, breaking down functional silos and laying the foundation for eliminating the organizational friction that characterizes CISO-only control. With top-management leadership, most institutions can implement a strategic security partnership immediately. For organizations that already have risk, CISO, and CIO teams, the approach requires no new hiring and no significant change in responsibilities. (For the sets of actions the transition will require, see the sidebar, "Moving risk from status-quo cybersecurity approaches to a strategic security partnership.")

A strategic security partnership establishes the needed relationships and perspectives up front. This advantage can be of great importance in the event of a cybersecurity incident: the CISO and the CIO will already have a risk-informed view and understand the risk to the business. The CRO, meanwhile, will understand what the CISO and the CIO can and cannot do. Under a strategic security partnership, all three leaders know how to work with one another and how to bring in the business units as needed. Crucially, they also understand the importance of clear, trustworthy internal and external communications during an incident, as the CISO and CIO teams get down to the business of containment, eradication, and remediation.

Fixing leaks . . . together

Given the number of functions involved and the complexity of the tasks, the processes of identifying and prioritizing risks, aligning the program, and agreeing upon and implementing initiatives can be time-consuming. An essential purpose of the model is to ensure that the CRO and the risk group understand cyberrisk at the level of each information asset and the relative business value entailed. Without this essential insight, risk prioritization cannot proceed. The principals involved can work to improve coordination, but they must allow enough time for these crucial processes to be completed properly, since the potential effectiveness of the outcomes will be much greater.

Fine tuning will probably be needed to sharpen the definition of roles, responsibilities, and decision rights. No one should be surprised if confusion arises about who owns what task, but proper planning can reduce the confusion. Exercises using "RACI" process diagrams are the best remedy. The acronym stands for "responsible, accountable, consulted, informed," and the diagrams are used to identify roles and responsibilities during an organizational change. "Water through the pipes" (WTTP) exercises are used for testing: process flows are initiated and where "leaks" in the clarity of the organizational plumbing are detected, the RACI-based diagram is repaired with agreed-upon changes. The diagrams are validated by the teams and aggregated with corresponding workflows into the comprehensive operating model. This additional exercise should completely remove any residual organizational friction. It sharpens roles and rights while laying the groundwork for good working relationships, as all concerned spend time around the table jointly solving problems to arrive at the optimal solution for all stakeholders.

Insights on model performance

For the model to perform optimally, decision makers should be few in number. They should be trusted members of each organization. They will

An essential purpose of the model is to ensure that the CRO and the risk group understand cyberrisk at the level of each information asset and the relative business value entailed.

Moving risk from status-quo cybersecurity approaches to a strategic security partnership

The strategic security partnership described in this article is a new cybersecurity approach, not yet common among large companies today. The status quo environment is more defined by two models, in which the role of risk is either to act mainly as a challenger or mainly as a policy setter and adherence checker. In the former model, risk is less involved in cybersecurity: tech-savvy risk-team members take the initiative to ask the teams of the chief information security officer (CISO) and the chief information officer (CIO) for answers to specific questions or to supply risk with more detailed reports. In the latter model, risk sets the cyberrisk policies to which the CISO and CIO teams are expected to adhere. As policy setter and adherence checker, risk also controls reporting to the executive leadership and board.

In our view, each of these widely deployed approaches is fundamentally inferior to the strategic security partnership. Depending on which approach prevails in an organization, different sets of actions will be needed to migrate risk to the superior model.

1. Risk as challenger

These are the status-quo roles:

- The CISO, sometimes in collaboration with the CIO, identifies and prioritizes cyberrisk, sets the agenda for cyberinvestments, and determines policy limits for IT and business behavior. The CISO is also responsible for the design and architecture of both technical and nontechnical security controls, and performs other first-line functions, such as security operations. The CISO may also own the resources necessary to implement control and operational initiatives, though more often these will come from the CIO organization. Importantly, the CISO is also in charge of all measurement and reporting of risk reduction to the executive leadership and the board.

- The CIO sometimes partners with the CISO for the more technical design aspects of the program. While the CISO may direct implementation, the CIO is usually responsible for the actual implementation work, sometimes reporting progress to the CISO, sometimes to the executive leadership directly. In some cases, the CIO may direct security operations, with the CISO acting as a “1.5” or second line of defense.

- The role of the risk team in the challenger model is to ask the right questions of the CISO or sometimes ask for more detailed reports. Effectiveness depends heavily on the timing of risk’s involvement, the stature of the risk team, and its level of technical knowledge. Without the right combination of these elements, risk may find it difficult to understand what is going on and can easily be sidelined.

These actions are needed to migrate from the challenger model to a strategic security partnership:

- The risk team will need to acquire additional skills and knowledge to engage the CISO and CIO teams on cybersecurity in a meaningful way.

- To provide a business-risk perspective on what is desirable and reasonable, risk needs to be present at meetings on policy planning, architecture, and the implementation of nontechnical controls. The role of risk will include helping the CISO and CIO teams understand how their concerns connect to business risk. Together, the three teams will then be able to shape the year’s cyberrisk agenda on an enterprise-wide basis.

- CISO and the chief risk officer (CRO) will together create a truly risk-reducing performance-management plan. The measurement and reporting activities performed by the CISO team need to be aligned with business objectives, following the model of the way risk works with business-unit leaders. Together the CISO and CRO teams will determine reasonable and achievable targets, bringing in the CIO team for the program-delivery plan. Metrics based on relevant insights and data sources can then be developed.

2. Risk as policy setter and adherence checker

These are the status-quo roles:

- Risk determines the cyberrisk policies that the CISO, the CIO, and business units are expected to follow and then assesses adherence to them. Ideally, policies are developed by cybersavvy members of the CRO team and implemented according to the enterprise-wide risk appetite, though the reality is often different. Risk also owns all reporting, including reporting on the top cyberrisks, on the policies to address them, the adherence levels of the CISO and CIO, and the status of the initiatives being implemented to address the top risks. While this reporting should be aligned with reports produced by the teams of the CISO and CIO, it is too often produced in a vacuum.

- The CISO receives the risk appetite and policies from risk and then designs (and may also build) technical and non-technical controls, sometimes in partnership with the CIO. The CISO or the CIO may direct security operations, according to service-level agreements (SLAs) and tolerance levels set by risk. The CISO is responsible for executing the program of initiatives, though the CIO's organization usually does the hands-on work. The CISO reports to risk and to the leadership and board on the progress and status of initiatives. Depending on the level of organizational friction, either the CISO or the CIO may remediate areas raised by risk.

These actions are needed to migrate from this model, with its divided and sometimes conflicting authority, to a strategic security partnership:

- Risk should involve the CISO team (and where appropriate the CIO team) in setting policy, to give them insight into enterprise risks and gain their buy-in to cyberrisk policies.

- The risk team should collaborate with the teams of the CISO and CIO to create targets for key risk indicators that are well within the enterprise risk appetite. With input from the CISO and the CIO, risk decides what should be measured and reports to executive leaders and the board on the status of the targets.

- Risk becomes an active partner in helping the CISO identify and clear barriers to implementation across the organization, especially within the business.

- Risk promotes the program to reduce cyberrisk that has been created jointly by the teams of the CISO, CIO, and CRO. The sense of shared objectives will increase the program's momentum and help measure and report on risk-appetite boundaries more effectively.

be given the authority to push respective teams for data and information needed to complete tasks on time. It is helpful if these decision makers from each organization meet regularly throughout the year as a working group. This will help build working camaraderie, keep the group abreast of changes, and magnify the focus on the common goal of reducing the institution's top cyberrisks.

■ ■ ■

With cyberthreats mounting in number and sophistication, large institutions can no longer protect against all risks equally. The threats posing the most danger to the business must be identified and neutralized first. For this to happen, the risk function must be deeply embedded in cybersecurity planning and operations. That is what the strategic-security-partnership model is all about. ■

Oliver Bevan is an associate partner in McKinsey's Chicago office; **Jim Boehm** is an expert associate partner in the Washington, DC, office; **Merlina Manocaran** is a partner in the New York office; and **Rolf Riemenschnitter** is a partner in the Frankfurt office.

A framework for improving cybersecurity discussions within organizations

Jason Choi, James Kaplan, and Harrison Lung

Clear and frequent communication is essential but often lacking in companies' cybersecurity programs. Here's how security professionals can create tighter bonds with some critical stakeholders.

The entire world is going digital; virtually every type of cross-border business transaction now has a digital component.[1] Companies' use of digital technologies is opening them up to new relationships with customers and business partners, and new business opportunities. But, as recent headlines have made clear, the very act of connecting to the outside world increases organizations' risks exponentially—of project failure, of data breach, or worse.

In this era of global digital flows, companies must take all possible steps to build robust cybersecurity capabilities. Protection strategies cannot be focused solely on

[1] For more, see *Digital globalization: The new era of global flows*, McKinsey Global Institute, February 2016.

Companies must invoke the human element as well. They must seek to build digitally resilient cultures in which cybersecurity is not an occasional concern but an everyday task for core business stakeholders at all levels, inside and outside the organization (Exhibit 1). In such cultures, discussions about asset protection are proactive rather than reactive, and communications among critical decision makers are open and frequent.

Trust among business stakeholders is a necessary component of digitally resilient cultures; without it, organizations will have a difficult time successfully shielding the customer data that nowadays is so critical for achieving business goals. The board needs to trust that senior management has a long-term view of cybersecurity, with a strategic road map and plans in place to adequately protect information assets and IT systems, regardless of where and how new threats emerge. The business units, the IT organization, and the cybersecurity team need to trust one another enough to get to a mutual agreement about how security protocols can be integrated into daily business processes without creating operational challenges and frustrations. Companies need to have faith that external partners—for instance, cloud vendors—are willing and able to protect shared data and infrastructure. And finally, government agencies need to trust that companies are proactively reporting breaches and sharing information that could help them spot and thwart major cyberincidents, particularly those spanning multiple industries and countries or involving state-sponsored attacks.

Trust among these stakeholders is often missing for a number of reasons, including conflicts of interest and lack of insight into the complicated technologies and concepts and technology professionals don't have a common understanding of cybersecurity issues, for instance, they may never properly execute security protocols, and their adoption of even the latest and greatest technologies may never yield the desired results.

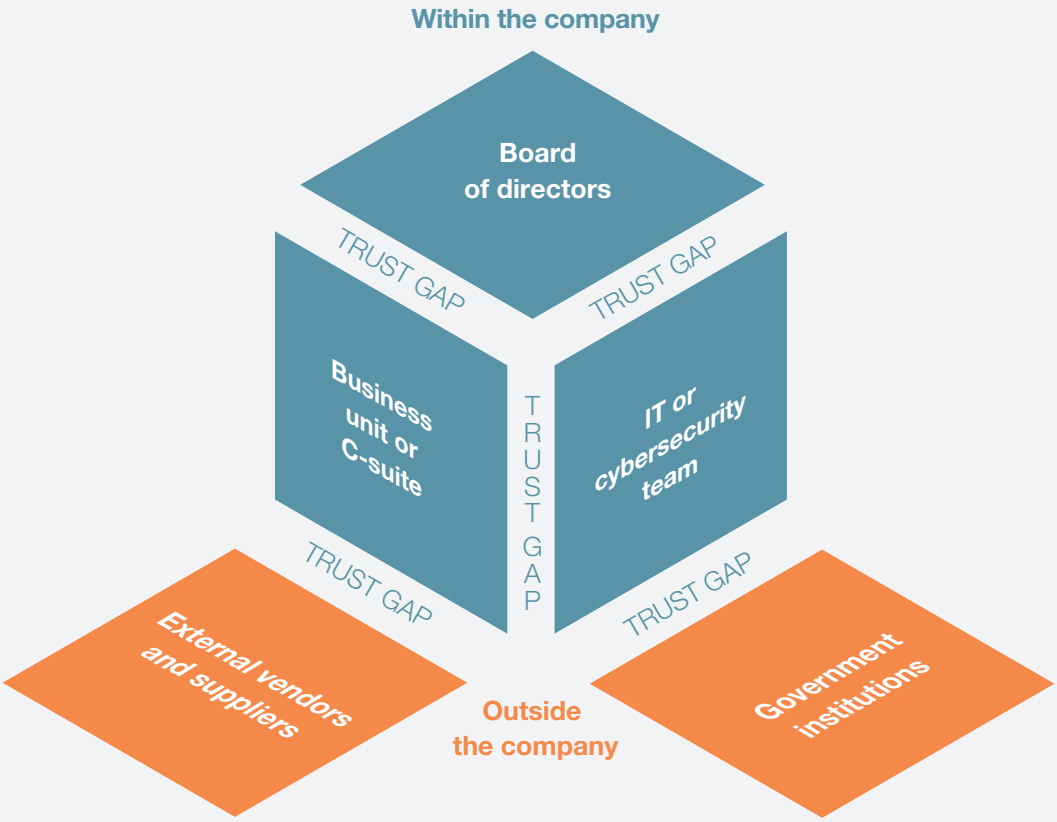
In this article, we explore the communication gaps that exist among these stakeholders, and we suggest ways to bridge these divides. We share our insights on the dysfunctional relationships that can develop within the corporate ecosystem, while acknowledging that the most complicated trust gap still exists between companies and customers. Clearly, no cybersecurity program can ever be 100 percent foolproof; the threat landscape is changing too quickly. But we believe the companies that can facilitate trusting relationships and productive discussions about how they secure critical business assets will be better prepared to respond to ever-advancing cyberthreats.

Trust gap 1: The board and the C-suite

The dynamic between board directors and the senior management team can be fraught for any number of reasons, but first on the list is that cybersecurity is usually not a top item on many board-meeting agendas; often it is presented as part of a larger discussion of IT issues, if it is mentioned at all. Many board directors therefore tend to be less informed about cybersecurity technologies and issues than they may be about standard financial and operational issues—apart from what they read in newspapers about the latest corporate or government security breach. They come to the table with questions about the company's cybersecurity programs. For instance, are the company's most critical assets being adequately protected, and is there a robust response-and-recovery plan in place if a breach does happen? Who actually owns the

Exhibit 1

Cybersecurity trust gaps can exist on many levels across the corporate ecosystem.



cybersecurity agenda, and does that individual or team have the appropriate level of power and influence to mobilize the required resources?

A trust gap develops when senior management falls short in answering these questions. In some cases, the senior-management team may not be able to properly opine on governance issues because it has not clearly defined owners for particular cybersecurity issues and activities—for instance, who should manage safety training modules: the leaders in the business units, or in IT? The senior-management team may not have the right data in hand to properly quantify the current levels of risk the company faces and present a comprehensive mitigation plan to the board. Or the members of the C-suite simply may not communicate with the board often enough when it comes to cybersecurity issues: despite the fact that transparency is a new norm in most companies, our research suggests that only 25 percent of companies present IT security updates to the board more than once a year, and up to 35 percent of companies report this information only on demand.

Finding common ground

Members of the C-suite need to create more transparency and forge stronger communication with board directors. Senior leaders should formally assess the maturity

of their cybersecurity programs regularly and present their findings to the board at least annually but preferably even more frequently. This exercise should involve a structured consideration, by members of the senior-leadership team and others in IT and the business units, of the severity and likelihood of attacks on major corporate assets. For instance, which internal and external threats are the biggest, and what is the business value at stake (Exhibit 2)?

Through this process, the C-suite can develop a dashboard or regular reporting mechanism to inform the board about past and present levels of risk and the potential effects of risk on the company. Such dashboards and reports should use clear, simple language rather than the acronyms often favored in technology discussions. And they should always include impact statements: What are the financial, operational, and technological implications of emerging threats to the business? By establishing regular reports about cybersecurity, the C-suite can signal the importance of the topic to the board—and the need to set cybersecurity apart from the board's review of general IT initiatives.

Trust gap 2: The business units and the IT organization

Trust-based relationships among individuals in the business units, the IT organization, and the cybersecurity function can be difficult to maintain—in part because these groups sometimes work at cross purposes. The cybersecurity team may impose certain safety protocols that are inconvenient for employees in the business units, or otherwise impede their daily operations. Consider your own reactions to IT requests to change passwords—coming up with yet another password that has the required length and complexity and that you can still remember. Such exasperation can escalate from the individual level to the business-unit level. (See sidebar, "How agile development can help close the trust gap between the business and IT.")

For their part, cybersecurity teams may get frustrated with business colleagues who complain about these perceived inconveniences and don't recognize the important role they play in defending digital business assets. When cybersecurity teams grant data- and system-access rights to employees, they must trust that individuals will act appropriately. The IT group expects employees to be generally aware of how corporate systems work, how their actions online are traceable, and how to safeguard their credentials and information. But, in fact, company insiders can pose significant cybersecurity risks. One cybersecurity study noted that 60 percent of all cyberattacks in 2015 involved insiders, an increase of 5 percentage points from the previous year.[2]

Bulking up training efforts

To help close the trust gap between the IT and cybersecurity function and the business, the organization can provide comprehensive cybersecurity training to staffers at all levels. This might include dedicated town-hall meetings, workshops, and training modules focused on identifying varying types of cyberthreats and outlining appropriate responses when employees witness suspicious activity.

Such training can help business-unit employees understand the rationale for cybersecurity protocols and raise their awareness. Even more important, it can signal to the business units

[2] 2016 *Cyber Security Intelligence Index*, IBM X-Force Research Index, IBM, 2016, ibm.com.

Exhibit 2

Companies should continually monitor assets for the likelihood and potential severity of cyberattacks.

that cybersecurity is a shared responsibility. Anyone who has access to confidential data and systems, at whatever level, must play an active role in ensuring their safety.

Companies may also want to develop mechanisms by which IT and cybersecurity professionals can learn more about the implications of any security initiatives on business operations. For instance, some companies are deploying a talent-factory model that encourages cybersecurity professionals to work in other areas of the company in short rotations to broaden their perspectives. Their assignments may be focused on learning more about technology topics outside the security area—for instance, network management, core IT infrastructure, and application development. In an ideal world, cybersecurity team members would be embedded in business units to learn more about product management, public affairs and communications, or finance. The result is often more knowledge sharing and better communication among teams.

The cybersecurity and IT groups should use all available tools and technologies at their disposal to learn as much as they can about people and processes, thereby creating more transparency about security issues. They should establish clear policies outlining

which employees at which levels can call up which categories of data, and when. Where permissible, they can back up these policies with a comprehensive identity-and-access management system—a rules-based platform that automatically monitors online activities, approves access rights, and issues alerts. Additionally, where permissible, they may use predictive analytics to identify risks before breaches can occur—for instance, using network information and log-in data to identify potentially malicious actors and activities inside the company.

Trust gap 3: The company and its vendors

The relationship between companies and their technology and supply-chain vendors has always been complex. Just as consumers rely on companies to keep their data safe and to use them only in ways that they have authorized, businesses must trust their IT and supply-chain vendors to hold competitive information close to the vest. Automakers, for instance, would need to be confident that their OEMs have enough cybersecurity controls in place to protect the intellectual property they are sharing.

This is especially true in an era in which more and more companies are outsourcing the management of their IT infrastructures or their cybersecurity operations. Businesses need to be assured that the access they provide to vendors and the offerings they get from vendors can be integrated with existing systems without opening up any security holes.

Bringing partners closer

To bridge this trust gap, company IT and business leaders should schedule regular conversations with vendors and supply-chain partners to assert the levels of security required to protect shared business information. Such meetings should take place quarterly or biannually; with more frequent contact, vendors and company officials can engage in a true business partnership rather than a simple transactional relationship. They can discuss and devise clear recovery and compensation plans.

Companies can take it a step further by actively collaborating with third-party providers and supply-chain partners to ensure sufficient data protection. They may jointly pursue security certifications, such as the Payment Card Industry Data Security Standard or the ISO 27001 standard, or conduct joint reviews and security audits of IT systems. They may even agree to open themselves up to a broader ecosystem of technology partners to provide additional checks and balances.

For their part, technology vendors may include conditions in their service-level agreements, for instance, for recovering data or restoring system availability within designated time frames. Or they may agree to provide insurance to cover any business the company loses as a result of an attack on the vendor's systems. Many insurance companies are beginning to incorporate cyberincidents into their actuarial tables. The typical coverage today is still narrow, but these policies may become another tool vendors and supply-chain partners can use to assure companies that they are being protected against cyberattack—thereby closing the trust gap.

Trust gap 4: The company and the government

It's no surprise that local, national, and federal governments have in recent years prompted private-sector organizations to become more aware of cybersecurity issues and more active in their data-protection efforts. Cyberattacks in major financial institutions can affect overall market stability. Energy-grid hacks can pose

How agile development can help close the trust gap between the business and IT

It's worth noting that, often, the cybersecurity trust gap between IT and the business units can spill over into product development, particularly in companies that provide online services and Internet of Things solutions. The business units want to establish feature-rich websites and mobile channels that facilitate the customer purchasing experience. Meanwhile, the IT and cybersecurity teams are compelled to introduce security protocols to ensure not only that customer data are protected but that company systems are not left open to attack. And such protocols are not always in sync with the business units' desire to create convenient paths for customers. The result is a lack of shared understanding and a strong sense of frustration—on the part of the business leaders, who view IT as an obstacle to innovation, and on the part of technology leaders, who view the business units' desire for unfettered experimentation as a critical cybersecurity risk.

Companies could instead explore agile approaches to product development—allowing cybersecurity experts to work alongside product owners from the business units as well as colleagues from across multiple functional areas. In this way, companies can establish a collaborative environment that breaks down silos between the IT organization, the cybersecurity team, and the business units. Under this approach, data-protection protocols can be factored into product designs at the outset, reducing potential conflicts or the need for system patches or rework later in the development process.

national threats, too, as we learned from the recent attempted break-ins at a dozen power plants in the United States. Government agencies need companies to report cyberattacks and other incidents in a timely fashion, in order to strengthen overarching protection efforts—for instance, spotting and addressing suspicious patterns of activity and alerting the public to any dangers.

Seeing the big picture

Neither side can afford to battle cyberattacks on its own. Companies need the official imprimatur and gravitas that government agencies can provide as facilitators of cybersecurity investigations and discussions of sensitive information. Governments need the feedback and technical resources that private-sector organizations can provide.

Across the globe, governments are taking steps to support businesses' improvements to their cybersecurity programs. The government of Australia hosts annual cybersecurity leadership meetings, where the prime minister and business leaders set strategy for bolstering cybersecurity efforts in both the private and public sectors. And the government of Singapore has also launched a series of public- and private-sector collaborations designed to strengthen the country's capabilities in cybersecurity research.

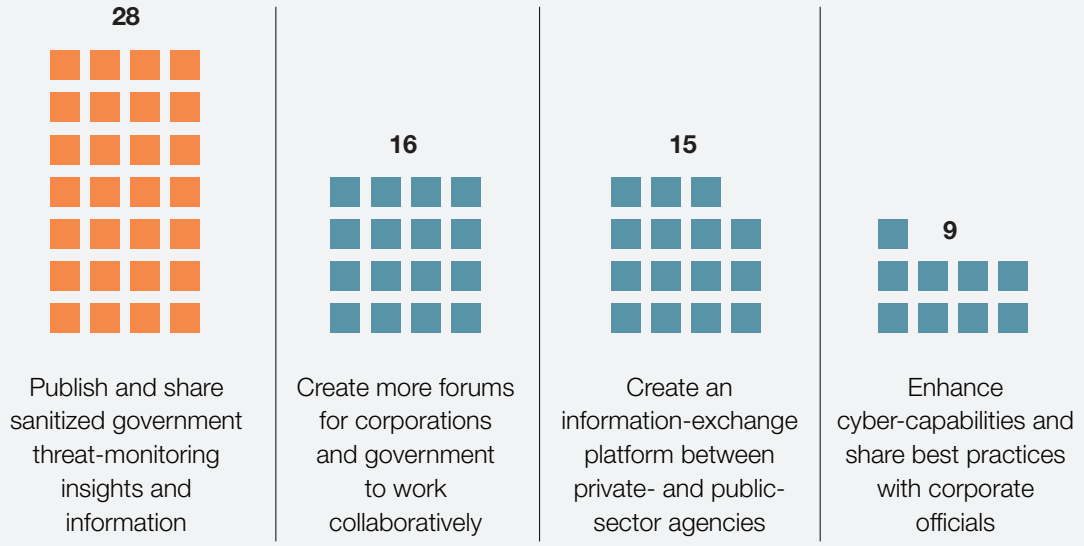
For their part, some companies believe there are ways to further improve public-private partnerships (Exhibit 3). One chief information security officer at a global bank cited the need to extend the national detection network. A CIO at a financial-services company advocated for increased sharing of actionable intelligence. "So far, there are only a few forums aimed at specific corporations. It's not enough for most companies," he told us.

◆◆◆

Exhibit 3

Companies and government agencies must improve how they share security-oriented information.

Q. What should the government do to improve information sharing?, number of times suggested by executives



Source: Insights derived from interviews with about 270 chief information security officers and other top executives at the World Economic Forum; McKinsey analysis.

Technology alone cannot hold cyberattackers at bay. A culture of trust is also important for corporate cybersecurity initiatives to succeed. All stakeholders in a company's ecosystem—board directors, IT leaders, businesspeople, vendors, and so on—must come to a mutual understanding of the risks the company faces and work together to decide on the best approach for addressing those risks.

As we've learned, it can be difficult to attain and preserve this level of agreement and trust—particularly because of the natural tensions built into data-protection efforts: the cybersecurity team's day-to-day work has consequences for the business and vice versa. But if companies recognize the human aspect in cybersecurity and take steps to close trust gaps by introducing more transparency, they can increase the odds that their cybersecurity programs will be successful—not just in the near term, but over the long haul, regardless of the kinds of threats that may emerge. ◆

Jason Choi is a consultant in McKinsey's Hong Kong office, where **Harrison Lung** is an associate partner; **James Kaplan** is a partner in the New York office.

The authors wish to thank Tom Barkin, Chandru Krishnamurthy, Suneet Pahwa, Chris Rezek, and Paul Willmott for their contributions to this article.

Designed by Global Editorial Services.

CORPORATE GOVERNANCE

The board's role in managing cybersecurity risks

Cybersecurity can no longer be the concern of just the IT department. Within organizations, it needs to be everyone's business — including the board's.

By Ray A. Rothrock, James Kaplan, Friso Van der Oord

This article was originally published on MIT Sloan Management Review

Today, more than ever, the demands posed by issues of cybersecurity clash with both the need for innovation and the clamor for productivity. Increasingly, cybersecurity risk includes not only the risk of a network data breach but also the risk of the entire enterprise being undermined via business activities that rely on open digital connectivity and accessibility. As a result, learning how to deal with cybersecurity risk is of critical importance to an enterprise, and it must therefore be addressed strategically from the very top. Cybersecurity management can no longer be a concern delegated to the information technology (IT) department. It needs to be everyone's business — including the board's.

Cybersecurity Enters the Boardroom

Network breaches have become so routine that only the most spectacular events, such as the recent breach at the credit reporting agency Equifax Inc. that affected some 143 million U.S. consumers, make headlines. Corporate boards of directors are expected to ensure cybersecurity, despite the fact that most boards are unprepared for this role. A 2017-2018 survey by the National Association of Corporate Directors (NACD) found that 58% of corporate board member respondents at public companies believe that cyber-related risk is the most challenging risk they are expected to oversee. The ability of companies to manage this risk has far-reaching implications for stock prices, company reputations, and the professional reputations of directors themselves. For example, following a 2013 data breach of Target Corp., in which the personal information of more than 60 million customers was stolen, a shareholder lawsuit charged directors and officers with having fallen short in their fiduciary duties by failing to maintain adequate controls to ensure the security of data. Although the board members were ultimately not found to be at fault, both the company's CEO and CIO resigned.

U.S. case law is based on and generally adheres to the "business judgment rule," which sets a high bar for plaintiffs pursuing legal action against board members. Similar protections for directors are in place in most "common law" countries, including Canada, England, and Australia. The Equifax cyberattack and future corporate breaches may prompt more challenges to the business judgment rule.

The view that directors are not sufficiently prepared to deal with cybersecurity risk has raised alarm bells in boardrooms nationwide and globally. Even as companies increase their investments in security, we are seeing more — and more serious — cyberattacks. If corporate boards are not sufficiently prepared to deal with cybersecurity, how will they be able to determine the effectiveness of current and proposed cybersecurity strategies? How can they know what operationally effective cybersecurity should look like and how it should evolve? And how can directors know what to ask so that they can make the right cybersecurity investment decisions?

Asking the Right Questions

In our work with dozens of companies and in surveys of executives, we have found that many directors currently cannot ask the right questions because they lack meaningful metrics to assess the cybersecurity of their business. In a 2016 poll of 200 CEOs conducted by RedSeal Inc., a cybersecurity analytics company in Sunnyvale, California, 87% of respondents reported needing a better way to measure the effectiveness of their cybersecurity investments, with 72% calling the absence of meaningful metrics a "major challenge." Often, executives as well as directors spend too much time studying technical reports on such things as the numbers of intrusion detection system alerts, antivirus signatures identified, and software patches implemented.

To improve the situation, companies need to address two issues. First, directors need to have basic training in cybersecurity that addresses the strategic nature, scope, and implications of cybersecurity risk. Within companies, managers involved in operations, security specialists, and directors alike need to adopt a common language for talking about cybersecurity risk. Second, top management needs to provide meaningful data about not just the state of data security as defined narrowly by viruses quarantined or the number of

intrusions detected, but also about the resilience of the organization's digital networks. This means having strategies to sustain business during a cybersecurity breach, to recover quickly in its aftermath, and to investigate needed improvements to the digital infrastructure. Networks constantly change, so tracking cyber risks and vulnerabilities over time and adapting accordingly is essential.

A few decades ago, when business computers were networked into systems of record, it made sense for organizations to focus exclusively on preventing outside attacks and protecting the network perimeter. However, now that computers have become systems of engagement, strategies geared toward perimeter defense are inadequate. Today's organizations have vast numbers of network connections and human-machine interactions taking place at all hours of the day and night. In this context, security strategies must extend far beyond the walls of a single organization to reflect interactions with suppliers, customers, and vendors. Networks are permeable, and the relevant question is no longer "Will the organization's cyberstructure be compromised?" but "What do we do when it is breached?" For organizations, the old challenge of detecting and neutralizing threats has expanded to include learning how to continue doing business during a breach and how to recover after one. In other words, it has expanded from security alone to security and resilience.

Increasing Resilience

Resilience is essential in any effective cyberdefense strategy. Our cyberadversaries are competent, determined attackers and only have to succeed once.

Resilience assumes that attacks are immutable features of the digital business environment and that some fraction of these attacks will inevitably result in breaches.

Resilience assumes that attacks are immutable features of the digital business environment and that some fraction of these attacks will inevitably result in breaches. Therefore, creating sufficient resilience both to continue doing business while dealing with a breach and to recover in the aftermath of a breach is the most critical element of a contemporary cyberdefense strategy.

Adequate organizational resilience is about operating the business while fighting back and recovering. Maintaining this level of performance requires the ability to measure an organization's digital resilience much the way a board oversees its financial health. For board members, no fiduciary obligation is more urgent than overseeing and, where necessary, challenging how executive leadership manages the risks to the company. Managing cybersecurity risk today requires protecting the digital networks essential to conducting business by ensuring effective security and a high level of resilience in response to those inevitable cyberattacks. This can be accomplished through policy, selection of leadership, and allocation of resources. It is a whole-enterprise issue, requiring both full board engagement and superior execution by management.

The 2017-2018 survey by NACD reveals that public company board members are significantly more skeptical about their company's cybersecurity efforts than are C-suite executives. Just 37% of respondents reported feeling "confident" or "very confident" that their company was "properly secured against a cyberattack"; 60% said they were "slightly" or "moderately" confident. Other surveys, including the 2016 poll of CEOs by RedSeal, pointed to similar weaknesses. Given the disconnect between the risk levels and degree of preparedness, we believe that most companies need to become more realistic about their vulnerability.

The problem isn't a lack of investment. In 2017, worldwide spending on information security was expected to reach $86.4 billion and to further increase to $93 billion in 2018, according to Gartner Inc. However, cybercrime losses are rising at more than twice the rate of expenditure increases. Many CEOs continue to focus their attention on keeping hackers

out of their networks rather than building resilience for dealing with hackers once they have broken in. Although most CEOs believe that cybersecurity is a strategic function that starts with executives, RedSeal found that 89% of CEOs surveyed treat it less as a whole-business issue than as an IT function, in that the IT team makes all budget decisions on cybersecurity.

Best Practices

Building on insights from the surveys cited above, we have developed a four-part approach to help organizations manage cybersecurity more effectively and formulate digital resilience strategies. It involves educating company leadership; developing a common language for management and corporate directors to discuss cybersecurity issues; understanding the difference between security and resilience; and making both security and resilience strategic corporate imperatives.

1. Educate company leadership. Cybersecurity risk shouldn't be treated strictly as an IT issue. In terms of risk management, both security and resilience need to be managed as issues of importance to the entire enterprise. Increasingly, directors and senior management are being held accountable for the security and resilience of networks and data. Board members must therefore understand the issues at stake and accept their fiduciary responsibility for their organization's cyberdefense posture. Company leadership must have an unambiguous understanding of the key elements of security and resilience. Both management and directors need to be aware of (1) the limitations of security (no practical cybersecurity strategy can prevent all attacks) and (2) the need for resilience (strategies to sustain business during a cyberattack and to recover quickly in the aftermath of a breach).

In order to be effective, directors need sufficient knowledge to understand and approach cybersecurity broadly as an enterprise-wide risk management issue. Directors need to understand the legal implications of cybersecurity risks as they relate to their company's specific circumstances.

2. Develop a common language. Boards must have adequate access to cybersecurity expertise, and their discussions about cybersecurity risk management should be a regular part of each board meeting agenda, with sufficient time allotted. Moreover, board engagement regarding cybersecurity issues should not be restricted to yearly or semiannual reports. A proprietary 2017 McKinsey survey on chief information security officer (CISO) and board reporting found that CISOs who had less-than-productive board interactions felt they needed more time with the board to explain and examine critical issues. One CISO who responded to the survey observed that "board members have to be able to ask questions that may be perceived by others to be ignorant." No question can be considered bad or inappropriate.

Digital security specialists, like all subject-area experts, must be able to communicate effectively with board members and other leaders. Meetings with CISOs and other security professionals mean nothing if

> Resilience (the ability to respond to incidents and breaches) should be prioritized over the forlorn hope of security alone as a silver bullet.

technical experts and directors are unable to understand one another. Information security executives must be capable of presenting information at a level and in a format that is accessible to nontechnical corporate directors. Ideally, assessments of cybersecurity, digital resilience, and cybersecurity budgeting should be expressed using metrics that objectively and unambiguously score issues of risk, reward, cost, and benefit. That said, directors should make themselves conversant in basic principles relevant to digital networking and security. The goal is for CISOs and other IT executives to engage in frank, mutually intelligible dialogue with the board and appropriate subcommittees. Wherever possible, IT and CISO reports should be focused on prioritized items on which the board can take action, especially those that can be addressed by the whole company.

3. Distinguish between security and resilience. Companies should create a clear distinction between digital security and digital resilience. Digital security focuses on essential security measures, including providing such traditional defenses as effective antivirus and antimalware software, adequate firewalls, and employee education in safe computing practices. Digital security is, therefore, a security issue.

In contrast, digital resilience is a business issue, which relates to how the whole organization conducts business in a digital environment. For example, balancing data accessibility with the necessity of protecting customer data and intellectual property involves a trade-off between security and interactivity that affects the customer experience, customer service, customer retention, acquisition of new customers, and so on. It is therefore a business issue. To the degree that an element of an organization's security implementation impedes business (for example, by arbitrarily restricting access to data), it may provide adequate security. But it is a poor business practice, which makes the company more liable to fail and therefore less resilient.

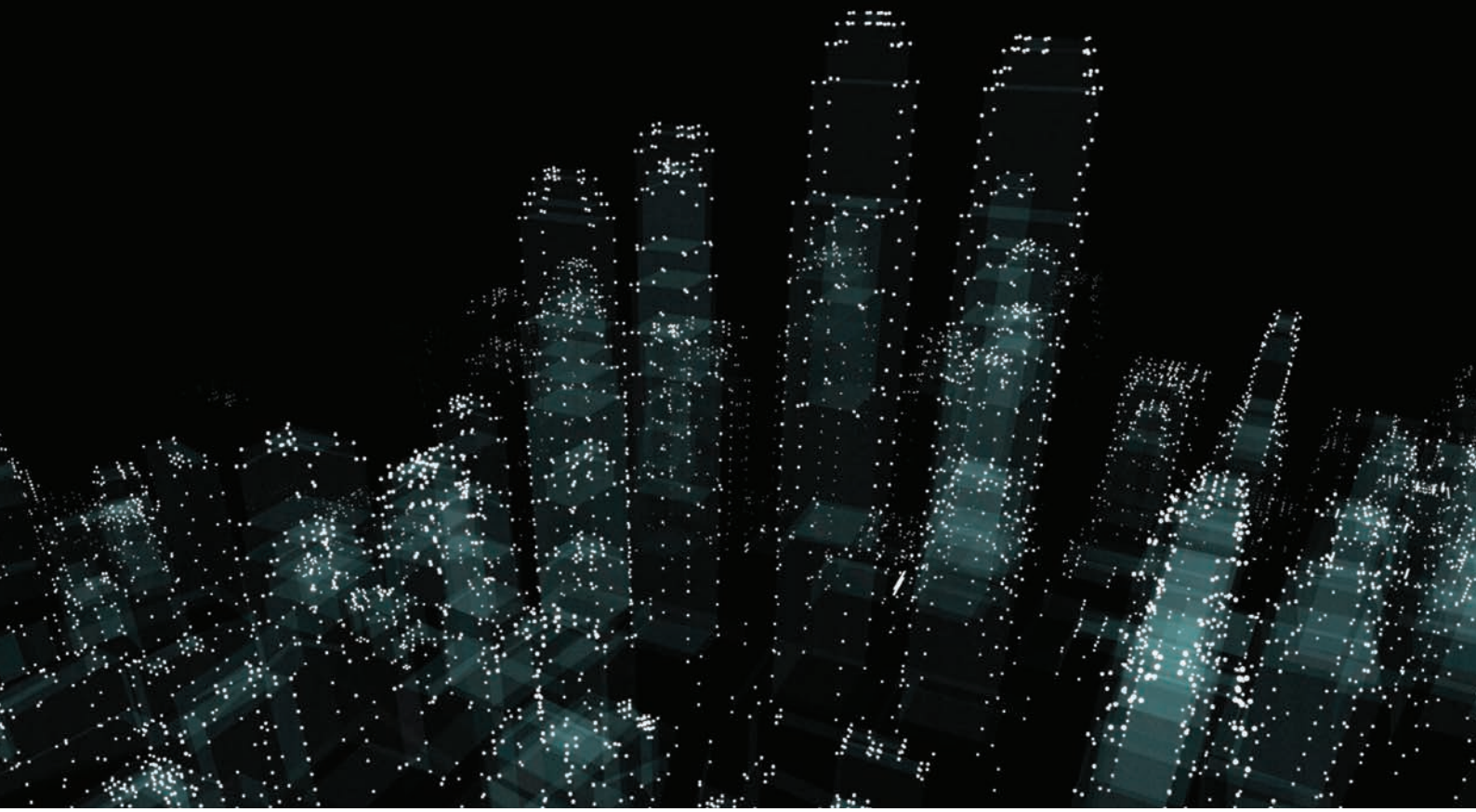
In assessing the organization's strategic cybersecurity policy, the board must balance resilience against security, with priority given to resilience. Over time, your network will be penetrated. Therefore, resilience (the ability to respond to incidents and breaches) should be prioritized over the forlorn hope of security alone as a silver bullet. Security will not enable you to continue to conduct business during a breach.Resilience will. The board must provide necessary leadership in advocating for whole-enterprise resilience policies and practices.

4. Make security and resilience strategic business issues. Directors must set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget. The board's discussions with management concerning cybersecurity risk should include identifying which risks to avoid, which to accept, and which to mitigate or transfer through insurance — as well as specific plans associated with each approach.

In concert with top management, the board should create a clear statement of its role in overseeing, evaluating, and challenging the company's digital security and resilience strategies. The statement should clearly define and assign responsibilities and must delineate the differing roles of the board and senior management. Within the board itself, cybersecurity and digital resilience must be the responsibility of all directors and not be relegated to a committee or subcommittee. Nevertheless, boards should consider assigning one cyber-savvy director to take the lead on issues of security and resilience, and, when recruiting new directors, companies should seek out people with appropriate cybersecurity expertise.

The board should continually reassess the overall budget for security and resilience and redirect investments as necessary. Given the reality that the number and seriousness of breaches are growing, it is clear that most organizations need to evaluate their cybersecurity investments more clearly and effectively. Improving the ability to measure and quantify cyber-related risks is vital to this step, because it allows cybersecurity and resilience to be evaluated for their impact on the entire business.

Ray A. Rothrock *(@rayrothrock) is CEO and chairman of RedSeal Inc.* ***James Kaplan*** *(@jmk37) is a partner in the New York office of McKinsey & Co.* ***Friso van der Oord*** *(@Frisovanderoord) is director of research at the National Association of Corporate Directors in Washington, D.C. Comment on this article at http://sloanreview.mit.edu/x/59221.*



Asking the right questions to define government's role in cybersecurity

There is no one-size-fits-all approach for governments to manage cybersecurity. But asking some key questions can help leaders get started.

Mary Calam, David Chinn, Jonathan Fantini Porter, and John Noble

Government leaders are increasingly aware that promoting prosperity and protecting national security includes providing cybersecurity. That means demonstrating that a nation, state, region, or city is a safe place to live and do business online. And it includes deterring cyberattacks, preventing cyber-related crime, and protecting critical national infrastructure while also maintaining an environment that makes technological progress easy.

It is a tall order. National security and criminality are different—and multifaceted—in the digital arena. Tools developed by governments to provide security are seized, weaponized, and proliferated by criminals as soon as they are released. Malware-development utilities are available on the dark web, enabling criminal activity even by those with only basic digital skills. Cyberthreats cross national boundaries, with victims in one jurisdiction and perpetrators in another—often among nations that don't agree on a common philosophy of governing the internet. And complicating it all, criminal offences vary, legal assistance arrangements are too slow, and operating models for day-to-day policing are optimized for crimes committed by local offenders.[1] Even relatively low-level threats can have impact on a vast scale.

Each country is addressing the challenge in its own way, just as companies tackle the issue individually. Approaches vary even among leading countries identified by the Global Cybersecurity Index, an initiative of the United Nations International Telecommunications Union. Differences typically reflect political and legal philosophy, federal or national government structures, and how far government powers are devolved to state or local authorities. They also reflect public awareness and how broadly countries define national security—as well as technical capabilities among policy makers. Despite such differences, our work with public- and private-sector organizations suggests a series of questions government leaders can ask to assess how prepared they are.

Who is accountable?

An effective national cybersecurity ecosystem crosses traditional institutional boundaries and includes a wide range of departments, agencies, and functions, both military and civilian. Many countries have yet to clarify who is accountable across all dimensions of cybersecurity or to impose a single governance structure. That lack of clarity can result in a confused response to crises and inefficient use of limited resources.

In our experience, a single organization should have overall responsibility for cybersecurity, bringing operational activity and policy together with clear governance arrangements and a single stream of funding. Particularly when responding to a cyberattack, clarity of leadership and decision making is vital to ensure the correct balance among helping victims recover quickly, taking measures to protect others (by increasing resilience and attacking the source of the attack), and performing a criminal investigation of those responsible. While some national and state governments have consolidated accountabilities into a clear structure, such as Estonia's Cyber Security Council, or have well-established and tested crisis-response mechanisms that they have adapted for use in cyberevents, as in Sweden, many others do not.

Key skills are often in short supply. Knowledge of the threat, resources, and authority to make decisions may all sit in different places across government. This reduces operational effectiveness and can also result in weak legislation, bad policy, and lack of investment. Some countries are starting to address these challenges. Germany, for example, has strengthened its Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) to lead its national cybersecurity strategy and establish shared cybersecurity services for government.

The United Kingdom's National Cyber Security Centre (NCSC) is also widely cited as a model for

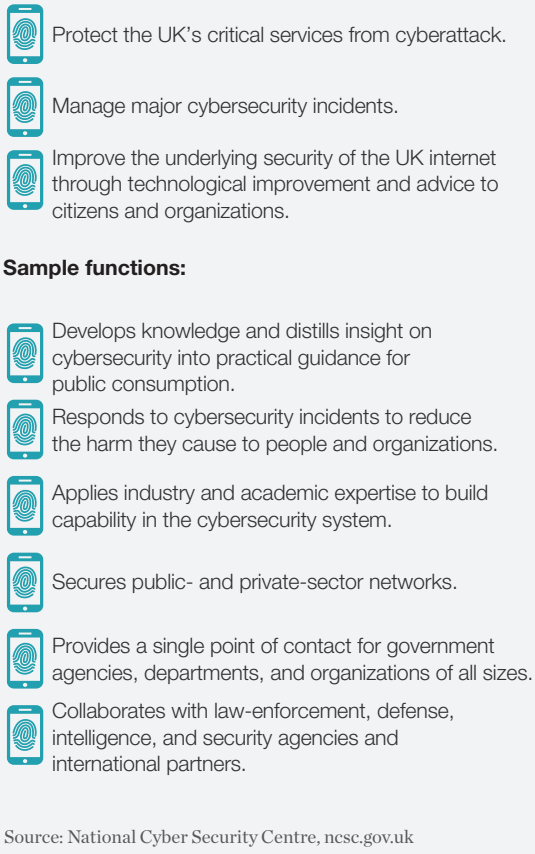
government-level cybersecurity. It brings together analysis, assessment, and crisis response to provide advice to critical national infrastructure organizations, businesses more broadly, and the public (exhibit). Its operating model involves both access to highly sensitive intelligence and dissemination of public information. And it brings together cybersecurity experts from government and the private sector in a single body.

Questions governments can ask include the following:

- Are lines of accountability and remits clear—both for policy and for crisis response?
- Is it clear how government priorities are decided and communicated?
- Is there a coherent, cross-government strategy? Is it reviewed and refreshed regularly?
- What performance metrics does the government have for the strategy? How are they monitored?
- What information does the government publish about progress on cybersecurity?
- Do the responsible parts of government come together regularly to agree on plans and review progress?

Exhibit

The National Cyber Security Centre leads the UK government's cybersecurity work.



Source: National Cyber Security Centre, ncsc.gov.uk

How centralized should you be?

Some countries have consolidated their audit and regulation functions in a centralized agency. Japan, for example, has its Cyber Security Strategic Headquarters, and Romania has its Association for Information Security Assurance. Others, such as India, have dispersed audit functions across multiple bodies. Both models can work, but as India's *National Information Security Policy and Guidelines* illustrates, a decentralized model—in this case, ministries are tasked to self-audit and bring in external auditors—requires clear national guidelines and standards. Israel's benchmarking and accreditation arrangements have also been key to raising standards across all sectors.

At the very least, governments can insist on reporting of cyberevents by victims and on sharing of vulnerabilities by suppliers into a single reporting, analysis, assessment, and response hub. In Germany, for example, federal legislators have sought to amend the law to require companies to register any cyberincidents in which they are a victim. Australia introduced a notifiable-data-breaches

scheme in 2017, making it a legal requirement to notify affected individuals and the Office of the Australian Information Commissioner of serious data breaches.[2] Ideally, governments will also make it easy for citizens and businesses to report such breaches through an automated platform to facilitate responses, advice, and feedback. Such platforms will also increase transparency around threats and steps to mitigate them.

Sectoral regulators have a more significant role to play in raising cybersecurity standards than has perhaps been recognized. There are moves toward a more regional approach to regulation, reflecting the cross-border digital world: for example, the EU Commission's proposals to develop a regionwide framework of cybersecurity standards.

Questions governments can ask include the following:

- To what extent do data protection and privacy regulations reflect the challenges of the digital age?
- How coherent is the approach to cyberregulation across different sectors of the economy and the wider information and communications technology supply chain? What advice does the government provide?
- Does the criminal law adequately address offenses committed online?
- How closely have policies and regulation been developed in partnership with private-sector operators who will be impacted?

How can you work with the private sector?

Governments do not have a monopoly on (or even the largest role in) cybersecurity. Open and trusting relationships with the private sector and academia are essential. Governments need commercial organizations to put more emphasis on cybersecurity, particularly as many companies operate across shared digital platforms. When companies and academic institutions have more knowledge, expertise, and capability, governments can work with them to develop the knowledge and tools needed to strengthen the ecosystem.

Many attacks could be prevented by basic security precautions and maintaining up-to-date patches, yet relatively few countries have invested significantly in education or training programs. One that has is Israel. Its investment in cybersecurity and integration of it into the educational curriculum, its extracurricular activities for high-school students, and its national military service have created a thriving, globally competitive, professional cybersecurity market. The Israeli government has also worked with the private sector, both to build capability and awareness and to grow the economy through the cybersecurity sector—by investing in R&D, for example.

Another example is Singapore, in which the National Cybersecurity R&D Programme supports public–private research partnerships. These are funded by $190 million Singapore dollars ($137.85 million) in the national strategy for developing research and the creation of the National Cybersecurity R&D Laboratory at the National University of Singapore.

And working with industry is also key to the United Kingdom's NCSC, where sharing of information and expertise includes a unique collaboration between a highly classified intelligence organization and the private sector. Its Cyber Essentials framework is a unified tool for assessing and guiding the development of cybersecurity for private-sector companies. Any company bidding for government contracts must confirm that it is compliant with the scheme. In conjunction with the Centre for the Protection of the National Infrastructure, NCSC also accredits companies under the government's cyberincident-response scheme as providers of technical-mitigation services.

Beyond that, few countries have made efforts to improve cybersecurity in small and medium-size businesses. These are likely to have the least resources and knowledge to build their own cybersecurity. Cybersecurity vulnerabilities in these companies can reduce their own economic value. But they can also be a weak link for bigger firms, creating vulnerabilities as they provide goods and services, including to governments.

Questions governments can ask include the following:

- To what extent does the government sponsor or invest in cybersecurity R&D?
- To what extent does the government support cybersecurity training, education, and awareness-raising for businesses, those in work, those in education, and those in the general population?
- Does the government engage the private sector or academia in its cybersecurity work? How effective are these partnerships?
- Does the government provide a platform for information sharing among organizations?
- What guidance on cybersecurity does the government provide to private-sector companies? How clear and coherent is that government advice to multiple stakeholders outside the government?

Are you operationally ready?

Countries vary dramatically in their ability to deal with cyberattacks and how they manage crises. It is often unclear how citizens and businesses should report cyberattacks or seek help. That confusion results in chronic underreporting and makes it hard to know the true scale of the problem and to build understanding to prevent future attacks.

To make matters worse, few countries yet have a workforce with sufficient cybersecurity skills to match demand. A study of the global information security workforce estimates that the world will fall 1.8 million short of the number of cyberskilled individuals needed by 2022.[3] Those who do have the relevant skills command premium salaries. And what cybersecurity skills others have are often concentrated in small pockets, such as in the intelligence agencies, and not available to governments more broadly. Most governments would do well to invest now in recruitment and training and to adopt more flexible approaches to recruitment and retention from outside traditional sources of talent. For the short term, consolidating existing scarce resources into a single place, as the United Kingdom's NCSC has done, can boost the value of available expertise, bringing the most highly skilled cyberexperts together as a single, government resource.

Some governments are taking a proactive stance on cyberdefense. From 2009, for example, the Australian government consolidated the internet gateways of various departments into seven certified "lead-agency gateways." These provide an initial foundation for consistent cybersecurity and a reduced attack surface.[4] The UK government launched a suite of initiatives in 2017 known as Active Cyber Defence, designed to "protect the majority of people in the UK from the majority of the harm caused by the majority of attacks, the majority of the time." As a result, UK-hosted phishing attacks fell by about 20 percent in the 18 months prior to February 2018, even as global volume itself rose by nearly 50 percent.[5]

Law-enforcement capabilities are often the least effective part of a government's response. Law-enforcement agencies spend up to 95 percent[6] of their budgets on staff, allowing only limited investment in technology. Staffing models are often highly traditional, making it more difficult to bring new technical skills into the organization at the scale and pace needed to address the volume of business that is cybercrime. Criminal-investigation

techniques, such as seizure of company servers in evidence, can hinder recovery from attack.

Questions governments can ask include the following:

- What are the emergency-response arrangements for a major cyberattack?
- Is there a national emergency-response team? Are there emergency-response teams for key sectors?
- What arrangements are there for the sharing of information to prevent and respond to a cyberattack? Are there clear reporting mechanisms for alerting the authorities to a cyberattack? What happens when a report is received?
- How often are response arrangements tested and exercised?
- How will the government ensure rapid recovery from a cyberattack?
- Which agency or agencies have responsibility for investigation of cyberattacks and online crime? What capabilities and capacity do those agencies have?
- What capabilities and capacity does the government have to gather intelligence on cyberthreats, assess them, and disseminate the analyses in a way that shapes action?

Where is multinational cooperation possible?

The transnational nature of cyberattacks means that even effective state or national coordination might not be sufficient. Mutual legal-assistance treaties were constructed for the predigital age, and mechanisms are too slow to keep pace with investigation of online crime. In 2013, a UN report on cybercrime estimated that mutual legal assistance took 150 days on average.[7]

Differences in political and ideological positions might make further progress on establishing international norms for the internet impossible. Instead, norms agreed by coalitions—such as the Tallinn Manual, sponsored initially by NATO—might emerge to shape responses to state-based attacks. Bilateral partnerships between other states, such as the one between the Czech Republic and Israel that focuses on the protection of critical assets and encourages private-sector innovation, are also developing. And a proposal before the European Parliament would strengthen its Agency for Network and Information Security in leading the union's cybersecurity efforts, including by having the agency act as a coordination hub for crises.

Questions governments can ask include the following:

- In which international forums on cybersecurity does the government participate?
- What arrangements with other nations do the government have to share information, best practices, or alerts?
- Does the government collaborate with other governments to prevent or investigate cybercrime? How effectively does it use mutual-legal-assistance mechanisms for cybercrime?

How have you defined critical national infrastructure?

If governments address no other aspect of cybersecurity, they must protect critical infrastructure. Many, such as the United States, have started to address cybersecurity from this perspective.[8]

What exactly constitutes critical infrastructure and the proper role of government in protecting it is not universally agreed upon. Some countries, such as France and Israel, have a centralized, regulatory approach toward companies perceived as critical. Both have legislation defining what is critical and related obligations. France formally designates both

public and private companies as critical operators, which must then meet a range of specified security requirements —and it defines the category broadly to include more than 250 public and private operating companies across 12 sectors.[9] Others, such as Switzerland, are more decentralized. In the United States, the Department of Homeland Security coordinates a national infrastructure-protection plan and requires sector-specific agencies to develop sector-specific plans. The Office of Infrastructure Protection offers tools and training for companies that are considered critical infrastructure. In the Czech Republic, the implementation of a cybersecurity legal framework has facilitated a more directive approach.

The digital world extends the definition of critical national infrastructure, lengthening the list of sectors and activities that are essential to the smooth functioning of the economy. Companies within those sectors might also have critical dependencies on other organizations, themselves outside the definition of critical national infrastructure. Yet few countries have domestic hardware and software industries of any scale, leaving them potentially vulnerable to cyberattack through foreign-owned infrastructure. Government decisions about inward investment might increasingly have to balance economic advantage with cybersecurity considerations.

Questions governments can ask include the following:

- Is there an agreed-upon definition of the critical national infrastructure?
- By what means does the government ensure the cybersecurity of critical infrastructure?
- How does the government support the companies and organizations it defines as critical?
- How does the government ensure compliance with security standards? How is that compliance measured?
- Is there a mechanism to ensure that cybersecurity is taken into account when considering major foreign-investment propositions?

Government's role in cybersecurity will only grow as the global demand and dependency on the internet and internet-connected devices continue to increase. With increasing threats and fewer opportunities to fail, governments must rise to the challenge to protect both national security and economic prosperity. ■

[1] *Real lives, real crimes: A study of digital crime and policing*, Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, December 2015, justiceinspectorates.gov.uk.

[2] "Notifiable data breaches scheme," Office of the Australian Information Commissioner, oaic.gov.au.

[3] *2017 Global Information Security Workforce Study*, Center for Cyber Safety and Education, iamcybersafe.org.

[4] "ASD certified gateways," Australian Signals Directorate, February 2017, acsc.gov.au.

[5] Ian Levy, "Active Cyber Defence – one year on," NCSC, February 5, 2018, ncsc.gov.uk.

[6] Review of published police-department budgets.

[7] "The mutual legal assistance problem explained," blog entry by Gail Kent, February 23, 2015, cyberlaw.stanford.edu.

[8] Interview with Daniel Prieto, former director of cybersecurity and technology, US National Security Council.

[9] *The critical infrastructure protection in France*, Secrétariat Général de la Défense et de la Sécurité Nationale, January 2017, sgdsn.gouv.fr.

Mary Calam is a senior expert in McKinsey's London office, where **David Chinn** is a senior partner and **John Noble** is an external advisor, and **Jonathan Fantini Porter** is a specialist in the Washington, DC, office.

Designed by Global Editorial Services.

How CEOs can tackle the challenge of cybersecurity in the age of the Internet of Things

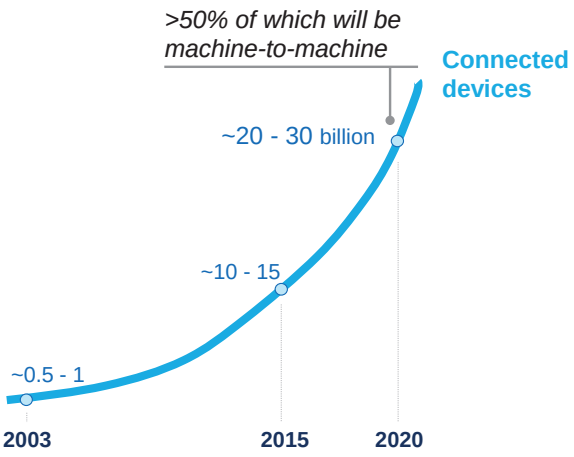
In the age of the "Internet of Everything", we are headed for a collision: billions of – often legacy – devices are being brought online, creating new vulnerabilities and headaches for executives. Here are six ways CEOs can take back control and avoid the collision.

In the last two decades, we have seen digitization rise to the top of the agenda of executive boards across the globe. As a result, cybersecurity skills and processes in most companies have also advanced – though at a slower pace. The fast growth of the so-called Internet of Things (IoT), however, is changing the game. Cybersecurity is more relevant and challenging than ever, and companies will need to pick up the pace of capability building in this area.

Companies are increasingly connecting their devices, products, or production systems, driving rapid growth of the IoT: conventional estimates put the number of connected devices at 20 - 30 billion devices in 2020, up from 10 - 15 billion devices in 2015 (Exhibit 1). The driver behind this is the enormous potential that the IoT has to make a company's products and services better or improve production efficiency. But this potential also comes with a sharp increase in security risk, taking the challenge of cybersecurity to another level for IoT technology users. To date, risking the confidentiality and integrity of information was a bigger concern than any risk regarding availability. In the IoT world, it is the other way around: lack of availability of key plants or – even worse – tampering with a customer product is the bigger risk. How can CEOs and senior executives hedge against that threat?

Exhibit 1: The number of connected devices globally will likely double over just 5 years

Estimated number of connected devices, including computers and smartphones



SOURCE: IHS; IDS; Gartner; ITU; McKinsey

The Internet of Things makes cybersecurity even more crucial and also more difficult to achieve

With the IoT, security challenges move from a company's traditional IT infrastructure into its connected products in the field and remain an issue through the entire product lifecycle – long after products have been sold. What is more, the industrial IoT, or Industry 4.0, means that security becomes a pervasive issue in production as well. Cyber threats in the world of IoT can have consequences beyond compromised customer privacy. Critical equipment, such as pacemakers and entire manufacturing plants, are now vulnerable, meaning that customer health and a company's total production capability are at risk.

As the IoT is connecting these additional "things" – be it products, production systems, or other devices – the sheer number of cybersecurity attack vectors increases dramatically. While in the past, the number of endpoints in a large corporate network would be somewhere between 50,000 and 500,000, with the IoT, we are talking about millions or tens of millions of endpoints. Unfortunately, many of these consist of legacy devices with either no or very insufficient security.

All in all, this added complexity makes the IoT a significantly more challenging security environment for companies to manage. If they are successful though, strong cybersecurity can become a differentiating factor in many industries, moving from a cost factor to an asset.

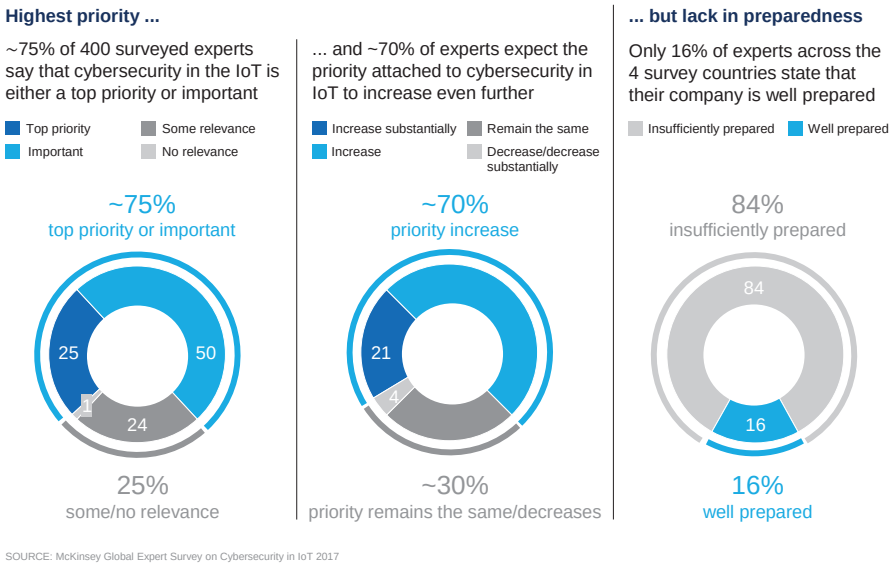
To explore the current perception of the relevance of and preparedness for IoT security, McKinsey conducted a multinational expert survey with 400 managers from Germany, the US, the UK, and Japan. The results indicate that there is a shocking gap between perceived priority and the level of preparedness.

- Of the IoT-involved experts surveyed, 75% say that IoT security is either important or very important – and that its relevance will increase – but only 16% say their company is well prepared for the challenge (Exhibit 2). Typically, low preparedness is also linked to insufficient budget allocated to cybersecurity in the IoT as indicated by the survey.

- Our interviews also revealed that along the IoT security action chain (predict, prevent, detect, react), companies are ill prepared at each step of the way. Especially weak are prediction capabilities (16% feel well prepared compared to 24 to 28% on prevent, detect and react).

- More than one-third of companies do not even have a cybersecurity strategy in place that also covers the IoT. The rest seem to have some sort of strategy but struggle with implementation.

Exhibit 2: **Striking gap between perceived importance of and readiness for IoT security**



SOURCE: McKinsey Global Expert Survey on Cybersecurity in IoT 2017

So why are companies' progress levels regarding cybersecurity implementation not commensurate with the size of the threat brought by IoT? As indicated by the survey results, the main reasons seem to be the following:

- **Lack of prioritization.** In general, the "act-now" mentality is in short supply among senior management. In many cases, IoT leaders have yet to make the business case for a specific IoT security strategy – i.e., a budget beyond what has already been allocated for a pre-IoT environment – which would, in turn, prioritize the effort and trigger the allocation of sufficient resources.

- **Unclear responsibility.** There needs to be a holistic cybersecurity concept for the entire IoT stack, but often no single player feels responsible for creating it. Between players, there is the question of whether initial responsibility lies with product makers or with suppliers. Within organizations, it has proven difficult to determine which unit (IT security, production, product development, customer service) should take the lead. Product or plant managers often do not have the cybersecurity expertise, while corporate IT does not have sufficient access to product teams or the industrial control systems (ICS) "behind the fence."

- **Lack of standards and technical skills.** There are some industry working groups, but IoT security standards are still largely nonexistent. Even if there were standards in place, the technical competence to implement them – the required mix of operational technology and IT security knowledge – is in very short supply.

With the advent of the IoT, cybersecurity affects the entire business model. Adequately addressing the threat means bringing together several business perspectives – including the market, the customer, production, and IT. Most often, the CEO is the only leader with the authority to make cybersecurity a priority across all of these areas. We believe that the issue of cybersecurity in many cases will require senior-executive or even CEO initiative.

Six recommendations for CEOs

There is no silver bullet for tackling cybersecurity in the IoT. However, three strategic lenses can help CEOs think about IoT security, and three actions can help CEOs and senior leaders set their organizations up for success:

Three ways to think strategically about cybersecurity in the Internet of Things

1. Understand what IoT security will mean for your specific industry and business model

Across all industries, a certain minimum level of IoT security will be required as a matter of "hygiene." As such, the recent "WannaCry" attack by and large compromised organizations with legacy operating systems, such as Windows XP, which had not appropriately been patched. Simple patch management – a matter of adequate IT management, not sophisticated cyber defense – is something that is expected as "hygiene" from companies, without customers needing to pay a price premium for it."

However, we think that there is potential for treating security as more than just "hygiene." In the last decade, many companies have witnessed how IT evolved from a cost center to a source of real differentiation, driving customer satisfaction and willingness to pay. A similar change could lie ahead for IoT security, and in an increasing number of industries, we are already witnessing it today. One example is the physical security industry. Door lock companies can already today demand a price premium for products with especially strong cybersecurity features, as cybersecurity can make or break the main function of the product.

Effective IoT security solutions consider an organization's business model, where it lies in the value chain, and the industry structures in which it operates. For examples of how industry impacts IoT security, please refer to the Text Box.

Text Box: **More trust, less downtime – examples for the role and relevance of IoT security by industry**

The goal of the IoT security strategy varies by industry and company type. Industries differ in their approach, depending on many factors, such as the role of cybersecurity in differentiating the product, the supply chain structure and incentives, and the level of maturity reached to date.

- *For an energy utility,* IoT security is mostly a production play, as it will mean dealing with a large installed base of legacy production systems that were never designed to be connected and, in turn, not designed with the defense against cyber attacks in mind. What is more, legacy systems have little additional capacity (e.g., computing performance, memory) that could be used for added security measures, and they are

often not accessible in the field. To still reap the huge benefits from connecting these systems, targeted counter-measures need to be taken. Process industry players in particular have leveraged their innate strength in industrial safety for creating new processes and safety measures, creating redundancy, and "sandboxing" key systems to avoid entire system failure. Challenges for industrials lie in the lack of cybersecurity expertise of many component suppliers and the lack of standardization incentives for many integrators.

- *For automotive OEMs,* IoT security is also a product play, and will become the new quality management for the era of connected cars. OEMs are facing a unique level of challenges given the increasing complexity of their product: A modern car is comprised of between 30 and 100 electronic control units (ECUs) and hundreds of millions lines of code – a complexity in which even the best programmers cannot avoid vulnerabilities. What's more, the automotive industry has one of the most fragmented supply chains. The 30 to 100 ECUs could easily be sourced from more than 20 different suppliers, creating additional complexity. Thus, a holistic concept is needed, one that addresses two aspects. On the one hand, cybersecurity needs to be embedded already in the design and development of the product, as well as in the maintenance and response architecture. On the other hand, OEMs must work closely with their ecosystem, e.g., with other industry players and regulatory bodies to set up standards, and with the end users who are directly involved in protecting their cars (e.g., by keeping software updated). However, solutions will have to scale well and be cost effective, as OEMs have to contend with users' limited willingness to pay for added cybersecurity.[1]

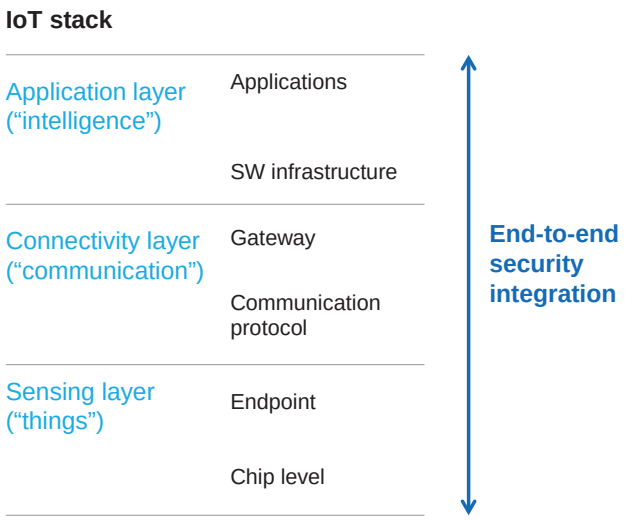
CEOs need to ensure they understand the role and relevance of IoT security in their industry and how they can monetize it in alignment with their specific business model. A thorough understanding of what IoT security means for a company cannot end on the strategic level though. CEOs need to be aware of the main points of vulnerability along the cybersecurity action chain of predict, prevent, detect, react. Typically, an overview of the top attack scenarios for a specific company and an understanding of attackers and their motivation will be a good base for further strategy development and budget allocations. Security investments must be targeted according to the risk most detrimental to the specific business or industry.

2. Set up clear roles and responsibilities for IoT security along your supply chain

IoT requires a holistic cybersecurity concept that extends across the entire IoT stack, i.e., all layers of the application, communication, and sensors. Of course, each individual layer needs to be secured, but companies also need to prepare for cross-layer threats (Exhibit 3).

1 For further details on cybersecurity in the automotive industry, please refer to the report "Shifting gears in cybersecurity for connected cars" by our McKinsey colleagues Wolf Richter, Simone Ferraresi and Corrado Bordonali

Exhibit 3: **IoT security requires layer-specific as well as cross-layer solutions**



SOURCE: McKinsey

This will require a strategic dialogue with upstream and downstream business partners – whether suppliers or customers – to sort out responsibilities for security along the entire supply chain. A starting point for this discussion should be identifying the weakest links in the holistic model; from an attacker's point of view, these will be targeted first to harm the entire chain. Who then takes on which role should depend on who has the competence and who has the incentives, which might include a monetization model. Industry players active in each part of the IoT stack bring certain advantages they can build on to provide an integrated solution:

- Device and semiconductor manufacturers active at the lower level of the stack can build on their design capabilities of low-level (hardware) security as an advantage for designing higher (software) security.
- Network equipment manufacturers profit from the fact that many key competencies in transport-layer security design are applicable to the application layer. Beyond that, they can build on their hardware design capabilities for offering an integrated solution.
- Application designers can leverage their control of application interfaces and/or customer access as an advantage in defining low-level architectures.

3. Engage in a strategic conversation with your regulator and collaborate with other industry players

A company's cybersecurity creates externalities that go far beyond the effects on the company's performance itself and thus needs to be tackled across the classic government-business divide. Most current cybersecurity standards fall short because they are neither industry specific nor detailed enough, and they neglect most layers of the IoT stack, including production and product development. Regulators will eventually be stepping in to address this gap, and companies need to get involved in the discussion, or even better, set the tone.

Industry leaders can shape these structures by proactively getting key players in the industry together to establish IoT security standards for their specific industry. Partnerships with other players, including competitors, can also lead to a mutually beneficial pooling of resources above and beyond official industry standards. For example, in the banking sector, one company got several competitors together to set up "shared assessments" to evaluate the security technology vendors, resulting in enormous efficiency gains for both the banks and the suppliers. Another example from the banking sector is FS-ISAC, an information community through which competing banks share information on security weaknesses, attacks, and successful countermeasures.

Three ways to set your organization up for success in IoT security

4. Conceive of cybersecurity as a priority for the entire product lifecycle, and develop relevant skills to achieve it

Security needs to be part of the entire product lifecycle, starting with product design, moving through the development process, and continuing each day of the product's use. Fundamental to the security of products while in the field is "security by design" in the product development stage. Security also needs to be ensured during the production/manufacturing process, given the role of Industry 4.0 in driving the proliferation of IoT on shop floors and in other production settings. Lastly, a concept is required for securing the products after they have been sold. To this end, companies need a strategy to deliver security patches to products in the field via, for example, over-the-air update capabilities.

Achieving cybersecurity along the entire product lifecycle requires organizational and technological changes. The organizational component involves clear responsibility for cybersecurity in the product and production environment. A few companies have acted by giving the CISO responsibility for both IT and OT cybersecurity. Whatever the structural setup: an alignment of goals is crucial, since strong collaboration between the CISO function and the respective other departments, be it product development, production, or even customer service, will be required. Additionally, new roles should be created that systematically integrate security into all relevant products and processes. A European telco and media company, for example, is leveraging large-scale training programs conducted by its core CISO organization to create a community of "security champions" throughout the organization. These security champions get additional decision making authority within their teams, e.g., product teams, as a result of achieving "cybersecurity capable" status. The CISO organization is able to leverage these trainings to grow its reach by a factor of 4.

5. Be rigorous in transforming mindsets and skills

Institutionalizing the notion that security is "everyone's business" starts at the top, with executives role-modeling security behavior and also cultivating a culture where security is constantly evolving and the identification of weak spots is rewarded rather than punished. To that end, some companies have implemented programs that reward employees for identifying security vulnerabilities.

Additionally, CEOs need to ensure that security-specific knowledge and qualifications become a standard requirement for employees in IT, product development, and production. On the one hand, additional training programs for current employees may help; on the other hand, specific IoT security talent needs to be developed. In the age of IoT, cybersecurity specialists must understand product development and production as well as IT security. To develop these new crossover skills at scale, companies should consider working with other players in the industry to, for example, create university programs and vocational training curricula.

6. Create a point-of-contact system for external security researchers and implement a post-breach response plan

Companies need to implement a single, visible point of contact for IoT-security-related notifications or complaints. In the last two years, and especially in the IoT context, there have been numerous examples of security researchers trying to notify a company several times after discovering a breach and the company either not following up at all or the researcher being handed from one department to the next without finding someone who could take responsibility for the matter.

In addition, companies need a response plan in place for different attack scenarios. Recent examples have shown that the fallout from an unprofessional response to an incident has been more damaging than the incident itself. In an IoT world, incidents can affect the heart of a company's operations, so cybersecurity, especially with regard to IoT incidents, needs to be part of business continuity management and disaster recovery planning. Maybe most importantly, a strong communication strategy needs to be designed, one that is scenario specific and delivers current, transparent, and appropriate messaging to customers, regulators, investors, and potentially the general public.

□□□

Cybersecurity remains much talked about, yet underleveraged as a differentiating factor on the business side. With the advent of the IoT, there is real opportunity to move ahead and designate the security of products, production process, and platforms as a strategic priority. The breadth of the challenge spans the entire supply chain and the whole product lifecycle and includes both the regulatory and the communication strategy. For CEOs in leading IoT organizations, we believe cybersecurity should be at the top of the agenda until rigorous processes are in place, resilience is established, and mindsets are transformed.

Authors

Dr. Harald Bauer
Senior Partner, Frankfurt
harald_bauer@mckinsey.com

Dr. Gundbert Scherf
Partner, Berlin
gundbert_scherf@mckinsey.com

Valerie von der Tann
Engagement Manager, Berlin
valerie_tann@mckinsey.com

Laura Klinkhammer
Associate, Cologne
laura_klinkhammer@mckinsey.com

The authors wish to thank Venky Anant, Tucker Bailey, James Kaplan, Mark Patel, Chris Rezek, Wolf Richter, Rolf Riemenschnitter, and Dominik Wee for their valuable contributions and for sharing their perspectives.

Advanced Industries
June 2017

Design contact: Visual Media Europe
www.mckinsey.com

Shifting gears in cybersecurity for connected cars

Automotive & Assembly April 2017

To secure products across the supply chain, the automotive sector must develop new ways to collaborate.

Corrado Bordonali,
Simone Ferraresi,
and Wolf Richter

Although connectivity has the power to enrich societies, economies, industries, and companies, it is not without its risks. Particularly in the automotive sector, cybersecurity threats are real, and for several basic reasons. Products are becoming more complex, with an increasing number of electronic control units and lines of code. Connectivity is burgeoning, with dangers at every turn. The supply chain is fragmented, so policing security is hard. And the integration of automotive systems can compromise any specific countermeasure.

We believe that the sector needs a holistic, two-front approach to cybersecurity. On the first front, solutions ought to address the design of the product, the way it's developed, and the maintenance-and-response architecture. On the second, OEMs should focus more effectively on the automotive environment at the sector level (for instance, by cooperating among themselves), on the concerns of regulatory bodies, and on the mind-sets of final users, who must actively protect their cars.[1] An OEM's chosen approach should always preserve innovation, the user experience, and cost competitiveness.

Products can be secure only if they are designed with security in mind. Quick fixes may add costs, much more complexity, and sometimes weight. They could also be relatively easy to circumvent because they may not solve the vulnerability challenge structurally—the architectural issues, for example. Penetration tests are at best a temporary solution. Other sectors (such as aviation, trains, and critical infrastructure) have adopted a variety of approaches to design, not just technologies, because no one "silver bullet" can eliminate cybersecurity issues. What's clear is that future automotive designs have to be "cybersecurity natives," integrating these concerns into the earliest stages of development.

A secure design, while necessary, won't guarantee full security over time. Solutions are effective only if they are implemented consistently, and high-quality components—software and hardware alike—implement the design. This requirement calls for a sound and managed development process, including reinforced collaboration between product-security teams and corporate IT-security teams. OEMs must thus create and enforce strict guidelines to minimize the chances of bugs and software-security gaps and to make modifying or patching systems easier.

[1] For example, by updating the software.

That's why over-the-air (OTA) updates—which have recently become available for some cars, though often for limited parts of the software—are clearly essential for connected systems: they help OEMs to counter attacks quickly and to eliminate specific vulnerabilities before malefactors can exploit them. These benefits have a price, however: implementing support for OTA updates is quite complex and expensive, both for cars and the back-end infrastructure. OEMs must therefore trade off the desired level of effectiveness (and the systems that can be updated) against the costs. That calls for a deep understanding of the architectures and peculiarities of these systems.

OEMs, which exclusively control the relationship with customers and are usually the final system integrators, bear the ultimate responsibility for integration risk and for ensuring that secure stand-alone systems aren't vulnerable when connected. These companies must ascertain that security practices have been implemented consistently throughout the full value chain, including suppliers. Procurement executives must therefore learn to negotiate over the cybersecurity features of components as rigorously as they do anything else. OEMs should also play an active role in shaping the sector's future standards—both regulations and best-practice guidelines.

In many sectors, including oil and gas, financial services, and aviation, alliances help companies to deal with regulators and to share intelligence on threats and vulnerabilities, both internally (among OEMs and suppliers) and externally (with regulatory bodies and the media). Such alliances also facilitate prompt responses to novel threats. Some automotive companies are already creating alliances; other OEMs and suppliers should consider joining them.

But the OEMs' best efforts will succeed only if car drivers understand the importance of cybersecurity, play their role in realizing it, and avoid anything that could facilitate threats. Unfortunately, recent research shows that despite this issue's resonance in the automotive community, car drivers largely ignore the problem.[2] OEMs must consider tools to increase their awareness by cultivating a culture of cybersecurity (through in-car screen guidance and functional inhibitors, for example) or by pushing for the introduction of cybersecurity questions in license exams.

As for regulators, though an increasing number of them have started focusing on cybersecurity in the automotive sector, the definition of formal rules is still at a preliminary stage. Since OEMs and relevant suppliers have a mutual interest in effective and realistic security guidelines, they should continue their collaborative discussions with regulators (for instance, by leveraging industry alliances). Who knows what might happen if, for example, scary but ill-informed newspaper headlines inspired new cybersecurity rules. OEMs and their suppliers should therefore help regulators to understand the actual risks and the countermeasures already in place to deal with them.

[2] Andy Greenberg, "Only one in 4 Americans remembers last year's epic Jeep hack," *Wired*, March 8, 2016, wired.com.

Critical resilience: Adapting infrastructure to repel cyber threats

As the digital world becomes increasingly connected, it is no longer possible for infrastructure owners and operators to remain agnostic in the face of evolving cyber threats. Here's what they can do to build an integrated cyber defense.

James Kaplan
Partner, New York
McKinsey & Company

Christopher Toomey
Vice president, Boston
CP&I Major Projects
McKinsey & Company

Adam Tyra
Expert, Dallas
McKinsey & Company

The BBC recently reported that researchers have discovered major security flaws—which affect flood defenses, radiation detection, and traffic monitoring—in the infrastructure for major cities in the United States and Europe.[1] Of those flaws, nearly ten are deemed "critical," meaning that a cyberattack on these systems would have a debilitating impact on essential infrastructure, including power grids, water treatment facilities, and other large-scale systems. It seems like the stuff of disaster films: A major city loses power. Huge amounts of the population panic. The roads clog. Planes are grounded. Coordinating a rescue effort—even communicating with the public—would be a colossal task.

While such scenarios may seem far-fetched, they are indeed reality. In 2015, Ukraine's power grid was the target of such an attack—in the hours that followed, nearly a quarter-million people were left without electricity—yet this and similar stories rarely reach the public consciousness.[2] As a result, there is little pressure from constituents and cyber threat operators are not top of mind.

The number and severity of cyber threats continue to grow exponentially as the world becomes increasingly connected. According to recent estimates from the research firm Gartner, by 2020 there will be 20.4 billion internet-connected devices, and approximately 37 percent of these will be used outside consumer settings—including large numbers dedicated to infrastructure monitoring and control.[3] While the proliferation of connected devices has created unprecedented productivity and efficiency gains, it has also exposed previously unreachable infrastructure systems to attack from a range of malicious groups with varying motivations.

Owners, planners, builders, and financiers routinely channel ample resources into mitigating any number of risks to an infrastructure asset. Yet they rarely if ever place as much care into anticipating potential cybersecurity incidents. There are many reasons for the lack of attention to cybersecurity. One is a common consensus in the industry that the technology governing physical infrastructure is fundamentally different from the technology used in other industries. In reality, it is not. While new technology solutions are emerging to deliver and operate infrastructure, these solutions still rely on the operating systems common to nearly all sectors.

Similarly, infrastructure leaders tend to think that they need industry-specific expertise when it comes to hiring cybersecurity specialists. But while having industry-specific expertise is helpful, it should not be viewed as essential; the tool kits across industries are largely the same. Owners and operators might not have the resources they need to make significant strides in their cybersecurity programs if they focus only on recruiting highly specialized talent, especially as it relates to people who can design and execute responses to cyber threats.

As it stands, infrastructure has a long way to go to catch up to other industries in terms of future-proofing for a cyber threat. To accomplish this, cities and organizations will need to integrate their defenses. They will need to recruit and retain new talent and develop a cybersecurity program. Furthermore, ensuring that infrastructure achieves and sustains resilience to cyberattacks in the midst of rapid digitization requires that designers and operators make a proactive mindset shift about cybersecurity—before hackers impose one.

Vulnerabilities do not expire or become obsolete

When considering digitized infrastructure, owners typically focus their energies on envisioning the improvements in efficiency and customer experience that can be realized by new technologies. Cyber

attackers, on the other hand, focus on uncovering the ways that new technology use cases rehash the same weaknesses and vulnerabilities of the old. Indeed, the problems faced by cybersecurity professionals—for example, authenticating users or protecting sensitive data from unauthorized access—largely stay the same over time, regardless of the technology in question. In a 2018 report, vulnerability scanning firm EdgeScan noted that approximately 54 percent of the vulnerabilities that it identified in customer networks that year originally became publicly known in the past ten or more years.[4] This is the cybersecurity equivalent of allowing yourself to remain susceptible to an infectious illness a decade after a vaccine becomes available. As a result, attack patterns that worked during the previous year will likely still work (in a modified form) against newly digitized infrastructure connecting to the internet today.

The takeaway is that infrastructure owners, engineers, and operators, many of whom are acutely aware of cybersecurity vulnerabilities in their information technology environments, must consider the operational technology that powers their digitized infrastructure to be vulnerable to the same issues.

Hackers have long exploited this insight. In February 2017, a cybersecurity researcher developed a ransomware variant that could successfully target and manipulate the control systems of a water treatment plant.[5] In theory, his malware could be used by an attacker threatening to poison a municipal water supply unless the ransom was paid. This may sound like a familiar scenario, because ransomware has been an increasingly common and disruptive cyber threat faced by business for the past three years. Even so, it is not possible for leaders to test for every possible risk or outcome. They will need to limit their attention to the most pressing threats. And the best way to determine those threats is to look at the issues affecting other, similar deployments of technology. By identifying similarities between new and old use cases for technology, infrastructure designers can ensure that cyber risks that were resolved in previous years don't recur in the infrastructure space.

Building cyber defenses for infrastructure

To build adequate defenses, infrastructure owners and operators should start by assuming that a cyber attack is imminent. Then they must build a unified, integrated cyber defense that best protects all relevant infrastructure assets. Going through the process of identifying what is relevant will often require the asset owner to understand what supporting infrastructure is also vulnerable—critical utilities, for instance—and ensure that it is reasonably protected as well. For example, a hotel that relies entirely on a local utility for its power supply may decide that it makes sense to find a redundant power source. In turn, the asset owner will be able to look beyond what would strictly be considered their responsibility, and consider the broader network in which they are included. By going beyond their "battery limit," so to speak, the hotel can gather more information about relevant vulnerabilities and threats.

Moreover, both utility owners and governments can work together in this area to create more—and more widely distributed—utility networks. If they can better isolate network vulnerabilities, they can help ensure service to any undamaged portions.

Start with the assumption that a cyber incident will occur

Since the March 2011 earthquake and tsunami that caused widespread damage to the northeast coast of Japan, including the Fukushima Daiichi nuclear plant, the country has constructed an estimated 245 miles of sea walls at a cost of approximately

$12.7 billion.[6] The same prudence is needed to protect infrastructure from cyber attacks. As a point of comparison, one cybersecurity research organization estimates that the cost of ransomware damages alone in 2019 could exceed $11 billion.[7] But in spite of an increasing torrent of cyber attacks afflicting internet-connected businesses and individuals globally, infrastructure owners largely continue to think of a cyber-attack as a mere possibility rather than a certainty.

By starting with an assumption that a future cyber attack *will* degrade, disable, or destroy key infrastructure functionality, owners and contractors can take action early to build resilience into their systems. For example, backups can be implemented for critical connected components, computers can be designed to fail safely and securely when compromised, and preparedness exercises can train operators to act decisively to ensure that cyber attacks aren't able to compromise connected infrastructure to threaten lives or property.

When planning incident response, leaders should look beyond the infrastructure sector for lessons learned from cyber incidents that caused outages in other sectors of the economy. The steps required for shipping firm Maersk to respond to a June 2017 ransomware outbreak are particularly informative. In order to purge itself of malware, the company executed a ten-day effort to overhaul its entire information technology (IT) infrastructure—a software reinstallation "blitz" that should have taken approximately six months under normal conditions.[8] While infrastructure owners are unlikely to have the same technology footprint as a global shipping company, understanding the steps required to respond to a major cyber incident can provide perspective on the level of effort and courses of action that may be required to respond to an attack in the infrastructure space.

An integrated defense is the only defense

Every infrastructure network has an associated IT network within which its owners and operators conduct their day-to-day business, such as sending and receiving emails and writing reports. Likewise, most organizations operating an IT environment—and some organizations operating a connected infrastructure environment—have cybersecurity programs in place to protect their data and technology assets. However, two discrete cybersecurity programs can't match the effectiveness of one unified program to protect both environments.

While the technology components deployed in the IT and infrastructure environments may differ significantly in their purpose and complexity, they're vulnerable to the same risks when connected to the internet. In the best known instance of this from recent years, hackers that breached the network of retailer Target Stores in 2013 made their initial entry through an internet-connected control system for the stores' air conditioning systems.[9] By connecting the infrastructure management network to the network through which Target executed its corporate functions and processed credit card payments, IT staff unwittingly elevated a minor risk into one with the potential to create catastrophic losses. While the Target breach was a case of attackers traversing an infrastructure environment to target the IT environment, attackers could just as feasibly have made the opposite leap, compromising an office network before leveraging connections to attack infrastructure.

Why wasn't Target's HVAC system cordoned off from its payment system network? The efficiencies gained from connecting networks are clear and undeniable, so preventing these types of technology interactions isn't a practical option. Instead, infrastructure owners must craft a cybersecurity program that takes a comprehensive view of all technologies in

the environment by working to understand how they're connected to each other and to the outside world. Then they must deploy security controls and defensive countermeasures to mitigate risks attributable to IT and connected infrastructure in a prioritized fashion.

Just as designers must take into account the physical resilience of infrastructure assets, owners should integrate cyber resilience. One way of ensuring this happens is to make cyber resilience an integral part of the design process. In addition to better incorporating protections, the Internet of Things has created a digital, keyboard-based operating culture that is often devoid of manual alternatives. Asset owners, notably those responsible for critical infrastructure, such as power plants and hospitals, should consider establishing core functionality that is either resistant to cyber attacks or that allows for an asset to more readily withstand the impact of a cyber attack. Some hospitals in urban areas, for example, might have digitally controlled HVAC systems, including all vents and windows. Having windows that can be opened manually—with the option to override digital controls and use mechanical switches or toggles to open them—could help create ventilation and allow operations to continue in the event of a cyber attack.

How to get started

We've identified three key steps for infrastructure owners starting the process of building their integrated cyber defense.

Recruit new talent. The cybersecurity industry is already severely constrained for talent, and infrastructure owners and operators often compete against other industries that offer higher-paying positions. Therefore, infrastructure groups need to get creative with where they look for cybersecurity talent. Infrastructure players might look to "cyber utilities," for instance, which are industry-aligned working groups that pool information and resources to improve cybersecurity effectiveness for their membership. These member-driven organizations—such as the Intelligence Sharing and Analysis Centers (ISAC) sponsored by the US Department of Homeland Security—were originally intended to serve as industry-sector-aligned cyber threat intelligence fusion centers for member companies. So, for instance, banks could join the financial services ISAC. However, the concept could be employed on a smaller scale to allow infrastructure owners in a particular region to share cybersecurity talent and resources for cybersecurity functions besides intelligence. For example, a cyber utility consortium in any given metropolitan area—hypothetically comprising a city government, a municipal utility district, and a publicly traded electricity company—could share a single cybersecurity team, rather than each entity competing to recruit their own.

Form a cyber response team. The first hours after the discovery of a cyber attack are the most critical in effectively mitigating losses, and their importance is magnified in the case of attacks against infrastructure where loss of life may be a possible second- or third-order effect. For this reason, selection and training of an incident response team *before* an incident occurs is key. Teams should include cybersecurity professionals skilled in cyber investigation and analysis, but they must also include experts familiar with the broader functioning of the infrastructure asset itself along with leaders who can make timely decisions about issues such as whether to shut down infrastructure or notify the public about an incident.

Cyber response teams should be subjected to regular incident exercises to build the muscle memory necessary to respond effectively and to uncover

potential weaknesses in response processes. The cyber utility concept described above might be specifically helpful in forming a response team, since skill sets such as cyber forensics are in particularly short supply.

Cultivate a mindset shift across the organization. Cybersecurity for infrastructure is often seen as a trendy topic—every other year something happens that makes headlines and then, weeks later, the industry has returned to the status quo. Owners and operators take a hard look at the situation and then lose interest when no clear path forward presents itself. This needs to change.

Two specific actions are key in beginning and subsequently sustaining the mindset shift required. To begin the mindset shift, organizations need to develop a perspective on what a cyber attack would actually look like *for them*. Cyber war gaming and table top exercises have long been a staple for developing this perspective in corporate environments, and they can be similarly effective for infrastructure. Effective exercise scenarios emulate the actions of timely real-world attackers to impose a series of difficult decisions on the team, creating numerous (and sometimes painful) learning opportunities. Through cyber war gaming, participants often learn that their organization lacks key response elements such as clear delineation of responsibilities in crisis situations, plans for how and when they should communicate with stakeholders or the public, and even procedures for shutting down compromised systems. The best programs deepen learning by establishing a regular cadence of exercises (e.g. quarterly or semi-annually) to accustom participants to the stress and confusion of a crisis situation and to continuously identify opportunities for improvement.

Once organizations begin to understand how bad an attack could be for them, they must remain focused on steady improvement. To sustain the mindset shift begun with cyber war games, infrastructure owners must integrate cyber resilience metrics into their regular performance measurement programs. As the cliché goes, "What gets measured gets done." By requiring their teams to continuously evaluate the organization's cyber resilience, leaders can ensure that the topic remains front of mind. Leading organizations take this a step further by integrating cyber metrics into the performance metrics for *specific individuals*, creating a culture of personal responsibility where bad cybersecurity can actually affect managers' compensation and prospects for promotion.

In a world steadily digitizing and becoming more interconnected, cyber attacks should be thought of as a certainty akin to the forces of nature. Just as engineers must consider the heaviest rains that a dam may need to contain in the next century or the most powerful earthquake that a skyscraper must endure, those digitizing infrastructure must plan for the worst in considering how an attacker might abuse or exploit systems that enable infrastructure monitoring and control. This shift in thinking will begin to lay the path to connected infrastructure that is resilient by design.

Cyber threats don't become obsolete or irrelevant in the same way that the technology underlying them does. So, in the context of cybersecurity, future-proofing infrastructure is primarily about ensuring that the steps taken to inject resilience into a system remain connected with the relevant threats of today and yesterday, rather than threats that may manifest tomorrow.

By starting with the assumption that not only will cyber attacks against infrastructure occur but also that they will likely be successful, infrastructure designers and operators can learn to trap many risks before they have the chance to develop into catastrophes. To do this, infrastructure owners and operators must first understand how old vulnerabilities will affect new technology and then develop integrated cybersecurity plans to apply the appropriate level of protection to their entire technology environment. The result will be safer and more resilient connected infrastructure delivering reliable services to customers for years to come.

[1] "Dave Lee, "Warning over 'panic' hacks on cities," BBC, August 9, 2018, bbc.com.

[2] "Ukraine power cut 'was cyber-attack'," BBC, January 11, 2017, bbc.com.

[3] *Gartner says 8.4 billion connected "things" will be use in 2017, up 31 percent from 2016*, Gartner, 2017.

[4] *2018 vulnerability statistics report*, edgescan, 2018.

[5] Michael Kan, "Researcher develops ransomware attack that targets water supply," CSO, February 14, 2017, csoonline.com.

[6] Megumi Lim, "Seven years after tsunami, Japanese live uneasily with seawalls," Reuters, March 8, 2018, reuters.com.

[7] Steven Morgan, "Global ransomware damage costs predicted to hit $11.5 billion by 2019," Cybersecurity Ventures, November 14, 2017, cybersecurityventures.com.

[8] Charlie Osborne, "NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs," ZDNet, January 26, 2018, zdnet.com.

[9] Brian Krebs, "Target hackers broke in via HVAC company," Krebs on Security, February 5, 2014, krebsonsecurity.com.

Cyber leadership

North America

Venky Anant, Partner
Venky_Anant@mckinsey.com

Tucker Bailey, Partner
Tucker_Bailey@mckinsey.com

Jim Boehm, Expert Associate Partner
Jim_Boehm@mckinsey.com

Salim Hasham, Partner
Salim_Hasham@mckinsey.com

Piotr Kaminski, Senior Partner
Piotr_Kaminski@mckinsey.com

James Kaplan, Partner
James_Kaplan@mcKinsey.com

Harrison Lung, Partner
Harrison_Lung@mckinsey.com

Derek Maki, Expert Associate Partner
Derek_Maki@mckinsey.com

Merlina Manocaran, Partner
Merlina_Manocaran@mckinsey.com

Mihir Mysore, Partner
Mihir_Mysore@mckinsey.com

Mike Newborn, Senior Expert
Mike_Newborn@mckinsey.com

Marc Sorel, Expert Associate Partner
Marc_Sorel@mckinsey.com

David Ware, Associate Partner
David_Ware@mckinsey.com

Europe

Mary Calam, Senior Expert
Mary_Calam@mckinsey.com

David Chinn, Senior Partner
David_Chinn@mckinsey.com

Pawel Jablonski, Partner
Pawel_Jablonski@mckinsey.com

Peter Merrath, Associate Partner
Peter_Merrath@mckinsey.com

Thomas Poppensieker, Senior Partner
Thomas_Poppensieker@mckinsey.com

Wolf Richter, Partner
Wolf_Richter@mckinsey.com

Rolf Riemenschnitter, Partner
Rolf_Riemenschnitter@mckinsey.com

Gundbert Scherf, Partner
Gundbert_Scherf@mckinsey.com

Asia

Aman Dhingra, Associate Partner
Aman_Dhingra@mckinsey.com

Juan Hincapie, Expert Associate Partner
Juan_Hincapie@mckinsey.com

Middle East

Mahir Nayfeh, Partner
Mahir_Nayfeh@mckinsey.com

Digital McKinsey and Global Risk Practice
March 2019

www.mckinsey.com