McKinsey & Company

Digital McKinsey and Global Risk Practice

Cybersecurity in a Digital Era

Introduction

Even before the advent of a global pandemic, executive teams faced a challenging and dynamic environment as they sought to protect their institutions from cyberattack, without degrading their ability to innovate and extract value from technology investments. CISOs and their partners in business and IT functions have had to think through how to protect increasingly valuable digital assets, how to assess threats related to an increasingly fraught geopolitical environment, how to meet increasingly stringent customer and regulatory expectations and how to navigate disruptions to existing cybersecurity models as companies adopt agile development and cloud computing.

We believe there are five areas for CIOs, CISOs, CROs and other business leaders to address in particular:

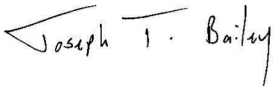
1. **Get a strategy in place that will activate the organization.** Even more than in the past cybersecurity is a business issue – and cybersecurity effectiveness means action not only from the CISO organization, but also from application development, infrastructure, product development, customer care, finance, human resources, procurement and risk. A successful cybersecurity strategy supports the business, highlights the actions required from across the enterprise – and perhaps most importantly captures the imagination of the executive in how it can manage risk and also enable business innovation.
2. **Create granular, analytic risk management capabilities.** There will always be more vulnerabilities to address and more protections you can consider than you will have capacity to implement. Even companies with large and increasing cybersecurity budgets face constraints in how much change the organization can absorb. Therefore, better cybersecurity requires the ability to make rigorous, fact-based decisions about a company's most critical risks – and which cybersecurity investments it should make.
3. **Build cybersecurity into business products and processes.** For digital businesses – and almost every company we know of aspires to be a digital business – cybersecurity is an important driver of product value proposition, customer experience and supply chain configuration. Digital businesses need, for example, design security into IoT products, build secure and convenient customer interaction processes and create digital value chains that protect customer data.
4. **Enable digital technology delivery.** Digital businesses cannot let slow technology delivery get in the way of business innovation, so they are scrambling to adopt agile development, DevOps, cloud computing. However, most companies have built their security architectures and processes to support waterfall development and on-premises infrastructure – creating a disconnect that can both increase risk and decelerate innovation. Forward-leaning CISOs are moving to agile security organizations that enable much more innovation technology organizations.
5. **Help the business address impacts of a global pandemic.** COVID-19 created three imperatives for cybersecurity teams: supporting continued business operations by enabling remote working, mitigating immediate risks – and helping their business partners transition to the next normal.

Over the past year, we've sought to publish cybersecurity articles in each of these areas that will help senior executives consider their options and make pragmatic decisions about how to move forward in making the right tradeoffs in managing technology risks. We hope you find this compendium of articles interesting and helpful. We, and our colleagues in McKinsey's cybersecurity practice, have appreciated the opportunity to comment on what we consider to be one of the most complex and important business issues today.

Thank you,

Kevin Buehler
Senior Partner, New York

Venky Anant
Partner, Silicon Valley



Tucker Bailey
Partner, Washington, DC

James Kaplan
Partner, New York

Mahir Nayfeh
Partner, Abu Dhabi

Wolf Richter
Partner, Berlin

Table of contents

Enable digital technology delivery

Help business address impact of global pandemic

Cybersecurity: Linchpin of the digital enterprise

As companies digitize businesses and automate operations, cyberrisks proliferate; here is how the cybersecurity organization can support a secure digital agenda.

by James Kaplan, Wolf Richter, and David Ware

Two consistent and related themes in enterprise technology have emerged in recent years, both involving rapid and dramatic change. One is the rise of the digital enterprise across sectors and internationally. The second is the need for IT to react quickly and develop innovations aggressively to meet the enterprise's digital aspirations. Exhibit 1 presents a "digitization index" – the results of research on the progress of enterprise digitization within companies, encompassing sectors, assets, and operations. As IT organizations seek to digitize, however, many face significant cybersecurity challenges. At company after company, fundamental tensions arise between the business's need to digitize and the cybersecurity team's responsibility to protect the organization, its employees, and its customers within existing cyber operating models and practices. If cybersecurity teams are to avoid becoming barriers to digitization and instead become its enablers, they must transform their capabilities along three dimensions. They must improve risk management, applying quantitative risk analytics. They must build cybersecurity directly into businesses' value chains. And they must support the next generation of enterprise-technology platforms, which include innovations like agile development, robotics, and cloud-based operating models.

Cybersecurity's role in digitization

Every aspect of the digital enterprise has important cybersecurity implications. Here are just a few examples. As companies seek to create more digital customer experiences, they need to determine how to align their teams that manage fraud prevention, security, and product development so they can design controls, such as authentication, and create experiences that are both convenient and secure. As companies adopt massive data analytics, they must determine how to identify risks created by data sets that integrate many types of incredibly sensitive customer information.

They must also incorporate security controls into analytics solutions that may not use a formal software-development methodology. As companies apply robotic process automation (RPA), they must manage bot credentials effectively and make sure that "boundary cases" – cases with unexpected or unusual factors, or inputs that are outside normal limits – do not introduce security risks.

Likewise, as companies build application programming interfaces (APIs) for external customers, they must determine how to identify vulnerabilities created by interactions between many APIs and services, and they must build and enforce standards for appropriate developer access.[1] They must continue to maintain rigor in application security as they transition from waterfall to agile application development.

Challenges with existing cybersecurity models

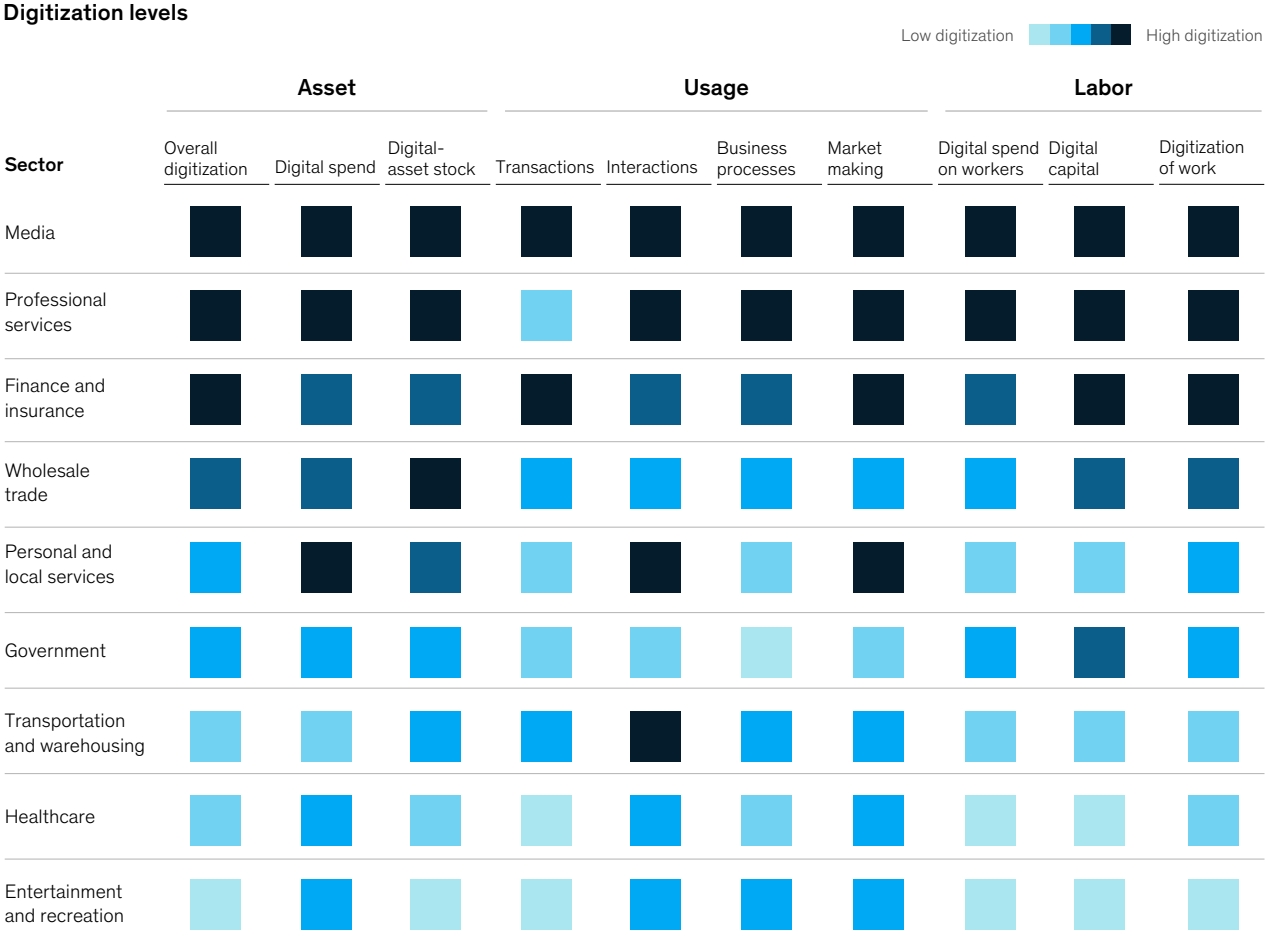
At most companies, chief information officers (CIOs), chief information-security officers (CISOs), and their teams have sought to establish cybersecurity as an enterprise-grade service. What does that mean? They have consolidated cybersecurity-related activities into one or a few organizations. They have tried to identify risks and compare them to enterprise-wide risk appetites to understand gaps and make better decisions about closing them. They have created enterprise-wide policies and supported them with standards. They have established governance as a counterweight to the tendency of development teams to prioritize time to market and cost over risk and security. They have built security service offerings that require development teams to create a ticket requesting service from a central group before they can get a vulnerability scan or a penetration test.

[1] An API is software that allows applications to communicate with each other, sharing information for a purpose.

Exhibit 1

Across sectors, companies are digitizing, with profound implications for cybersecurity functions.

Digitization levels



Source: Appbrain; Blue Wolf; ContactBabel; eMarketer; Gartner; IDC; LiveChat; US Bureau of Economic Analysis; US Bureau of Labor Statistics; US Census Bureau; Global Payments Map by McKinsey; McKinsey Social Technology Survey; McKinsey analysis; McKinsey Global Institute analysis

All these actions have proven absolutely necessary to the security of an organization. Without them, cybersecurity breaches occur more frequently – and often, with more severe consequences. The needed actions, however, exist in tension with the emerging digital-enterprise model – the outcome of an end-to-end digital transformation – from the customer interface through the back-office processes. As companies seek to use public cloud services, they often find that security is the "long pole in the tent" – the most intractable part of the problem of standing applications on public cloud infrastructure.

At one financial institution, development teams were frustrated with the long period needed by the security team to validate and approve incremental items in their cloud service provider's catalog for production usage. Developers at other companies have puzzled over the fact that they can spin up a server in minutes but must wait weeks

their application to production. IT organizations everywhere are finding that existing security models do not run at "cloud speed" and do not provide enough specialized support to developers on issues like analytics, RPA, and APIs (Exhibit 2).

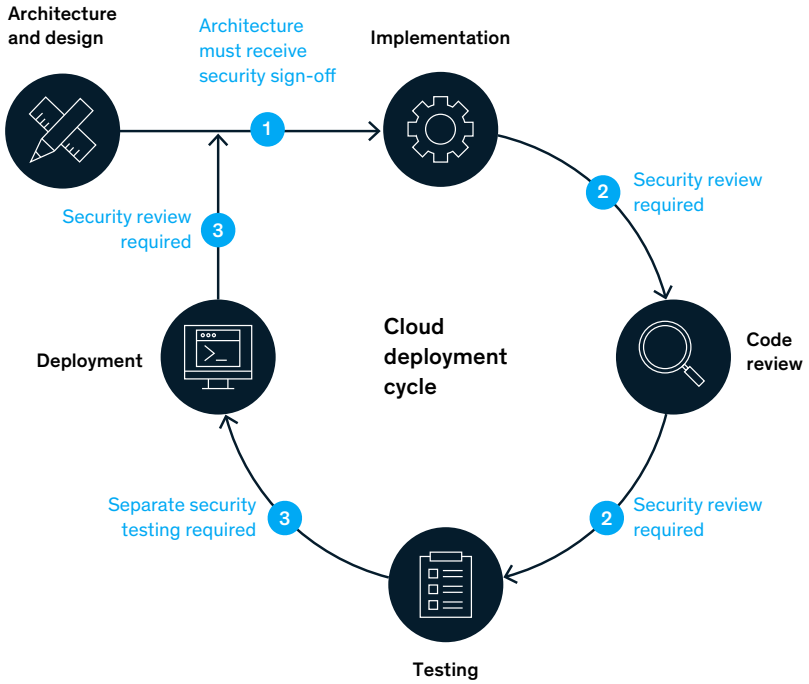
The misalignment between development and cybersecurity teams leads to missed business opportunities, as new capabilities are delayed in reaching the market. In some cases, the pressure to close the gap has caused increased vulnerability, as development teams bend rules to work around security policies and standards.

Cybersecurity for the digital enterprise

In response to aggressive digitization, some of the world's most sophisticated cybersecurity functions are starting to transform their capabilities along the three dimensions we described: using quantitative risk analytics for decision making, building cybersecurity into the business value chain, and enabling the new technology operating platforms that combine many innovations. These innovations include agile approaches, robotics, cloud, and DevOps (the combination of software development and IT operations to shorten development times and deliver new features, fixes, and updates aligned with the business).

Exhibit 2

Current cybersecurity operating models do not operate at 'cloud speed.'



Stage gates

1. Designing secure architecture requires special knowledge
2. Secure code review, test design, and implementation require specially trained developers not available to many teams
3. Cloud environments must be configured to security standards and instrumented with monitoring before deployment into production

Activities

Architecture and design	Implementation	Code review	Testing	Deployment
– Analyze resource availability from cloud service provider – Analyze capacity requirements – Develop initial solution design – Design interfaces	– Instantiate development and testing environments – Begin solution implementation	– Review code – Conduct automated code scanning – Accept code into code base	– Develop test cases – Do continuous testing – Fix bugs and errors; make changes – Do regression testing	– Instantiate cloud infrastructure – Establish cloud services – Deploy production application – Do final testing

Using quantitative risk analytics for decision making

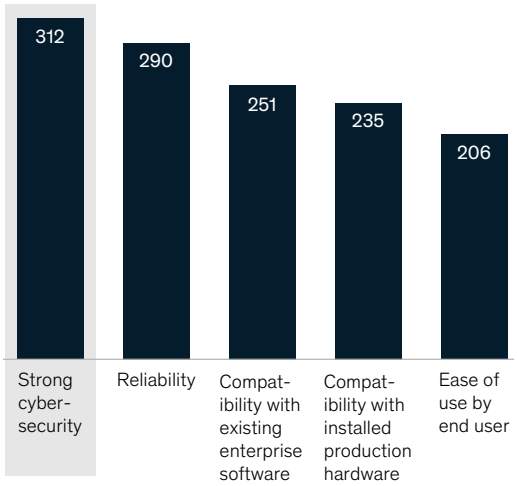
At the core of cybersecurity are decisions about which information risks to accept and how to mitigate them. Traditionally, CISOs and their business partners have made cyberriskmanagement decisions using a combination of experience, intuition, judgment, and qualitative analysis. In today's digital enterprises, however, the number of assets and processes to protect, and the decreasing practicality and efficacy of onesize- fits-all protections, have dramatically reduced the applicability of traditional decision-making processes and heuristics.

In response, companies are starting to strengthen their business and technology environments with quantitative risk analytics so they can make better, fact-based decisions. This has many aspects.

Exhibit 3

Priority requirements have changed for acquiring Internet of Things products: Cybersecurity has moved to the top.

Top 5 priorities when buying IoT products,[1] number of survey responses



[1] IoT = Internet of Things. Besides basic functionality.

Source: McKinsey 2019 IoT Pulse Survey of more than 1,400 IoT practitioners (from middle managers to C-suite) who are executing IoT at scale (beyond pilots). Composition was 61% from US, 20% from China, and 19% from Germany, with organizations of $50 million to more than $10 billion in revenue. This question on IoT-product purchases received 1,161 responses.

It includes sophisticated employee and contractor segmentation as well as behavioral analysis to identify signs of possible insider threats, such as suspicious patterns of email activity. It also includes risk-based authentication that considers metadata – such as user location and recent access activity – to determine whether to grant access to critical systems. Ultimately, companies will start to use management dashboards that tie together business assets, threat intelligence, vulnerabilities, and potential mitigation to help senior executives make the best cybersecurity investments. They will be able to focus those investments on areas of the business that will yield the most protection with the least disruption and cost.

Building cybersecurity into the business value chain

No institution is an island when it comes to cybersecurity. Every company of any complexity exchanges sensitive data and interconnects networks with customers, suppliers, and other business partners. As a result, cybersecurity-related questions of trust and the burden of mitigating protections have become central to value chains in many sectors. For example, CISOs for pharmacy benefit managers and health insurers are having to spend significant time figuring out how to protect their customers' data and then explaining it to those customers. Likewise, cybersecurity is absolutely critical to how companies make decisions about procuring group health or business insurance, prime brokerage, and many other services. It is the single most important factor companies consider when purchasing Internet of Things (IoT) products (Exhibit 3).

Leading companies are starting to build cybersecurity into their customer relationships, production processes, and supplier interactions. Some of their tactics include the following:

— Use design thinking to build secure and convenient online customer experiences. For example, one bank allowed customers to customize their security controls, choosing simpler passwords if they agreed to two-factor authorization.

— Educate customers about how to interact in a safe and secure way. One bank has a senior executive whose job it is to travel the world and teach high-net-worth customers and family offices how to prevent their accounts from being compromised.

— Analyze security surveys to understand what enterprise customers expect and create knowledge bases so that sales teams can respond to customer security inquiries during negotiations with minimum friction. For instance, one software-as-a-service (SaaS) provider found that its customers insisted on having particularly strong data-loss-prevention (DLP) provisions.

— Treat cybersecurity as a core feature of product design. For instance, a hospital network would have to integrate a new operating-room device into its broader security environment. Exhibit 4 presents an example of how security is embedded in a product-development process.

— Take a seamless view across traditional information security and operational technology security to eliminate vulnerabilities. One autoparts supplier found that the system holding the master version of some of its firmware could serve as an attack vector to the fuel-injection systems it manufactured. With that knowledge, it was able to put additional protections in place. Pharma companies have found that an end-toend view of information protection across their supply chains was needed to address certain key vulnerabilities (Exhibit 5).

— Use threat intelligence to interrogate supplier technology networks externally and assess risk of compromise.

Done in concert, these actions yield benefits. They enhance customer trust, accelerating their adoption of digital channels. They reduce the risk of customers or employees trying to circumvent security controls. They reduce friction and delays as suppliers and customers negotiate liability and

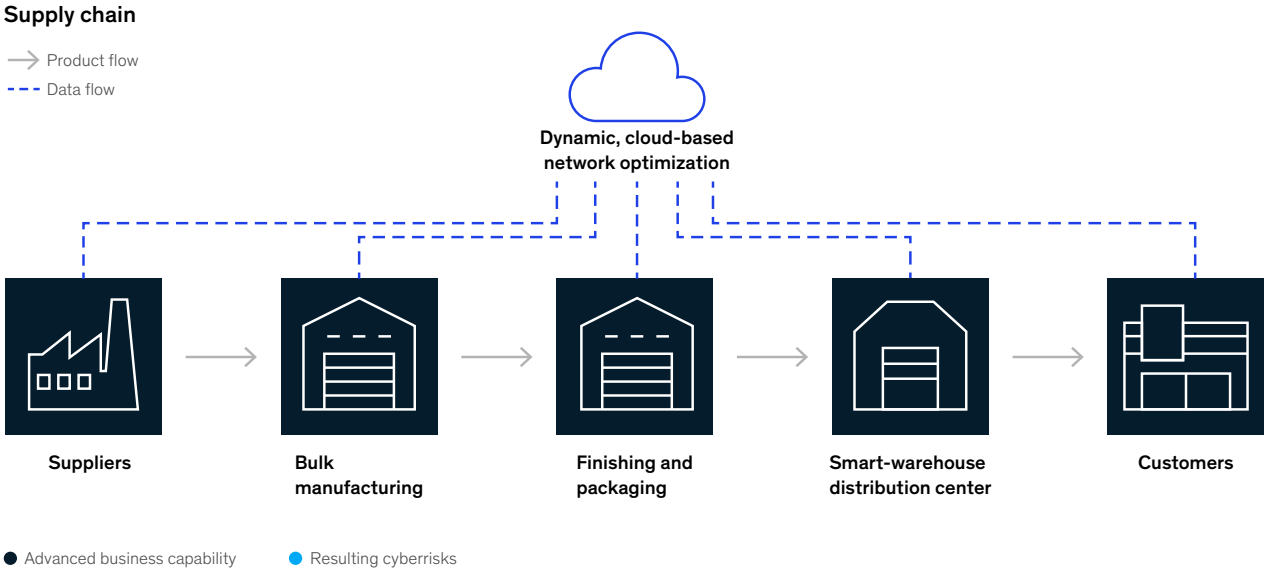
Exhibit 4

How to embed security into a product-development process.

From treating security and privacy as afterthoughts …			… to incorporating them by designing and building an agile security-and-privacy model	
Developers are unclear when security and privacy requirements are mandatory	Product owners don't consider security and privacy tasks during sprint planning	**Requirements**	Prioritize security and privacy tasks according to product risk level	Make product owners aware of need to prioritize security and privacy tasks and be accountable for their inclusion in releases
		Design		
Unclear how to handle distribution of tasks within development team	Chief information-security and privacy officers (CISPOs) have limited capacity to support development teams	**Development**	Security and privacy champions (tech leads) assist teams in distributing tasks	Add capacity through CISPOs, who clarify security and privacy requirements with champions and product owners
No unified real-time standardized monitoring of state of security and privacy tasks		**Testing**	Product-assessment dashboards give developers real-time views of security and privacy within products	
Security and privacy needs are often dealt with before deployment, causing launch delays	Teams unclear how often to engage CISPOs	**Deployment**	Launch delays eliminated as security and privacy tasks are executed across life cycles	Simplified predeployment activities with CISPOs only for releases meeting risk criteria
Unclear accountability for security and privacy in product teams	Lack of integration in security and privacy tool sets introduces complexity	**Throughout process**	Define and communicate roles and responsibilities during agile ceremonies	Integrate and automate security- and privacy-related testing and tracking tools

Exhibit 5

An end-to-end view of information across the pharma supply chain is needed to address vulnerabilities.



responsibility for information risks. They build security intrinsically into customer-facing and operational processes, reducing the "deadweight loss" associated with security protections.

Enabling an agile, cloud-based operating platform enhanced by DevOps

Many companies seem to be trying to change everything about IT operations. They are replacing traditional software-development processes with agile methodologies. They are repatriating engineering talent from vendors and giving developers self-service access to infrastructure.

Some are getting rid of their data centers altogether as they leverage cloud services. All of this is being done to make technology fast and scalable enough to support an enterprise's digital aspirations. In turn, putting a modern technology model in place requires a far more flexible, responsive, and agile cybersecurity operating model. Key tenets of this model include the following:

— Move from ticket-based interfaces to APIs for security services. This requires automating every possible interaction and integrating cybersecurity into the software-development tool chain. That will allow development teams

to perform vulnerability scans, adjust DLP rules, set up application security, and connect to identify and gain access to management services via APIs (Exhibit 6).

— Organize security teams into agile scrum or scrumban teams that manage developer-recognizable services, such as identity and access management (IAM) or DLP. Also, recruiting development-team leaders to serve as product owners for security services can help, just as business managers are product owners for customer journeys and customeroriented services.

— Tightly integrate security into enterprise end-user services, so that employees and contractors can easily obtain productivity and collaboration tools via an intuitive, Amazon-like portal.

— Build a cloud-native security model that ensures developers can access cloud services instantly and seamlessly within certain guardrails.

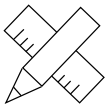
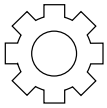
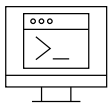
— Collaborate with infrastructure and architecture teams to build required security services into standardized solutions for massive analytics and RPA.

— Shift the talent model to incorporate those with "e-shaped" skills – cybersecurity professionals with several areas of deep knowledge, such as in integrative problem solving, automation, and development – as well as security technologies.

Exhibit 6

Automation, orchestration technology, and application programming interfaces can eliminate manual security processes and interactions.

Automation opportunities in a notionally secure DevOps model

	 Architecture and design	 Implementation	 Code review	 Testing	 Deployment
App application programming interfaces (APIs)	API-configurable application-level controls designed into new applications	APIs for configuration and debugging (eg, test instrumentation) added during implementation phase	Automated code-review systems modified to search for application-specific threat scenarios	Automated and configurable security test cases added to nightly testing regime	Fully configured, production-ready application possible via API calls alone
Process APIs	New application-level API options added to deployment-configuration process	Configurable security tests added to nightly testing regime	Configurable automated code reviews added to precommit/preacceptance process for newly written code	Nightly testing results collected and curated for individual developers/teams via configurable test-management system	Predeployment security-review process replaced by automated tests and configuration checks
Infrastructure APIs	API for deployment and instantiation processes rearchitected to accommodate new applications	Configuration options for instantiation of automated, project-specific development environment made available	Automated code scanning implemented for deployed web applications to maintain quality and code integrity	Cloud environments regularly tested for security via automated vulnerability assessment and identification tools	Security tools and configuration options applied via API to new environments at deployment time

Security-trained developers and engineers enable automation and orchestration throughout cloud-development, -deployment, and -operations phases

Sidebar

How a large biopharma company built cybersecurity capabilities to enable a digital enterprise

A large biopharma company had recently concluded a major investment program to enhance its foundational cybersecurity capabilities, dramatically reducing its risk profile. However, the business strategy began to evolve in new ways, with expanding online consumer relationships, digitally enabled products, enhanced supply-chain automation, and massive use of analytics. The company now needed new cybersecurity capabilities that would both address new business risks and facilitate business and technology innovation.

To get started, the cybersecurity team engaged a broad set of business partners, capturing current and planned strategic initiatives. It then mapped out the new risks that these initiatives would create and the ways in which cybersecurity protections might slow or block the capture of business opportunities. At the same time, the cybersecurity team looked at a broad set of emerging practices and techniques from the pharma industry and other sectors, including online services, banking, and advanced manufacturing. Based on all this, it developed an overarching vision for how cybersecurity could protect and enable the company's digital agenda, and it prioritized 25 initiatives. Some of the most important were the following:

- Collaborating with the commercial team to build patient trust by designing security into online patient journeys
- Collaborating with the manufacturing team to enhance transparency into configuration of plant assets
- Collaborating with the broader technology team to create the application programming interfaces (APIs) and the template to ensure secure configuration of systems running in the public cloud
- Dramatically expanding automation of the security environment to reduce time lags and frustrations developers and users experienced when interacting with the cybersecurity team

The cybersecurity team then used its vision and initiatives to articulate to senior management how it could enable the company's digital business strategy and the support and assistance it would require from other organizations to do so.

Taken together, these actions will eliminate roadblocks to building digital-technology operating models and platforms. Perhaps more importantly, they can ensure that new digital platforms are inherently secure, allowing their adoption to reduce risk for the enterprise as a whole (see sidebar, "How a large biopharma company built cybersecurity capabilities to enable a digital enterprise").

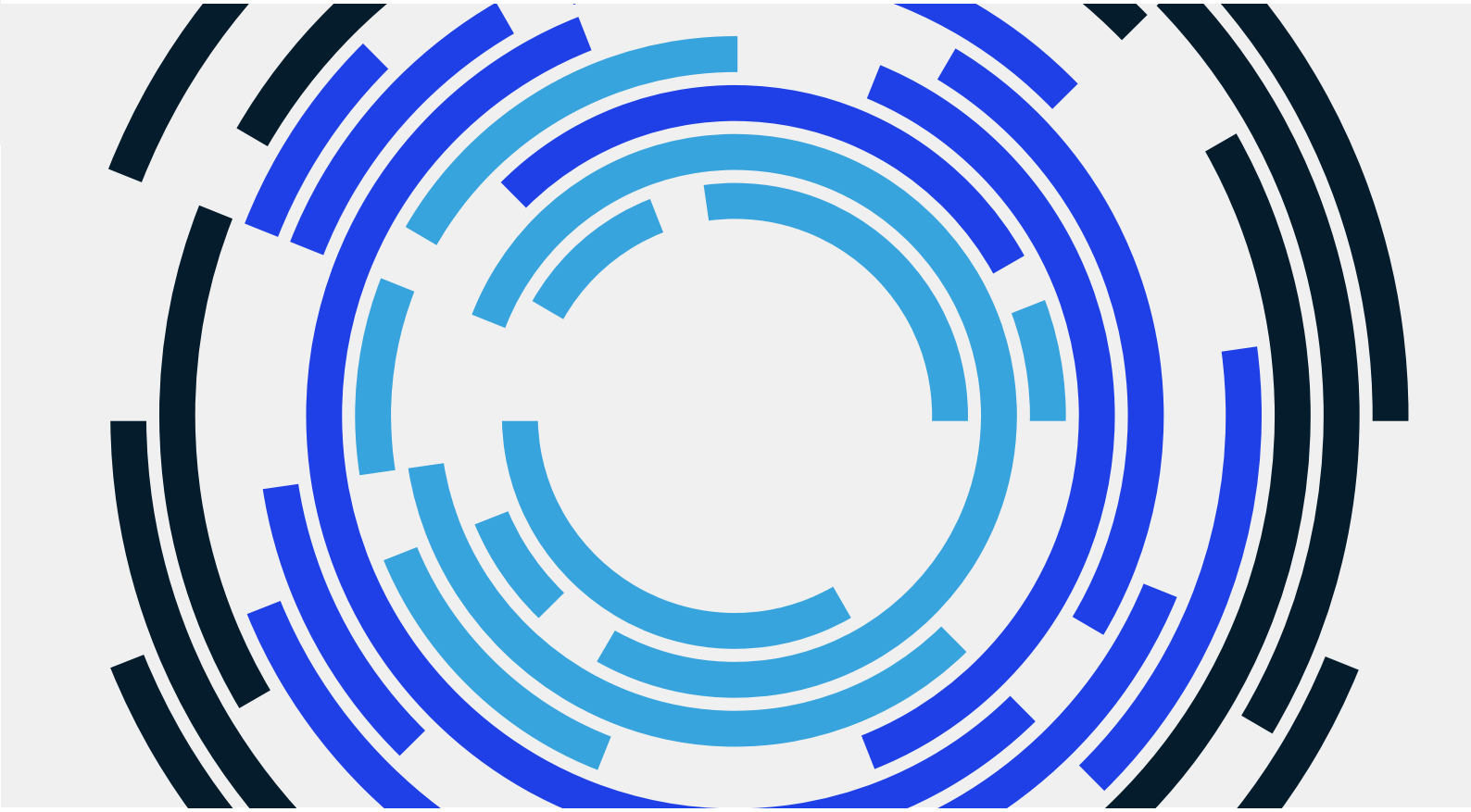
With digitization, analytics, RPA, agile, DevOps, and cloud, it is clear that enterprise IT is evolving rapidly and in exciting and value-creating ways. This evolution naturally creates tension with existing cybersecurity operating models. For organizations to overcome the tension, they will need to apply quantitative risk analytics for decision making, create secure business value chains, and enable operating platforms that encompass the latest innovations. These actions will require significant adaptation from cybersecurity organizations. Many of these organizations are still in the early stages of this journey. As they continue, they will become more and more capable of protecting the companies while supporting the innovative goals of the business and IT teams.

James Kaplan is a partner in McKinsey's New York office, **Wolf Richter** is a partner in the Berlin office, and **David Ware** is an associate partner in the Washington, DC, office.

The risk-based approach to cybersecurity

The most sophisticated institutions are moving from a “maturity based” to a “risk based” approach for managing cyberrisk. Here is how they are doing it.

by Jim Boehm, Nick Curcio, Peter Merrath, Lucy Shenton, and Tobias Stähle



Top managers at most companies recognize cyberrisk as an essential topic on their agendas. Worldwide, boards and executive leaders want to know how well cyberrisk is being managed in their organizations. In more advanced regions and sectors, leaders demand, given years of significant cybersecurity investment, that programs also prove their value in risk-reducing terms. Regulators are challenging the levels of enterprise resilience that companies claim to have attained. And nearly everyone – business executives, regulators, customers, and the general public – agree that cyberrisk is serious and calls for constant attention (Exhibit 1).

What, exactly, organizations should do is a more difficult question. This article is advancing a "risk based" approach to cybersecurity, which means that to decrease enterprise risk, leaders must identify and focus on the elements of cyberrisk to target. More specifically, the many components of cyberrisk must be understood and prioritized for enterprise cybersecurity efforts. While this approach to cybersecurity is complex, best practices for achieving it are emerging.

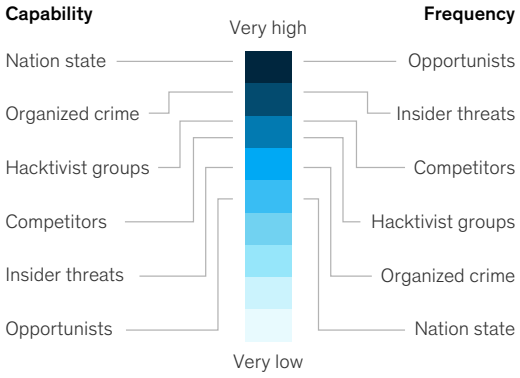
To understand the approach, a few definitions are in order. First, our perspective is that cyberrisk is "only" another kind of operational risk. That is, cyberrisk refers to the potential for business losses of all kinds – financial, reputational, operational, productivity related, and regulatory related – in the digital domain. Cyberrisk can also cause losses in the physical domain, such as damage to operational equipment. But it is important to stress that cyberrisk is a form of business risk.

Furthermore, cyberrisks are not the same as cyberthreats, which are the particular dangers that create the potential for cyberrisk. Threats include privilege escalation, vulnerability exploitation, or phishing.[1] Cyberthreats exist in the context of enterprise cyberrisk as potential avenues for loss of confidentiality, integrity, and availability of digital assets. By extension, the risk impact of cyberthreats includes fraud, financial crime, data loss, or loss of system availability.

Exhibit 1

Cyberthreats are growing in severity and frequency.

Cyberthreat capacity and frequency today, threat actor



Decisions about how best to reduce cyberrisk can be contentious. Taking into account the overall context in which the enterprise operates, leaders must decide which efforts to prioritize: Which projects could most reduce enterprise risk? What methodology should be used that will make clear to enterprise stakeholders (especially in IT) that those priorities will have the greatest risk reducing impact for the enterprise? That clarity is crucial in organizing and executing those cyber projects in a focused way.

At the moment, attackers benefit from organizational indecision on cyberrisk – including the prevailing lack of clarity about the danger and failure to execute effective cyber controls.

Debilitating attacks on high-profile institutions are proliferating globally, and enterprise-wide cyber efforts are needed now with great urgency. It is widely understood that there is no time to waste: business leaders everywhere, at institutions of all sizes and in all industries, are earnestly searching for the optimal means to improve cyber resilience. We believe we have found a way to help.

[1] Privilege escalation is the exploitation of a flaw in a system for purpose of gaining unauthorized access to protected resources. Vulnerability exploitation is an attack that uses detected vulnerabilities to exploit (surreptitiously utilize or damage) the host system.

The maturity-based cybersecurity approach: A dog that's had its day

Even today, "maturity based" approaches to managing cyberrisk are still the norm. These approaches focus on achieving a particular level of maturity by building certain capabilities. To achieve the desired level, for example, an organization might build a security operations center (SOC) to improve the maturity of assessing, monitoring, and responding to potential threats to enterprise information systems and applications. Or it might implement multifactor authentication (MFA) across the estate to improve maturity of access control. A maturity-based approach can still be helpful in some situations: for example, to get a program up and running from scratch at an enterprise that is so far behind it has to "build everything." For institutions that have progressed even a step beyond that, however, a maturity-based approach is inadequate. It can never be more than a proxy for actually measuring, managing, and reducing enterprise risk.

A further issue is that maturity-based programs, as they grow organically, tend to stimulate unmanageable growth of control and oversight. In monitoring, for example, a maturity-based program will tend to run rampant, aspiring to "monitor everything." Before long, the number of applications queued to be monitored across the enterprise will outstrip the capacity of analysts to monitor them, and the installation of monitors will bog down application-development teams. The reality is that some applications represent more serious vulnerabilities – and therefore greater potential for risk – than others. To focus directly on risk reduction, organizations need to figure out how to move from a stance of monitoring everything to one in which particular applications with high risk potential are monitored in particular ways. Another issue related to the monitor-everything stance is inefficient spending. Controls grow year after year as program planning for cybersecurity continues to demand more spending for more controls. But is enterprise risk being reduced? Often the right answers lie elsewhere: for example, the best return on investment in enterprise-risk reduction is often in employee awareness and training. Yet a maturity-based model does not call for the organization to gather enough information to know that it should divert the funding needed for this from additional application monitoring. Spending on both will be expected, though the one effort (awareness and training) may have a disproportionate impact on enterprise-risk reduction relative to the other.

If the objective is to reduce enterprise risk, then the efforts with the best return on investment in risk reduction should draw the most resources. This approach holds true across the full control landscape, not only for monitoring but also for privileged-access management, data-loss prevention, and so forth. All of these capabilities reduce risk somewhat and somehow, but most companies are unable to determine exactly how and by how much.

The final (and most practical) drawback of maturity-based programs is that they can create paralyzing implementation gridlock. The few teams or team members capable of performing the hands-on implementation work for the many controls needed become overloaded with demand. Their highly valuable attention is split across too many efforts. The frequent result is that no project is ever fully implemented and program dashboards show perpetual "yellow" status for the full suite of cyber initiatives.

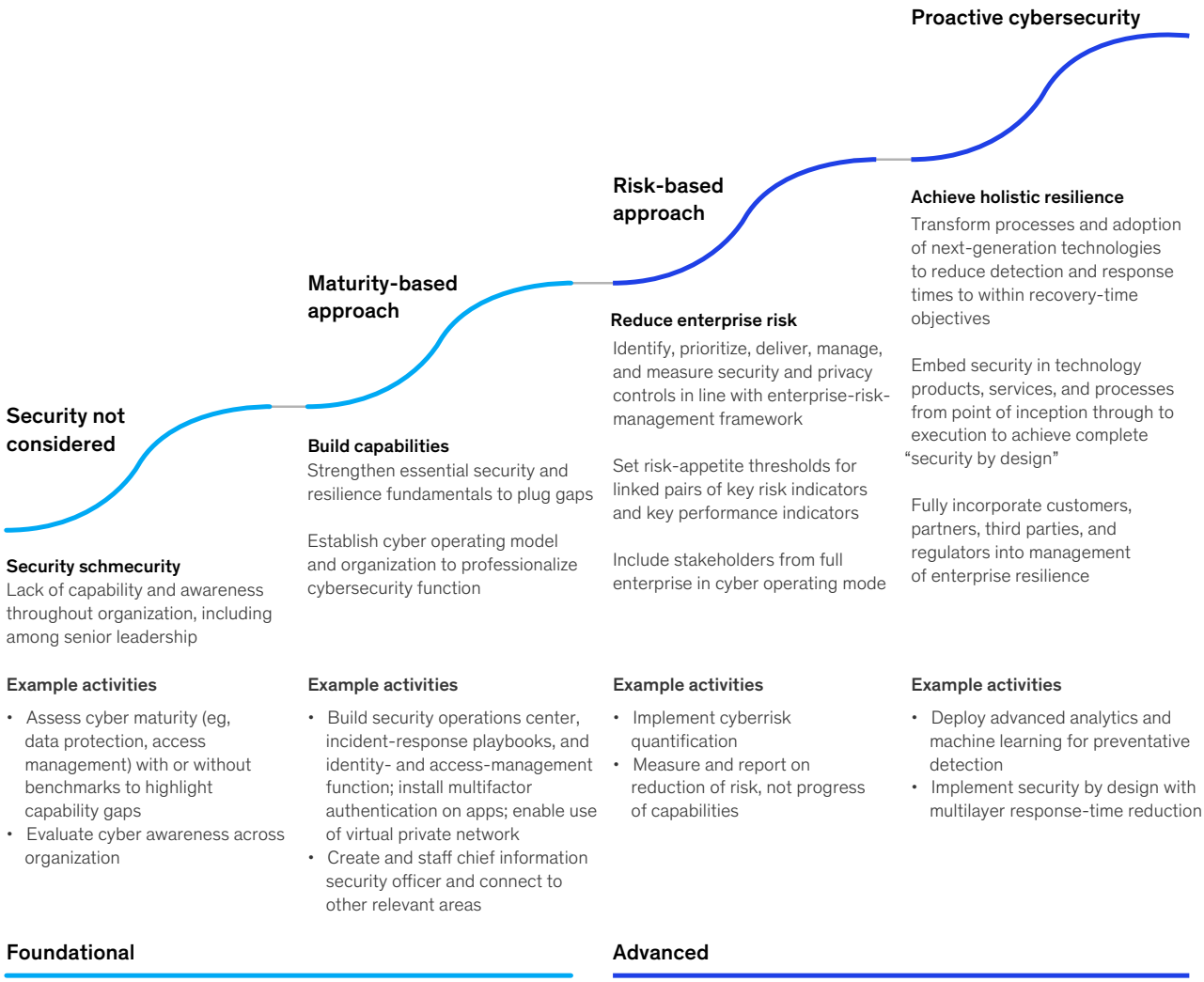
The truth is that in today's hyperconnected world, maturity-based cybersecurity programs are no longer adequate for combatting cyberrisks. A more strategic, risk-based approach is imperative for effective and efficient risk management (Exhibit 2).

Reducing risk to target appetite at less cost

The risk-based approach does two critical things at once. First, it designates risk reduction as the primary goal. This enables the organization to prioritize investment – including in implementationrelated problem solving – based squarely on a cyber program's effectiveness in reducing risk. Second, the program distills top management's risk-reduction targets into

Exhibit 2

For many companies, the risk-based approach is the next stage in their cybersecurity journey.



precise, pragmatic implementation programs with clear alignment from the board to the front line. Following the risk-based approach, a company will no longer "build the control everywhere"; rather, the focus will be on building the appropriate controls for the worst vulnerabilities, to defeat the most significant threats – those that target the business's most critical areas. The approach allows for both strategic and pragmatic activities to reduce cyberrisks (Exhibit 3).

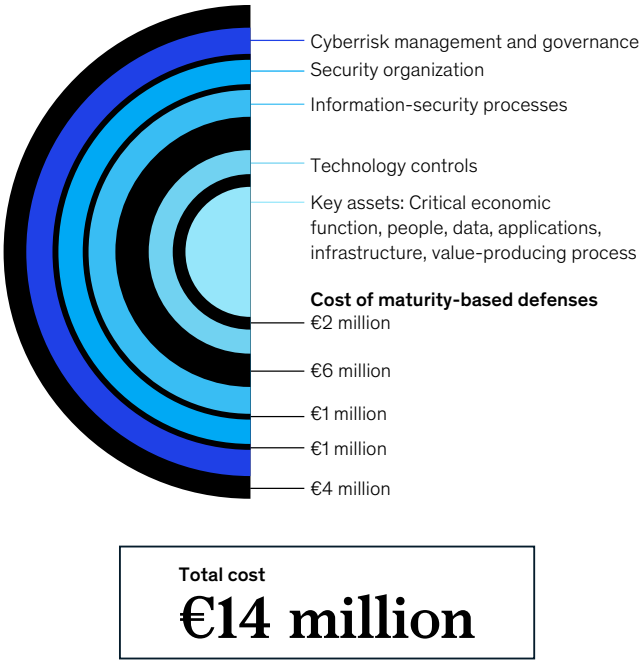
Companies have used the risk-based approach to effectively reduce risk and reach their target risk appetite at significantly less cost. For example, by simply reordering the security initiatives in its backlog according to the risk-based approach, one company increased its projected risk reduction 7.5 times above the original program at no added cost. Another company discovered that it had massively overinvested in controlling new software-development capabilities as part of an agile transformation. The excess spending was deemed necessary to fulfill a promise to the board to reach a certain level of maturity that was, in the end, arbitrary. Using the risk-based approach, the company scaled back controls and spending in areas where desired digital capabilities were being heavily controlled for no risk-reducing reason. A particular region of success with the risk-based approach has been Latin America, where a number of companies have used it to leapfrog a generation of maturity-based thinking (and spending). Instead of recapitulating past inefficiencies, these companies are able to build exactly what they need to reduce risk in the most important areas, right from the start of their cybersecurity programs. Cyber attackers are growing in number and strength, constantly developing destructive new stratagems. The organizations they are targeting must respond urgently, but also seek to reduce risk smartly, in a world of limited resources.

Exhibit 3

A risk-based approach builds customized controls for a company's critical vulnerabilities to defeat attacks at lower overall cost.

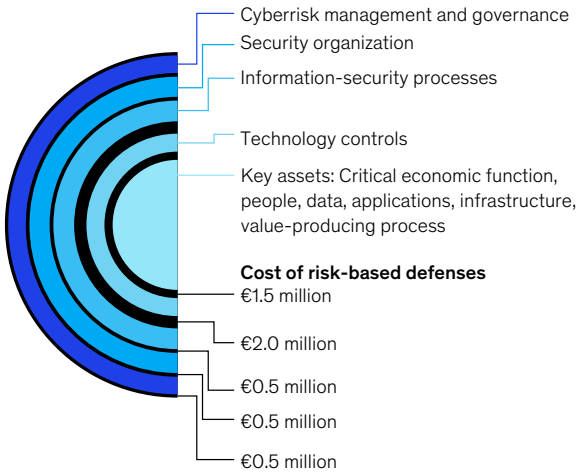
Maturity-based versus risk-based cybersecurity

Maturity-based approach: Builds highest level of defense around everything.



Total cost
€14 million

Risk-based approach: Optimizes defensive layers for risk-reduction and cost. Critical assets are highly protected, but at less expense and in ways that improve productivity.



Total cost
€5 million

Note: Costs are illustrative but extrapolated from real-world examples and estimates.

A transformation in sequential actions

Companies adopting the risk-based approach and transforming their "run" and "change" activities accordingly inevitably face the crucible of how to move from maturity-based to risk-based cybersecurity. From the experience of several leading institutions, a set of best-practice actions has emerged as the fastest path to achieving this transformation. These eight actions taken roughly in sequence will align the organization toward the new approach and enable the appropriate efforts to reduce enterprise risk.

1. Fully embed cybersecurity in the enterpriserisk- management framework.
2. Define the sources of enterprise value across teams, processes, and technologies.
3. Understand the organization's enterprise-wide vulnerabilities – among people, processes, and technology – internally and for third parties.
4. Understand the relevant "threat actors," their capabilities, and their intent.
5. Link the controls in "run" activities and "change" programs to the vulnerabilities that they address and determine what new efforts are needed.
6. Map the enterprise risks from the enterprise-risk-management framework, accounting for the threat actors and their capabilities, the enterprise vulnerabilities they seek to exploit, and the security controls of the organization's cybersecurity run activities and change program.
7. Plot risks against the enterprise-risk appetite; report on how cyber efforts have reduced enterprise risk.
8. Monitor risks and cyber efforts against risk appetite, key cyberrisk indicators (KRIs), and key performance indicators (KPIs).

1. Fully embed cybersecurity in the enterprise-risk-management framework

A risk-based cyber program must be fully embedded in the enterprise-risk-management framework. The framework should not be used as a general guideline, but rather as the organizing principle. In other words, the risks the enterprise faces in the digital domain should be analyzed and categorized into a cyberrisk framework. This approach demystifies cyberrisk management and roots it in the language, structure, and expectations of enterprise-risk management. Once cyberrisk is understood more clearly as business risk that happens in the digital domain, the organization will be rightly oriented to begin implementing the riskbased approach.

2. Define the sources of enterprise value

An organization's most valuable business work flows often generate its most significant risks. It is therefore of prime importance to identify these work flows and the risks to which they are susceptible. For instance, in financial services, a loan process is part of a value-creating work flow; it is also vulnerable to data leakage, an enterprise risk. A payment process likewise creates value but is susceptible to fraud, another enterprise risk. To understand enterprise risks, organizations need to think about the potential impact on their sources of value.

Identifying the sources of value is a fairly straightforward exercise, since business owners will have already identified the risks to their business. Cybersecurity professionals should ask the businesses about the processes they regard as valuable and the risks that they most worry about.

Making this connection between the cybersecurity team and the businesses is a highly valuable step in itself. It motivates the businesses to care more deeply about security, appreciating the bottom-line impact of a recommended control. The approach is far more compelling than the maturity-based approach, in which the cybersecurity function peremptorily informs the business that it is implementing a control "to achieve a maturity of 3.0."

The constituents of each process can be defined – relevant teams, critical information assets ("crown jewels"), the third parties that interact with the process, and the technology components on which it runs – and the vulnerabilities to those constituent parts can be specified.

3. Understand vulnerabilities across the enterprise

Every organization scans its infrastructure, applications, and even culture for vulnerabilities, which can be found in areas such as configuration, code syntax, or frontline awareness and training. The vulnerabilities that matter most are those connected to a value source that particular threat actors with relevant capabilities can (or intend to) exploit. The connection to a source of value can be direct or indirect. A system otherwise rated as having low potential for a direct attack, for example, might be prone to lateral movement – a method used by attackers to move through systems seeking the data and assets they are ultimately targeting.

Once the organization has plotted the people, actions, technology, and third-party components of its value-creating processes, then a thorough identification of associated vulnerabilities can proceed. A process runs on a certain type of server, for example, that uses a certain operating system (OS). The particular server – OS combination will have a set of identified common vulnerabilities and exposures. The same will be true for storage, network, and end-point components. People, process, and third-party vulnerabilities can be determined by similar methodologies.

Of note, vulnerabilities and (effective) controls exist in a kind of reverse symbiosis: where one is present the other is not. Where sufficient control is present, the vulnerability is neutralized; without the control, the vulnerability persists. Thus, the enterprise's vulnerabilities are most practically organized according to the enterprise-approved control framework.[2] Here synergies begin to emerge. Using a common framework and language, the security, risk, IT, and frontline teams can work together to identify what needs to be done to close vulnerabilities, guide implementation, and report on improvements in exactly the same manner and language. Experience confirms that when the entire organization shares a common way of thinking about vulnerabilities, security can be significantly enhanced.

[2] This can include the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), NIST National Vulnerability Dataset (NIST 800-53), International Organization for Standardization 27001/2 (standards for information-security-management systems), and Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC CAT).

Experience confirms that when the entire organization shares a common way of thinking about vulnerabilities, security can be significantly enhanced.

4. Understand relevant threat actors and their capabilities

The groups or individuals an organization must worry about – the threat actors – are determined by how well that organization's assets fit with the attackers' goals – economic, political, or otherwise. Threat actors and their capabilities – the tactics, techniques, and procedures they use to exploit enterprise security – define the organization's threat landscape.

Only by understanding its specific threatlandscape can an organization reduce risk. Controls are implemented according to the most significant threats. Threat analysis begins with the question, Which threat actors are trying to harm the organization and what are they capable of? In response, organizations can visualize the vulnerabilities commonly exploited by relevant threats, and appropriate controls can then be selected and applied to mitigate these specific vulnerability areas.

In identifying the controls needed to close specific gaps, organizations need to size up potential attackers, their capabilities, and their intentions – the threat actors' strength and will (intention) to create a risk event. This involves collecting information on and understanding how the attackers connect, technically and nontechnically, to the people, process, and technology vulnerabilities within the enterprise.

5. Address vulnerabilities

To defeat threat actors, vulnerabilities discovered in the third action we describe will either be closed by existing controls – normal run activities or existing change initiatives – or will require new control efforts. For existing controls, the cyber governance team (for "run") and the program management team (for "change") map their current activities to the same control framework used to categorize vulnerabilities. This will show the controls already in place and those in development. Any new controls needed are added to the program backlog as either stand-alone or composite initiatives.

While an organization may not be able to complete all initiatives in the backlog in a single year, it will now be able to choose what to implement from the full spectrum of necessary controls relevant to the enterprise because they are applicable for frustrating relevant threat capabilities. The risk-based approach importantly bases the scope of both existing and new initiatives in the same control framework. This enables an additional level of alignment among teams: delivery teams charged with pushing and reporting on initiative progress can finally work efficiently with the second and third lines of defense (where relevant), which independently challenge control effectiveness and compliance. When the program-delivery team (acting as the first line of defense) sits down with the second and third lines, they will all be speaking the same language and using the same frameworks. This means that the combined groups can discuss what is and is not working, and what should be done.

6. Map the enterprise-risk ecosystem

A map of enterprise risks – from the enterpriserisk-management framework to enterprise vulnerabilities and controls to threat actors and their capabilities – makes visible a "golden thread," from control implementation to enterprise-risk reduction. Here the risk-based approach can begin to take shape, improving both efficiency in the application of controls and the effectiveness of those controls in reducing risks. Having completed actions one through five, the organization is now in a position to build the riskbased cybersecurity model. The analysis proceeds by matching controls to the vulnerabilities they close, the threats they defeat, and the value-creating processes they protect. The run and change programs can now be optimized

according to the current threat landscape, present vulnerabilities, and existing program of controls. Optimization here means obtaining the greatest amount of risk reduction for a given level of spending. A desired level of risk can be "priced" according to the initiatives needed to achieve it, or the entry point for analysis can be a fixed budget, which is then structured to achieve the greatest reduction in risk.

Cybersecurity optimization determines the right level and allocation of spending. Enterprise-risk reduction is directly linked to existing initiatives and the initiation of new ones. The analysis develops the fact base needed for tactical discussions on overly controlled areas whence the organization might pull back as well as areas where better control for value is needed.

By incorporating all components in a model and using the sources of value and control frameworks as a common language, the business, IT, risk, and cybersecurity groups can align. Discussions are framed by applying the enterprise control framework to the highest sources of value. This creates the golden-thread effect. Enterprise leadership (such as the board and the risk function) can identify an enterprise risk (such as data leakage), and the cybersecurity team can report on what is being done about it (such as a data-loss prevention control on technology or a social-engineering control on a specific team). Each part is connected to the other, and every stakeholder along the way can connect to the conversation. The methodology and model is at the center, acting both as a translator and as an optimizer. The entire enterprise team knows what to do, from the board to the front line, and can move in a unified way to do it.

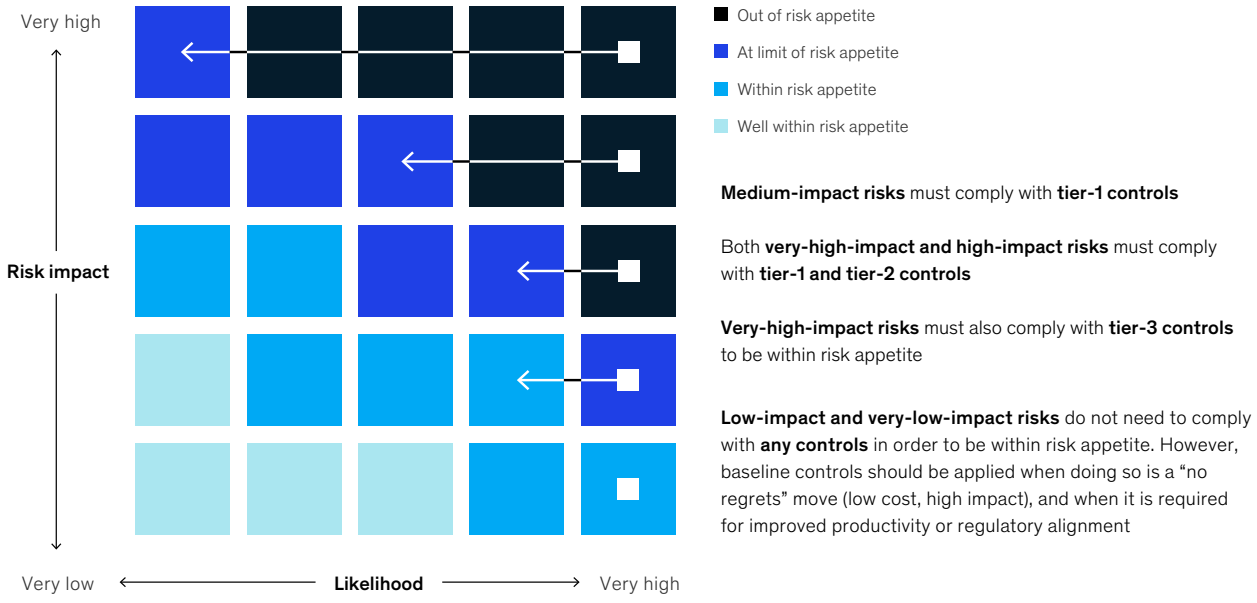
7. Plot risks against risk appetite; report on risk reduction

Once the organization has established a clear understanding of and approach to managing cyberrisk, it can ensure that these concepts are easily visualized and communicated to all stakeholders. This is done through a risk grid, where the application of controls is sized to the potential level of risk (Exhibit 4).

Exhibit 4

The risk-based approach applies controls according to the risk appetite and the likelihood and potential impact of a risk event.

Risk events by size of impact and likelihood of occurrence



The assumption in this use of the classic risk grid is that the enterprise-risk appetite has been defined for each enterprise risk. The potential impact for each enterprise-risk scenario can then be plotted on the risk grid. Once the relationships among the threats, vulnerabilities, and applied controls are modeled and understood, the risks can be evaluated according to their likelihood. As more controls are applied, the risk levels are reduced to the risk appetite. This is the way the cyber program can demonstrate impact in terms of enterprise-risk reduction.

As new threats emerge, new vulnerabilities will become apparent. Existing controls may become ineffective, and enterprise risks can move in the opposite direction – even to the point where riskappetite limits are exceeded. For information-security-management systems, the risk grid allows stakeholders to visualize the dynamic relationships among risks, threats, vulnerabilities, and controls and react strategically, reducing enterprise risks to the appropriate risk-appetite level.

8. Monitor risks and cyber efforts using risk appetite and key cyberrisk and performance indicators

At this point, the organization's enterprise risk posture and threat landscape are understood, and the risk-based cybersecurity program is in place. The final step is to monitor and manage for success.

Many companies attempt to measure cyber maturity according to program completion, rather than by actual reduction of risk. If a security function reports that the data-loss-prevention (DLP) program is 30 percent delivered, for example, the enterprise assumption is that risk of data leakage is 30 percent reduced. If a multifactor authentication initiative is 90 percent implemented, the assumption is that the risk of unauthorized access is almost eliminated. These assumptions are false, however, because actual risk-reducing results are not being measured in these examples.

Sidebar

Linking a KRI to a KPI

A data-loss-prevention program (DLP) is a helpful control to reduce the enterprise risk of data leakage. The critical assets identified by the enterprise-risk-management function as requiring DLP coverage can become the output metric, or key risk indicator (KRI). Assuming that the KRI is not 100 percent, then the linked input metric, or key performance indicator (KPI) could be the proportion of critical assets covered since the last reporting period versus the total expected to be covered. Enterprise leaders will see these two metrics on the reporting dashboard. They can then assess the progress towards the appetite-linked thresholds and with delivery teams discuss what if anything is needed to continue meeting (or possibly exceeding) expectations.

With KRIs and KPIs systematically incorporated into a digital dashboard, executives have complete risk-based measurement and reporting at their fingertips. They can actively participate in risk-reduction efforts – influencing their progress, projections, performance, and achievement of risk thresholds.

Metrics need to measure both inputs and outputs; inputs, in this case, are risk-reduction efforts undertaken by the enterprise, while the output is the actual reduction in enterprise risk. The input metric here is a key performance indicator (KPI): measuring the performance of a program or a "run" function. The output metric is really a key risk indicator (KRI), measuring the risk level associated with a potential risk scenario. The thresholds for the KRIs must be tied directly to risk-appetite levels (the KPI thresholds can also be linked in this way). For example, if risk appetite for data leakage is zero, then the systemic controls (and corresponding "red" thresholds) must be higher than they would be if a certain percentage of leakage is allowed over a certain period. Of course, tolerances for cyber incidents may be not always be set at zero. In most cases, it is impossible to stop all cyber attacks, so sometimes controls can be developed that tolerate some incidents.

One way to think about KRIs and KPIs is with regard to the relationship between altitude and trajectory. A KRI gives the current risk level of the enterprise (the "risk altitude") while the KPI indicates the direction towards or away from the enterprise-risk-appetite level ("risk trajectory"). An enterprise may not yet have arrived at the leadership's KRI target but a strong KPI trajectory would suggest that it will soon. Conversely, an enterprise may have hit the desired KRI threshold, but the KPIs of the run activity may be backsliding and give cause for concern.

Executives are often forced to make sense of a long list of sometimes conflicting metrics. By linking KRIs and KPIs, the cybersecurity team gives executives the ability to engage in meaningful problem-solving discussions on which risks are within tolerances, which are not, and why (see the sidebar, "Linking a KRI to a KPI").

The risk-based approach to cybersecurity is thus ultimately interactive – a dynamic tool to support strategic decision making. Focused on business value, utilizing a common language among the interested parties, and directly linking enterprise risks to controls, the approach helps translate executive decisions about risk reduction into control implementation. The power of the risk-based approach to optimize for risk reduction at any level of investment is enhanced by its flexibility, as it can adjust to an evolving risk-appetite strategy as needed.

Many leading companies have a cyber-maturity assessment somewhere in their archives; some still execute their programs to achieve certain levels of maturity. The most sophisticated companies are, however, moving away from the maturity-based cybersecurity model in favor of the risk-based approach. This is because the new approach allows them to apply the right level of control to the relevant areas of potential risk. For senior leaders, boards, and regulators, this means more economical and effective enterprise-risk management.

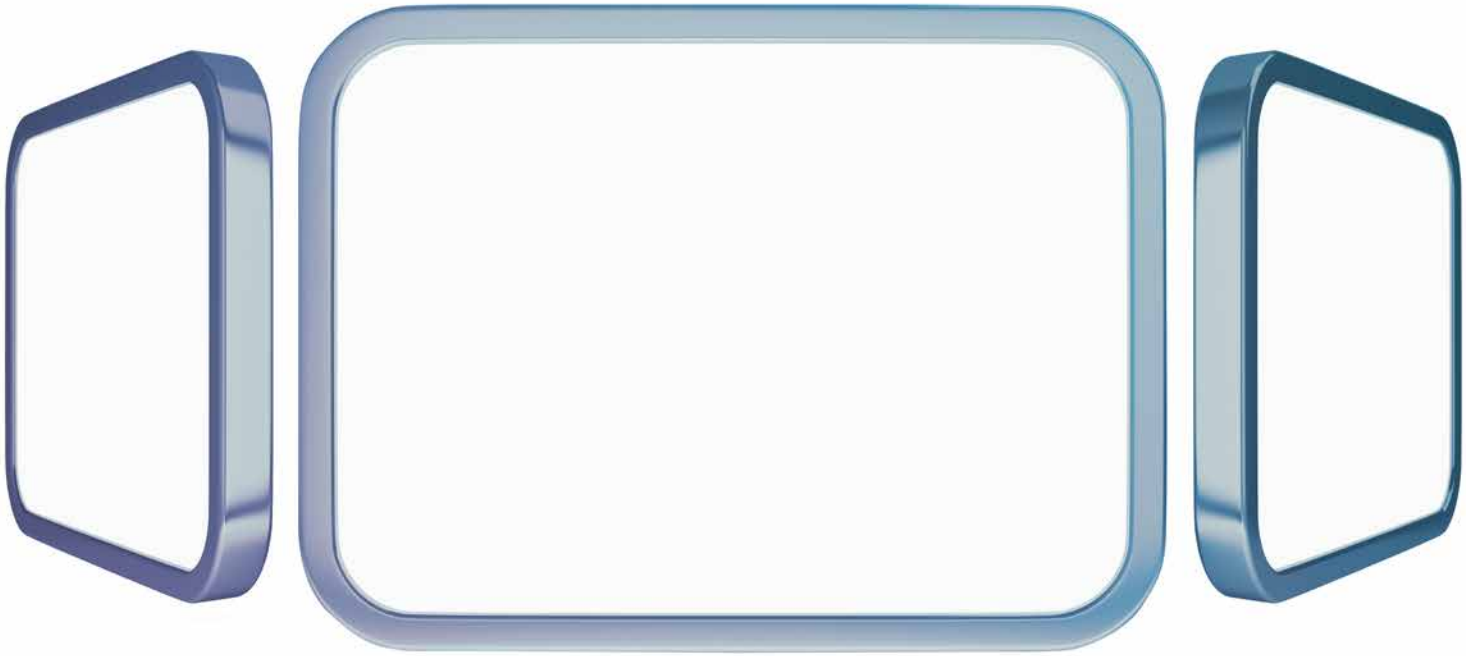
Jim Boehm is an associate partner in McKinsey's Washington, DC, office; **Nick Curcio** is a cyber solutions analyst in the New York office; **Peter Merrath** is an associate partner in the Frankfurt office, where **Tobias Stähle** is a senior expert; and **Lucy Shenton** is a cyber solutions specialist in the Berlin office.

The authors wish to thank Rich Isenberg for his contributions to this article.

Enhanced cyberrisk reporting: Opening doors to risk-based cybersecurity

New cyberrisk management information systems provide executives with the risk transparency they need to transform organizational cyberresilience.

by Jim Boehm, James Kaplan, Peter Merrath, Thomas Poppensieker, and Tobias Stähle



Executives in all sectors have deepened their understanding of the dangers cyberrisk poses to their business. As hacks, cyberattacks, and data leaks proliferate in industry after industry, a holistic, enterprise-wide approach to cybersecurity has become a priority on board agendas. Companies are strengthening protections around their business models, core processes, and sensitive data. Regulators are applying their own pressures, and privacy demands are sharpening.

We asked executives at financial institutions in Europe and North America about their actual experiences with cyberrisk management and reporting. What they told us was instructive. They said cyberrisk management can be effective only when the information it is based on is accurate. Yet cyberrisk reporting at many companies is inadequate, failing to provide executives with the facts they need to make informed decisions about countermeasures. Because of the information gaps, managers often apply a standard set of controls to all company assets. As a result, low-priority assets can be overprotected, while critical assets remain dangerously exposed.

Fortunately, some leading organizations are pioneering an effective, efficient approach to cyberrisk reporting that helps executives increase corporate resilience – one that also provides transparency on cyberrisk and allows companies to integrate cyberrisk reporting with legacy systems.

Risk managers are flying blind

Many companies rely on a patchwork of reports from different sources to manage cyberrisk. Executives at these companies are unable to assess the returns from their cybersecurity investments. They lack needed information about cyberrisk levels, the effectiveness of countermeasures, and the status of protection for key assets. Available data are incomplete, inconsistent, and not reliable as a basis for decision making. Executives also question the complexity of their cyberrisk-management tools, finding them overly complicated and their results incomprehensible.

Risk decision makers reserve particular criticism for governance-risk-compliance (GRC) systems. These complex software solutions can take years to implement and rarely produce a satisfying result. Like many risk-management systems, GRC software was created by technicians, and specialized expertise is required to make sense of the output. In one survey, more than half of executive respondents said cybersecurity reporting was too technical for their purposes.[1] In fact, GRC does not even focus on cyberrisk but rather covers a wide range of risk types, including financial, legal, natural, and regulatory risks. It therefore cannot create the overview of cybersecurity that board members and regulators need. In effect, many cyberrisk managers are flying blind.

[1] "How boards of directors really feel about cyber security reports", Bay Dynamics, June 2016, baydynamics.com.

"We need to bring rigor to the risks related to data and protect our top assets effectively."
—Advanced industries CIO

“The current situation is a mess. We do not have the facts to decide on actions. This paralysis puts our business at risk.”

—Financial-services chief information-security officer

At a leading European financial institution, executives were dissatisfied with the existing cyberrisk-reporting regime. In attempting to improve it, they first assessed their experience:

— Cyberrisk reports were compiled by IT specialists for other IT specialists. As a result, the reports were very technical in nature and provided little to no guidance for executive decision making. Executives found that the reports did not help them interpret how cyberrisk is related to other risks the institution faces, such as legal or financial risks.

— At the same time, the reporting had many gaps: almost no information was provided on top risks, key assets, recent incidents, counter-risk measures, implementation accountability, the institution’s resilience in the face of cyberthreats, or the return on investments in cybersecurity.

— The reporting was structured by systems, servers, and applications rather than by business units, business processes, functions, countries, or legal entities. Most reports were compiled as stand-alone documents, with no integrated view of cyberrisk across the group .

The executives had no clear sense of the overall magnitude of the risk from cyberattacks, malware, and data leaks. Neither did they know what was needed to improve protection of their key assets against the biggest threats. Several mitigating initiatives were in progress, but the reporting did not make clear what contributions, if any, these actions made to reducing risk. Cyberrisk managers found it difficult to decide on the areas of focus for cybersecurity investments or to justify their ultimate decisions to the board. For want of reliable reporting, the entire cybersecurity strategy was undifferentiated: all controls were being applied to all assets.

The chief information-security officer (CISO) did not know whom to contact about a given issue. Regulators reproached the institution for incomplete information. For example, the institution did not compile data on the share of employees that had completed mandatory cybersecurity training in any one location. Within the undifferentiated group-level data, high attendance in one country could easily mask low attendance in another. The training gap could be contributing to unacceptable levels of cyberrisk exposure in that country, which, however, would be invisible.

The objectives of effective cyberrisk reporting

State-of-the-art cyberrisk management requires an information system that consolidates all relevant information in one place. The most important risk metrics – key risk indicators (KRIs) – present a consistent evaluation across assets to enable the tailored application of cyberrisk controls. A given asset can be protected with the controls appropriate to its importance and the threat levels to which it is exposed.

To ready their companies for the challenges of the evolving cyberrisk-threat landscape, executives need to upgrade their approach to cyberrisk reporting and management. To address the magnitude and the complexity of the threat, companies should build a high-performing cyberrisk management information system (MIS) with three fundamental objectives.[2]

[2] See also Thomas Poppensieker and Rolf Riemenschnitter, “A new posture for cybersecurity in a networked world,” McKinsey on Risk, March 2018, McKinsey.com.

— **Transparency on cyberrisk.** Make the cyberrisk status of the institution's most valuable assets fully transparent, with data on the most dangerous threats and most important defenses assembled in a way that's accessible and comprehensible for nonspecialists.

— **Risk-based enterprise overview.** Provide decision makers with a risk-based overview of the institution so they can focus their cybersecurity invest-ments on protecting the most valuable assets from the most dangerous threats.

— **Return on cyber investments.** Ensure the efficiency of counterrisk measures by requiring a high return on investment.

A dedicated cyberrisk MIS is not a substitute for GRC systems but rather a reporting solution addressing cyberrisk. It must be compatible with legacy systems and serve decision makers rather than specialists. It is designed to provide the information that executives need to prioritize threats and devise effective controls; it enables informed board discussions on cyberrisk strategy and helps optimize the allocation of funds.

The cyberrisk MIS should not become a burden on executives, reduced to yet another software system they must learn. Rather, it should be integrated into the existing business-intelligence system, drawing initially on existing data sources. A good cyberrisk MIS should also aspire to be future-proof, adaptable to new technologies, and able to integrate more granular data sources and more sophisticated algorithms for risk assessment as they become available.

For optimal performance, the cyberrisk MIS should be tailored to the needs of a given company. However, even a basic setup can create substantial impact. This is because a cyberrisk MIS acts as a catalyst for better, more informed decision making. Even the process of setting it up forces executives to come to a common understanding of the level of cyberrisk the company is willing to tolerate.

A strong analytical backbone

Analytics is the backbone of the cyberrisk MIS; having a strong, smart analytical system in place enables users to integrate data from different sources across a network and aggregate risks as needed. Ideally, the cyberrisk MIS should have a pyramid structure, with risk data organized hierarchically. The starting point is a simple overview, with the most important data at the highest level of aggregation. These data would describe, for example, the top global risks, differentiated by potential loss and probability. More detailed information can be added as needed, including KRIs and countermeasures for individual divisions, countries, assets, processes, and even buildings. The contact details of the people responsible for implementing the specific countermeasures can also be included.

As shown in Exhibit 1, a top-down approach for risk-data aggregation typically involves the use of qualitative risk assessments based on scenarios. Top down is a good way to begin: it requires the least amount of data and provides significant insight in a short time. Eventually, enough risk data will become available to introduce a bottom-up approach.

The movement from top down to bottom up helps achieve cyberrisk MIS objectives quicker – by clarifying definitions of the elements of cyberrisk, providing executives with the information they need to make strategic decisions, and enhancing transparency on risk exposure and the efficacy of risk-mitigation initiatives.

Exhibit 1

The cyberrisk management information system begins with top-down risk aggregation and proceeds to a bottom-up approach.

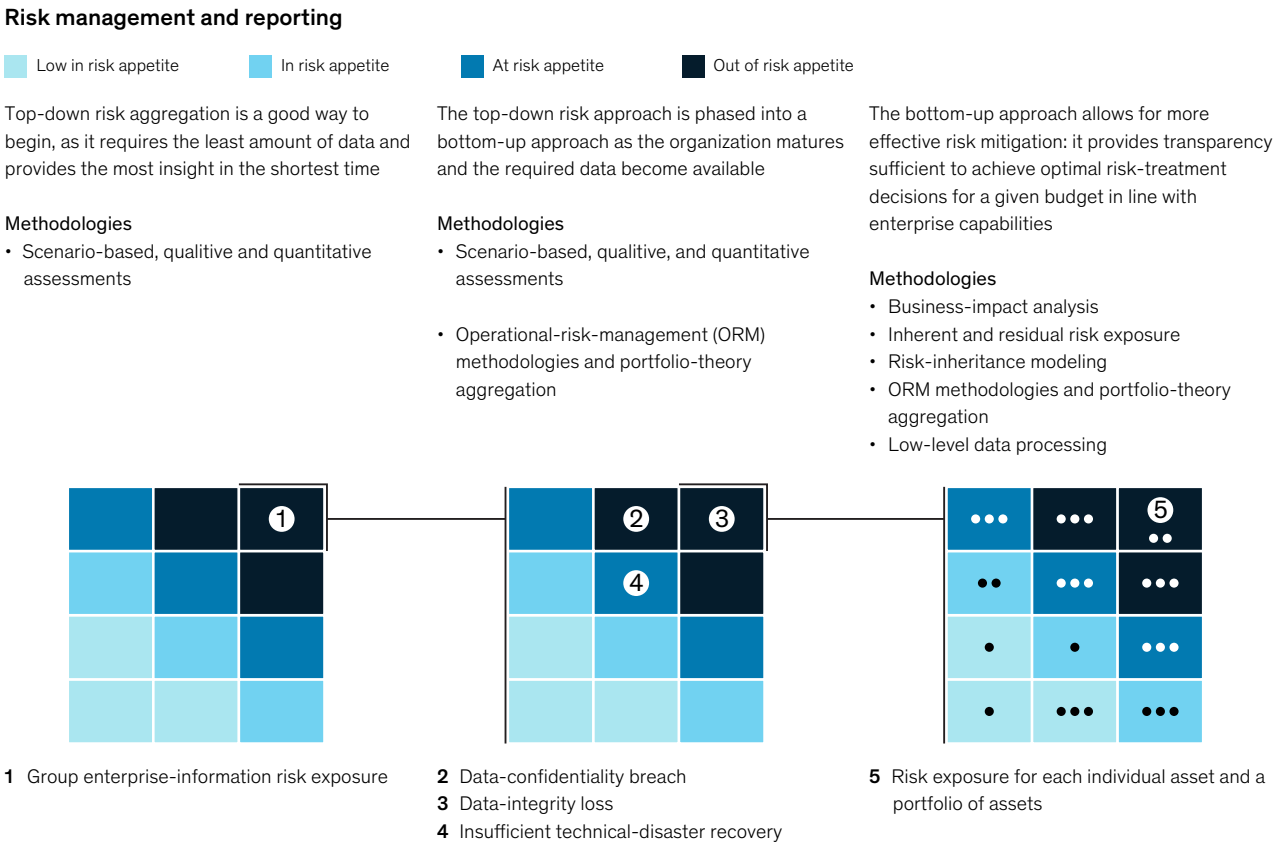


Exhibit 2 presents the "path to green": the risk-mitigation initiatives enabled by the mature bottom-up approach that bring risk indicators within the risk appetite.

A high-performing cyberrisk MIS is much more than a reporting tool. It is an integrated decision-support system, creating visibility on all relevant assets – end-user devices, applications, infrastructure, networks, and buildings. It gives decision makers access to detailed information on organizational units, regions, and legal entities. It embodies the principles of good cyberrisk governance, from definition and detection to treatment and measurement.

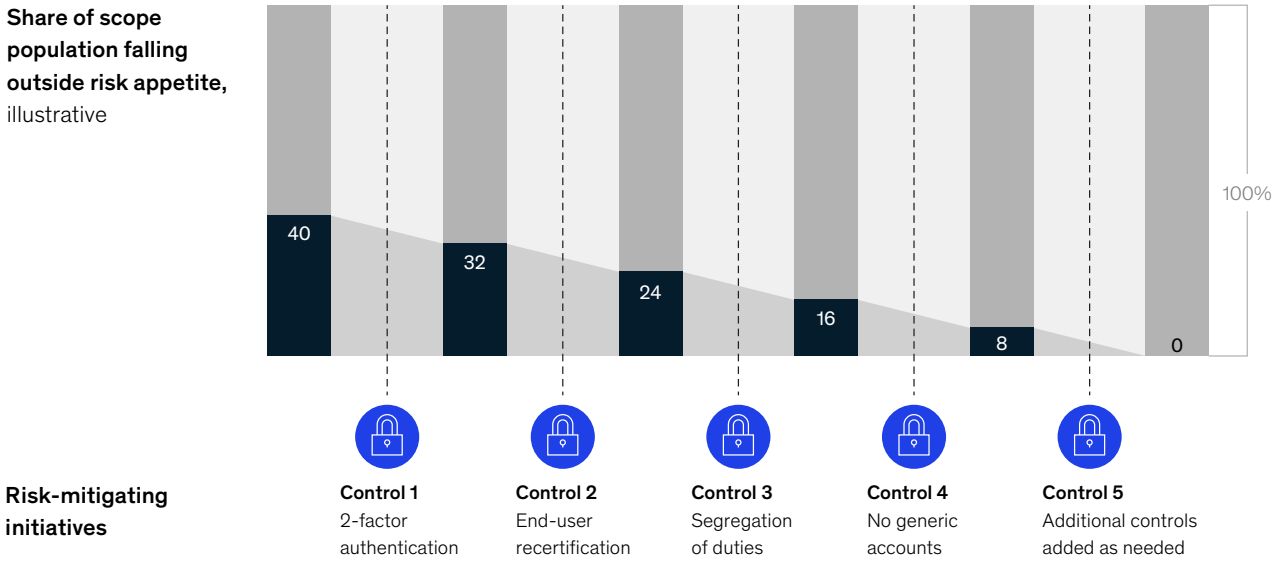
Implementation of the cyberrisk MIS is as critically important as its design. Even the finest aggregated scorecard or the most granular breakdown of KRIs will be useless if executives do not rely on the output for decision making. This is why a good cyberrisk MIS should be customized, reflecting the specific needs of decision makers at levels one and two of a company's hierarchy.

Catalyzing a cybersecurity transformation

The cyberrisk MIS can catalyze a comprehensive cybersecurity transformation. This happens in the MIS implementation, which in itself is an opportunity to transform the ways companies gather information about cyberrisk and make decisions about countermeasures.

Exhibit 2

Risk-mitigation initiatives indicated by the bottom-up aggregation approach provide the 'path to green.'



The description of a successful cyberrisk MIS implementation is remarkably congruent with that of a cybersecurity transformation. The steps are as follows:

— **Define the scope and objectives.** Leaders work up front to define objectives and deliverables. They begin by taking stock of how cyberrisk information is gathered and how executives decide on countermeasures. Cybersecurity governance and organization should be established across the whole company, with common standards and best-in-class reporting for systematic risk identification and prioritization.

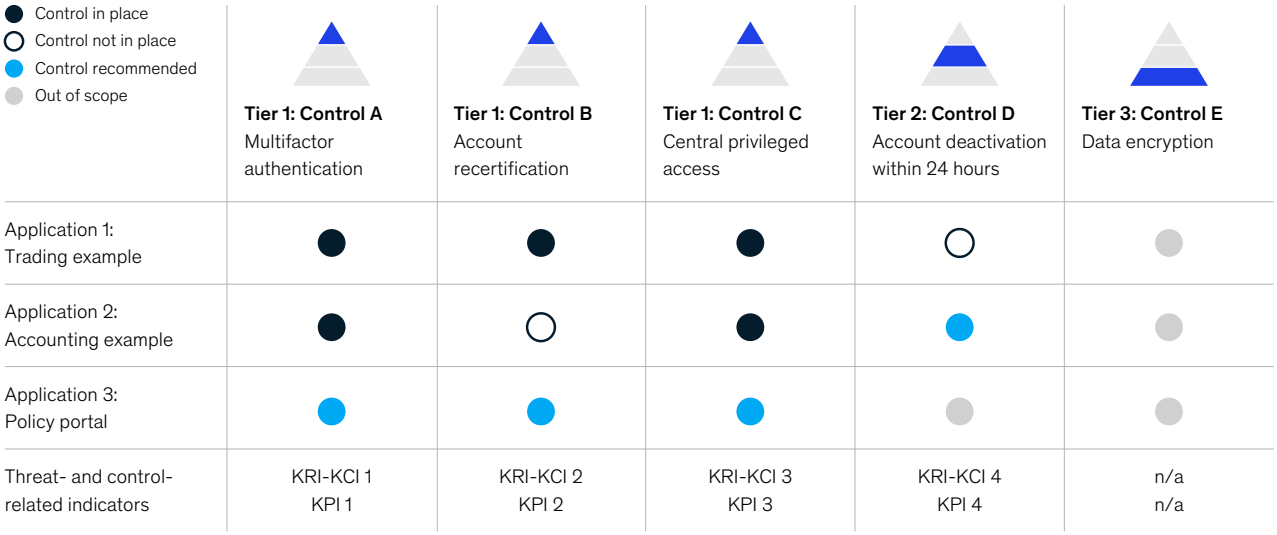
"We don't want to reinvent the wheel. We need a cyberrisk management information system that has a user-friendly interface. It should integrate the best, most recent data from our own sources. It has to be a lean machine. At the same time, it should give us more transparency than we have today."

—Financial-services chief information-security officer

Exhibit 3

The cybersecurity transformation enabled through a cyberrisk management information system includes more effective, less costly differentiated controls.

Cyberrisk management information system, example



Effective information-security risk management is based on asset-centric indicators, including key risk indicators (KRIs), key compliance indicators (KCIs), and key performance indicators (KPIs), revealing compliance issues as well as current and forecasted residual risk exposure.

— **Avoid patchwork solutions.** The cyberrisk MIS must not be regarded as another patch. It should be comprehensive and more accessible than the previous assemblage of stand-alone reports. A good cyberrisk MIS can accommodate different degrees of maturity in different business units. For example, a module can be included that enables managers to upload static reports until dynamic data become available for automatic updates. Generally, the MIS should supply decision makers with the most pertinent information available at any given time.

— **Enhance consistency.** With improved transparency comes improved consistency. As the transformation proceeds, executives should calibrate their understanding of cyberrisk and cybersecurity. They should ask, "As an institution, how much risk are we willing to accept? What are our biggest threats? What level of protection renders a given asset safe?" Even a seemingly trivial risk topic can initiate fruitful discussions. For example, in defining cyberrisk-warning thresholds, executives can arrive at a common understanding of risk appetite, asset relevance, regulatory requirements, and the return on investments in cybersecurity.

— **Shift to a risk-based approach.** One of the most powerful benefits of a good cyberrisk MIS is the risk-based approach to controls (Exhibit 3), which replaces the undifferentiated "all controls for all assets" approach. The risk-based approach focuses on the most important assets and the biggest, most probable threats. Decision makers can then allocate investments accordingly. Resilience is thereby improved without an increased cybersecurity budget. In many cases, a state-of-the-art cyberrisk MIS allows reductions in operating expenditure as well.

One company used the fact base it created in implementing its cyberrisk MIS to introduce a tiered control regime. The company subjected only its most critical, most vulnerable assets (class one) to the full arsenal of controls – from multifactor user authentication to deleting, after 24 hours, the accounts of anyone who left the company. By contrast, it applied only basic controls to the least critical assets (Exhibit 3). As a result of this tiered approach, the company was able to improve

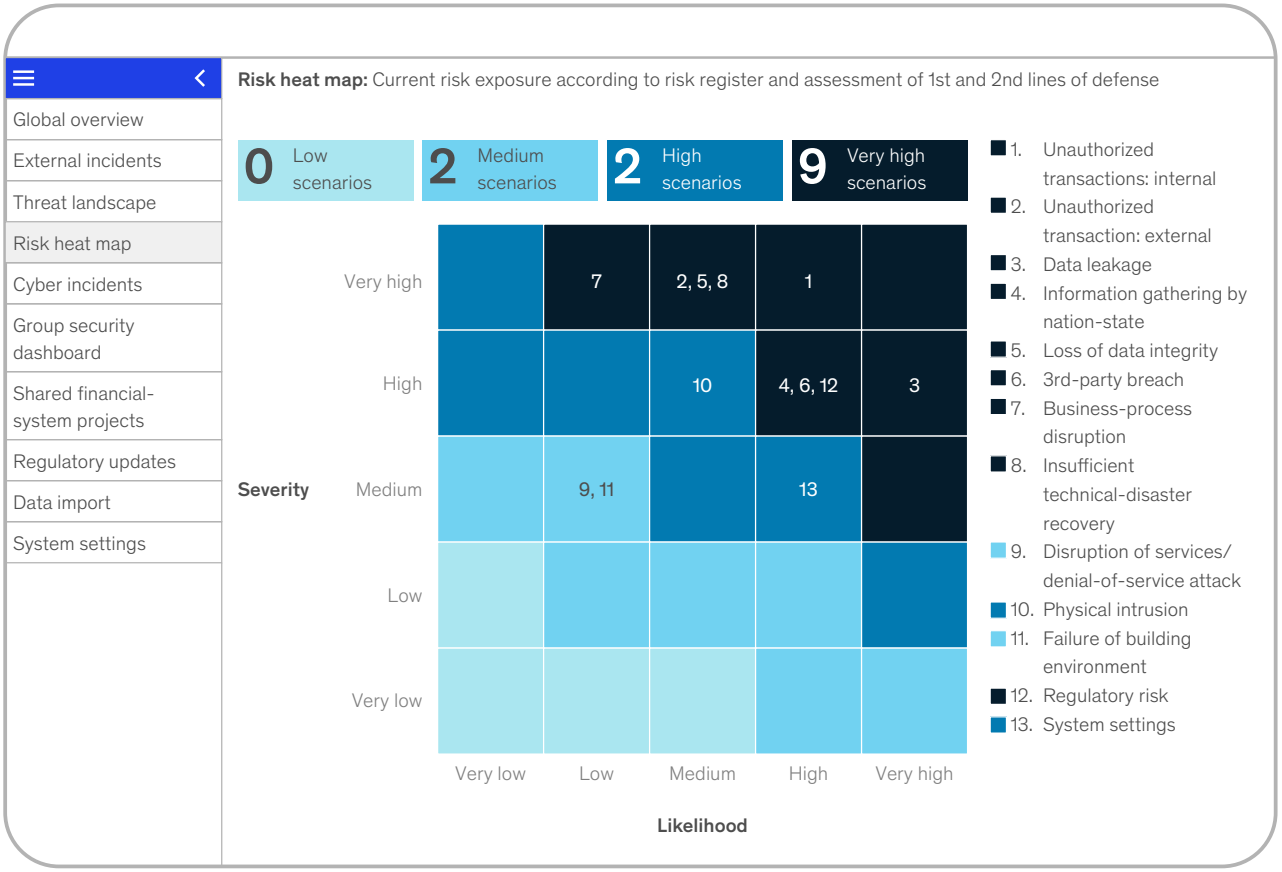
compliance with relevant regulatory requirements while reducing the residual risk level. At the same time, it also reduced costs: both direct costs (such as for software licenses) and indirect costs (such as those incurred through the use of cumbersome, undifferentiated controls, even those for lowlevel applications).

With the right approach, a cyberrisk MIS cybersecurity transformation will provide board-level executives with a concise and easily digestible overview of top cyberrisks. Exhibit 4 shows an MIS cyberrisk dashboard, with the risk heat-map tab open. Other tabs provide the chief risk officer and the chief information officer with the KRIs, KPIs, controls, and progress reports for different functions, organizational levels, and applications. The transformation will foster the use of a common language and a fact-based approach to cyberrisk across the entire institution. Over time, the institution will accrue the benefits of greater cyberrisk transparency, improved cybersecurity efficiency, and greater cyberresilience.

Exhibit 4

The cyberrisk dashboard includes a risk heat map.

Cyberrisk dashboard, example



The fast track to impact

The modular design of the recommended cyberrisk MIS makes it possible to implement a viable version in parts over a period of three to six months, depending on an organization's needs and complexity. For many companies, the most important components – the underlying data structure, the analytical backbone, and the visualization interface – are already in place. In all likelihood, the initial version of a next-generation cyberrisk MIS will not be fully customized to the needs of a given company, but it will be a real working product, not a dummy. The implementation journey begins with a project team, experts, risk managers, data owners, IT, and other stakeholders jointly determining specific requirements, relevant processes, and data availability. In the building stage, live trial sessions

> “Step by step, we made the cyber-risk MIS our own. The whole process took less than half a year, and yet the finished product really feels like something that was made for us, not like an off-the-shelf solution.”
>
> —Cyberrisk MIS user

are held to give executives a chance to provide feedback on MIS utility. After needed adjustments, the scope is widened and the system is deployed to the entire organization.

Leading institutions that have implemented state-of-the-art cyberrisk management information systems have seen significant improvement in the efficacy of cyberrisk detection and remediation. The platform links operational data with groupwide enterprise-risk-management information accurately and consistently. These cyberrisk systems can become the basis for a comprehensive cybersecurity transformation and part of a holistic risk-based approach to cybersecurity, reducing risk, raising resilience, and controlling costs.

Jim Boehm is an associate partner in McKinsey’s New York office, where **James Kaplan** is a partner; **Peter Merrath** is an associate partner in the Frankfurt office, where **Tobias Stähle** is a senior expert; and **Thomas Poppensieker** is a senior partner in the Munich office.

The authors wish to thank Rolf Riemenschnitter for his contributions to this article.

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.

by James Kaplan, Christopher Toomey, and Adam Tyra

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

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.

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

[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.

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,

[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.

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.

James Kaplan is a partner in the New York office. **Christopher Toomey** is a vice president in the Boston office, and **Adam Tyra** is an expert in the Dallas office.

The consumer-data opportunity and the privacy imperative

As consumers become more careful about sharing data, and regulators step up privacy requirements, leading companies are learning that data protection and privacy can create a business advantage.

by Venky Anant, Lisa Donchak, James Kaplan, and Henning Soller

As consumers increasingly adopt digital technology, the data they generate create both an opportunity for enterprises to improve their consumer engagement and a responsibility to keep consumer data safe. These data, including location-tracking and other kinds of personally identifiable information, are immensely valuable to companies: many organizations, for example, use data to better understand the consumer's pain points and unmet needs. These insights help to develop new products and services, as well as to personalize advertising and marketing (the total global value of digital advertising is now estimated at $300 billion).

Consumer data are clearly transforming business, and companies are responsible for managing the data they collect. To find out what consumers think about the privacy and collection of data, McKinsey conducted a survey of 1,000 North American consumers. To determine their views on data collection, hacks and breaches, regulations, communications, and particular industries, we asked them pointed questions about their trust in the businesses they patronize.

The responses reveal that consumers are becoming increasingly intentional about what types of data they share – and with whom. They are far more likely to share personal data that are a necessary part of their interactions with organizations. By industry, consumers are most comfortable sharing data with providers in healthcare and financial services, though no industry reached a trust rating of 50 percent for data protection.

That lack of trust is understandable given the recent history of high-profile consumer-data breaches. Respondents were aware of such breaches, which informed their survey answers about trust. The scale of consumer data exposed in the most catastrophic breaches is staggering. In two breaches at one large corporation, more than 3.5 billion records were made public. Breaches at several others exposed hundreds of millions of records. The stakes are high for companies handling consumer data: even consumers who were not directly affected by these breaches paid attention to the way companies responded to them.

Proliferating breaches and the demand of consumers for privacy and control of their own data have led governments to adopt new regulations, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in that US state. Many others are following suit.

The breaches have also promoted the increased use of tools that give people more control over their data. One in ten internet users around the world (and three in ten US users) deploy ad-blocking software that can prevent companies from tracking online activity. The great majority of respondents – 87 percent – said they would not do business with a company if they had concerns about its security practices. Seventy-one percent said they would stop doing business with a company if it gave away sensitive data without permission.

Because the stakes are so high – and awareness of these issues is growing – the way companies handle consumer data and privacy can become a point of differentiation and even a source of competitive business advantage. The main findings of our research are presented below. We then offer prescriptive steps for data mapping, operations, and infrastructure, as well as customer-facing best practices. These can help companies position themselves to win that competitive advantage.

A matter of trust – or a lack thereof

Consumer responses to our survey led to a number of important insights about data management and privacy. First, consumer-trust levels are low overall but vary by industry. Two sectors – healthcare and financial services – achieved the highest score for trust: 44 percent. Notably, customer interactions in these sectors involve the use of personal and highly sensitive data. Trust levels are far lower for other industries. Only about 10 percent of consumer respondents said that they trust consumer-packaged-goods or media and entertainment companies, for example (Exhibit 1).

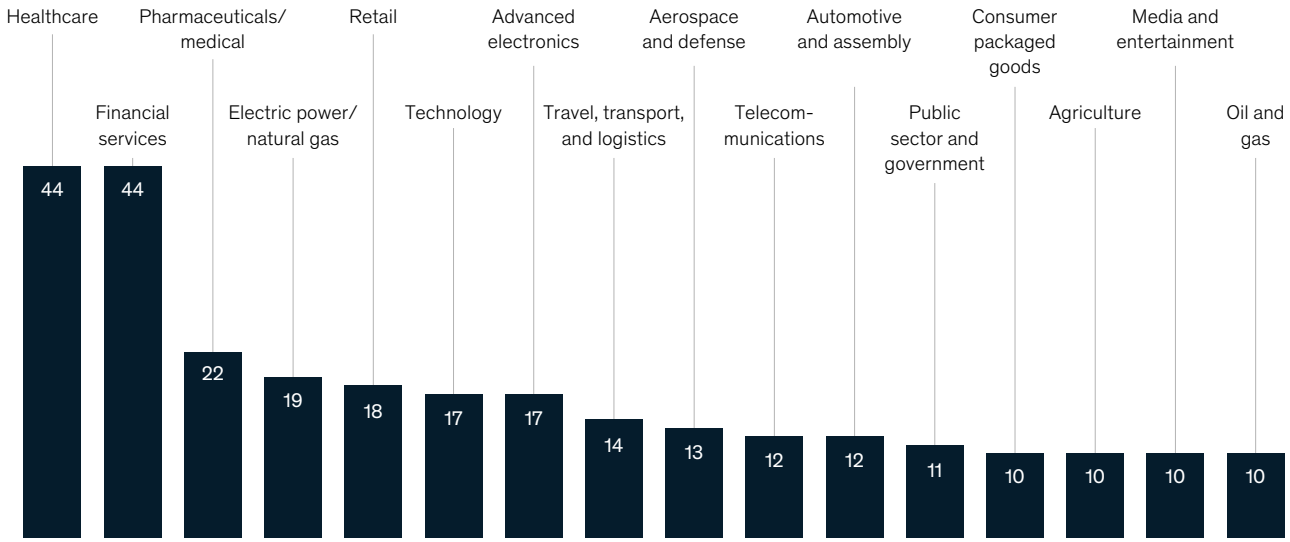
About two-thirds of internet users in the United States say it is "very important" that the content of their email should remain accessible only to those whom they authorize and that the names and identities of their email correspondents remain private (Exhibit 2).

About half of the consumer respondents said they are more likely to trust a company that asks only for information relevant to its products or that limits the amount of personal information requested. These markers apparently signal to consumers that a company is taking a thoughtful approach to data management.

Exhibit 1

Consumers view healthcare and financial-services businesses as the most trustworthy.

Respondents choosing a particular industry as most trusted in protecting of privacy and data, % (n = 1,000)

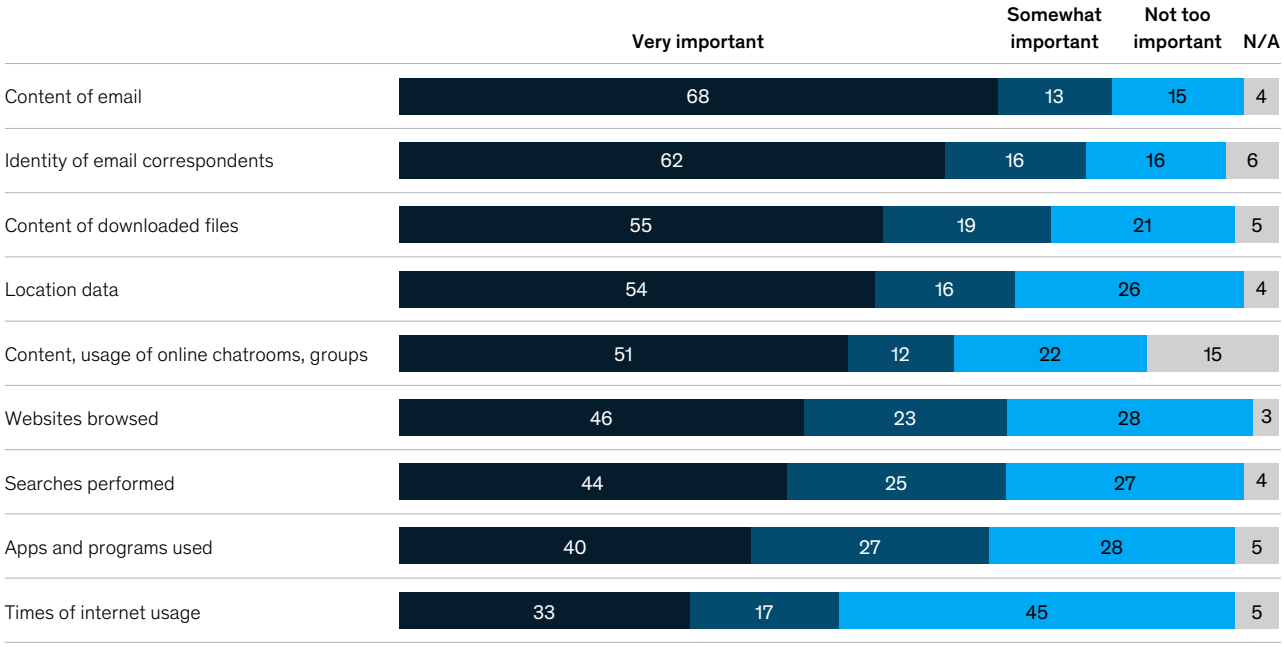


Source: McKinsey Survey of North American Consumers on Data Privacy and Protection, 2019

Exhibit 2

Consumer privacy and protection concerns vary by type of digital data.

Relative importance by data type, % of respondents (n = 792)

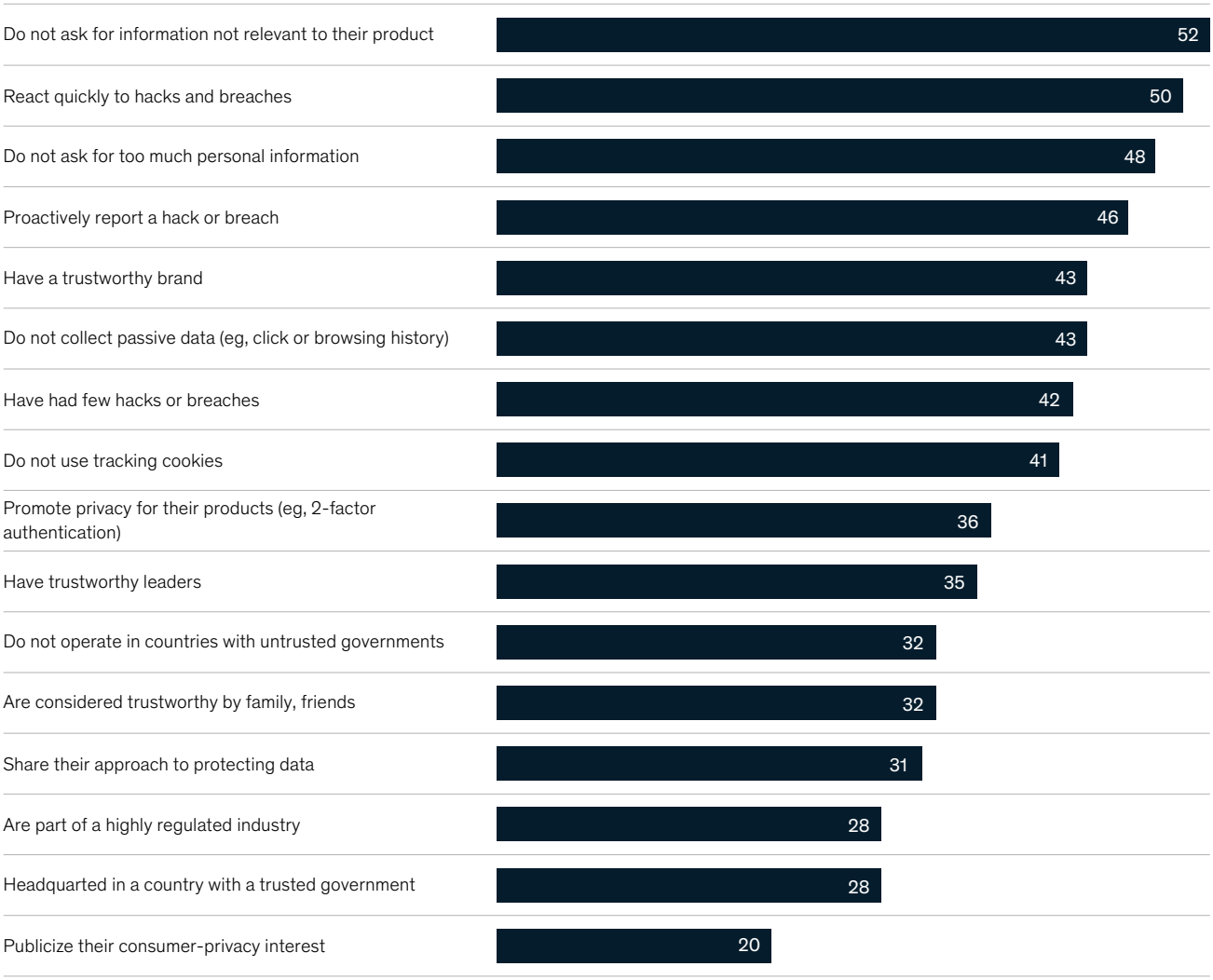


Source: Internet & American Life Project, Pew Research Center

Exhibit 3

Consumers trust companies that limit the use of personal data and respond quickly to hacks and breaches.

Respondent trust by practices, % (n = 1,000)



Source: McKinsey Survey of North American Consumers on Data Privacy and Protection, 2019

Half of our consumer respondents are also more likely to trust companies that react quickly to hacks and breaches or actively disclose such incidents to the public. These practices have become increasingly important both for companies and consumers as the impact of breaches grows and more regulations govern the timeline for data-breach disclosures.

Other issues are of lesser importance in gaining the consumer's trust, according to the survey: the level of regulation in a particular industry, whether a company has its headquarters in a country with a trustworthy government, or whether a company proactively shares cyber practices on websites or in advertisements (Exhibit 3).

Consumer empowerment and actions

Given the low overall levels of trust, it is not surprising that consumers often want to restrict the types of data that they share with businesses. Consumers have greater control over their personal information as a result of the many privacy tools now available, including web browsers with built-in cookie blockers, ad-blocking software (used

on more than 600 million devices around the world), and incognito browsers (used by more than 40 percent of internet users globally). However, if a product or service offering – for example, healthcare or money management – is critically important to consumers, many are willing to set aside their privacy concerns.

Consumers are not willing to share data for transactions they view as less important. They may even "vote with their feet" and walk away from doing business with companies whose data-privacy practices they don't trust, don't agree with, or don't understand. In addition, while overall knowledge of consumer privacy is on the rise, many consumers still don't know how to protect themselves: for example, only 14 percent of internet users encrypt their online communications, and only a third change their passwords regularly (Exhibit 4).

Evolving regulations

Privacy regulations are evolving, with a marked shift towards protecting consumers: the GDPR, for example, implemented in Europe in May 2018, gives consumers more choices and protections about how their data are used. The GDPR gives consumers easier access to data that companies hold about them and makes it easier for them to ask companies to delete their data.

For companies, the GDPR requires meaningful changes in the way they collect, store, share, and delete data. Failure to comply could result in steep fines, potentially costing a company up to 4 percent of its global revenue. One company incurred a fine of $180 million for a data breach that included log-in and payment information for nearly 400,000 people.[1] Another was fined

$57 million for failure to comply with GDPR. A side effect of this regulation is an increased awareness among consumers of their data-privacy rights and protections. About six in ten consumers in Europe now realize that rules regulate the use of their data within their own countries, an increase from only four in ten in 2015.

The GDPR has been considered a bellwether for data-privacy regulation. Even in Europe, policy makers are seeking to enact additional consumer-privacy measures, including the ePrivacy regulation (an extension of GDPR), which focuses on privacy protection for data transmitted electronically. Its status as a regulation (rather than a directive) means that it could be enforced uniformly across EU member states. The ePrivacy regulation is likely to be enacted in 2020.

Beyond Europe

Governments outside Europe have also begun to enact data-privacy regulations. In Brazil, for example, the Lei Geral de Proteção de Dados, or LGPD (General Data Protection Law) will go into effect in August 2020. Brazil's previous data-protection regulations were sector based. The LGPD is an overarching, nationwide law centralizing and codifying rules governing the collection, use, processing, and storage of personal data. While the fines are less steep than the GDPR's, they are still formidable: failing to comply with the LGPD could cost companies up to 2 percent of their Brazilian revenues.

In the United States, the California Consumer Privacy Act (CCPA) went into effect in the state in January 2020. It gives residents the right to know which data are collected about them and to prevent the sale of their data. CCPA is a broad measure, applying to for-profit organizations that do business in California and meet one of the following criteria: earning more than half of their annual revenues from selling consumers' personal information; earning gross revenues of more than $50 million; or holding personal information on more than 100,000 consumers, households, or devices.

The CCPA is the strictest consumer-privacy regulation in the United States, which as yet has no national data-privacy law. The largest fine for mishandling data was, however, issued by the US Federal Trade Commission (FTC).

Compliance investments

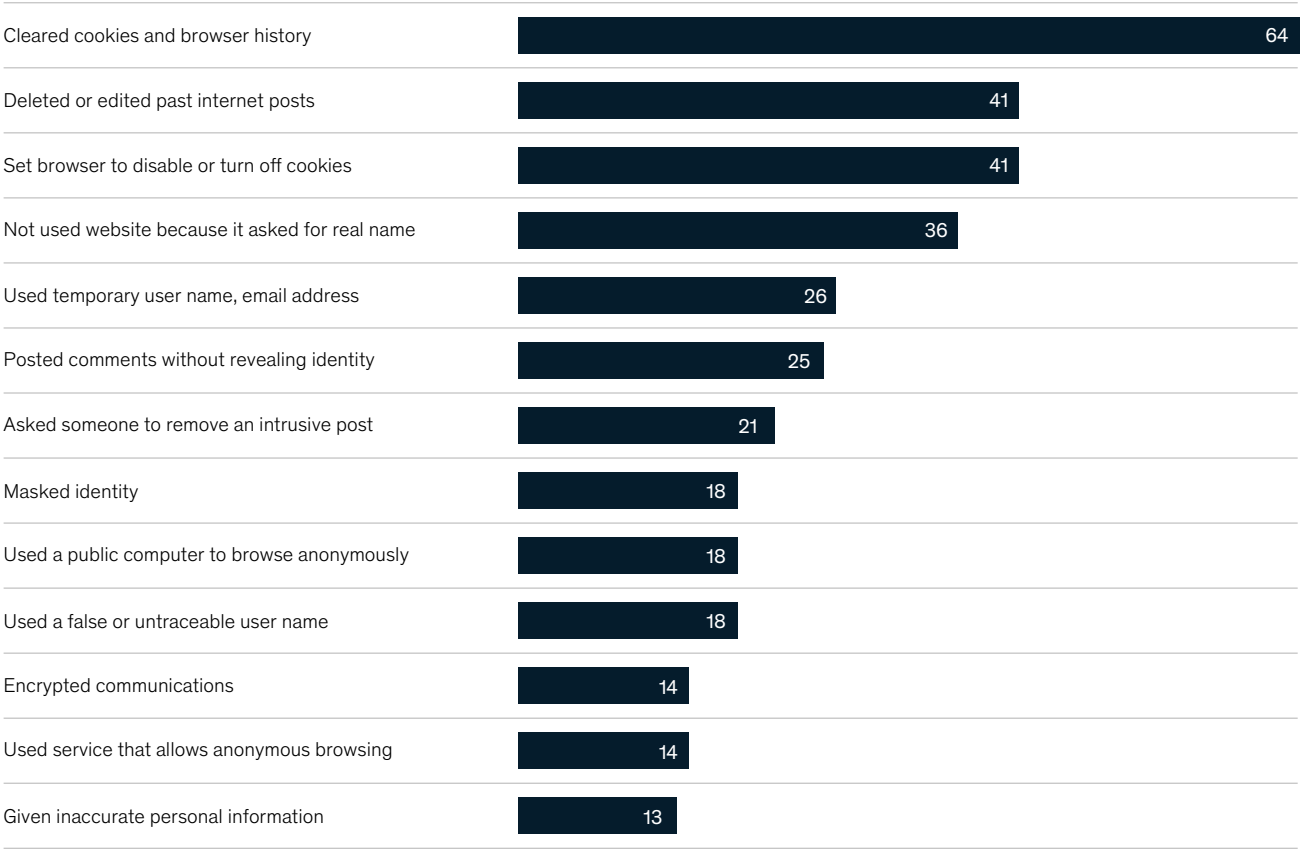
Companies are investing hefty sums to ensure that they are compliant with these new regulations. In total, Fortune Global 500 companies had spent $7.8 billion by 2018 preparing for GDPR, according to an estimate by the International Association of Privacy Professionals. Companies have hired data-protection officers, a newly defined corporate position mandated by the GDPR for all companies handling large amounts of personal data. Despite these measures, few companies

[1] The fine was imposed by the Information Commissions Office, the British data regulator, and is currently under regulatory process review.

Exhibit 4

Consumer concerns over data collection and privacy are mounting, but few take adequate protective precautions.

Respondents taking action, % (n = 792)



Source: Internet & American Life Project, Pew Research Center

feel fully compliant, and many are still working on scalable solutions.

A central challenge – particularly for companies that operate internationally – is the patchwork nature of regulation. Requirements are very different from one jurisdiction or market to another. To address regulatory diversity and anticipate future regulations, many companies have begun systematizing their approach to compliance. Some have begun creating regulatory roles and responsibilities within their organizations. Many are trying to implement future-proof solutions. Rather than meeting CCPA requirements only in California, Microsoft is applying them to all US citizens, though other states do not yet have policies as restrictive as the CCPA. This practice will probably become more common, as many companies are using the most restrictive legal requirements as their own standard. For most companies in the United States, this means following CCPA's guidelines.

Another difficult aspect of privacy regulation has to do with the deletion and porting of data: regulations allow consumers to request that their data be deleted or that enterprises provide user data to individual consumers or other services. For many companies, these tasks are technically challenging. Corporate data sets are often fragmented across varied IT infrastructure, making it difficult to recover all information on individual consumers. Some data, furthermore, may be located outside the enterprise, in affiliate or third-party networks. For these reasons, companies can struggle to identify all data from all sources for transfer or deletion.

Companies should develop clear, standardized procedures to govern requests for the removal or transfer of data.

Proactive steps for companies

Several effective actions have emerged for companies that seek to address enhanced consumer-privacy and data-protection requirements. These span the life cycle of enterprise data, and include steps in operations, infrastructure, and customer-facing practices, and are enabled by data mapping.

Data mapping

Leading companies have created data maps or registers to categorize the types of data they collect from customers. The solution is best designed to accommodate increases in the volume and range of such data that will surely come. Existing data-cataloging and data-flow-mapping tools can support the process.

Companies need to know which data they actually require to serve customers. Much of the data that is collected is not used for analytics and will not be needed in the future. Companies will mitigate risk by collecting only the data they will probably need. Another necessary step is to write or revise data-storage and -security policies. The best approaches account for the different categories of data, which can require different storage policies.

Of further importance is the growing appetite for applied analytics. Today, leading companies need robust analytics policies. Given the proliferation of advanced machine-learning tools, many organizations will seek to analyze the high volumes of data they collect, especially by experimenting with unsupervised algorithms. But unless companies have advanced model-validation approaches and thoughtfully purposed consumer data, they should proceed with extreme caution, probably by focusing specifically on supervised-learning algorithms to minimize risk.

Operations

Leading organizations have developed identity- and access-management practices for individuals according to their roles, with security-access levels determined for different data categories. About one-third of the breaches in recent years have been attributed to insider threats. This risk can be mitigated by ensuring that data sets are accessible only to those who need them and that no one has access to all available data. Even the most robust practices for identity and access management can fail – some breaches can be caused by individuals with approved access – so additional activity monitoring can be helpful.

To act quickly when breaches do occur, organizations will want to pressure-test their crisis-response processes in advance. People who will be involved in the response must be identified and a strong communications strategy developed. One of the highest predictors of consumer trust is the speed of company reporting and response when breaches occur. Indeed, most new regulations require companies to disclose breaches very quickly; the GDPR, for example, mandates the announcement of a breach within 72 hours of its discovery.

Companies should develop clear, standardized procedures to govern requests for the removal or transfer of data. These should ensure expedited compliance with regulations and cover consumer requests for the identification, removal, and transfer of data. The processes should support data discovery in all pertinent infrastructure environments within a company and across its affiliates. Most companies today use manual processes, which creates an opportunity for streamlining and automating them to save time and resources. This approach also prepares infrastructure environments for future process developments.

Working closely with third parties, affiliates, and vendors, companies can gain an understanding of how and where their data are stored. This knowledge is especially important when third

parties are supporting the development of products and features and need access to consumer data. Some companies are considering establishing review boards to support decisions about sharing data with third parties.

Infrastructure
Organizations are working to create infrastructure environments that can readily accommodate the increasing volumes of data collected, as well as attending technological innovations. Best practice is to store data in a limited number of systems, depending on data type or classification. A smaller systems footprint reduces the chance of breaches.

Customer-facing best practices
Leading companies are building "privacy by design" into consumer-facing applications, with such features as automatic timed logouts and requirements for strong passwords. Security and privacy become default options for consumers, while features strike a balance with the user experience.

It is important for organizations to communicate transparently: customers should know when and why their data are being collected. Many companies are adding consumer privacy to their value propositions and carefully crafting the messages in their privacy policies and cookie notices to align with the overall brand.

Our research revealed that our sample of consumers simply do not trust companies to handle their data and protect their privacy. Companies can therefore differentiate themselves by taking deliberate, positive measures in this domain. In our experience, consumers respond to companies that treat their personal data as carefully as they do themselves.

Venky Anant is a partner in McKinsey's Silicon Valley office, where **Lisa Donchak** is a consultant; **James Kaplan** is a partner in the New York office; **Henning Soller** is a partner in the Frankfurt office.

Consumer-data privacy and personalization at scale: How leading retailers and consumer brands can strategize for both

Customer concerns about the security and privacy of their online data can impede personalized marketing at scale. Best-practice companies are building protections into their digital properties.

by Julien Boudet, Jess Huang, Kathryn Rathje, and Marc Sorel

Personalization at scale is where retailers and consumer brands are competing to win. But in focusing on "playing offense" to capture value, executives are often overlooking their "defense": preserving, protecting, enabling, and accelerating the hard-won gains of their digital efforts by ensuring that personalization at scale keeps personal data secure and private.

As the enterprise risk of collecting, holding, and using consumer data to personalize offerings grows, so do the business-impairing consequences for those who fail to get it right. Despite these challenges and opportunities, most marketing leaders remain surprisingly unconcerned with how to manage data security and privacy.

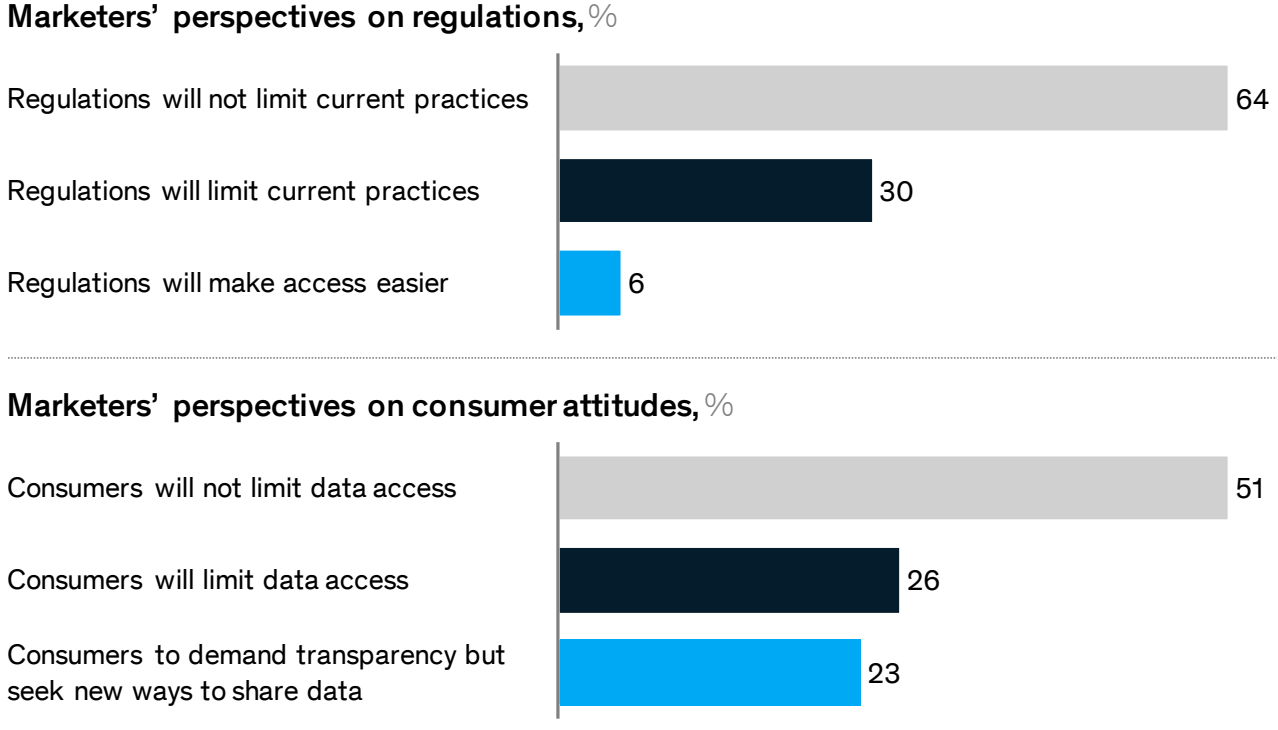
In a recent McKinsey survey of senior marketing leaders, 64 percent said they don't think regulations will limit current practices, and 51 percent said they don't think consumers will limit access to their data (Exhibit 1) – this despite other recent surveys showing that more than 90 percent of consumers are concerned about their online privacy, and nearly 50 percent have limited their online activity because of privacy concerns.[1]

Getting the security and privacy of personalization wrong can slow time to market for new applications, constrain remarketing and consumer-data collection, result in significant fines, or – worse – cause material harm to brand reputation through negative consumer experience. Getting it right reduces time to market, puts security and privacy at the heart of the company's value proposition, boosts customer-satisfaction scores, and materially reduces the likelihood of regulatory fines.

[1] Brian Byer, "Internet users worry about online privacy but feel powerless to do much about it," Entrepreneur, June 20, 2018, entrepreneur.com; and Rafi Goldberg, "Lack of trust in internet privacy and security may deter economic and other online activities," National Telecommunications

Exhibit 1

Many marketers feel confident that neither regulations nor consumer sentiment will limit data collection in the future.



Source: 2018 senior management personalization survey: Based on question 27: How do you expect regulations to affect personalization practices in your industry? And question 28: How do you expect customer behavior regarding data collection to evolve over the next six years?

Where to start

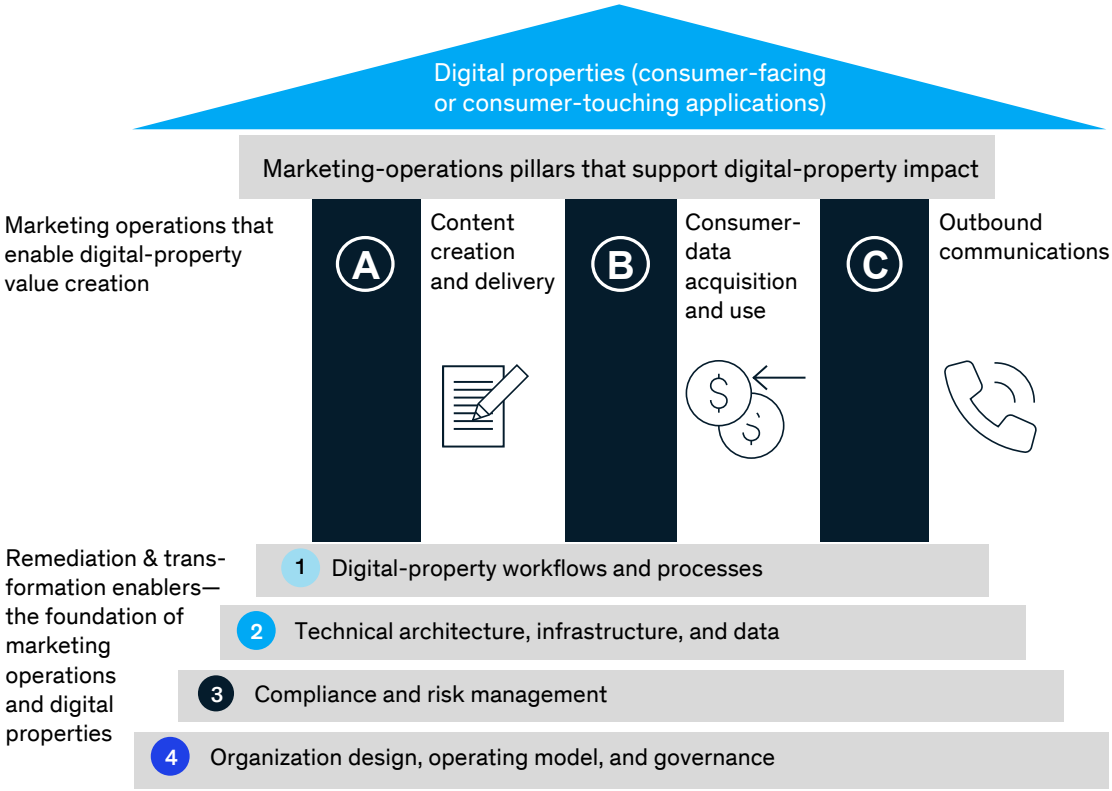
For most companies, getting security and privacy right begins with remediating and transforming the digital-marketing applications and systems that generate, transmit, consume, store, or dispose of consumer data (Exhibit 2). Leading brands make this part of a broader baseline assessment of data security and privacy across people, processes, and technology and tie it to business use cases.

They also put marketing at the center of the effort, educating teams on the value at stake through, for example:

- Establishing and enforcing standards on security and privacy for creative agencies
- Using best practices for data protection in their day-to day-work
- Tokenizing consumer data ensuring consent compliance
- Sanitizing data before using them in outbound communications and remarketing
- Being accountable for incidents when they occur

Exhibit 2

The marketing structure should enable digital-property remediation and transformation.



Descriptions (not exhaustive):

A
- a) **Content development** for consumer-facing brand websites
- b) **Content delivery through e-commerce and merchandising** portraying products and brands in a way that allows the enterprise to "do business" with its customers

B
- a) **Cookie management** to granularly track and collect consumer-behavior data across properties as customers engage with them
- b) **Remarketing** by using data to drive portrayal and placement of products and brands with which the consumer engages

C
- a) **Using consumer data from digital properties and other sources to drive outbound marketing** (such as pay-per-click, advertising, digital display)

1. Where and how digital assets/properties should be created and maintained
2. Technical capabilities, such as data lake or discovery scan tools, to facilitate collection, storage, management, and testing of consumer data
3. The global vs local policies, processes, and tools to adopt, follow, and validate to meet security-and-privacy obligations in a variety of regulatory environments
4. Agile organization and operating model that clarifies roles and responsibilities across functions and rationalizes external partners/agencies

The dialogue with marketing and other stakeholders in this context should be ongoing, to match the enterprise's evolving needs for data and technical capabilities and to capture the value from use cases.

An imperative on security and privacy can help with many things – from eliminating tech debt to breaking down silos – by opening iterative dialogue on data needs and new operational requirements between the business and the security and privacy functions. Aligning on core beliefs and a framework to approach the effort (Exhibit 3) can help the team quickly get the needed conviction and buy-in.

How to move quickly at scale

As the transformation of data management is piloted and scaled, prioritizing a few key actions to improve security and privacy will ensure outcomes that enable rather than disable the business.

Build a risk register for digital properties
Taking a risk-back approach can help the executive team defend its decisions on where and how to allocate spend on security and privacy. Understanding how properties such as information systems and assets map to each other, to the threat landscape, and to the business value chain also clarifies where eliminating risks can enhance enterprise value.

Clarify data strategy, governance, and policies, and build in the roles and requirements to make them work
The details of programs for data security and privacy may vary by company, industry, or the local regulatory climate. Consumer and retail enterprises, for example, often hold consumer data for no more than 13 months, in order to track consumer patterns through seasons and holidays. Auto retailers, on the other hand, often hold data longer, to reflect the longer time between automotive purchases, which tend to be multiyear, not annual. Other companies may tailor their global privacy policy to meet local regulatory requirements, such as General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA).

Exhibit 3

Company alignment on the core principles for transforming digital properties will enable personalization at scale.

Manage digital property the way you manage your people. Knowing the identity, performance, and safety of your applications is as important as knowing the identity, performance, and reliability of your people.

Anchor the approach in use cases. For a successful transformation, understand which business use cases the transformed digital properties will support, and clarify the architectural gaps you need to fill to support both properties and use cases.

Create and maintain a risk-based asset inventory. This will help to clarify your enterprise digital-property landscape, as well as compliance issues and business risk, and is an essential tool for prioritizing transformation initiatives.

Align risk with enterprise appetite. A risk-back, minimum viable approach to building security-and-privacy protections into the transformation of digital properties is a commercial imperative for personalization at scale.

Clarify roles, responsibilities, decision rights, and talent requirements across the organization. This is the key to ensuring you can quickly embed the cross-functional capabilities needed to bring new properties to market.

Implement the transformation by deploying cross-functional teams in agile sprints. This will not only mitigate execution risk—a requirement, not an option—but also enable you to capture value at scale and demonstrate that the process is iterative.

But some best practices are emerging as enterprises focus on data privacy and security. One leading privacy policy is the tokenization and sanitization of data before using them in remarketing. Further, leading institutions will align on the "minimum viable data and controls" required to preserve a long-term view of consumers and empathetically engage them at scale. To embed awareness of security and privacy across an enterprise, some companies find it useful to create roles for business-information security and privacy officers (BISPOs) or "security and privacy ambassadors." Such programs can not only empower employee teams to become knowledgeable about organization practices on security and privacy but also ensure that the integrity of digital properties continues long after they are transformed and remediated.

In the event of a breach of data security or privacy, it is helpful to have in place incident-response plans that are "living documents" formed through the test-and-learn iterative process of simulation. These can help executive teams make better decisions faster about managing their digital properties – and their relationships with regulators.

Build security and privacy into enterprise analytics and application development

Consider the example of an enterprise seeking to transform itself into a platform company using consumer and customer data to cocreate application programming interfaces (APIs) to transform how consumers engaged with the brand. Before the enterprise built security requirements into its application development, it had missed at least one major market opportunity because of regulators' security concerns, frequently experienced application launch delays because of security-related rework requirements, and lacked capacity to verify whether around 80 percent of the business-support applications it developed annually complied with its requirements on security and privacy.

By building those requirements into its software-development policies, the enterprise made the software-developer team responsible for meeting them right from the start, in the design phase. The security-and-privacy team would only involve itself "by exception," if a development team declined to meet a specified requirement. This approach ensured that standards on security and privacy were met in more than 90 percent of applications developed, which reduced downstream rework, accelerated time to market, and put data protection at the center of the enterprise's value proposition to consumers.

Create and deliver role-based training on security and privacy

Given that more than 80 percent of enterprise cybersecurity incidents begin with a human clicking on malware, regular training tailored to key roles is essential to reduce the risks of personalization. Marketing teams, for example, might need to learn best practices for remarketing, such as parsing data to eliminate personal identifiability while preserving business value.

There are about 15 core employee behaviors that can be addressed and transformed through a focused campaign of annual training supported by unpredictable reminders, such as occasional emails and text messages or antiphishing test campaigns. Similarly, building security and privacy standards into performance reviews – for example, setting a threshold for the number of security or privacy incidents in a line of business over a period of time – can ensure that the entire business, not just the experts on security and privacy, owns the problem and the solution.

Personalize security and privacy for the consumer

Leading financial institutions have already unlocked the value of increasing net promoter scores (NPS) by taking the hassle out of consumer validation processes. By reducing hold times, simplifying and tailoring multifactor authentication to meet consumer preferences, and placing data-protection controls for consumer-facing applications in the hands of the consumer, they are improving customer experience without compromising underlying security and privacy.

Leading retailers and consumer brands can adopt a product-management mind-set and delight consumers by building data-protection options into consumer-facing applications and support functions. By partnering with cutting-edge technology innovators, they can tailor processes to what is most convenient for the consumer. Good places to start are multifactor authentication by text, call, or randomly generated code, or built-in strong-password-generating tools to simplify password recall for consumers accessing a retailer's direct-to-consumer application. Measuring performance over time through commonly available customer-experience

dashboards such as NPS can ensure that attempts to build security and privacy into consumer-facing applications are refined quickly and iteratively.

The opportunity around personalization at scale for consumer brands and retailers has never been more critical to capture. At the same time, the need to create a net positive consumer experience while avoiding the downsides of reputational, operational, legal, and financial risks is a hard balance to strike. Several core questions can help clarify where your enterprise stands – and what to do about it:

1. How does your personalization technology measure your customer's security and privacy experience?
2. What is your enterprise's critical-asset or -system risk register for data security and privacy?
3. How complete is your security-and-privacy technology stack, and how do you determine this?
4. How are you managing your data to derive value-creating analytic insight from personalization without causing value-destroying financial or operational loss due to privacy or security incidents?
5. What is the state of your secure software-development life cycle program?
6. How are you ensuring the secure operation of your cloud environment?
7. How are you ensuring that security and privacy are every employee's responsibility?
8. What is your capability aspiration for customer-data security and privacy, how are you measuring progress toward that aspiration, and how are you reporting progress to the board?

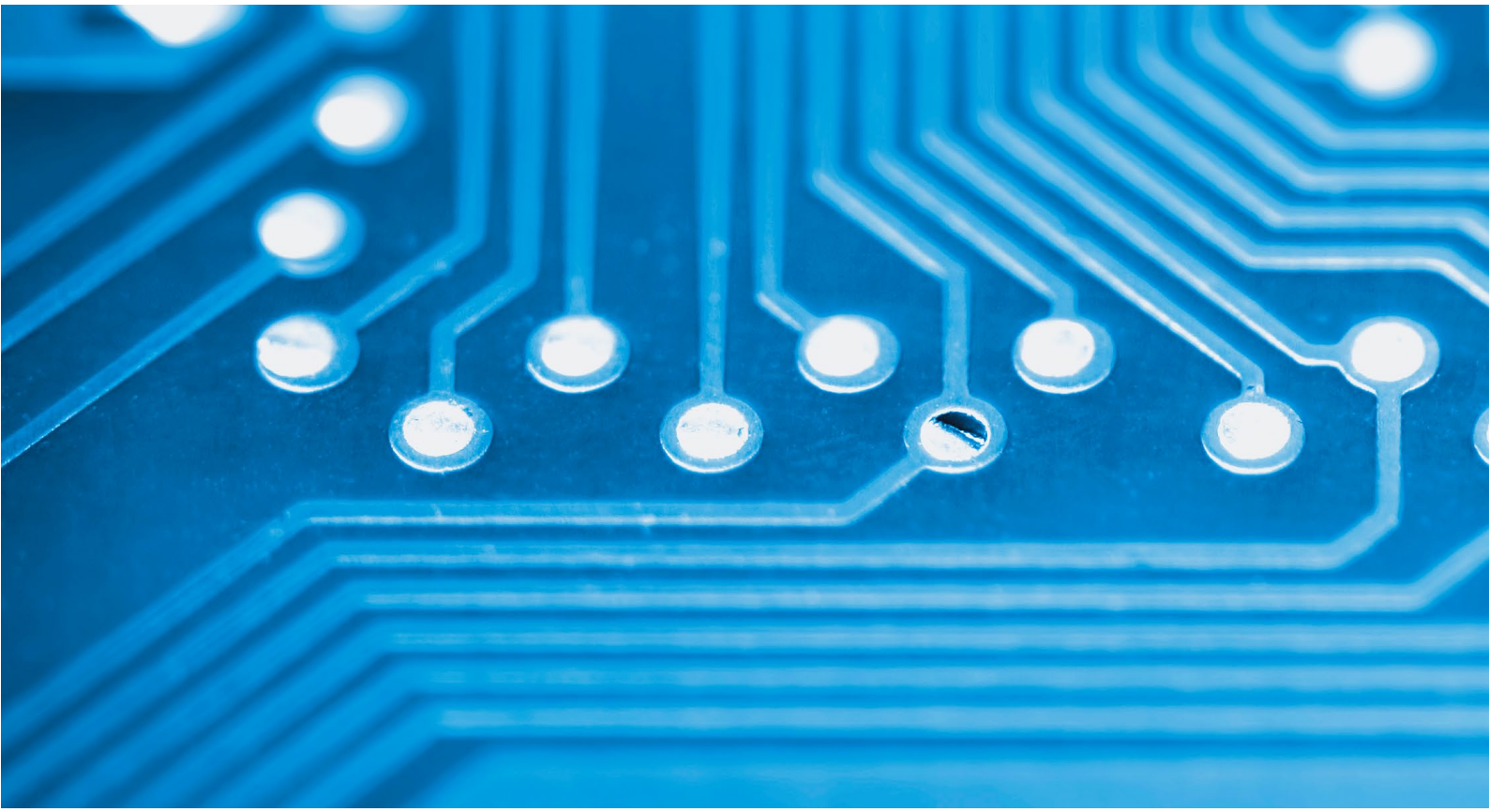
By answering these questions, companies can help ensure that personalization at scale is only a benefit, not a bane, to any consumer and brand.

Julien Boudet is a partner in McKinsey's Southern California office, **Jess Huang** is a partner in the Silicon Valley office, **Kathryn Rathje** is an associate partner in the San Francisco office, and **Marc Sorel** is a consultant in the Washington, DC, office.

Financial crime and fraud in the age of cybersecurity

As cybersecurity threats compound the risks of financial crime and fraud, institutions are crossing functional boundaries to enable collaborative resistance.

by Salim Hasham, Shoan Joshi, and Daniel Mikkelsen



In 2018, the World Economic Forum noted that fraud and financial crime was a trillion-dollar industry, reporting that private companies spent approximately $8.2 billion on anti-money laundering (AML) controls alone in 2017. The crimes themselves, detected and undetected, have become more numerous and costly than ever. In a widely cited estimate, for every dollar of fraud institutions lose nearly three dollars, once associated costs are added to the fraud loss itself.[1] Risks for banks arise from diverse factors, including vulnerabilities to fraud and financial crime inherent in automation and digitization, massive growth in transaction volumes, and the greater integration of financial systems within countries and internationally. Cybercrime and malicious hacking have also intensified. In the domain of financial crime, meanwhile, regulators continually revise rules, increasingly to account for illegal trafficking and money laundering, and governments have ratcheted up the use of economic sanctions, targeting countries, public and private entities, and even individuals. Institutions are finding that their existing approaches to fighting such crimes cannot satisfactorily handle the many threats and burdens. For this reason, leaders are transforming their operating models to obtain a holistic view of the evolving landscape of financial crime. This view becomes the starting point of efficient and effective management of fraud risk. The evolution of fraud and financial crime Fraud and financial crime adapt to developments in the domains they plunder. (Most financial institutions draw a distinction between these two types of crimes: for a view on the distinction, or lack thereof, see the sidebar "Financial crime or fraud?") With the advent of digitization and automation of financial systems, these crimes have become more electronically sophisticated and impersonal. One series of crimes, the so-called Carbanak attacks beginning in 2013, well illustrates the cyber profile of much of present-day financial crime and fraud. These were malware-based bank thefts totaling

[1] World Economic Forum Annual Meeting, Davos-Klosters, Switzerland, January 23–26, 2018; LexisNexis risk solutions 2018 True Cost of Fraud study, LexisNexis, August 2018, risk.lexisnexis.com.

Sidebar

Financial crime or fraud?

For purposes of detection, interdiction, and prevention, many institutions draw a distinction between fraud and financial crime. Boundaries are blurring, especially since the rise of cyberthreats, which reveal the extent to which criminal activities have become more complex and interrelated. What's more, the distinction is not based on law, and regulators sometimes view it as the result of organizational silos. Nevertheless, financial crime has generally meant money laundering and a few other criminal transgressions, including bribery and tax evasion, involving the use of financial services in support of criminal enterprises. It is most often addressed as a compliance issue, as when financial institutions avert fines with anti-money laundering activities. Fraud, on the other hand, generally designates a host of crimes, such as forgery, credit scams, and insider threats, involving deception of financial personnel or services to commit theft. Financial institutions have generally approached fraud as a loss problem, lately applying advanced analytics for detection and even real-time interdiction. As the distinction between these three categories of crime have become less relevant, financial institutions need to use many of the same tools to protect assets against all of them.

more than $1 billion. The attackers, an organized criminal gang, gained access to systems through phishing and then transferred fraudulently inflated balances to their own accounts or programmed ATMs to dispense cash to waiting accomplices (Exhibit 1).

Significantly, this crime was one simultaneous, coordinated attack against many banks. The attackers exhibited a sophisticated knowledge of the cyber environment and likely understood banking processes, controls, and even vulnerabilities arising from siloed organizations and governance. They also made use of several channels, including ATMs, credit and debit cards, and wire transfers. The attacks revealed that meaningful distinctions among cyberattacks, fraud, and financial crime are disappearing. Banks have not yet addressed these new intersections, which transgress the boundary lines most have erected between the types of crimes (Exhibit 2).

A siloed approach to these interconnected risks is becoming increasingly untenable; clearly, the operating model needs to be rethought.

As banks begin to align operations to the shifting profile of financial crime, they confront the deepening connections between cyber breaches and most types of financial crime. The cyber element is not new, exactly. Until recently, for example, most fraud has been transaction based, with criminals exploiting weaknesses in controls. Banks counter such fraud with relatively straightforward, channel-specific, point-based controls. Lately, however, identity-based fraud has become more prevalent, as fraudsters develop applications to exploit natural or synthetic data. Cyber-enabled attacks are becoming more ambitious in scope and omnipresent, eroding the value of personal information and security protections.

Exhibit 1

The new cyber profile of fraud and financial crime is well illustrated by the Carbanak attacks.

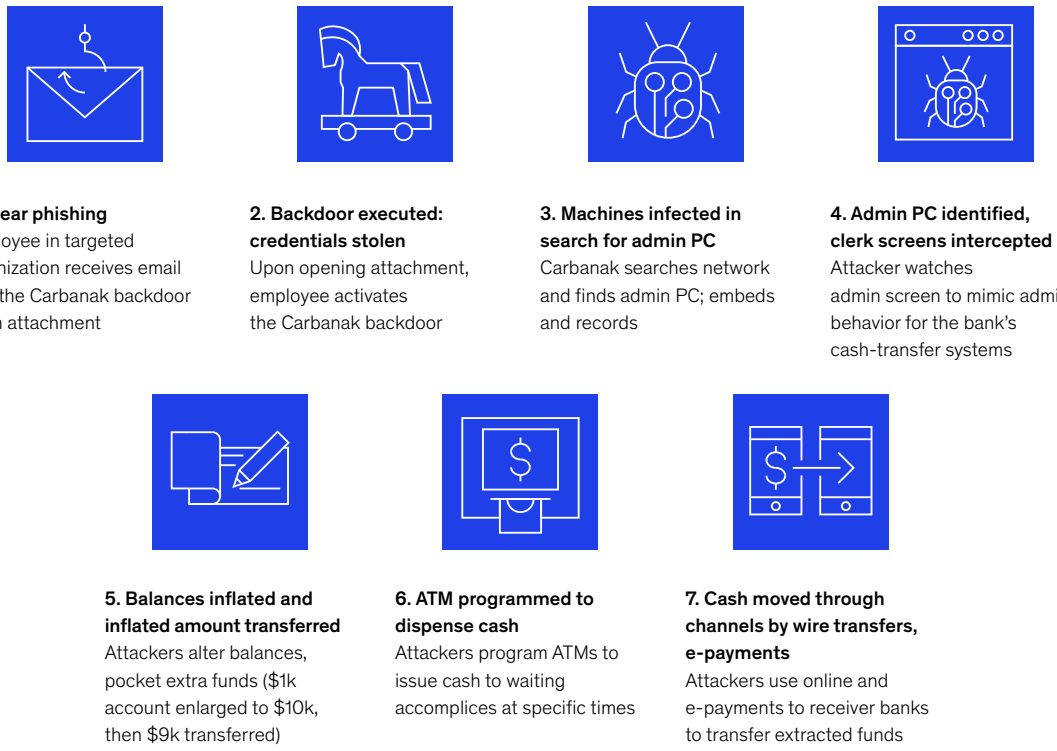
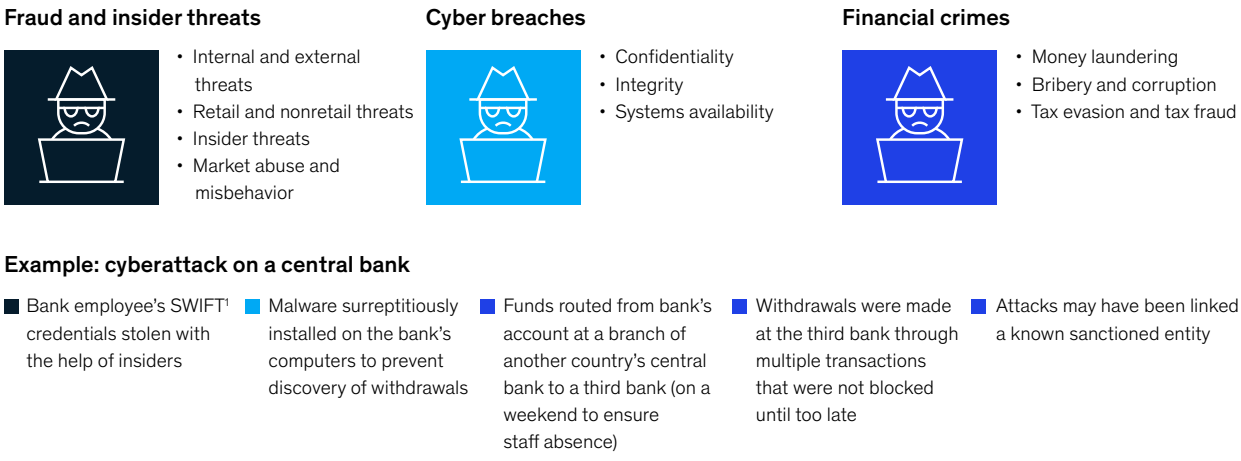


Exhibit 2

Crime pathways are converging, blurring traditional distinctions among cyber breaches, fraud, and financial crimes.



[1] Society for Worldwide Interbank Financial Telecommunication.

In a world where customers infrequently contact bank staff but rather interact almost entirely through digital channels, "digital trust" has fast become a significant differentiator of customer experience. Banks that offer a seamless, secure, and speedy digital interface will see a positive impact on revenue, while those that don't will erode value and potentially lose business. Modern banking demands faster risk decisions (such as real-time payments) so banks must strike the right balance between managing fraud and handling authorized transactions instantly.

The growing cost of financial crime and fraud risk has also overshot expectations, pushed upward by several drivers. As banks focus tightly on reducing liabilities and efficiency costs, losses in areas such as customer experience, revenue, reputation, and even regulatory compliance are being missed (Exhibit 3).

Bringing together financial crime, fraud, and cyber operations

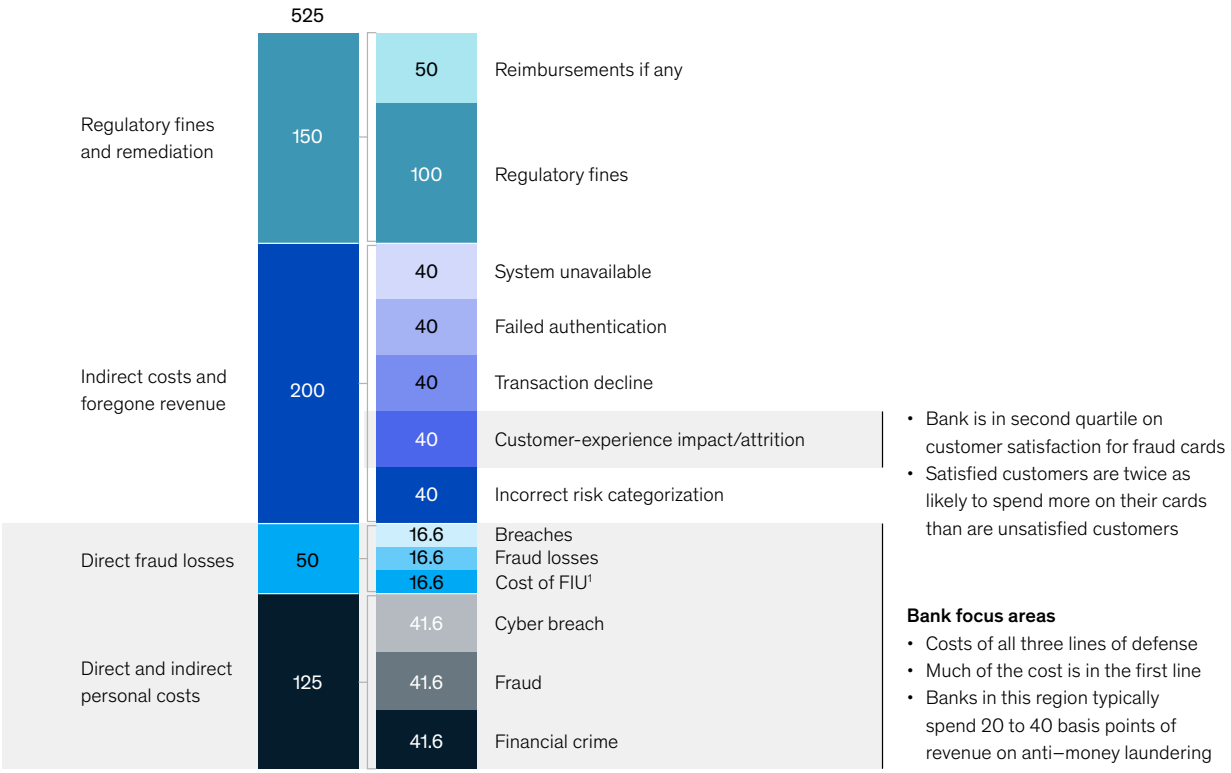
At leading institutions the push is on to bring together efforts on financial crime, fraud, and cybercrime. Both the front line and back-office operations are oriented in this direction at many banks. Risk functions and regulators are catching on as well. AML, while now mainly addressed as a regulatory issue, is seen as being on the next horizon for integration. Important initial steps for institutions embarking on an integration effort are to define precisely the nature of all related riskmanagement activities and to clarify the roles and responsibilities across the lines of defense. These steps will ensure complete, clearly delineated coverage – by the businesses and enterprise functions (first line of defense) and by risk, including financial crime, fraud, and cyber operations (second line) – while eliminating duplication of effort.

All risks associated with financial crime involve three kinds of countermeasures: identifying and authenticating the customer, monitoring and detecting transaction and behavioral anomalies, and responding to mitigate risks and issues. Each of these activities, whether taken in response to fraud, cybersecurity breaches or attacks, or other financial crimes, are supported by many similar data and processes. Indeed, bringing these data sources together with analytics materially improves visibility while providing much deeper insight to improve detection capability. In many instances it also enables prevention efforts.

Exhibit 3

Banks often focus on only a fraction of total financial-crime, fraud, and cybersecurity costs.

Example of financial-crime, fraud, and cybersecurity costs, $ million



[1] Financial intelligence unit.

In taking a more holistic view of the underlying processes, banks can streamline business and technology architecture to support a better customer experience, improved risk decision making, and greater cost efficiencies. The organizational structure can then be reconfigured as needed. (Exhibit 4).

From collaboration to holistic unification

Three models for addressing financial crime are important for our discussion. They are distinguished by the degree of integration they represent among processes and operations for the different types of crime (Exhibit 5).

Generally speaking, experience shows that organizational and governance design are the main considerations for the development of the operating model. Whatever the particular choice, institutions will need to bring together the right people in agile teams, taking a more holistic approach to common processes and technologies and doubling down on analytics – potentially creating "fusion centers," to develop more sophisticated solutions. It is entirely feasible that an institution will begin with the collaborative model and gradually move toward greater integration, depending on design decisions. We have seen many banks identify partial integration as their target state, with a view that full AML integration is an aspiration.

Exhibit 4

At their core, all functions perform the same three roles using similar data and processes.

	Identification: "Who is my customer?"	Monitoring: "What transactions are legitimate?"	Response: "How do I respond to a threat?"
Financial crime	• Client risk rating • Client due diligence; enhanced due diligence	• Transaction monitoring • Name screening • Payments screening	• Suspicious-activity monitoring • Financial intelligence unit • List management • Do not bank
Fraud	• Identity verification, including digital and nondigital presence	• Transaction monitoring and decision making • Device and voice analytics	• Investigations and resolutions teams
Cybersecurity	• Credentials management	• Security-operations center (SOC) and network-operations center, which enable monitoring	• SOC • Forensics • Resolution teams
Synergies across functions	• Risk scoring of customers using common and similar customer data, such as financials, digital footprint, nondigital records	• Risk scoring of transactions using similar analytics and common use cases based on timing, destination, source, value and frequency, device, and geolocation intelligence	• Common feedback loop to develop a holistic view on modus operandi and drive top-down use-case development • Pooling of resources and capabilities

1. **Collaborative model.** In this model, which for most banks represents the status quo, each of the domains – financial crime, fraud, and cybersecurity – maintain their independent roles, responsibilities, and reporting. Each unit builds its own independent framework, cooperating on risk taxonomy and data and analytics for transaction monitoring, fraud, and breaches. The approach is familiar to regulators, but offers banks little of the transparency needed to develop a holistic view of financial-crime risk. In addition, the collaborative model often leads to coverage gaps or overlaps among the separate groups and fails to achieve the benefits of scale that come with greater functional integration. The model's reliance on smaller, discrete units also means banks will be less able to attract top leadership talent.
2. **Partially integrated model for cybersecurity and fraud.** Many institutions are now working toward this model, in which cybersecurity and fraud are partially integrated as the second line of defense. Each unit maintains independence in this model but works from a consistent framework and taxonomy, following mutually accepted rules and responsibilities. Thus, a consistent architecture for prevention (such as for customer authentication) is adopted, risk-identification and assessment processes (including taxonomies) are shared, and similar interdiction processes are deployed. Deeper integral advantages prevail, including consistency in threat monitoring and detection and lower risk of gaps and overlap. The approach remains, however, consistent with the existing organizational structure and little disrupts current operations. Consequently, transparency is not increased, since separate reporting is maintained. No benefits of scale accrue, and with smaller operational units still in place, the model is less attractive to top talent.
3. **Unified model.** In this fully integrated approach, the financial crimes, fraud, and cybersecurity operations are consolidated into a single framework, with common assets and systems used to manage risk across the enterprise. The model has a single view of the customer and shares analytics. Through risk convergence, enterprise-wide transparency on threats is enhanced, better revealing the most important underlying risks. The unified model also captures benefits of scale across key roles and thereby enhances the bank's ability to attract and retain top talent. The disadvantages of this model are that it entails significant organizational change, making bank operations less familiar to regulators. And even with the organizational change and risk convergence, risks remain differentiated.

Exhibit 5

The three models address financial crime with progressively greater levels of operational integration.

	Traditional: collaboration	Ongoing: partial integration[1]	Future: complete integration
Model features	• Independent reporting, roles, and responsibilities for each type of financial crime • Independent framework built by each unit	• Each financial-crime unit maintains independence but uses a consistent framework and taxonomy with agreed-upon rules and responsibilities: – Fraud and cybersecurity join on prevention (eg, on customer authentication) – Consistent processes for risk identification and assessment – Similar processes (eg, interdiction)	• Consolidated unit under a single framework using common assets and systems to manage risks: – Single view of the customer – Shared analytics
Pluses and minuses	⊕ Least disruptive: maintains the status quo ⊕ Regulators most familiar with the model ⊖ Less visibility into overall financial-crime risk ⊖ Potential gaps, overlap among groups ⊖ No scale benefits ⊖ Smaller units less able to attract top talent	⊕ More unified approach with lower risk of gaps/overlaps ⊕ Consistent organizational structure with status quo ⊕ Limited disruption from current state ⊖ Maintains separate reporting; does not increase transparency ⊖ No scale benefits ⊖ Smaller units less able to attract top talent	⊕ Underlying risks are converging ⊕ Enhanced ability to attract and retain talent ⊕ Standard and common framework on what is being done ⊕ Benefits of scale across key roles ⊖ Largest organizational change ⊖ While converging, risks remain differentiated ⊖ Regulators are less familiar with setup

Banks have begun by closely integrating cybersecurity and fraud while stopping short of a fully integrated unit

[1]Mainly cybersecurity and fraud.

The imperative of integration

The integration of fraud and cybersecurity operations is an imperative step now, since the crimes themselves are already deeply interrelated. The enhanced data and analytics capabilities that integration enables are now essential tools for the prevention, detection, and mitigation of threats. Most forward-thinking institutions are working towards such integration, creating in stages a more unified model across the domains, based on common processes, tools, and analytics. AML activities can also be integrated, but at a slower pace, with focus on specific overlapping areas first.

The starting point for most banks has been the collaborative model, with cooperation across silos. Some banks are now shifting from this model to one that integrates cybersecurity and fraud. In the next horizon, a completely integrated model enables comprehensive treatment of cybersecurity and financial crime, including AML. By degrees, however, increased integration can improve the quality of risk management, as it enhances core effectiveness and efficiency in all channels, markets, and lines of business.

Strategic prevention: Threats, prediction, and controls

The idea behind strategic prevention is to predict risk rather than just react to it. To predict where threats will appear, banks need to redesign customer and internal operations and processes based on a continuous assessment of actual cases of fraud, financial crime, and cyberthreats. A view of these is developed according to the customer journey. Controls are designed holistically, around processes rather than points. The approach can significantly improve protection of the bank and its customers (Exhibit 6).

Exhibit 6

With a 'customer journey' view of fraud, banks can design controls with the greatest impact.

Potential fraud attacks in a customer journey, retail-banking example

	Open an account	Change account	Make a payment	Make a deposit
Customer-initiated actions	Customer opens a new account or adds another account through online, mobile, branch, or ATM channels	Customer updates existing account, eg, adding a beneficiary or changing address	Customer pays self or third party through wire, credit or debit card, or online transaction	Customer makes a transfer or deposit into their account
Attack channel				
ATM	• Identity theft • Synthetic ID • Employee-generated account • Malware	• Malware	• Card skimming or trapping • Fake PIN pad • Cash trapping • Shoulder surfing • Duplicate card • Malware • Transaction reversal	• Money laundering or terror financing • Malware (balance multiplier)
Cards and e-commerce		• Account takeover • Address change • Secondary card • Malware	• Card-not-present fraud • Card skimming • Malware • Cyberattack	
E-banking and wire		• Addition of false beneficiary • Account takeover • Malware	• Cyberattack • Malware • Employee-driven transaction	
Branch		• Account takeover	• n/a	

To arrive at a realistic view of these transgressions, institutions need to think like the criminals. Crime takes advantage of a system's weak points. Current cybercrime and fraud defenses are focused on point controls or silos but are not based on an understanding of how criminals actually behave. For example, if banks improve defenses around technology, crime will migrate elsewhere – to call centers, branches, or customers. By adopting this mind-set, banks will be able to trace the migratory flow of crime, looking at particular transgressions or types of crime from inception to execution and exfiltration, mapping all the possibilities. By designing controls around this principle, banks are forced to bring together disciplines (such as authentication and voice-stress analysis), which improves both efficacy and effectiveness.

Efficiencies of scale and processes

The integrated fraud and cyber-risk functions can improve threat prediction and detection while eliminating duplication of effort and resources. Roles and responsibilities can be clarified so that no gaps are left between functions or within the second line of defense as a whole. Consistent methodologies and processes (including risk taxonomy and risk identification) can be directed towards building understanding and ownership of risks. Integrating operational processes and continuously updating risk scores allow institutions to dynamically update their view on the riskiness of clients and transactions .

Data, automation, and analytics

Through integration, the anti-fraud potential of the bank's data, automation, and analytics can be more fully realized. By integrating the data of separate functions, both from internal and

external sources, banks can enhance customer identification and verification. Artificial intelligence and machine learning can also better enable predictive analytics when supported by aggregate sources of information. Insights can be produced rapidly – to establish, for example, correlations between credential attacks, the probability of account takeovers, and criminal money movements. By overlaying such insights onto their rules-based solutions, banks can reduce the rates of false positives in detection algorithms. This lowers costs and helps investigators stay focused on actual incidents.

The aggregation of customer information that comes from the closer collaboration of the groups addressing financial crime, fraud, and cybersecurity will generally heighten the power of the institution's analytic and detection capabilities. For example, real-time risk scoring and transaction monitoring to detect transaction fraud can accordingly be deployed to greater effect. This is one of several improvements that will enhance regulatory preparedness by preventing potential regulatory breaches.

The customer experience and digital trust

The integrated approach to fraud risk can also result in an optimized customer experience. Obviously, meaningful improvements in customer satisfaction help shape customer behavior and enhance business outcomes. In the context of the risk operating model, objectives here include the segmentation of fraud and security controls according to customer experience and needs as well as the use of automation and digitization to enhance the customer journey. Survey after survey has affirmed that banks are held in high regard by their customers for performing well on fraud.

Unified risk management for fraud, financial crime, and cyberthreats thus fosters digital trust, a concept that is taking shape as a customer differentiator for banks. Security is clearly at the heart of this concept and is its most important ingredient. However, such factors as convenience, transparency, and control are also important components of digital trust. The weight customers assign to these attributes varies by segment, but very often such advantages as hassle-free authentication or the quick resolution of disputes are indispensable builders of digital trust.

A holistic view

The objective of the transformed operating model is a holistic view of the evolving landscape of financial crime. This is the necessary standpoint of efficient and effective fraud-risk management, emphasizing the importance of independent oversight and challenge through duties clearly delineated in the three lines of defense. Ultimately, institutions will have to integrate business, operations, security, and risk teams for efficient intelligence sharing and collaborative responses to threats.

How to proceed?

When banks design their journeys toward a unified operating model for financial crime, fraud, and cybersecurity, they must probe questions about processes and activities, people and organization, data and technology, and governance (see sidebar "The target fraud-risk operating model: Key questions for banks").

Sidebar

The target fraud-risk operating model: Key questions for banks

In designing their target risk operating model for financial crimes, fraud, and cybersecurity, leading banks are probing the following questions.

— Processes and activities

- What are the key processes or activities to be conducted for customer identification and authentication, monitoring and detection of anomalies, and responding to risks or issues?
- How frequently should specific activities be conducted (such as reporting)?
- What activities can be consolidated into a "center of excellence"?

— People and organization

- Who are the relevant stakeholders in each line of defense?
- What skills and how many people are needed to support the activities?
- What shared activities should be housed together (for example, in centers of excellence)?
- What is the optimal reporting structure for each type of financial crime – directly to the chief risk officer? To the chief operations officer? To IT?

— Data, tools, and technologies

- What data should be shared across cybersecurity, fraud, and other financial-crime divisions? Can the data sit in the same data warehouses to ensure consistency and streamlining of data activities?
- What tools and frameworks should converge (for example, riskseverity matrix, risk-identification rules, taxonomy)? How should they converge?
- What systems and applications do each of the divisions use? Can they be streamlined?

— Governance

- What are the governance bodies for each risk type? How do they overlap? For example, does the same committee oversee fraud and cybersecurity? Does committee membership overlap?
- What are the specific, separate responsibilities of the first and second lines of defense?
- What measurements are used to set the risk appetite by risk type? How are they communicated to the rest of the organization?

Most banks begin the journey by closely integrating their cybersecurity and fraud units. As they enhance information sharing and coordination across silos, greater risk effectiveness and efficiency becomes possible. To achieve the target state they seek, banks are redefining organizational "lines and boxes" and, even more important, the roles, responsibilities, activities, and capabilities required across each line of defense.

Most have stopped short of fully unifying the risk functions relating to financial crimes, though a few have attained a deeper integration. A leading US bank set up a holistic "center of excellence" to enable end-to-end decision making across fraud and cybersecurity. From prevention to investigation and recovery, the bank can point to significant efficiency gains. A global universal bank has gone all the way, combining all operations related to financial crimes, including fraud and AML, into a single global utility. The bank has attained a more holistic view of customer risk and reduced operating costs by approximately $100 million.

As criminal transgressions in the financial-services sector become more sophisticated and break through traditional risk boundaries, banks are watching their various risk functions become more costly and less effective. Leaders are therefore rethinking their approaches to take advantage of the synergies available in integration. Ultimately, fraud, cybersecurity, and AML can be consolidated under a holistic approach based on the same data and processes. Most of the benefits are available in the near term, however, through the integration of fraud and cyber operations.

Salim Hasham is a partner in McKinsey's New York office, where **Shoan Joshi** is a senior expert; **Daniel Mikkelsen** is a senior partner in the London office.

Critical infrastructure companies and the global cybersecurity threat

How the energy, mining, and materials industries can meet the unique challenges of protecting themselves in a digital world.

by Adrian Booth, Aman Dhingra, Sven Heiligtag, Mahir Nayfeh, and Daniel Wallance

Whether they generate or distribute power, or extract or refine oil, gas, or minerals, heavy industrial companies comprise critical infrastructure for the global economy. As a result, they are attractive targets for cyber crimes. Already by 2018, nearly 60 percent of relevant surveyed organizations had experienced a breach in their industrial control (ICS) or supervisory control and data-acquisition (SCADA) systems.[1]

Heavy industrials face unique cybersecurity challenges, given their distributed, decentralized governance structures and large operational technology (OT) environment – an environment that does not lend itself readily to traditional cybersecurity controls.[2] Furthermore, many heavy industrials have invested in becoming "cyber mature," as have other at-risk industries, such as financial services and healthcare. The investment gap has left most heavy industrials insufficiently prepared for the mounting threats.

As awareness of the threat environment grows, however, many top executives at these companies are now sharpening their focus on cybersecurity. They are asking important questions like: What does it take to transform our cybersecurity capabilities? What investments will address the most risk? How much should we be spending? Leading companies are now rethinking their cybersecurity organizations and governance models. Some are taking advantage of new security tools for OT offered by innovative start-ups. Most are adopting a risk-based approach to security – identifying their critical assets and seeking appropriate controls based on risk levels (see sidebar, "A cybersecurity transformation in oil and gas").

Evolution of the threat landscape

Several factors underlie the growing threat landscape for the heavy industrial sector. One is the rise in geopolitical tensions, which has led to attacks targeting critical national infrastructure.

Heavy industrials can become collateral damage in broader attacks even when they are not the target, given IT security gaps and OT networks connected to IT networks through new technologies. Obviously, these threats have become a major concern for top managers, boards, and national government bodies.

Attacks on national infrastructure

Among the most significant attacks on critical national infrastructure of the past few years are these:

- In 2014, a Western European steel mill suffered serious damage in its operational environment from a phishing attack used first to penetrate its IT network and then its OT network where attackers gained control of plant equipment.
- The 2015 to 2016 attacks on an Eastern European power-distribution grid cut power to 230,000 people. In this case, attackers compromised a third-party-vendor's network, which was connected to an energy company's OT network, allowing the attackers to make changes to the control system.
- In 2017, attackers gained access to a Middle Eastern petrochemical plant's ICS and attempted to sabotage operations and trigger an explosion.

Recent discoveries in the networks of electrical-distribution companies based in the European Union and the United States indicate that threat-actors established vantage points within OT networks from which to launch attacks at a future date. An example of this is the Dragonfly syndicate, which has been blamed for the breach of EU and US electrical companies to gather intelligence and build cyber capabilities to compromise OT systems.

Groups like Dragonfly are increasingly procuring private-sector offensive tools, enabling them to deliver highly sophisticated cyberattacks. Given the sensitivity of the targets, this has quickly

[1] Forrester consulting study commissioned and published by Fortinet, May 2018.

[2] Operational-technology systems include centralized, human-interface control systems such as supervisory control and data-acquisition systems (SCADA), industrial control systems (ICS), distributed control systems (DCS), industrial Internet of Things (IoT) devices that send and receive feedback from machinery, and programmable logic controllers (PLC) that relay commands between SCADA and IoT field devices.

Sidebar

A cybersecurity transformation in oil and gas

A large state-owned oil-and-gas company was facing frequent cyberattacks, even as it was undertaking a digital transformation that increased the exposure of its critical systems. A successful attack on its assets would harm the economy of an entire nation.

Over 18 months, this multibillion-dollar organization was able to protect its assets and improve its overall digital resilience by transforming its cybersecurity posture. The transformation engaged 30,000 employees across 450 sites in addressing security issues every day. This experience offers a good example of how a critical-infrastructure company can meet the global cybersecurity threat and commit to the cyber-resilience journey.

The company operates across the industry value chain, upstream, midstream, and downstream. It had suffered attacks on both its IT and operational technology (OT) systems, which, as in most companies, were siloed from each other. Attacks hit IT network security and the supervisory control and data-acquisition (SCADA) systems. The company suffered a ransomware attack, email phishing campaigns, and defacement of its website. As the company was digitizing many systems, including critical controllers, massive amounts of data were exposed to potential manipulation that could trigger disastrous accidents. The company focused on three important steps.

First, it defined and protected its "crown jewels": its most important assets. It comprehensively mapped its business assets and identified the most critical, from automated tank gauges that manage pressure and oil levels on oil rigs to employee health records and customer credit-card information. The company created a library of controls

to protect these crown-jewel assets, which are now being brought on line.

Second, the company focused on rapidly building capabilities. To address siloed IT and OT operations, it created an integrated cybersecurity organization under a chief security officer aligned with the risk function (see Exhibit 1 accompanying this article). The company also tailored industrial security standards to the oil-and-gas industry and its regional context. A security operation center was established to monitor and react to threats, and a data-loss-prevention program was set up to avoid leaks.

Third, the company outlined its plan for a holistic cybersecurity transformation, including a three-year implementation program with prioritized initiatives, estimated budget, and provisions to integrate cybersecurity into the digitization effort. To ensure that effort did not create new vulnerabilities, the company created the new digital systems to be "secure by design," creating secure coding guidelines and principles.

The achievements were impressive. The cybersecurity organization is now fully built, with a focus on improving resilience daily. The company is on its way to ensuring that it can continue to reliably supply the energy its nation needs, supporting a major share of the country's GDP growth.

become a matter of national security involving government bodies and intelligence agencies.

Collateral damage in nonspecific attacks

The electricity, oil-and-gas, and mining sectors have been rapidly digitizing their operational value chains. While this has brought them great value from analysis, process optimization, and automation, it has also broadened access to previously isolated ICS and SCADA devices by users of the IT network and third parties with physical and/or remote access to the OT network. In many cases, this digitization has allowed access to these OT devices from the wider internet, as well. According to analysis of production OT networks by CyberX, an industrial cybersecurity company, 40 percent of industrial sites have at least one direct connection to the public internet, and 84 percent of industrial sites have at least one remotely accessible device.[3]

[3] CyberX report on global industrial control systems and Internet of Things risk (2018).

In response to the danger, ICS manufacturers can analyze USB-born threats to detect and neutralize those that could seriously disrupt operations.

Ransomware poses an additional threat. One well known example was WannaCry, which disrupted 80 percent of gas stations of a major Chinese oil company by exploiting a vulnerability in a dated and unsupported version of Windows. NotPetya was far more devastating. This malware wiped IT devices around the world, affecting about 25 percent of all oil-and-gas companies.

More recently, botnets with the ability to detect and infect SCADA systems have been discovered, and those targeting Internet of Things (IoT) devices have become pervasive. The past year has also seen the massive growth of crypto-mining malware targeting ICS computers, severely affecting productivity by increasing load on industrial systems.

These types of sweeping, nontargeted attacks disproportionately affect industries, including heavy industrial companies with less cyber maturity and many devices to protect. Moreover, heavy industrials have the dual challenge of protecting against new digital threats while maintaining a largely legacy OT environment. Most companies still operate with their founding cybersecurity initiatives like patch management and asset compliance. More than half of OT environments tested in one study had versions of Windows for which Microsoft is no longer providing security patches. Fully 69 percent had passwords traversing OT networks in plain text.[4]

Unique security challenges facing heavy industrials

Electricity, mining, and oil-and-gas companies have revealed four unique security challenges that are less prevalent in industries of greater cyber maturity, such as financial services and technology. One challenge stems from the digital transformations that many energy and mining companies are undertaking. Others relate to their distributed footprint, their large OT environment, and exposure to third-party risk.

The overlooked costs of security in digital transformations

Most heavy industrials are undergoing major digital transformations or have recently completed them. When building the business case for these transformations, leaders often overlook the cost of managing the associated security risks. Security is not often a central part of the transformation, and security architects are brought in only after a new digital product or system has been developed. This security-as-afterthought approach increases the cost of digitization, with delays due to last-minute security reviews, new security tools, or increases in the load on existing security tools. For example, instead of building next-generation security stacks in the cloud, most enterprises are still using security tools hosted on premise for their cloud infrastructure, limiting the cloud's cost advantages.

Additionally, security capabilities that are bolted on top of technology products and systems are inherently less effective than those built in by design. Bolt-on security can also harm product usability, causing friction between developers and user-experience designers on one side, and security architects on the other. This sometimes results in users circumventing security controls, where possible.

Protecting the 'crown jewels'

The expansive geographical footprint typical for these heavy industrials can harm their cybersecurity efforts in several ways. It limits their ability to identify and protect their key assets – their "crown jewels." They may have difficulty managing vulnerabilities across end devices. And

[4] Ibid.

while they tend to have a good handle on IT assetsmanaged centrally, they have little or no visibility over assets managed by business units or third parties. Examples of crown-jewel assets include IT, OT, and management assets:

- Information technology: network diagrams, system logs, and network access directory
- Operational technology: programmable logic controllers, SCADA protocols, and system-configuration information
- Management assets: internal strategy documents, executive and board communications, customer and employee personal information

Governance structures typically leave central security leaders without responsibility for security in the business units or operations. Many heavy industrials we surveyed could not identify a party responsible for OT security. The chief information-security officer (CISO) may set policy and develop security standards but often has no responsibility for implementing OT security in the operations, or for auditing adherence to it. At the same time, many operational units have no clear security counterpart responsible for deploying, operating, and maintaining OT security controls at the plant level. Therefore, they often neglect OT security.

Challenges of protecting operational technology

Most of today's OT networks consist of legacy equipment originally designed to be perimeter protected ("air gapped") from unsecure networks. Over time, however, much of it has become connected to IT networks. Most security efforts to protect OT involve network-based controls such as firewalls that allow data to leave the OT network for analysis, but do not allow data or signals to enter it. Although important, these perimeter controls are ineffective against attacks originating from within the OT network, such as malware on removable devices. Additionally, malware has been discovered that exploits vulnerabilities in VPNs (virtual private networks) and network-device software.

Many traditional security tools cannot be applied to the OT environment. In some cases, these tools can harm the sensitive devices that control plant equipment. Even merely scanning these devices for vulnerabilities has led to major process disruptions. Applying security patches (updates) to address known vulnerabilities in high-availability systems presents yet another operational risk, as few sites have representative backup systems on which to test the patches. Because of these risks of disruption, operational-unit leaders are hesitant to allow changes in their OT environment. This requires security teams to implement workarounds that are

Many traditional security tools cannot be applied to the operational technology environment.

far less effective in managing risk. Adding even more risk and complexity are newer technologies such as industrial IoT devices, cloud services, mobile industrial devices, and wireless networking.

Beyond technology is the human factor, as many industries face a shortage in cybersecurity skills. The problem is worse for heavy industrials, which need to staff both IT and OT security teams, and to attract talent to remote operational locations. In a 2017 report on the global information-security workforce, the cybersecurity professional organization (ISC)2 predicted that the gap between qualified IT professionals and unfilled positions will grow to 1.8 million by 2022. OT security expertise is even more specialized and difficult to acquire, making it particularly expensive to staff.

Exposure to third-party risk

Compared with IT, the OT environment is highly customized, as it supports a process specific to a given operation. The proprietary nature of OT equipment means that companies rely on the OEM to maintain it and make changes. This equipment is often a "black box" to its owner, who has no visibility into security features or levels of vulnerability. Furthermore, companies are increasingly outsourcing maintenance and operation of OT, or adopting build-operate-transfer contracts. These types of relationships require third parties to gain physical access to OT networks. Where remote maintenance is required, the owner needs to establish connections to the OEM networks. These remote connections are mostly unsupervised by the owner organizations, introducing a blind spot. Several heavy industrials have reported that third parties frequently connect laptops and removable storage devices directly into the OT network without any prior cybersecurity checks, despite the obvious dangers of infection.

Vendor assessments and contracts for OEMs often fail to include a cybersecurity review. This failure prevents companies from enforcing security standards without renegotiating contracts. Where they do conduct precontract security assessments, results are rarely pursued. OEM vendors that do have security features in their products report that operational buyers rarely want them. In some cases, even if security features are included by default, or at no additional cost, the buyer does not use them.

Emerging solutions

Considering the complexity of these challenges, companies in heavy industrial sectors have been slow to invest in cybersecurity programs that span both IT and OT, especially when compared with manufacturing and pharmaceutical companies. The only exception is the US electricity production and distribution grid, acting in response to emerging regulation in this sector. The good news is that solutions for heavy industrials are becoming more sophisticated. Several incumbent OEM providers, and a growing number of start-ups, have developed new approaches and technologies focused on protecting the OT environment.

Leaders that deploy these solutions must first carefully consider the unique challenges and process requirements they face. They can then combine the solutions with appropriate operational changes. Below we describe the challenges they will have to address along the way and the investments that will be needed, both internally and through OEMs and start-ups, to achieve cyber maturity.

Integrate cybersecurity earlier, across OT and IT

As companies undergo digital transformation, leaders are integrating cybersecurity earlier, in both the OT and IT environments. If heavy industrials are to manage risk and avoid security-driven delays during their digital transformations, they will need to embed security earlier in the process, with investments in developer training and oversight. At the same time, these companies should expect increased convergence between their OT and IT systems. Therefore, their investments in cybersecurity transformation programs should span both, while they more deeply integrate their security functions into both the OT and IT ecosystems.

One way to accomplish this is to create an integrated security operations center that covers both OT and IT, housing detailed escalation protocols and incident response plans for OT-related attack scenarios. An example comes from Shell, which is working with some of its IT networking providers and some OT OEMs to develop a unified security-management solution for plant-control systems across 50 plants.[5] Solutions like these enable centralized asset management, security monitoring, and compliance, dynamically and in real time.

Improving governance and accountability for security across IT and OT

The decentralized nature of heavy industries makes it particularly vital that they integrate security into all technology-related decisions across IT and OT, and deep into different functions and business units. This integration will become even more important as they become digital enterprises. Accomplishing this will require new governance models.

For instance, mature heavy industrials have established architecture-review committees to vet new technologies introduced into the IT or OT environments, and changes to existing technologies. Emerging as a second line of defense are teams that do information risk management (IRM), including strategy, compliance, and reporting. Additionally, some companies have enlisted their internal audit function as a truly independent third line of defense.

But few have reached such a level of maturity. A look at four typical approaches to IT and OT security reveals that only one approach integrates security under a chief security officer (CSO) aligned with the risk function (Exhibit 1). In the first three, accountabilities are insufficiently defined.

But in the fourth approach, the CSO role spans both IT and OT. The CSO reports directly to the COO, thus protecting security from IT cost cutting, and preventing security from being sidestepped by IT programs.

In this optimal approach, the CSO sets policy, creates standards, and works with process engineers to create security architectures that incorporate operational specifics. In an ideal scenario, deployment and operation of OT security resides in plant-level functions, staffed with OT experts who are cross-skilled in security. However, this separation between policy setting and deployment can lead to misunderstandings, perhaps allowing some risks to fall through the cracks. Companies can mitigate this by creating local security-review task forces, including tenured business-unit security officers who represent the security organization regionally or locally. Metrics and reporting structures can be managed by a company-wide cyber governance committee that reports into the board.

Emerging technical solutions

To overcome difficulties in OT security, consider emerging technical solutions. Several providers focused on protecting the OT environment are bringing new capabilities to tackle issues. Although several proofs of concept have resulted in successful, large-scale deployments, the technology is still evolving quickly. As companies compete to differentiate their solutions, winners have yet to emerge. Here, however, are some solutions to consider:

— **Firewalls to limit attackers' ability to move across the network after one section is compromised.** Enhancements in controls at the gateway between the OT and IT networks enable companies to inspect the traffic

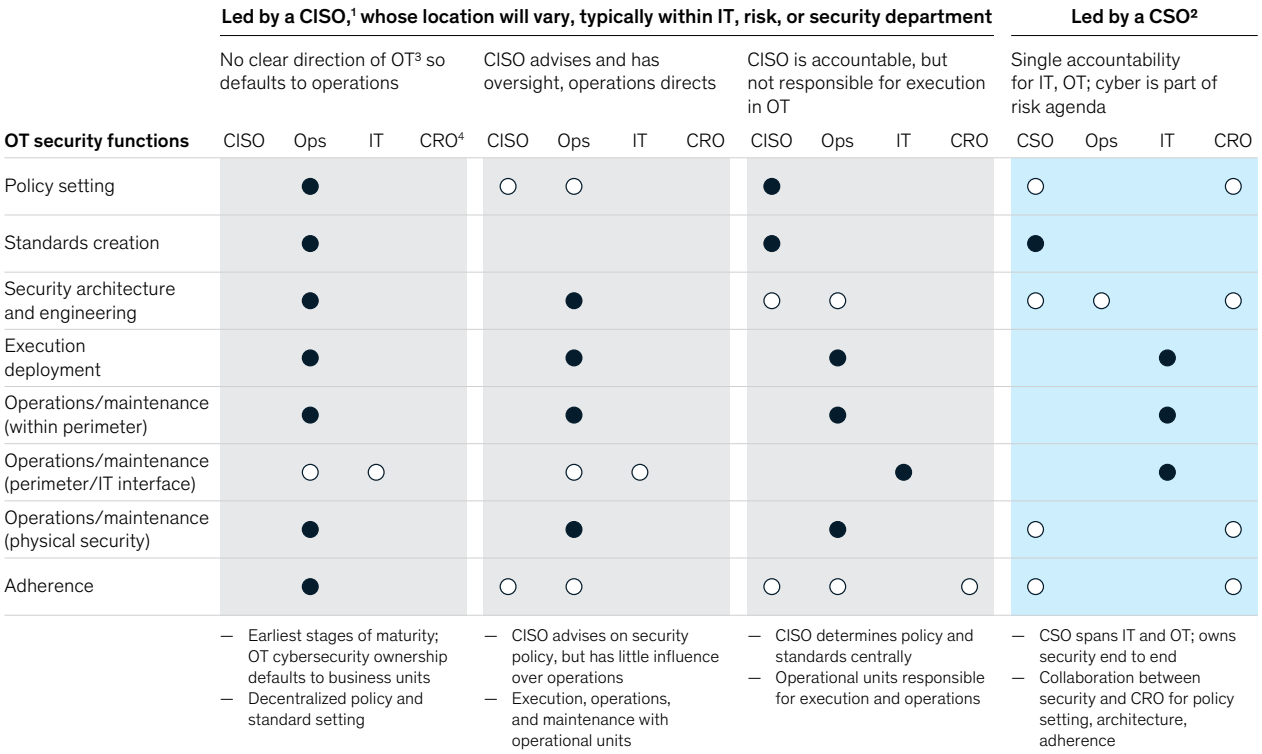
[5] "Shell Oil Strengthening Cybersecurity," ciab.com.

Exhibit 1

Of four approaches to IT and OT security, only one integrates them, using a CSO aligned with the risk function.

Distribution of responsibilities, by security approach

● Primary responsibility ○ Shared responsibility



[1]Chief information-security officer.
[2]Chief security officer.
[3]Operational technology.
[4]Chief risk officer.

traversing that gateway. They also automate a system's ability to execute policy changes and block newly identified threats. Best practice also calls for placing critical assets and systems in separate zones to limit the impact from a compromise; for example, a fail-safe system in a separate zone from the SCADA. Incumbent firewall providers are tailoring their solutions for OT.

— **Unified identity and access management.** These tools allow the company to centralize adding, changing, and removing user access to OT systems and devices. This is linked to the organization's identity-management system, providing robust authentication. This approach, pervasive in IT, has been adopted as a standard in OT environments in the US electricity sector. It reduces the risk of attack by limiting "super-user" accounts. It allows the company to trace who

has access to critical assets, and it helps identify sources of attack. It also has safety applications; a Chinese power plant, for instance, uses it to allow security administrators to remotely close facility doors for improved safety management.

— **Asset inventory and device authorization.** These tools help keep companies aware of all devices connected to their OT network. They can identify vulnerabilities in specific devices based on the device type, manufacturer, and version. They are also used for controlling authorizations of devices and communications. In addition to security applications, these tools can optimize efficiency and identify faults in connected devices.

— **OT network monitoring and anomaly detection.** A plethora of passive OT network monitoring tools have emerged that monitor traffic in a noninvasive way. These tools use machine-learning algorithms to identify and alert known threats and anomalies.

— **Decoys to deceive attackers.** These relatively new IT tools, tailored for OT environments, create asset and user-credential decoys and fictitious OT devices, including SCADAs, to throw off attackers.

While all these tools are useful, the organizational issues mentioned above have thus far inhibited their adoption. For one thing, security buyers have little or no influence over the OT environment. Incumbent OT OEMs, who own the relationship with the operational decision makers, have made some plays directly, and through partnerships in some verticals. However, low cyber awareness among the decision makers has thus far limited the number of such deals.

Third-party risk management

Cost and timing sometimes interfere with a company's responsibility to assess vendor security compliance, both before the contract and on a regular basis. Sector-specific collaboration groups such as information sharing and analysis centers (ISACs) have become important in reducing these costs. For instance, the health ISAC, which includes pharmaceutical and medical-device manufacturers with large OT contingents, has implemented a tool that automates evidence collection and sector-specific risk assessments, to measure third-party vendors for security and data risk. This ISAC has also created a standardized vendor repository for evidence collected by others.

Enablers to drive progress

Given the investment required to achieve digital resilience, and the increasing calls from business executives to get there, we have identified some important enabling factors that will help drive progress. These include increased cybersecurity regulation (by industry groups or government), higher and smarter investments in digital resilience programs, and greater industry-level collaboration.

Evolving cybersecurity regulations

Among heavy industries, cybersecurity regulation is now quite limited. One potential model is emerging in the United States. An electrical-industry agency, the North American Electric Reliability Corporation (NERC), is empowered in federal law to set standards known as Critical Infrastructure Protection (CIP). These standards regulate technical and procedural controls. NERC issued 12 penalties in 2017, totaling over $1.7 million, and stepped up its work in 2018, issuing millions of dollars in penalties that year. One serious violation resulted in a penalty of $2.7 million against an electric utility for data exposure by a vendor. Existing and emerging EU and UK regulations for critical infrastructure are a first step to creating consistency at an industry-wide level. However, most heavy industrial companies are struggling to develop their own standards for IT and OT security, patching them

together from numerous industry standards. As attacks on critical infrastructure continue, more regulation in this sector is likely to follow, either from industry, government, or both. This will bring a much-needed mandate for CISOs and CSOs to take action, and create a clearer path to setting consistent standards across industries.

Higher and smarter investment in cybersecurity programs

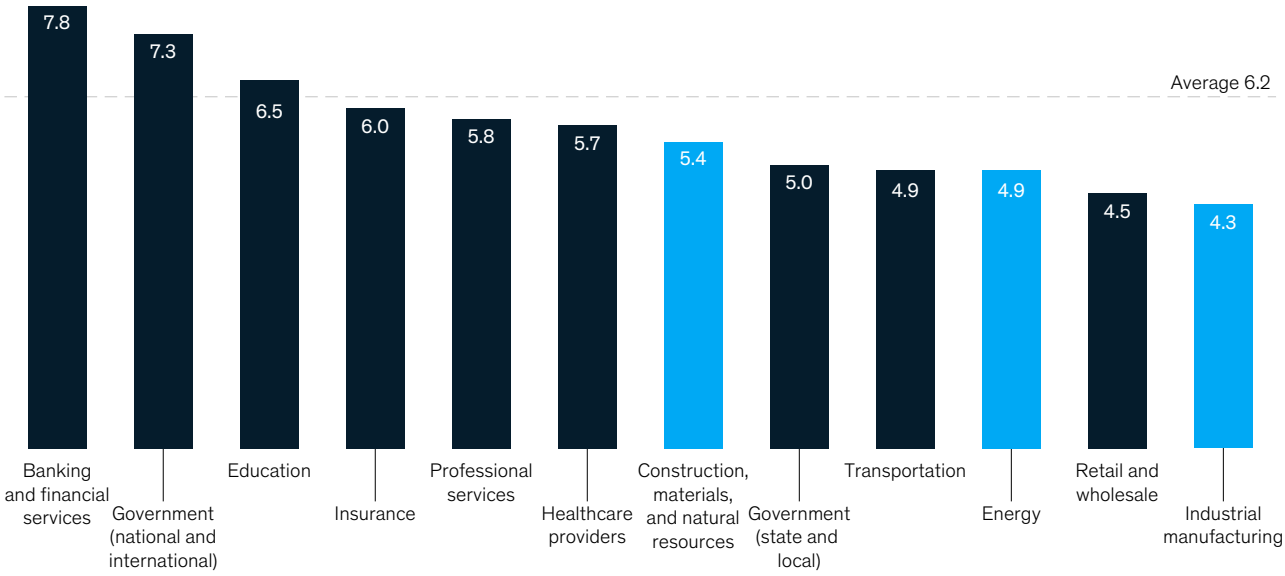
The average electrical-energy company spends just 4.9 percent of its IT budget on security, with mining coming in at 5.4 percent. This is compared with an all-industries average of 6.2 percent and financial services at 7.8 percent (Exhibit 2).

Cybersecurity spending benchmarks are not the only factor to consider when deciding on what investment is required for a particular company. At the early stages of a cybersecurity transformation, program costs may spike before the company can reach a steady state. Spending mix is another important factor to consider. Companies at lower maturity levels tend to spend most of their cyber budget on compliance-driven, reactive activities. This mix changes substantially as companies mature, spending far more on forward-looking, proactive activities such as threat intelligence, hunting, and deception. Companies that conduct a comprehensive assessment of their current cyber maturity and sources of vulnerability can drive smarter long-term spending.

Exhibit 2

Heavy industrial companies lag behind most sectors in IT security spending.

IT security spending as a % of all IT spending, 2017



Source: IT Key Metrics Data 2018: Key IT Security Measures: By Industry, Gartner.com, 2018

Greater industry-wide collaboration

Knowledge-sharing initiatives have started to emerge across heavy industrial sectors, but much more can be done. Some good examples come from ISACs and other regional and sector-specific groups, which have supported rapid maturity building through information sharing, resource pooling (such as shared vendor assessments), and capability building (such as cross-sector crisis simulations). Although a few ISACs exist for heavy industrials, companies have much more to do to establish the high levels of collaboration and value seen in other sectors. Being part of a digitized, connected economy, organizations can be successful only if they apply the power of cooperation within and across sectors. Other industries such as financial services, insurance, and healthcare have built robust networks of security professionals, using roundtables and other collaborations to address common threats and build a more secure industry for all.

Finally, it is worth noting that neither spending nor regulatory compliance are reliable indicators of digital resilience. Using the frameworks and tools we have identified in this article, companies can build that resilience by consistently applying a risk-based approach – identifying their critical assets and applying controls appropriately based on risk levels. This can then help them create cyber transformation programs that buy down risk to tolerable levels and prioritize the activities that address the most risk per dollar spent.

As senior leaders set the stage for cyber transformation, they must ensure collaboration and buy-in from both security and risk professionals and the businesses. With such cooperation, companies will be truly able to transform cybersecurity, helping keep them out of harm's way in a digital world.

Adrian Booth is a senior partner in McKinsey's San Francisco office, **Aman Dhingra** is an associate partner in the Singapore office, **Sven Heiligtag** is a senior partner in the Hamburg office, **Mahir Nayfeh** is a partner in the Abu Dhabi office, and **Daniel Wallance** is a consultant in the New York office.

The authors wish to thank Rhea Naidoo and Rolf Riemenschnitter for their contributions to this article.

The cybersecurity posture of financial-services companies: IIF/McKinsey Cyber Resilience Survey

Cyberrisk has become one of the top risk concerns among financial-services firms, and new research from the Institute of International Finance (IIF) and McKinsey can help provide an understanding of ways firms can enable and strengthen cyber resilience.

A recent joint survey on cyber resilience by the Institute of International Finance (IIF) and McKinsey found significant concerns regarding third-party security, and our survey determined that 33 percent of financial-services firms do not have proper vendor remote-access management with multifactor-authentication controls.

The survey was designed to provide an understanding of current and planned practices that financial firms are undertaking to enable and strengthen firm- and sector-level cyber resilience. Twenty-seven globally active firms participated in the survey, and more than 50 companies participated in group discussions in meetings we convened with chief risk officers in the Americas, Asia, Europe, and the Middle East.

The report IIF/McKinsey Cyber Resilience Survey: Cybersecurity posture of the financial-services industry focuses on four different areas: firm-level cyber resilience, sector-level cyber resilience, costs and full-time-equivalent employees, and next-generation trends (exhibit). A key theme is around building up cybersecurity controls around supply chains, including third- or fourth-party risks, in areas such as vendor remote-access management, activity monitoring, and concentration risk.

Key challenges reported by firms include regulations, cloud adoption, digitization, and the talent gap. Firms said they are active in platforms to share threat intelligence and participate frequently in sectorwide cyber exercises. Automation is seeing extensive adoption, and this could soon be followed by elements of cognitive computing. The report also includes a number of recommendations and industry practices, collected through the survey, that companies can draw on to enhance their cybersecurity posture.

The four survey sections revealed a diversity of challenges.

Section	Topic	Summary of findings
A Firm-level cyber resilience	**Capabilities of each firm in developing and strengthening firm-level resilience** across 7 financial-services-sector cybersecurity-profile (FSSCP) functions	• Firms with >$1 trillion in assets have better cyber resilience • Largest vulnerability could be supply-chain and dependency management • Out-of-date infrastructures are at risk for hacking • 37% said it takes >3 months to remediate a vulnerability • Companies are willing to share information with peers
B Sector-level cyber resilience	**Information on collaboration between financial-sector firms** and public sector to enhance sectorwide cyber resilience	• Many are willing to work together to raise resilience for all (eg, 40% would do joint 3rd-party and vendor due diligence) • Many would also participate in public platforms or initiatives
C Costs and full-time-equivalent (FTE) employees	**Participants' cyber-risk-dedicated spending and FTE numbers,** including roles and responsibilities	• 58% self-reported underspending • Protect function gets most resources, some others are lacking
D Next-generation questions	**Future topics** and integration of next-generation technology, agile methodologies, and cyber-insurance coverage	• Cyber-insurance levels are insufficient • Key challenges include cloud adoption, digital innovation, and talent gap • Cloud adoption is both a challenge and an opportunity • Automation and artificial intelligence will see continued adoption

Source: IIF/McKinsey Cyber Resilience Survey 2019

A practical approach to supply-chain risk management

In supply-chain risk management, organizations often don't know where to start. We offer a practical approach.

by Tucker Bailey, Edward Barriball, Arnav Dey, and Ali Sankur

In the last decade, a number of organizations have been rocked by unforeseen supply-chain vulnerabilities and disruptions, leading to recalls costing hundreds of millions of dollars in industries ranging from pharmaceuticals and consumer goods to electronics and automotive. And multiple government organizations and private businesses have struggled with cybersecurity breaches, losing critical intellectual property due to failures in the supplier ecosystem.

At the heart of these crises is a common theme – the lack of robust processes to identify and successfully manage growing supply-chain risks as the world becomes more interconnected. New threats, such as cyber-ransom attacks, are emerging alongside more traditional and longer-acknowledged supplier risks, such as supplier bankruptcy.

The challenge of supply-chain risk management has been exacerbated by globalization, where even sensitive products like defense systems use raw materials, circuit boards, and related components that may have originated in countries where the system manufacturer did not even know it had a supply chain. This increased complexity has brought with it more potential failure points and higher levels of risk.

Yet progress in addressing these risks has been slow. In our 2010 survey of 639 executives covering a range of regions and industries, 71 percent said their companies were more at risk from supply-chain disruption than previously, and 72 percent expected those risks to continue to rise (from "The challenges ahead for supply chains:

McKinsey Global Survey Results," Nov 2010, McKinsey.com). In 2018, the United States government stood up multiple agencies and task forces to better address supply-chain risk (including the Critical Infrastructure Security and Cybersecurity Agency in the Department of Homeland Security and the Protecting Critical Technology Task Force at the Department of Defense), and the private sector continues to seek a uniform and proven methodology for assessing and monitoring risks in a way that truly minimizes business disruption.

We believe public- and private-sector organizations have struggled to progress significantly on this topic for several reasons:

1. **Supply-base transparency is hard (or impossible) to achieve.** In modern multi-tier supply chains, hundreds or thousands of suppliers may contribute to a single product. Even identifying the full set of suppliers from the raw-material sources to a final assembled system can require a significant time investment.
2. **The scope and scale of risks is intimidating.** The probability and severity of many risks is difficult to ascertain (How likely are certain weather patterns? How often will a supplier's employee be careless in cybersecurity practices?), and therefore difficult to address, quantify, and mitigate.
3. **Proprietary data restrictions impede progress.** In complex products, Tier 1 or 2 suppliers may consider their supply chains to be proprietary, limiting visibility at the purchaser or integrating-manufacturer level.

Rather than admiring the problem and these difficulties, we suggest organizations begin to tackle issues in a structured way, cataloging and addressing known risks while improving the organization's resilience for the inevitable unknown risk that becomes a problem in the future.

A structured approach to supply-chain risk management

We recommend that organizations start by thinking of their risks in terms of known and unknown risks.

Known risks can be identified and are possible to measure and manage over time. For instance, a supplier bankruptcy leading to a disruption in supply would be a known risk. Its likelihood can be estimated based on the supplier's financial history, and its

The challenge of supply-chain risk management has been exacerbated by globalization.

impact on your organization can be quantified through consideration of the products and markets the supplier would disrupt. Newer risks such as cybersecurity vulnerabilities in the supply chain are also now quantifiable through systems that use outside-in analysis of a company's IT systems to quantify cybersecurity risks.

Organizations should invest time with a cross-functional team to catalog a full scope of risks they face, building a risk-management framework that determines which metrics are appropriate for measuring risks, "what good looks like" for each metric, and how to rigorously track and monitor these metrics. This team can also identify gray areas where risks are hard to understand or define (e.g., tiers of the supply chain where no visibility exists). This analysis can dimensionalize the scale and scope of unknown risks.

Unknown risks are those that are impossible or very difficult to foresee. Consider the sudden eruption of a long dormant volcano that disrupts a supplier you didn't know was in your supply chain, or the exploitation of a cybersecurity vulnerability buried deep the firmware of a critical electronic component. Predicting scenarios like these is likely impossible for even the most risk-conscious managers.

For unknown risks, reducing their probability and increasing the speed of response when they do occur is critical to sustaining competitive advantage. Building strong layers of defense combined with a risk-aware culture can give an organization this advantage.

Managing known risks

Organizations can use a combination of structured problem solving and digital tools to effectively manage their known-risk portfolio through four steps:

Step 1: Identify and document risks

A typical approach for risk identification is to map out and assess the value chains of all major products. Each node of the supply chain – suppliers, plants, warehouses, and transport routes – is then assessed in detail (Exhibit 1). Risks are entered on a risk register and tracked rigorously on an ongoing basis. In this step, parts of the supply chain where no data exist and further investigation is required should also be recorded.

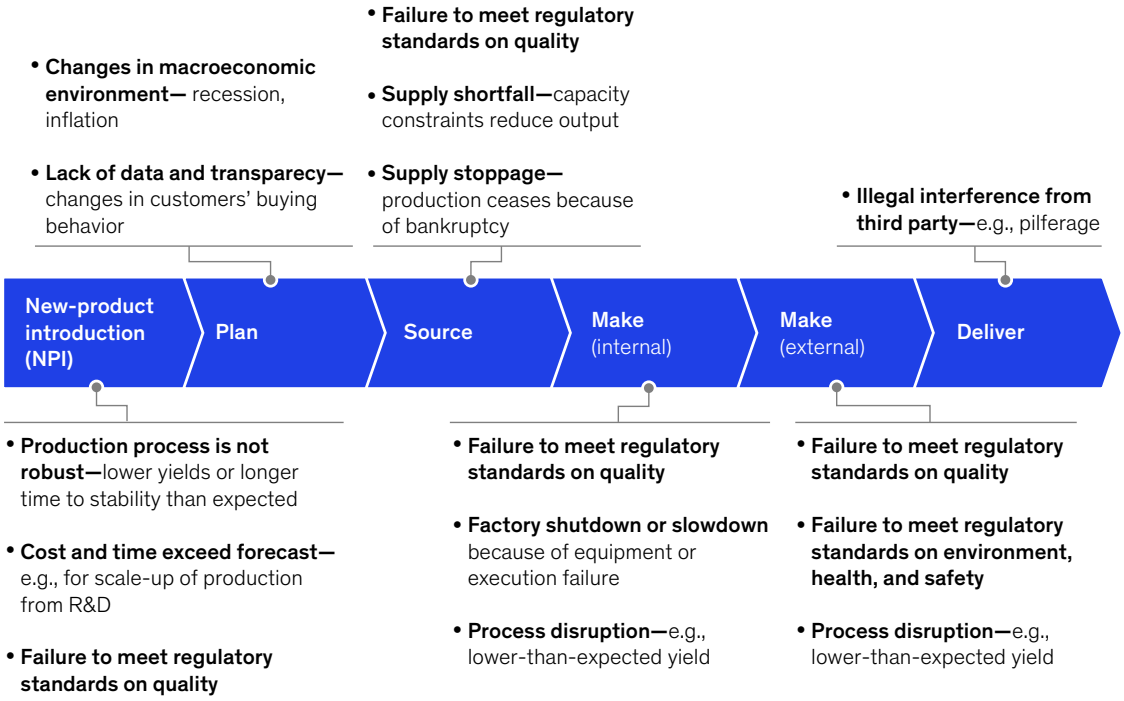
Step 2: Build a supply-chain risk-management framework

Every risk in the register should be scored based on three dimensions to build an integrated risk-management framework: impact on the organization if the risk materializes, the likelihood of the risk materializing, and the organization's preparedness to deal with that specific risk. Tolerance thresholds are applied on the risk scores reflecting the organization's risk appetite.

It is critical to design and use a consistent scoring methodology to assess all risks. This allows for prioritizing and aggregating threats to identify the highest-risk products and value-chain nodes with the greatest failure potential.

Exhibit 1

Assess value-chain nodes to identify key risks.



Step 3: Monitor risk

Once a risk-management framework is established, persistent monitoring is one of the critical success factors in identifying risks that may damage an organization. The recent emergence of digital tools has made this possible for even the most complex supply chains, by identifying and tracking the leading indicators of risk. For example, a large organization operating in a regulated industry identified 25 leading indicators of quality issues at its plants and contract manufacturers, ranging from structural drivers including geographical location and number of years in operation to operational performance metrics, such as "right first time" and deviation cycle times. These 25 indicators were carefully weighted to develop a quality risk-exposure score, and then tracked on a regular cadence.

Successful monitoring systems are customized to an organization's needs, incorporating impact, likelihood, and preparedness perspectives. Hence, while one organization may track deviations on manufacturing lines to predict quality issues, another may follow real-time Caribbean weather reports to monitor hurricane risk at its plants in Puerto Rico. Regardless, it is critical to have an early warning system to track top risks to maximize the chances of mitigating, or at the very least limiting, the impact from their occurrence.

Step 4: Institute governance and regular review
The final critical step is to set up a robust governance mechanism to periodically review supply chain risks and define mitigating actions, improving the resilience and agility of the supply chain.

An effective supply-chain risk-management governance mechanism is a cross-functional risk board with participants representing every node of the value chain. It typically includes line managers who double-hat as risk owners for their function, giving them ownership of risk identification and mitigation. In most cases, the risk board receives additional support from a central risk-management function, staffed with experts to provide additional guidance on identifying and mitigating risks.

An effective board will meet periodically to review the top risks in the supply chain and define the mitigation actions. The participants will then own the execution of mitigation actions for their respective functional nodes. For example, if the board decides to qualify and onboard a new supplier for a critical component, the procurement representative on the board will own the action and ensure its execution.

Additionally, in many organizations the risk board will also make recommendations to improve the agility and resilience of the supply chain, ranging from reconfiguring the supply network, finding new ways of reducing lead times, or working with suppliers to help optimize their own operations. Increasing supply-chain agility can be a highly effective mitigation strategy for organizations to improve their preparedness for a wide range of risks.

Managing unknown risks
Unknown risks are, by their nature, difficult or impossible to predict, quantify, or incorporate into the risk-management framework discussed above for known risks. In our experience, mitigating unknown risks is best achieved through creating strong defenses combined with building a risk-aware culture.

Building strong defenses
Strong defenses, from request-for-proposal (RFP) language to worker training, all contribute to an organization identifying and stopping unknown risks before they affect operations. Exhibit 2 outlines typical layers of defense organizations employ to defend against unknown risks.

Building a risk-aware culture
A risk-aware culture helps an organization both establish and maintain strong defensive layers against unknown risks, as well as respond more quickly when an unknown risk surfaces and threatens operations.

— **Acknowledgement.** Management and employees need to feel empowered to pass on bad news and lessons from mistakes. This openness fosters an environment where it is okay to voice and deal with issues. Culturally, it is critical that the organization not get discouraged or point fingers when a risk event occurs, and instead works harmoniously towards a rapid resolution.

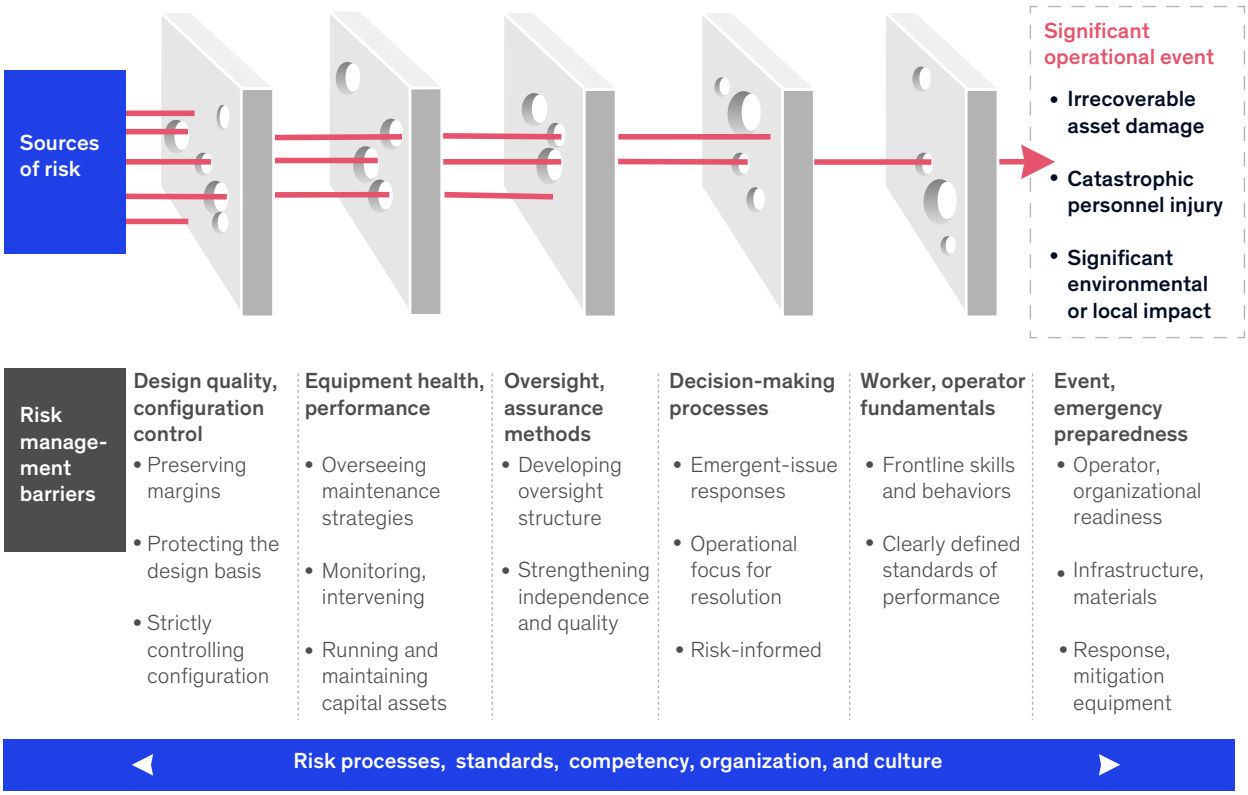
— **Transparency.** Leaders must clearly define and communicate an organization's risk tolerance. Risk mitigation often has an associated incremental cost, and so it is important to align on which risks need to be mitigated and which can be borne by the organization. An organization's culture should also allow for warning signs of both internal and external risks to be openly shared.

— **Responsiveness.** Employees need to be empowered to perceive and react rapidly to external change. This can be enabled by creating an ownership environment, where members feel responsible for outcome of actions and decisions.

— **Respect.** Employees' risk appetites should be aligned with an organization, so that individuals or groups do not take risks or actions that benefit themselves but harm the broader organization.

Exhibit 2

Layers of defenses help organizations manage unknown risks.



The road ahead

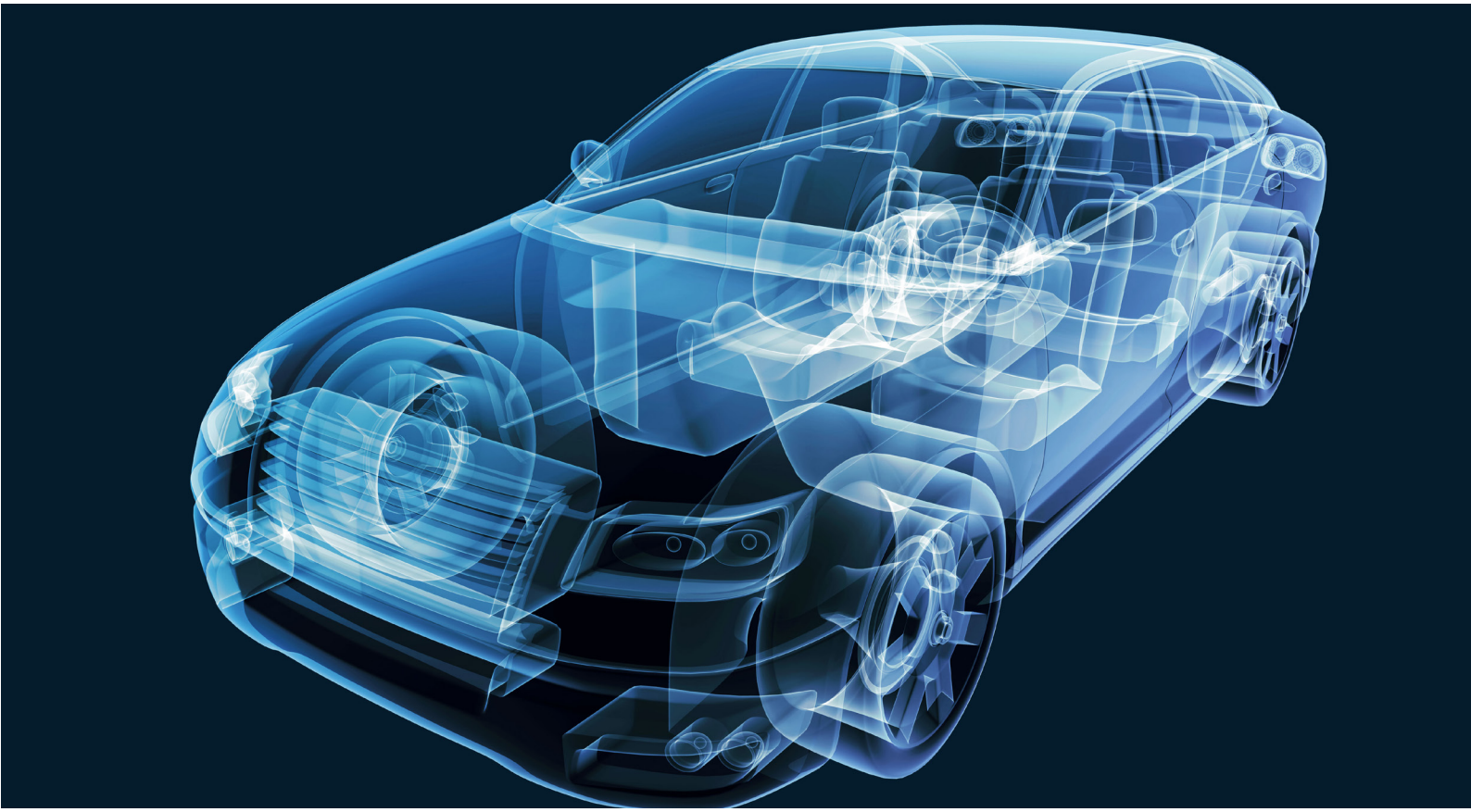
Global supply chains are irreversible, as are the supply-chain risks that globalization has brought with it. Our experience suggests that it is critical for organizations to build robust programs for managing both known and unknown supplychain risks. Leaders should also recognize that risk management is not merely about setting up processes and governance models, but also entails shifts in culture and mind-sets. By employing these approaches, organizations increase their chances of minimizing supply-chain disruptions and crises, while capturing the full value of their supply-chain strategies.

Tucker Bailey and **Edward Barriball** are partners in McKinsey's Washington, DC office. **Arnav Dey** is an engagement manager in the Boston office, and **Ali Sankur** is a senior practice manager in Chicago.

The race for cyber-security: Protecting the connected car in the era of new regulation

The car industry's digital transformation exposes new cyber-security threats. Learn what OEMs can do to protect their cars and customers from hackers.

by Johannes Deichmann, Benjamin Klein, Gundbert Scherf, and Rupert Stützle



In the past, what happened in your car typically stayed in your car. That is no longer the case. The influx of digital innovations, from infotainment connectivity to over-the-air (OTA) software updates, is turning cars into information clearinghouses. While delivering significant customer value, these changes also expose vehicles to the seamier side of the digital revolution. Hackers and other black-hat intruders are attempting to gain access to critical in-vehicle electronic units and data, potentially compromising critical safety functions and customer privacy.

Cybersecurity becomes a core product and value-chain issue

Cybersecurity has risen in importance as the automotive industry undergoes a transformation driven by new personal-mobility concepts, autonomous driving, vehicle electrification, and car connectivity. In fact, it has become a core consideration, given the digitization of in-car systems, the propagation of software, and the creation of new, fully digital mobility services. These services include arrays of car apps, online offerings, vehicle features that customers can buy and unlock online, and charging stations for e-vehicles that "talk" to on-board electronics.

Today's cars have up to 150 electronic control units; by 2030, many observers expect them to have roughly 300 million lines of software code. By way of comparison, today's cars have about 100 million lines of code. To put that into perspective, a passenger aircraft has an estimated 15 million lines of code, a modern fighter jet about 25 million, and a mass-market PC operating system close to 40 million. This overabundance of complex software code results from both the legacy of designing electronics systems in specific ways for the past 35 years and the growing requirements and increasing complexity of systems in connected and autonomous cars. It generates ample opportunity for cyberattacks – not only in the car but also along the entire value chain (Exhibit 1).

The cybersecurity playing field tilts in favor of attackers

To be sure, the economics of car cybersecurity are inherently unfair: with the right state-of-theart tools, attacks are relatively affordable, loweffort affairs. Mounting a coherent defense for the complex value chain and its products, on the other hand, requires increasingly higher effort and investment. So far, this reality tilts the playing field in favor of the attackers. Examples abound across the industry. For example, white-hat hackers took control of the infotainment system in an electricvehicle model. They exploited a vulnerability in the in-car web browser during a hacking contest, causing the electric-vehicle maker to release a software update to mitigate the problem. In another white-hat hack, a Chinese security company found 14 vulnerabilities in the vehicles of a European premium-car maker in 2018. Another global automaker recalled approximately 1.4 million cars in 2015 in one of the first cases involving automotive cybersecurity risks. The impact of the recall was significant, with a potential cost for the OEM of almost $600 million, based on our calculations.

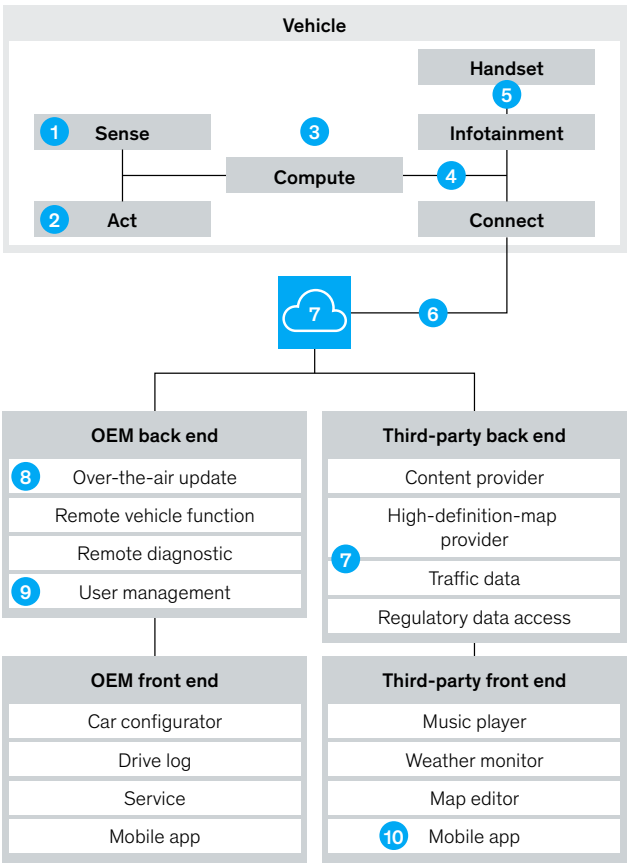
The automotive industry lacks a standard approach for dealing with cybersecurity

For an industry used to breaking down complex challenges and standardizing responses, cybersecurity remains an unstandardized anomaly. Thus far, automotive suppliers have a hard time dealing with the varying requirements of their OEM customers. Consequently, they try to balance the use of common security requirements that go into their core products against those via the software adjustments made for individual OEMs. However, current supplier relationships and contractual arrangements often do not allow OEMs to test the end-to-end cybersecurity of a vehicle platform or technology stack made up of parts sourced from various suppliers. That can make it difficult for both suppliers and OEMs to work together to achieve effective cybersecurity during automotive software development and testing.

Exhibit 1

The advancement of electrical and electronic architecture and digitalization of the car ecosystem increases attack surface and leads to increasing cyberrisk.

Vehicle ecosystem, illustrative



Emerging cyberrisks, not exhaustive

1. **Sensor spoofing:** Access autonomous-drive functions, engine, and brakes through vulnerability in sensors
2. **Take over:** Take over of safety-critical control units such as engine control or brakes
3. **Espionage:** Listen to voices in cars by misusing voice-recognition module
4. **Physical access:** Secure direct access to on-board diagnostics for manipulation of vehicle data, engine characteristics, and tuning chips
5. **Entertainment content:** Access infotainment system via Bluetooth, USB, or Wi-Fi
6. **Telematics:** Remotely unlock cargo doors through vulnerability in external connectivity modules
7. **Denial of service:** Stop cars that rely on back-end servers to provide data
8. **Over the air:** Access vehicle software though online updates
9. **Unauthorized access:** Access back-end vehicle services and user data
10. **Data theft:** Access car owner's private information via unsecure third party

Source: McKinsey analysis

Regulatory change in product cybersecurity is imminent

The difficulty is about to change. Regulators are preparing minimum standards for vehicle software and cybersecurity that will affect the entire value chain. Cybersecurity concerns now reach into every modern car in the form of demands made by regulators and type-approval authorities. For example, in April 2018, California's final regulations on autonomous-vehicle testing and deployment came into effect, requiring autonomous vehicles to meet appropriate industry standards for cyber-security. While these regulations have an immediate impact on a limited fleet, the World Forum for Harmonization of Vehicle Regulations under the United Nations Economic Commission for Europe (UNECE) is expected in 2020 to finalize its regulation on cybersecurity and software updates. This will make cybersecurity a clear requirement for future vehicle sales; the associated regulationswill affect new vehicle-type approvals in more than 60 countries (Exhibit 2). Industry experts see the upcoming UNECE regulation only as the beginning of a new era of technical compliance regulation in the automotive sector addressing the increase and significance of software and connectivity within the industry.

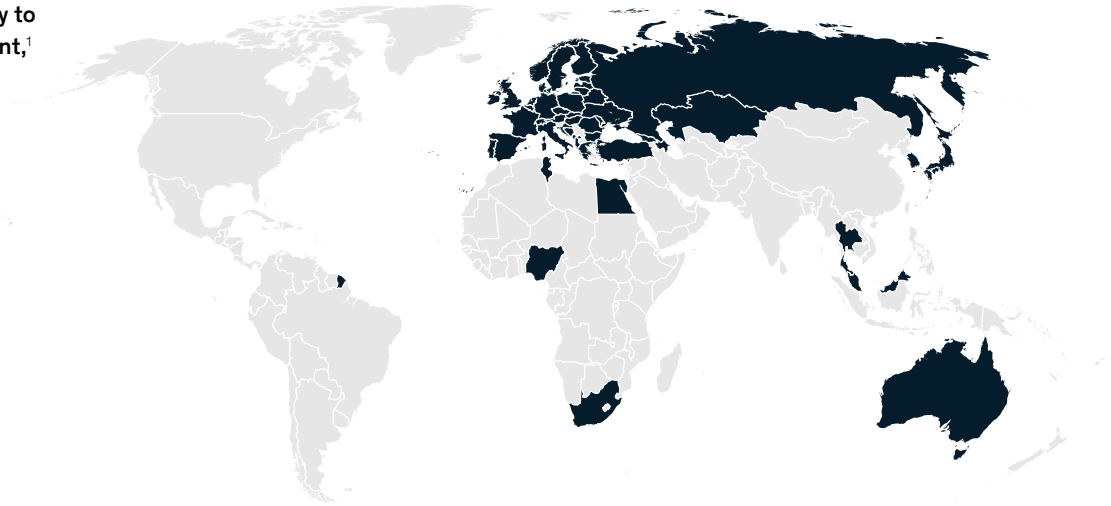
Shifting gears to make cybersecurity a core consideration

While still relatively new, the in-car cybersecurity threat will remain an ongoing concern. As such, automakers must now consider cybersecurity an integral part of their core business functions and development efforts.

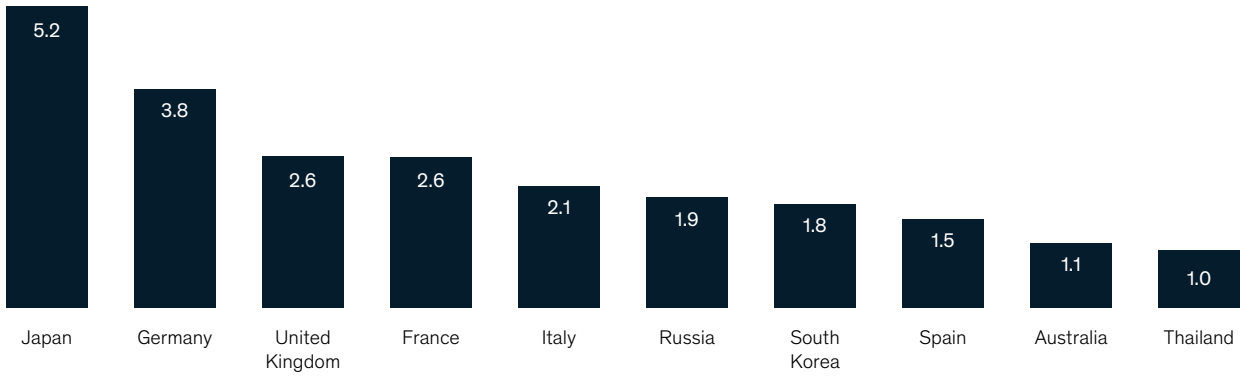
Exhibit 2

More than 24 million cars will be affected under the new World Forum for Harmonization of Vehicle Regulations on cybersecurity and software updates.

Countries party to 1958 Agreement,[1] as of Dec 2018



Top 10 countries party to 1958 Agreement by vehicle sales, 2019 estimate, million



[1]Agreement concerning Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations (original version adopted in Geneva on Mar 20, 1958).

What is more, the industry can no longer view cybersecurity as purely an IT topic. Instead, automakers need to assign ownership and responsibility for it along core value-chain activities (including among their numerous suppliers) and embrace a security culture among core teams. Likewise, suppliers in the automotive industry need to embrace OEM concerns on cybersecurity, develop capabilities to embed security best practices in their components, and collaborate effectively with OEMs on integration and verification of end-to-end cybersecurity solutions.

This requires the creation of a real, software-centric cybersecurity culture, given the pervasiveness of the cybersecurity threat along the entire value chain. Carmakers themselves have a strong record of establishing a culture of safety – but not yet in cybersecurity. Looking beyond automotive-industry borders, it becomes clear that many digital natives have demonstrated how to build strong security cultures in their engineering departments (not just in IT). At the best digital companies, everyone understands the importance of cybersecure coding practices, and the organizations maintain engineering-outreach and -education programs that train people in cybersecurity, enticing them to look below the surface and raise the cybersecurity bar constantly.

Including cybersecurity in design from the start

Carmakers must securely design vehicle platforms and related digital mobility services from the start.

That is because the inherent complexity of vehicle platforms, with their long development cycles and complex supply chains, do not allow for late-stage architectural changes. Furthermore, regulators form strict requirements for OEMs to obtain type approvals for new vehicles (Exhibit 3).

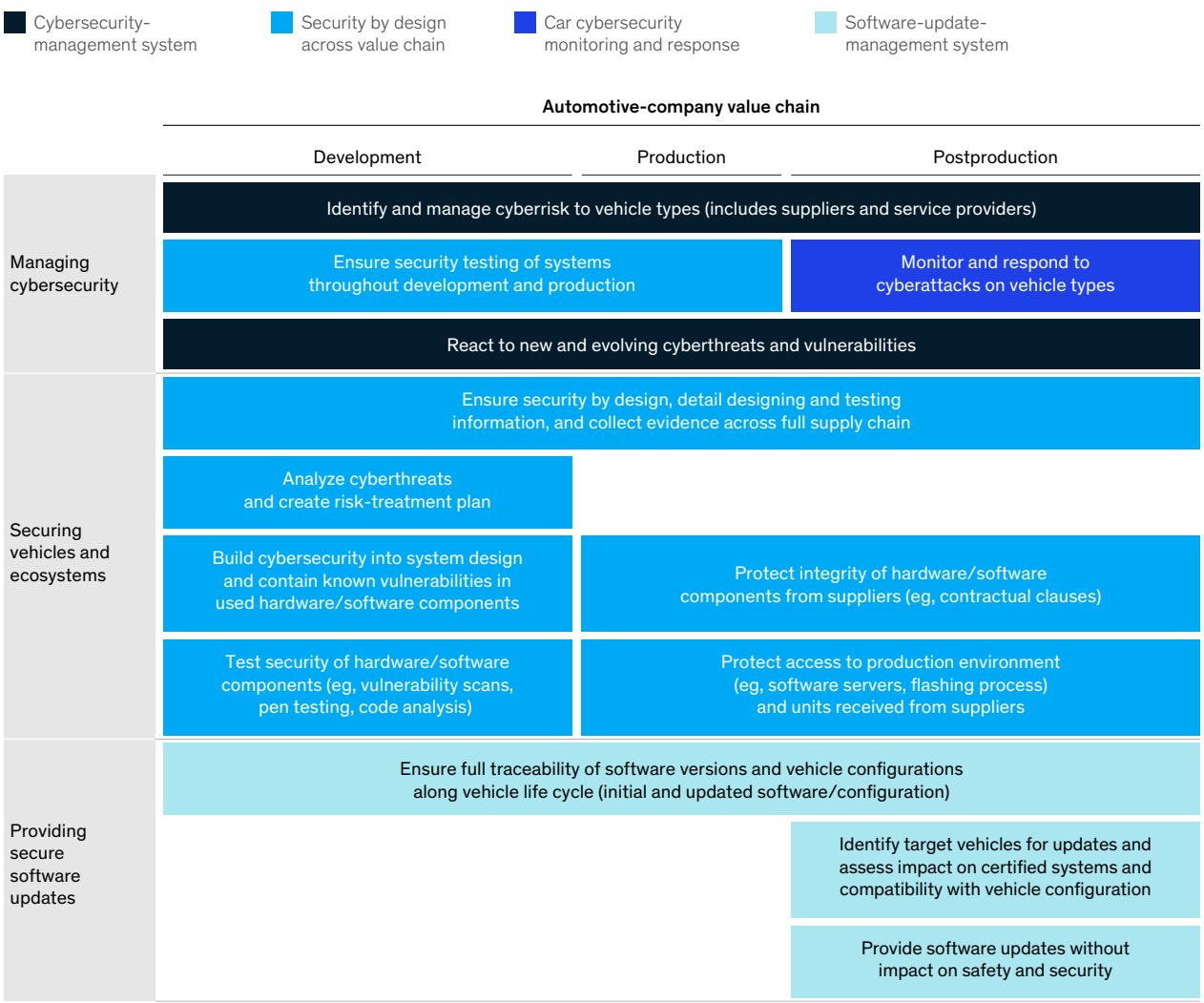
Automotive players must consider cybersecurity over the entire product life cycle and not just up to when the car is sold to a customer, because new technical vulnerabilities can emerge at any time. These issues can have a direct impact on customers and cars already on the road, thus effectively requiring OEMs to provide security-related software patches well into the car's ownership life cycle.

High-tech companies, such as smartphone suppliers, currently deal with this issue by releasing software updates and security fixes for their products after the initial sales (in many cases, new operating-system fixes also support some oldergeneration products). However, this is typically limited to a period of two to three years, while vehicles have an average service life of a decade or even more. With the advent of OTA software upgrades, automakers could maintain the fleets on the road in a cost-effective way, in contrast with the current practice of costly reprogramming ("reflashing") of car electronic control units at the dealer.

Exhibit 3

Upcoming regulations require automotive OEMs to step up cybersecurity activities along the entire value chain.

United Nations Economic Commission for Europe cybersecurity requirements



Source: "Draft recommendation on cybersecurity software updates of the task force on cybersecurity and over-the-air issues," ISO/SAE 21434:2018 Committee, United Nations Economic Commission for Europe, World Forum for Harmonization of Vehicle Regulations; McKinsey analysis

The automotive industry must therefore develop common cybersecurity standards to keep development and maintenance costs under control. On this issue, OEMs and suppliers must speak one language to ensure manageable, end-to-end secure solutions.

Focusing on four core cybersecurity themes

We believe automakers should attack the new cybersecurity and software-update challenges both along the value chain and across the digital life cycle of their cars. To do this, they should focus on four core themes:

1. Establish a clear baseline to execute against. The essence of a good baseline involves understanding requirements from relevant legislation in the OEM markets and leveraging existing international standards around cybersecurity and software engineering. Doing so will enable OEMs to deliver cybersecurity practices as demanded by regulatory authorities and international standards and to develop and maintain secure software. A management system for cybersecurity (CSMS) can help ensuring a relentless application of cyber practices across cars and the digital-mobility ecosystem.
2. Create a true digital-security-by-design culture in engineering, quality assurance, and other core value-chain functions and promote car-software architectures with security built-in. This might require OEMs to overhaul their software engineering and software quality-assurance practices that oftentimes do not follow rigorous software-engineering processes as seen in software-native industries. This security-by-design culture should focus on secure development practices, enhanced software-testing processes, and new supplier-audit processes that include cyber issues. Other helpful elements include state-of-th-eart supplier contracts that allow the testing of a component's cybersecurity, and cyber-awareness training for involved technical personnel and customer-facing staff.
3. Ramp up expertise and capabilities to monitor the cybersecurity of cars on the road. The focus should include fixing issues in a timely manner without costly product recalls and media scrutiny. That likely means fully managing the digital life cycle of cars and having full transparency over a vehicle's configuration (for example, using digital twins) and, ultimately, setting up a security-operations center for cars that receives data from the vehicles and the broader digital ecosystem – in line with dataprivacy laws (for instance, back-end systems). The security-operations center would use correlation and artificial intelligence to detect adverse events and to launch clear incidentresponse activities, eventually leading to the provision of software updates to cars.
4. Adapt software-engineering practices that embrace function-based development, solid version control, and integration testing. This approach effectively allows an OEM to assess the potential impact of individual software updates to its vehicles and their relevant safetyand type-approval systems. Establishing such systems – version control for vehicle software, configuration management, and softwareupdate management – thus helps to ensure operational safety when updating software in vehicles. The approach can also help when considering changes to a vehicle's configuration and assessing the impact on a car.

Sensing an opportunity, hackers have begun to focus more energy on compromising connected cars, posing a new challenge for automakers and suppliers alike. While consumers will largely take cybersecurity for granted until the first consequential breach, regulators will increase pressure on automakers and suppliers to ensure greater protection against attacks. The overall security of modern mobility services will depend on how well the industry addresses cyberrisks in and around connected cars, as well as on the strategic actions key players take today to prepare for future attacks.

Johannes Deichmann is an associate partner in McKinsey's Stuttgart office, and **Benjamin Klein** is a specialist in the Berlin office, where **Gundbert Scherf** and **Rupert Stützle** are both partners.

The authors wish to thank Georg Doll, Ralf Garrecht, and Wolf Richter for their contributions to this article.

Defense of the cyberrealm: How organizations can thwart cyberattacks

Governments and companies have much work to do to protect people, institutions, and even entire cities and countries from potentially devastating large-scale cyberattacks.

In this episode of the McKinsey Podcast, Simon London speaks with McKinsey senior partner David Chinn and cybersecurity expert Robert Hannigan, formerly the head of GCHQ (Government Communications Headquarters), about how to address the major gaps and vulnerabilities in the global cybersecurity landscape.

Podcast transcript

Simon London: Hello, and welcome to this edition of the McKinsey Podcast, with me, Simon London. 2018 was a year of good news and bad news in cybersecurity. The year passed without a major international incident, certainly nothing on the scale of the WannaCry ransomware attack, in 2017. And yet every few weeks brought news of another big data breach at another big company. So where do we stand going into 2019? Are we winning, in any sense? When and where will the next so-called tier-one attack occur? And, importantly, what is the role of government in helping to ensure national cybersecurity. To find out more, I sat down in London with David Chinn, a McKinsey senior partner who works with public- and private-sector organizations on these issues, and also with Robert Hannigan, who is the former head of GCHQ, the UK government's electronic-surveillance agency. Robert also led the creation of the UK National Cyber Security Centre, or NCSC. Today he's a McKinsey senior adviser. Robert and David, welcome to the podcast.

David Chinn: Thank you, Simon. Glad to be here.

Robert Hannigan: Thanks.

Simon London: I think for a layperson, the general question around cybersecurity is, probably, are we winning?

Robert Hannigan: No, I think we are making progress, but I think it would be very rash to say we're winning. If you look at the two big trends, the rise in volume of attacks and the rise in sophistication, they are both alarming. On volume, particularly of crime, there were something like 317 million new pieces of malicious code, or malware, [in 2016]. That's nearly a million a day, so that's pretty alarming.

On the sophistication, we've seen, particularly, states behaving in an aggressive way and using very sophisticated state capabilities and that bleeding into sophisticated criminal groups. It's a rise in the sheer tradecraft of attacks. So no, I don't think we're winning, but I think we're doing the right things to win in the future.

David Chinn: I would agree with Robert. We may not have seen a single attack that brought down multiple institutions in the same way that WannaCry did, but look at the list of institutions reporting very sizable breaches of increasingly sensitive data.

Now we've got some more regulation forcing people to be more transparent about the breaches and the length of time that attackers were inside networks before being discovered. And it's not always clear to those attacked what they've lost. I'm broadly pessimistic.

Simon London: When you think about where the next tier-one attack might come, what are some of the vulnerabilities that in business and government people are thinking about, talking about?

Robert Hannigan: I think most of the focus now is on supply-chain and upstream risk, because even the best-defended companies now realize that their vulnerability is either those who are connected to their vendors, their suppliers, even their customers. And, increasingly, government is worrying about the IT infrastructure, so the global supply chain, both hardware and software, and its integrity.

And some of the state attacks we've seen in the last couple of years have been against the backbone of the internet, if you like. Routers, switches, places that give you massive options to do different things with internet traffic [Exhibit 1]. It's going deeper and more sophisticated.

David Chinn: I think there's different versions of what tier one might feel like. I think that the increasing ability of both criminals and states to attack critical infrastructure [is one of them]. Taking out power to a city might have relatively limited impact in terms of the actual damage done, but could have a huge impact on the way people feel.

Robert Hannigan: There's a difference between a genuinely catastrophic damaging attack and a politically sensitive attack that spreads fear and terror or a lack of trust in data. It's fairly easy to imagine things that will lead to public panic.

You've seen big public controversies over airlines and banks being unable to function, often not through cyberattacks. But if you were to multiply that and see it as a malicious attack, you could see genuine public disquiet, a lot of political pressure to do something about it.

Simon London: Yes, it's interesting, because when you talk about critical infrastructure of the modern economy, you often think about things, like, as you say, the internet backbone.

It's those kind of things. Or maybe financial services, the financial system. But just talk a little

bit more about the supply chain, for example. That's one that I think in the broad conversation and the broad business public is less discussed.

David Chinn: If you think about, at the simplest level, how a pint of milk gets onto the supermarket shelf, there are many stages in that, from the farm – by the way, the cows are milked by a machine, which is probably connected to a network – through to the transport network. The cold chain. The monitoring of the cold chain.

You don't need to disrupt anything except the record that says the milk was kept cold for it no longer to be a product that can be given to the public. The integrity of that data is the essential glue that sticks it all together.

Robert Hannigan: If you think of the big ransomware attacks of WannaCry and NotPetya a couple of years ago, one of the lessons from those is that although they almost certainly weren't targeting big manufacturing enterprises in Europe, they effectively disabled quite a lot of household-name companies. They simply couldn't do business, couldn't manufacture for, in one case, several weeks. It was a wake-up call to sectors of the economy who thought they weren't a target for cyberattacks because they didn't have great IP or data that was worth stealing.

The Internet of Things is simply connecting more processes and more devices to the internet. And it is quite striking that the level of security built into those is usually very low because they're designed and built and procured on cost [Exhibit 2]. There will probably be a role for regulation to improve the standards there.

But it does mean companies are, both through digitization and through the Internet of Things,

Exhibit 1

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

increasing their attack surface, making it harder for them to understand the perimeters of their own networks, harder to see where their vulnerabilities are. That is a real problem for the next five, ten years.

Simon London: And is this one of the reasons that people are very interested, for example, in blockchain? The application of blockchain in the supply chain.

Robert Hannigan: Yes, I think blockchain holds a massive potential because of the holy grail, really, of having a ledger that is distributed and unchangeable and visible to everybody. That has great benefits in cybersecurity. It's got a bad name because it's used for Bitcoin, and Bitcoin has a bad name, but I think blockchain technology is fantastic.

It's not straightforward to apply, and I think there's a lot of talk about it. The application in particular sectors for particular uses is still to be developed, to be honest. But it certainly ought to be a net gain for security, and particularly for data integrity, because one of the big future worries is it's one thing to destroy data or steal it or ransom it. To change it and undermine trust in data, particularly in financial services, could be catastrophic.

Simon London: Or, indeed, milk, which is what gave me the thought. It's a very, very simple example, but it underlines how much of the economy runs on trust in that data.

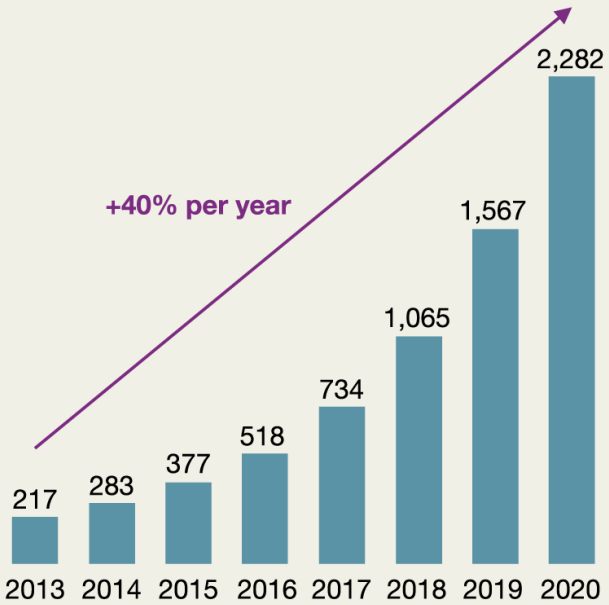
Robert Hannigan: We're just seeing criminals moving in this direction and looking at ways of looking at the corruption of data to, for example, affect stock prices. There's a huge potential there

Exhibit 2

Many professional building managers are not addressing Internet of Things security threats.

Installed base of connected smart-building solutions is expanding rapidly …

Millions of units



… but most building managers have not addressed cybersecurity risks

% of building facility managers (n = 224)

78% **Do not feel knowledgeable** about cybersecurity issues related to building-automation systems

46% **Do not monitor** their building-automation systems **for cyberattacks**

45% **Have not involved their company's IT department** in implementing security measures

63% **Have not developed a response plan** in event of cyberattack

71% **Have not taken measures to improve cybersecurity**

Source: Gartner; IBM; smart-building facility-manager survey in *Building Operating Management*, Jan 2015

to use the changes to data, or to put out false data, to affect the value of a company.

David Chinn: Fake news is a great example. They haven't affected the integrity of the core data. They're just simply putting out noise. In the reports on the attacks of the integrity of the electoral system in the United States, in a system which is highly distributed, where different standards and technologies are used across the United States, there was clear evidence of attempts to penetrate electoral registers. You imagine changing the electoral register so that people of a certain party simply didn't appear. In the hustle and bustle of Election Day, they probably wouldn't get to place their votes. That could dramatically undermine trust in democracy.

Simon London: Robert, we're lucky to have you on the podcast today. Why don't you talk a little bit about what is the role of government in all of this?

Robert Hannigan: It's a challenge that every government is grappling with in different ways and has been over the last ten years. There are a couple of things that make cyber particularly difficult. One is cyberdefense undercuts the assumption that government can do defense for everybody.

David has spent a lot of his time dealing with government defense in a traditional sense. And you, as a citizen, expect government to defend you using the armed forces. It's unrealistic to expect government to do cyberdefense in the same way for the whole economy, because of the scale of it, and because most of what you're dealing with is outside government. Quite apart from the fact that the skills and resources just aren't there in government to do it on that scale. So that's one problem.

The other problem is that cyber is crosscutting in every sense. It is in a new domain, so it's a bit like discovering water or air. Every department, every part of the economy, is dependent on this, increasingly, as we digitize more and become more dependent. You can't really point to a single bit of government and say, "You're responsible for cyber." That was the tendency in the early days.

The answer has to be to find a way of organizing government that gives sufficient speed and command and control to deal with the pace at which digital networks work and cyberattacks work but that actually drags out the whole of government to be good at cybersecurity, because if any one bit is bad at it, the whole system suffers.

David Chinn: Robert, it's interesting what you say because in a sense, government has three challenges. One, it is an actor in cyberspace in service of national interest, usually in secret.

Second, it has to protect itself from cyberattack. And third, it has to create, at the minimum, an environment which protects the citizens and businesses of the country.

My observation would be that, at least reportedly, the UK is very good in the first. Your old institution is a world-class actor in the national interest in cyberspace. The second is quite hard, defending government, because there's so much of it.

The technical skills of government, government IT, are continually in the newspapers and in the public accounts committee as being something that we struggle to do well. Simple things, like putting a working computer on everybody's desk, let alone defending those networks.

Robert Hannigan: Most governments, including the UK, have focused their attention on protecting government networks, sometimes interpreted slightly more broadly to take in some critical bits of national infrastructure that really, really matter, but to encourage the rest of the economy to get better. So we spent ten, 15 years, in a sense, preaching at companies to get them to raise their standards.

There was quite a critical shift, certainly in the UK, about three or four years ago, where we decided that a security model that depended on everybody and every company doing the right thing all the time was almost bound to fail. The whole system was not designed with security in mind, so the people who invented the internet and then the web that sits on it didn't have security at the front of mind, and so we are retrofitting that, and have been over the last 15 years.

Things like scanning websites for vulnerabilities, which is, again, being done across government, you could do nationally, and you could make that available nationally. One of the problems, I think, is that because the internet wasn't designed with security in mind, security is seen as something you need to add on rather than something that's built in.

We need to reach a point where security is designed in and is there by default, particularly with the Internet of Things. That may require some regulation and certainly will require bits of the economy, including insurance, to start to drag up standards.

David Chinn: Do you think government's been remiss on regulation? My observation would be that GDPR [Exhibit 3], which is not a cyberregulation, but that puts significant penalties on institutions for allowing private information to be misused, which includes being stolen, is having quite a big impact already in terms of reporting and transparency, which is then going to inevitably lead to more investment and more focus by organizations on protecting that data. Do you think government missed the boat a little bit on regulation?

Robert Hannigan: I think government, certainly in this country, has been reluctant to regulate, for all sorts of reasons. In cyber, there's a particular reason why regulation can be difficult, because it can end up being very prescriptive and very tick box, and it doesn't take account of the speed at which technology is changing and the particular networks that a company may have. We preferred an advisory, "Here are objectives you should meet" – a risk-based approach, I suppose.

Exhibit 3

The General Data Protection Regulation sets out guiding principles for data protection.

Principle	Explanation
Lawfulness	Data should be processed only when there is a **lawful basis** for such processing (eg, consent, contract, legal obligation)
Fairness	The organization processing the data should provide data subjects with **sufficient information** about the processing and the **means to exercise their rights**
Transparency	The **information provided** to data subjects should be in a **concise and easy-to-understand format** (eg, the purpose of consent should not be buried in a lengthy document of terms and conditions)
Purpose limitation	Personal data may be collected only for a **specific, explicit, and legitimate purpose** and should not be further processed
Data minimization	The processing of personal data should be **adequate, relevant, and limited to what is necessary** in relation to the purposes for which those data are used
Accuracy	Data should be **accurate and kept up to date**
Storage limitation	**Data should not be held** in a format that **permits personal identification any longer than necessary**
Security	Data should be processed in a manner that **ensures security and protection against unlawful processing, accidental loss, damage, and destruction**
Accountability	The **data controller** is responsible for **demonstrating compliance**

Source: Regulation (EU) 2016/679 of the Council of the European Union, European Commission, and European Parliament

Simon London: Best practices and these kind of things.

Robert Hannigan: Yes. Then there is a good case for saying we need a tougher approach on regulation. I think the EU is moving in that direction. I think GDPR has been a net benefit, because essentially there are two sides to most cyberattacks. There's "Did you do the right things to prevent it, and then how did you handle it afterward?"

So GDPR has been particularly strong on the second bit. First of all, it's removed the debate in companies about whether they reveal the attack and how long, because they have to. That's good. It's raised awareness in boardrooms and so, to some degree, panic in boardrooms.

But I think the best regulation probably is in the states. It's interesting to see that California is introducing some hardware-IT supply-chain regulation, which will have a big impact, I think, given that so much of it is designed there, even if it's mostly made in China. There is a place for regulation, and we probably should have done more of it. The difficulty is lack of skills, again. I think most governments don't have sufficient skills.

Simon London: Ah, well, that was going to be my next question. Yes. To your point, David, I mean government IT doesn't have a massively positive reputation in the world at large. Sometimes unfairly. But yes, do governments have the technical skills in cyber to protect their own networks?

David Chinn: The interesting thing about cyber is that the source of innovation in attacks is mostly coming from inside governments. Many governments have very highly skilled people who when their knowledge leaks into the public domain gets adopted quickly by criminals. We have the equivalent of government weapons proliferation into cyberspace.

If you follow the cyberindustry, where there's a huge number of start-ups, effectively, each year's retiring crop of government hackers is bringing new innovation from inside the secret domains of government in an appropriately, hopefully appropriately, modified way to the benefit of those who are under attack, often from other governments. One can't say that there are no skills in government. The best skills are probably in government.

Robert Hannigan: That's true, but I wouldn't underestimate the creativity and innovation of criminal groups. They are genuinely creative. They are talking to each other about, "How could we do this in a better way? How could we defraud this particular bank? What technique is going to work best? What's the best way of delivering it?"

They are doing what so many traditional companies are trying to do, which is pull in skills from around the internet. Not necessarily colocated. They've clocked something about how to harness young innovative skills and do creative things. We have quite a bit to learn from them, I think. I agree that governments have been very good in quite a small and narrow way, but the criminal world is also pretty innovative.

David Chinn: I think this is similar, certainly in the UK, to the crisis in STEM education. If people don't study STEM subjects, we're just not going to have the inflow into the economy, whether it be for government or private industry.

I've been particularly impressed by the way that Israel has effectively said that this is a national defensive-capability issue, but it's a national industrial-growth issue. The country decided they wanted to have one of the world's leading cyberindustry platforms and that to do that they had to make a massive investment in skills.

They started with after-school activities in the most deprived areas, because they recognized that if you start young enough in a country where almost every home has a computer, even those with very low means, who think that having a computer is important, that you can build those skills, in a sense, in parallel to formal education.

Many people who are extremely talented in the cyberdomain actually don't do particularly well at school. It's an outlet for those people, and I think it's been very, very successful. It's created a great pipeline of talent into government and private industry.

Simon London: I think about another interesting question for government is how you manage this tension between the need for transparency and bringing the whole economy with you, and yet at the same time there is an element of secrecy, acting in the national interest and so on. How do you manage that tension in practice?

Robert Hannigan: I think the key insight of the last ten years has been that you can't do cybersecurity in secret. You can't do it behind a wall in the intelligence agencies. For the obvious reason that the attacks are out there in open source in the economy, on the internet. It's all visible. Well, most of it visible.

It makes no sense to try to do it in the way that you've tackled traditional security threats, which may be very, very secret and coming from very sophisticated governments. There is a side of that that is true for cyber, but most of it is not. Most of what people experience in cyber, whether companies or individuals, is crime. Some of it's state-backed crime, but still crime. And it simply doesn't work to be referring constantly to a secret world that can't really communicate.

The obvious development here has been to create a national cybersecurity center that was outside the secret world, but under the aegis and under the control of GCHQ, which is where the skills sat. And to have a blend of both. In the headquarters you've got access to secret systems for some people, but the key point is that you have openness to industry, and you have industry people sitting alongside government experts.

It goes back to our discussion of regulation. What you need in cyber, you can't simply have cyberregulators who do it for everybody, because so much is domain-specific. You need to understand the energy sector to regulate or advise on how to do cybersecurity of energy, or for any other sector. It's different. Therefore, the idea is to have experts from those particular sectors sitting literally alongside a deep cyberexpert.

Simon London: To your point, David, it sounds like a lot of companies are struggling with this same cultural pull between the secrecy but the need to share information really to be effective, or to be more effective and to collaborate with your peers and share information.

David Chinn: Yes, and I think we'll see the information commissioner shaping the environment around transparency quite actively in the very near future.

Simon London: This is your point around regulation?

David Chinn: Yes. I think that will really change people's understanding of how much they can legitimately keep secret.

Simon London: Can we just internationalize the conversation a little bit? If you look across the international context, what are other governments who are doing this well and innovatively, and who we can all learn from?

Robert Hannigan: I would say Singapore and Israel are doing it very well, in slightly different models. Australia has chosen a model that's similar to the UK model [Exhibit 4]. Having it all in one place effectively. Certainly, the operational side of cyber.

Most governments are organizing and constantly tweaking the system. There are very different models, and in Europe, perhaps in Germany especially, the cyber agencies are purely civilian.

And then there is a secret-world element of cyber, and I think they're also looking at how to bring those two together in a way that works for them, given the different constitutional setup.

The military in many countries has a primacy in cyber, and certainly in Germany they've been given a strong lead in cyberdefense. That brings both opportunities, because the military always have a lot of resources and they're very good at organizing stuff. But also challenges, because they're not used to dealing with defending banks and the economy, and it's a culture shock for them. They don't necessarily feel that's part of their remit. There are difficulties in the military.

The US, everybody looks to, but I think it's so large, with its multiplicity of agencies, that it's struggling. It has fantastic capabilities, obviously. The private sector is probably better organized, particularly in financial services, than anywhere in the world. But you often get the criticism or complaint from the private sector that the links to government are not quite right yet.

That I think reflects partly the fact that it's still evolving; the Department of Homeland Security, that was given this leadership under the Bush administration, is still developing. It's not straightforward, particularly on that scale. I don't think anybody has a perfect answer.

David Chinn: I think the military is a very interesting subset of government because I don't think there was even one model in the military. Some countries are creating cybercommands.

Others are building cyber in all of their commands. Others are concentrating in their intelligence services, and then combining those in different ways. And that's also changing over time.

Exhibit 4

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

Responsibilities:

- Protect the UK's critical services from cyberattack.
- Manage major cybersecurity incidents.
- Improve the underlying security of the UK internet through technological improvement and advice to citizens and organizations.

Sample functions:

- Develops knowledge and distills insight on cybersecurity into practical guidance for public consumption.
- Responds to cybersecurity incidents to reduce the harm they cause to people and organizations.
- Applies industry and academic expertise to build capability in the cybersecurity system.
- Secures public- and private-sector networks.
- Provides a single point of contact for government agencies, departments, and organizations of all sizes.
- Collaborates with law-enforcement, defense, intelligence, and security agencies and international partners.

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

Simon London: It sounds like we're in an era of institutional innovation, in many ways – to some degree, institutional improvisation to try and figure out what models work in what context.

Robert Hannigan: Absolutely. I think the military's a very good example, particularly outside the US. The US is ahead of anybody, I think, in developing cyberskills in the military at scale.

On the broader point about civilian structures and civilian/military, I think the one thing that is probably key is that many of the questions are the same, starting with, "What does government actually want to achieve?" And not being overambitious in what government can achieve, and what's the appropriate role of government, is a good starting point. And trying to define what people expect from their government. Things like a single source of advice, incident response, protection of certain networks. I think that is a conversation that just about every government is having in different ways.

David Chinn: But I think there's a paradox here, because if you were to interview the chairman or chief executive of any large corporation and ask them what's their top three risks, cyber would be on that top three, for every single one. And for many of them, it would be number one. Yet, if we look at what governments are doing, this is the one area of national security, of crime prevention and prosecution of critical national infrastructure, that governments have, to a large extent, abdicated their responsibility. Great, some small steps. And sorry, I don't mean to be critical of what was a big small step. But exalting the private sector to do better feels like a very different role that government takes in almost every aspect of life that would feature for most people in their top three risks. I think there's a lot more to do, but unfortunately we may have to wait for a genuine event – people talk of the cyber 9/11 – to create a big change in focus, understanding, spending, and so on.

Simon London: Let me just put that back to you. What should be done?

David Chinn: What would your list be, Robert?

Robert Hannigan: Your criticism is very fair. I mean I think the government has moved from an absolutely sort of hands-off position to say, "Well, we'll look after our networks, but everybody else should get better." And sort of slightly hectoring them when they're not good enough. To saying, "Yes, there are things that we could do at national scale."

The problem, I suppose, at the risk of sort of making excuses, is that the nature of cyberspace, however defined, makes politicians feel quite impotent, because it cuts across jurisdictions. They can pass laws in their own parliament that really have zero effect. They can regulate their own companies, but not necessarily others. That is a real problem.

For cybercrime, for example, most of it is based in countries which are either endemically corrupt or unwilling to do anything about it for geopolitical reasons. What do you do about that? I mean there's a much bigger context here of international relations, and we are a million miles from getting any kind of international agreements on the security and safety of cyberspace.

Simon London: David, you were the rousing voice of critique just now. What should be done?

David Chinn: First, a sophisticated debate around the legislative and regulatory environment. The use of product liability has been very effective in other sectors for changing the game for the manufacturers. A robust thinking about product liabilities, extension to the technology arena, would frankly have quite a chastening effect on industry.

Simon London: In other words, selling a product that has technology embedded that is deemed to be insecure could be breaking the law.

David Chinn: Well, not necessarily breaking the law, but would expose you to civil action that could have severe financial consequences. Effectively, it would create a market mechanism for valuing more secure products. Second, there is room for some better and some more regulation. For example, if you want to sell anything to the UK government, you have to meet a minimum standard called Cyber Essentials. This is not the most sophisticated, but, as we've discussed, most of the attacks are not the most sophisticated attacks.

These kind of standards are very helpful because they're easily adopted by people for their own supply chains. I think a promulgation of standards, ideally with some degree of harmonization. And it's very interesting, in the US the national standards organization, NIST (National Institute of Standards and Technology), has created a number of models, which have got global acceptance. Once an authority puts it out there in a world where

there's a lot of uncertainty, there's a lot of demand for good standards.

The traditional tools of government around legislation, regulation, standards setting, and so on could be used quite a lot more, without throttling innovation. Industry always says, "You're going to throttle innovation." What they mean is it's going to cost them more. But the cost to society of insecurity is high and is going to get higher.

Simon London: One of my takeaways from this conversation, tell me if this is right or wrong, is that there will be one or more significant tier-one, we might call them attacks, on critical national infrastructure. We're recording this in London, but it may not be based in the UK. But that will come. We know where it will come. And that will probably shift the debate into a higher gear. That probably will shift the international debate about what is to be done and, in some ways, get this taken more seriously, perhaps at government policy and regulatory level. Is that a correct takeaway?

Robert Hannigan: I think for most people, most of what they would experience, and most companies, is still crime. So that's the volume, but everybody understandably gets excited about the catastrophic attack and that there is a range of possibilities for and the insurance industry worries a lot about systemic failure. So systemic failure of cloud providers, for example. Systemic failure of some major financial institutions, two or three of which would bring down the system or could bring down the system. So those are the kind of real tier one. But there may be some political tier-one problems and attacks that will have the kind of effect that David was talking about earlier, of panic and political pressure.

Simon London: Trust.

Robert Hannigan: Yes, either trust or an attack that leads to loss of life. It might not be massive loss of life, but it would put huge pressure, as terrorism does, on politicians to react.

Simon London: So what's that Churchill phrase, this is not the beginning of the end. This is the end of the beginning?

Robert Hannigan: Well, I don't think it's even really the end of the beginning. I think we're still at very early stages of this technology. For most people, it's 15, 20 years old. Even if you look back to the ARPANET (Advanced Research Projects Agency Network.), it's, what, 40, 50 years old? That's not long, and it's developing incredibly fast.

We are about to add a massive amount of new processing power, and therefore new data to the system, mostly through the Internet of Things. We have a whole new issue emerging with quantum computing, and people have not quite woken up, including the regulators, to the fact that current encryption will cease to be useful once quantum arrives.

We need now to be building in quantum-safe encryption standards, which are available through NIST and through others. But if we don't do that, everything, every company's records, every bit of financial data, every transaction is going to be readable from the moment that quantum computing really arrives at scale. It's a wonderful innovation, and it has obviously lots of possibilities on the other side of the equation, but it is one that we need to start thinking about in regulatory terms now.

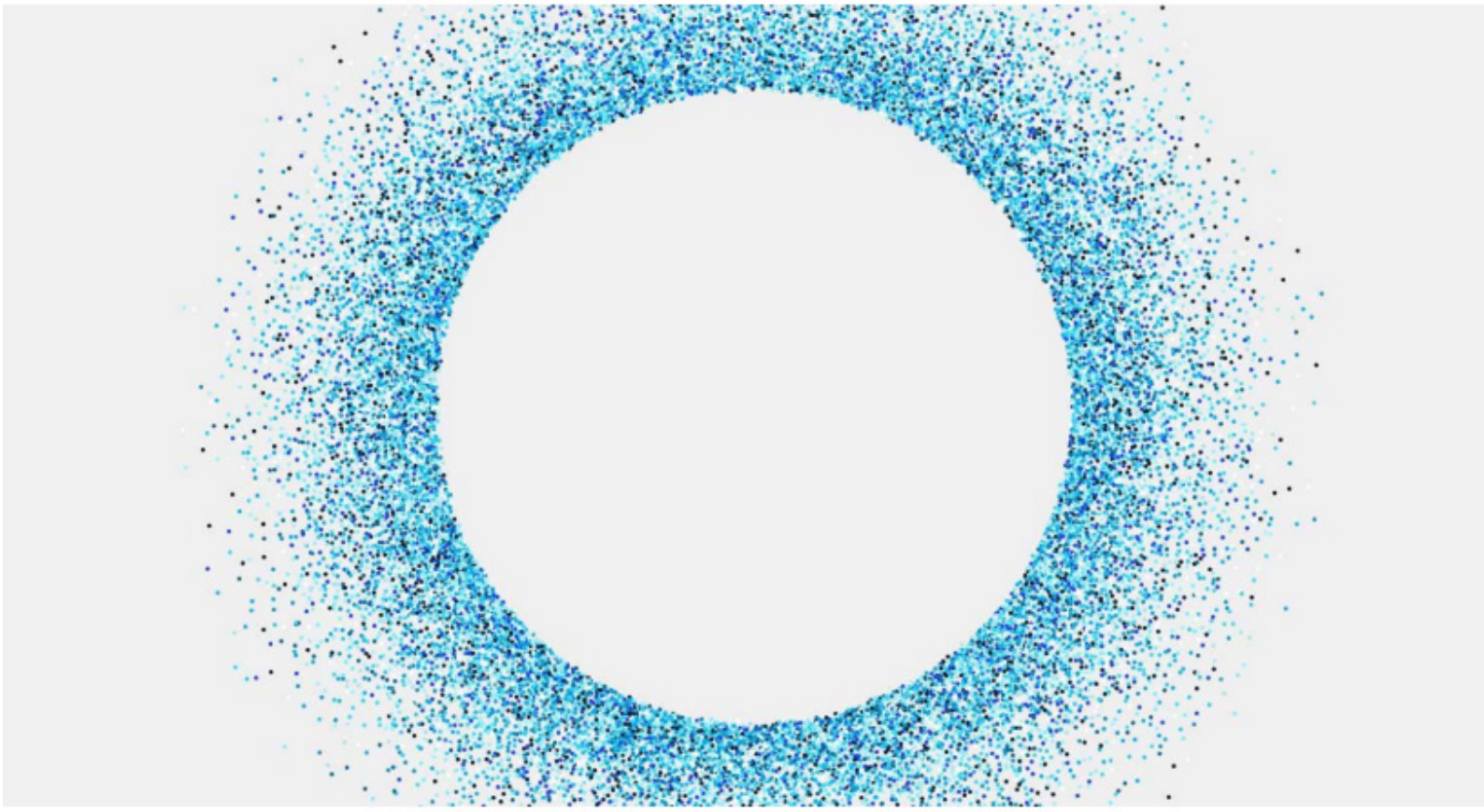
Simon London: All right. Well, I think that's all we have time for. Robert and David, thank you so much, and thanks, as always, to you, our listeners, for tuning in. To learn more about our work on cybersecurity, technology, and related matters, please go to McKinsey.com.

David Chinn is a senior partner in McKinsey's London office, and **Robert Hannigan,** the former head of GCHQ, is a senior adviser to McKinsey. **Simon London,** a member of McKinsey Publishing, is based in McKinsey's Silicon Valley office.

Understanding the uncertainties of cybersecurity: Questions for chief information-security officers

Given the dynamic nature of the cybersecurity environment, CISOs need to address a set of questions that will shape their strategies over time.

by Venky Anant, Tucker Bailey, Rich Cracknell, James Kaplan, and Andreas Schwarz



At a highly dynamic moment of change in the way companies use technology, cybersecurity is probably the most dynamic of all corporate technology domains. The field and the companies that rely on it are being transformed as an uncertain geopolitical environment emboldens potential cyberattackers, rapid technological innovation creates new ways to launch and repel cyberattacks, and cybersecurity's emergence as a critical business function prompts experimentation with organizational and operating models alike.

In such an environment, perfect foresight is impossible. Yet business, technology, and security executives all have a responsibility to understand the important uncertainties and to develop practical working hypotheses about how to manage them. To help these senior managers, we've compiled a list of the key questions they ought to ask over the next 12 to 18 months.

Evolving market expectations

Two of these questions focus on market expectations: whether consumers will start to care about security issues and the way differing regulatory, political, and cultural expectations about data protection shape security across national boundaries.

1. Will consumers start to care about privacy and security?

Anyone who has observed the procurement of group health insurance, pharmacy-benefits management, prime brokerage, or IT-outsourcing services knows that corporate customers care a lot about how their suppliers protect sensitive data. But with a few exceptions – such as high-net-worth or mass-affluent purchasers of financial services – the consumer market just doesn't seem to care about privacy or security. Most breaches involving personally identifiable information haven't affected revenues or market share in any sustained way.

Yet in view of the relentless attention to privacy and security issues in the press and the political arena, this indifference could certainly change. Companies have a responsibility to protect all consumer data, but when senior executives think through their risk appetites, levels of investment, and incident-response plans, they must consider not only how sensitive consumers in general are but also who may be the most sensitive consumers and which perceptions and actions (or failures to act) might heighten their concerns.

2. How will different regulatory, political, and cultural expectations about data protection across national boundaries shape the security environment?

Perhaps paradoxically, while consumers have been relatively blithe about their data, privacy and security have continued to be hot-button political and regulatory issues. Jurisdictions such as Brazil, California, and the European Union have started to implement tough new requirements on data privacy. But regulations in different jurisdictions may contradict each other or create conflicts between compliance and security – particularly by constraining the forensics a company can perform on its own network to identify insider threats or compromised accounts. (Regulators might perceive those actions as inimical to the privacy rights of employees.) Authoritarian states may demand that companies limit security or privacy protections for their customers or employees as a condition of doing business in those places. That in turn may spark public frustration and anger elsewhere.

Going forward, companies will certainly have to think about tailoring their security models to the requirements of different national markets. Some may have to make tough choices about whether they can reconcile expectations about privacy and security in all the markets where they might ideally like to do business.

Evolving risks

The next set of questions focuses on evolving risks: whether companies will be collateral damage, coopted or directly targeted by nation-state actors; how companies will protect their data in a world of pervasive sensors and protect their machine-learning capabilities; and how quickly quantum computing will become a security threat.

3. To what extent will companies be collateral damage, coopted or directly targeted by nation-state actors?

As the NotPetya attack showed, nation states increasingly use cybertools as weapons of domestic and military tradecraft. Originally directed at targets in Ukraine, NotPetya wreaked havoc on unprotected networks around the world. Another harbinger of what's to come: it has been widely reported that NotPetya was derived from

a stolen exploit originally developed by the US National Security Agency.[1]

In an era of renewed great-power conflict, countries increasingly promote their global interests by means other than war. During the past several years, asymmetric approaches (such as cybertheft, cyberattacks, malign influence, and media manipulation) have taken advantage of unsuspecting content providers, critical national-infrastructure operators, and intellectual-property producers.

When global tensions rise and economic interventions become increasingly common in great-power conflict, companies will be collateral damage; in fact, they will probably be targeted directly in state-against-state cybercampaigns. Similarly, nation states may increasingly use for-profit companies as proxies, partners, and conduits for asymmetric activities. Businesses must therefore determine how much risk they face from either intentional state-sponsored attacks on them or, as collateral damage, from attacks on other targets.

4. How will companies protect data in a world of pervasive sensors?

The Internet of Things (IoT) dramatically raises the stakes for cybersecurity — at least potentially, cyberattackers could manipulate devices that are now becoming connected to networks: for instance, automobiles; heating, cooling, and ventilation systems; and industrial machinery. The IoT involves huge numbers of network-connected sensors that will generate massive amounts of sensitive data. The security functions of companies will have to understand what kind of data the devices installed on their networks collect, who might benefit from compromising the data, and how to secure a whole new technological environment.

Although that goal is challenging, it is at least more straightforward than protecting sensitive information in the consumer IoT. Companies prohibit their executives and managers from working with sensitive documents on any personal device and from transmitting them via personal email accounts. Will companies also have to prevent employees from making or receiving company-related telephone calls at home in rooms with voice-activated smart devices?

5. How can companies protect their machine-learning capabilities?

Businesses are racing to implement machine-learning systems to detect fraud, improve pricing, rationalize supply chains, and optimize dozens of other business decisions. For all these use cases, decision algorithms improve over time as more data generate better insights about the connections between inputs and the objective function to be optimized. This is a fundamental change — analysts can no longer replicate algorithms on a pad of graph paper, as they could with traditional decision tools. It may therefore be all but impossible to determine whether a cyberattack has subtly compromised a business capability (by reducing the ability to detect fraud, for example). Security organizations and their business partners may need to develop new ways to ensure the validity of machine-learning algorithms.

6. How quickly will quantum computing create security threats?

All security relies on encryption — and on the assumption that massive computing resources would be required to decrypt data protected by even a moderately capable encryption algorithm. But quantum computers that could crack the RSA-1024 encryption standard in less than 24 hours may be only a decade away.[2] At a stroke, many of the security technologies the modern world depends on would become ineffective: for example, what would happen to investments in business processes based on blockchain if the encryption it requires could be compromised quickly?

Of course, defensive capabilities advance just as offensive ones do, and quantum encryption will probably attempt to protect users against quantum decryption. Yet the National Academy of Sciences estimates that it will take 20 years to make enterprise networks less vulnerable to quantum-based attacks.[3] That time frame, and the risk that some attackers may have access to quantum capabilities well before the next decade's end, mean that companies — especially in critical infrastructure sectors — have a responsibility to start early planning for the transition to a quantum world.

1 Andy Greenberg, "The untold story of NotPetya, the most devastating cyberattack in history," Wired, August 22, 2018, wired.com.
2 Martin Giles, "Quantum computers pose a security threat that we're still totally unprepared for," MIT Technology Review, December 3, 2018, technologyreview.com.
3 Emily Grumbling and Mark Horowitz, editors; Quantum Computing: Progress and Prospects, Washington, DC: National Academies Press, 2019, nap.edu.

Evolving security protections and platforms

The next group of questions addresses evolving security protections and platforms: how quickly a zero-trust model could be adopted, the future of passwords, the evolution of the security-tech market, and the security problems of cloud services.

7. How quickly could zero trust be adopted?
Most chief information-security officers (CISOs) have believed for years that the perimeter is less important than it used to be, though they continue to make investments in perimeter-based controls. Now, as companies start to accelerate their move into the public cloud, these traditional perimeters may become irrelevant for larger and larger parts of the corporate environment.

In the zero-trust model, applications base no trust assumptions on whether a user (or another application) is inside the network perimeter. This has several advantages: organizations can set the right level of protection for each application and dramatically limit the ability of attackers to move laterally across technology environments.

Yet companies have decades worth of legacy applications that assume the existence of a network perimeter, and very few technology organizations have developers with the skills to develop zero-trust applications. Less than 10 percent of the CISOs McKinsey surveyed believed they could adopt the zero-trust model, even for cloud applications, in the next two or three years.[4] The key to success in zero trust is the ability to understand and go on tracking users, assets, and controls simply, but at a granular level — or, if necessary, to reengineer or reshape them. CISOs will have to caucus with their application-development and infrastructure colleagues to determine how quickly their companies can develop the required capabilities.

8. When will we finally be able to kill passwords?
Passwords are terrible. Users hate them, forget them, write them down on publicly displayed sticky notes, and use them across accounts — including consumer accounts from providers with security vulnerabilities. Eliminating passwords could both reduce that vulnerability and improve the user experience dramatically.

What might a postpassword world look like? It would probably combine biometric authentication or authentication based on devices (such as phones, which use biometrics) with behavioral analytics that can determine, probabilistically, if users are legitimate. The advent of the WebAuthn standard for using devices to authenticate online services might be a critical enabler.[5]

But a successful transition will require device manufacturers, service providers, and commercial-software developers to adopt relevant standards and incorporate them into their offerings. In many cases, companies may want to develop the behavioral analytics to complement biometric authentication. Given the momentum, CISOs and other executives may want to start putting plans in place now.

9. How will the security-technology market evolve?
The cybersecurity-tooling market has recently been among the most fragmented in enterprise technology. Systems architects might have only a few practical choices for app servers or database-management systems. But their security colleagues must sort through dozens of endpoint-protection or antimalware products. Despite the problematic complexity, attempts to create integrated security platforms have met with limited success, to date.

Enterprise security leaders planning investments should ask the larger market participants to explain what makes their integrated offerings compelling. If they can't, it isn't clear whether proprietary products will continue to dominate this space or companies will seek to optimize their security expenditures by adopting open-source products. Equally important, how will the answers to these questions differ across market segments — say, between larger and smaller companies or between companies facing threats that are more sophisticated or less sophisticated?

10. When will large companies be able to consume cloud services securely?
The case for public-cloud infrastructure is exciting: access to innovative services for developers, near-infinite capacity on demand, and (at least potentially) lower costs. Yet for large, complicated companies — especially in heavily regulated industries — the pace of adoption has been slow.

[4] Arul Elumalai, James Kaplan, Mike Newborn, and Roger Roberts, "Making a secure transition to the public cloud," January 2018, McKinsey.com.
[5] Francis Navarro, "A world without passwords? The web's weakest link gets long-overdue fix," komando.com.

Some companies with thousands of applications (and more than 100,000 servers) desperately want to leverage the infrastructure of the public cloud but have succeeded only in running fewer than ten applications there.

Legacy applications never designed to run efficiently in the cloud are part of the problem, but security is a major bottleneck as well. Security teams are racing to perform risk assessments of hundreds of cloud services – first to learn if capabilities such as identity and access management (I&AM) and monitoring work in them and, second, to build the level of automation that would make it possible to configure systems securely in the cloud. Companies thus need to determine just how quickly they can build cloud-enabled security capabilities, which acceleration opportunities they have, and what that means for the overall journey to the cloud.

11. Will smaller companies use cloud services to reduce their security footprint dramatically?
Some security professionals talk about the cybersecurity poverty line: companies that annually spend even $50 million or $100 million a year on IT may struggle to afford all the cyber-security tools they need and to attract the talent to deploy and manage them. The transition to cloud services has challenged larger companies scrambling to recast their security architectures and operations to support a cloud-based infrastructure.

But the cloud may be a security godsend for smaller companies. Their technology executives (or counterparts in small, independent divisions of larger companies) should ask themselves if they could dramatically reduce their internally managed technology footprint, their surface area, and therefore their level of risk by accelerating the transition to business applications based on software as a service (SaaS) and to SaaS-based desktop environments, voice communications, and network connectivity. This question will be especially relevant for private-equity firms, which invest in many midmarket companies.

Evolving security operating models

The final set of questions focuses on evolving operating models for security: whether the cyberinsurance market will protect against cyberrisks, how the scope of security organizations will develop, and how cybersecurity talent pools will react to demand.

12. Will the cyberinsurance market protect against material cyberrisks?
For the past decade, market observers have suggested that cyberinsurance is the next major growth area for insurance carriers. Sceptics have rejoined that it will always be the next major growth area. For now, the sceptics seem to be right: the cyberinsurance market has grown only incrementally and still doesn't cover most cyberrisks except customer-data-breach mitigation and regulatory penalties. Direct costs, reputational risks, and intellectual-property theft do not get meaningful coverage. Since companies cannot effectively hedge cyberrisks, they adopt new technologies relatively slowly for fear of their adverse cybersecurity implications.

As for the insurance carriers, they don't have good actuarial data for cyberthreats, know how to model cyberrisks well, or truly understand the cyberrisks they would insure or the returns on the relevant investments. However, new quantitative methods are emerging to assess the likelihood of long-tail cyberevents, and one or more carriers may succeed in quantifying and insuring cyberrisks. If so, companies may be able to transfer risks they have so far been accepting or mitigating at high cost. But that will come to pass only if carriers can dramatically improve their underwriting.

13. How will the scope of security organizations develop?
Cybersecurity has become a more important issue for boards and senior management teams alike. Many companies have therefore started to expand the remit of what used to be the information-security organization, recasting it as the IT-risk group, responsible not only for information security but also for technology compliance, the quality of software, disaster recovery, and business continuity. The goal is to have one executive and one team make integrated decisions about protecting corporate information and systems from both accidents and attacks.

Other companies, thinking that no clear line separates cybersecurity from physical security in an increasingly digital world, have integrated them. A few companies have combined cybersecurity with fraud control because they think that most fraud has an online component and want integrated analytics to oppose it. A few other companies combine the security and privacy teams, on the theory that customers care only about the misuse of their data and don't distinguish between

security and privacy. Meanwhile, many companies have moved much of their security-related service delivery and technology support into the technology-infrastructure organization, so that CISOs and their teams can focus on strategy and risk management.

In short, the organizational structure for cybersecurity hasn't stabilized. Senior managers must watch developments in their industries to see which organizational structures succeed.

14. How will cybersecurity talent pools evolve in relation to demand?

CISOs disagree on many things, but they almost universally believe that cybersecurity talent is in short supply. When people chose majors and courses of study in the past, almost nobody expected cybersecurity to be as big an issue as it is today. But for several years now, demand signals indicating a pressing need for cybersecurity expertise have been penetrating the talent marketplace. Computer-science students are beginning to take cybersecurity courses, security specialists trained in the military have entered civilian labor markets, and lawyers and other professionals have gone back to school to retrain themselves as cybersecurity experts.

Technology executives should think about their cybersecurity operating models: what to outsource, how aggressively to automate, and which skills to foster internally. As they do, they must know how much cybersecurity talent is available and whether it aligns with their overall strategy. People with low-end cybersecurity skills, for example, may become more available long before companies can find enough experts with the advanced skills required to face off against business leaders on cybersecurity issues or to direct the automation of cybersecurity.

Policy decisions, investment choices, and security incidents now confront security, business, and technology executives with pressing (and often exhausting) cybersecurity issues they must address in the short – and sometimes very short – term. Yet in view of the cybersecurity environment's highly dynamic nature, CISOs and other executives have a responsibility to think through the longer-term questions raised in this article.

Companies can address some of the issues described here – for instance, quantum computing, pervasive sensors, and the cyberinsurance market – as events unfold in coming years. Other issues, such as evolving consumer expectations and regulatory demands, require more immediate attention because they could have a dramatic impact in the next year or two. To withstand the coming security onslaught, companies will have to change in important ways. The questions posed in this article are the natural starting point.

Venky Anant is a partner in Silicon Valley office of McKinsey. **Tucker Bailey** is a partner in McKinsey's Washington DC office. **Rich Cracknell** is a manager of solution delivery in Silicon Valley. **James Kaplan** is a partner in the New York office, where **Andreas Schwarz** is an expert.

Protecting the business: Views from the CIO's and CISO's offices

At JPMorgan Chase, CISOs and CIOs work together to align cybersecurity with business goals.

by James Kaplan

In an increasingly digital era, protecting information and systems from cyberattack is one of the most important and challenging responsibilities of every IT organization. In some cases, business-unit chief information officers (CIOs) and enterprise chief information security officers (CISOs) can have very different perspectives and agendas, creating friction and reducing organizational effectiveness.

At JPMorgan Chase & Co., which has one of the world's largest private-sector technology environments, two of the four business-unit CIOs have previously served as the bank's enterprise CISO.

McKinsey's James Kaplan spoke with several members of JPMorgan Chase's Global Technology leadership team, led by Lori Beer, Global CIO and member of the company's Operating Committee, about effective collaboration between the security and business-unit technology functions, what makes a good CISO, and how being a CISO can be valuable preparation for being a CIO.

Rohan Amin is CIO of Consumer & Community Banking, Anish Bhimani is CIO of Commercial Banking, George Sherman is CIO of Global Technology Infrastructure, and Jason Witty is JPMorgan Chase's global CISO. All are managing directors. Prior to their current roles, both Amin and Bhimani served as JPMorgan Chase's global CISO..[1]

The attributes of an effective CISO

Jason Witty: Being a successful CISO these days involves wearing many hats, from business to risk to technology to software engineer. You must be aware of the threat landscape and understand human behavior. You also have to know how to work with regulators and gain trust from multiple stakeholders.

Doing those things gives you a firmwide view of what's going on in the business, what's going on in technology, what's going on in risk, and what's going on in the legal and regulatory landscape. This allows you to connect the dots in a way that other roles simply do not provide.

You must constantly be shifting, adapting, and learning. I spend about two hours every morning just digesting what's changed since I went to bed, be it new threats, bad actors, or vulnerabilities. Then you need to translate this into digestible content for a non-technical audience, which requires good soft skills as well.

A CISO drives and controls an agenda, and building trust is critical in implementing that agenda, because trust is a force multiplier. As a CISO, my priorities are to protect the firm, enable the firm to drive growth, and make this growth as seamless as possible from a security standpoint.

George Sherman: I think the best CISOs are the ones who have learned about policy and controls but at their core are very strong technologists. The CISO role must evolve with the threat landscape and technologies. You must understand the technical side of cybersecurity. But information security and protecting against cyberthreats are also about people and process, not just technology, so you have to understand all three dimensions in order to fully appreciate what you have to do to protect the firm.

Sometimes you have to go slow to go fast. It's the old race-car analogy. You can go really fast in a race car because you're wearing a fireproof suit, you're in a protective cage, you have an automatic fire-extinguishing system, and you were trained. This allows you to drive superfast.

But getting to that point can feel slow. CISOs who "get it" spend a little bit more time up front being thoughtful about their execution.

The changing role of the CISO

Jason Witty: The role of the CISO has already changed. It's about measured risk taking, not risk elimination. This measured risk taking must also evolve with the availability of new technologies. You must constantly adapt, train, and educate so that you can adjust the control environment to enable the things the business is trying to accomplish.

Rohan Amin: If you want to help the builders, you have to know how to build. As a CISO, if you are not close to the modernization agenda—modern architectures, cloud, data, machine learning, and so on—then it's hard to effectively guide an organization in the right direction.

[1] r the full interviews with each interviewee, see "The benefits of a CISO background to a business-unit CIO" (Rohan Amin), "Enterprise-wide security is both a technology and business issue" (Anish Bhimani), "Robust cybersecurity requires much more than great technology" (George Sherman), and "The modern CISO: Managing scale, building trust, and enabling the business" (Jason Witty), March 2020, McKinsey.com.

George Sherman: You can go back a decade and see how much has changed. Everything seemed much simpler. The successful CISOs of the future can't be process managers. They must have a deep understanding of technology. Imagine leading thousands of software engineers but never having actually written a line of code. At some point, you have to ask yourself how you can relate to that community. And how will that community relate to you? Those questions are just as relevant to today's and tomorrow's CISOs.

Anish Bhimani: I used to go to the board of directors and the audit committee annually for about 20 minutes. We now meet with the board eight times a year for at least an hour each time.

The value of CISO experience to CIOs

Anish Bhimani: Every CIO should spend time in a security role, since it makes you think differently. Regardless of your role, you're never out of security. With new technologies, including automation, security is a layered process. It's built into the fabric of the organization, from process to people.

Rohan Amin: When we think about what matters most to our customers, running a disciplined environment with stability, resiliency, controls, and data privacy are non-negotiables. Being in the CISO role obviously instilled a lot of that in me.

The other aspect that's helpful in having a CISO background is a deep understanding of non-functional requirements and how to make them easier to adopt. For example, modernizing our applications and striving for platform-centric thinking help to focus our engineers on the most relevant business functions, which are the features and value for customers.

As a CISO, you have a global view of risk and what the issues are and how you think about enterprise management in the application-development context. Some CISOs are policy and governance focused only, while others have a stronger technical and business background. Having a technical background and being able to effectively communicate complex issues to the business have served me well.

George Sherman: We are unique and fortunate in that three of our CIOs are former CISOs. This makes the current CISO's life much easier, specifically as it relates to how you design, deliver, and execute the business-process automation efforts. Thanks to our security background, we tend to think about data protection and security earlier in our processes and require that security and controls be embedded into all the technology we deliver.

I use my technical-security skills on a daily basis. With new technology and connectivity platforms, many of our older security paradigms are being stressed. In the past, you could get away with not having the most robust identity or authorization constructs and authentication and authorization metrics. This is no longer the case, as the dynamic nature of these modern technologies requires dynamic management of the trust chain.

If you add to this the complexity of the multivendor cloud environments connecting into our companies, you must have a strong understanding of the "threatscape" and how you deal with cybersecurity issues. Everyone within the organization must understand that cybersecurity is non-negotiable. We have to get it right all the time. The bad actors only have to get it right once.

How being CISO helped in becoming a CIO

Anish Bhimani: I spent my entire career aspiring to be the CISO of a large bank, and when I got the job, it was a significant accomplishment in my career. When I then became a CIO, it meant shifting to more of an implementation approach, and I was eager to work with the business. But despite my excitement, I was clear that job number one is having a secure operating environment. If you don't do job one, you don't earn the right to do job two, which is to deliver value to the business.

Rohan Amin: In the CIO role, you get a deep appreciation for the importance of the control environment and security. You learn that everyone understands the importance of controls but wants control adoption to be more seamless and part of the engineering process.

Security and controls teams face a continuing challenge to figure out how to make this stuff simple and easy to use. This requires the engineering work to make it easy to adopt, easy to innovate on the platform, and easy for engineers to do the right thing. People can't be forced to read thousands of pages of policy to figure out the right thing to do. The right thing to do should be easy and baked into the platforms and enabled via software, so that something as simple as "you should encrypt your data" isn't something every engineering team has to figure out for itself. Make security the easy answer, not the hard answer.

The impact of the cloud

Anish Bhimani: When moving to the cloud, the first priority is figuring out your technology and business priorities and then striking a balance. Services and architecture templates need to be validated and automated for cloud configuration. Secondly, cloud security can be a business enabler, and we know that businesses need to grow and thus must move fast.

Why do you have brakes on a car? It's not to stop. It's so you can go fast, secure in the knowledge that you can stop whenever you want or need to. Security done right enables businesses to go at the speed they want while being able to manage risk appropriately.

George Sherman: Technology is going to become more segmented but also more hyperconnected. You can see that in the evolution of the private, public, and hybrid cloud and with a combination of infrastructure-as-a-service, platform-as-a-service, and software-as-a-service providers clamoring to support new growth. But with this hyperconnectivity comes hypercomplexity, and with that comes fragility. Fragility leads to reliability and security issues. The enemy of a good security program is complexity. If we're not careful in our execution, CISOs could end up with a "least common denominator" problem where their environments are only as secure as their weakest controls.

Cybersecurity advice for newcomers

Rohan Amin: Spend time with the folks in the business who have to use the stuff you're creating. If your objective is to help the business—which is what it should be—then you need to spend time in the business to understand what it takes to deliver something to a customer. If you spend time only in security land, you really don't understand the complexities the builders go through to deliver. Knowing what I know now, building simplicity into security-control adoption is where I'd recommend they focus.

Anish Bhimani: My first advice is that life never moves in a straight line. You need to be able to adapt to constantly changing circumstances. Well-roundedness is critical, and everything you do should get you a step closer to your goals. Rotations are valuable in gaining experience in security and infrastructure.

Focusing on the future

Jason Witty: "Deepfakes" ar e a concern, so having the ability to prove that who you are talking to is actually the person you think you are talking to is vital. Artificial-intelligence (AI) and natural-language-processing algorithms are also advancing rapidly, posing new reputational and financial threats in addition to opening new doors for business growth.

Safely enabling AI and maintaining our ability to keep up with the velocity of automated attacks is also something being much discussed. We'll continue to modernize software engineering around the cloud to ensure security and resiliency and to further unlock its business value. Finally, we're looking into crypto-agility and decoupling the encryption process from the software-development process.

Rohan Amin: Authentication is often the first experience a consumer has with an organization, so we're working on the authentication strategy of the future. Previously, authentication was thought about as a channel-specific thing, meaning how do we authenticate you in the branch? How do we authenticate you when you call in? How do we authenticate you online or on mobile?

We're working to bring these experiences together in a secure and more integrated manner. We're thinking about ways of putting the customers at the front of the design and about the multichannel ways people interact with us differently than in the past.

George Sherman: Resiliency, availability, and security are everyone's responsibility, regardless of whether you're involved with infrastructure, applications, or both. Everyone must believe that operational risk and information security are core requirements of their role, so you need to invest in training and move this to the forefront of your team's minds, or you will end up with yet another remediation program.

Secure by design is critical. You can build systems that are reliable and available, but they may not necessarily be secure. But when you build secure systems, you often end up with ones that are both reliable and available. The disciplines around security tend to lend themselves to the same disciplines as resiliency and availability or operational efficiency and effectiveness.

James Kaplan is a partner in McKinsey's New York office.

The modern CISO: Managing scale, building trust, and enabling the business

The modern CISO is uniquely positioned to bridge gaps across technology, processes, automation, and cybersecurity.

Securing the information of a multibillion-dollar enterprise with more than a quarter of a million employees is a daily Herculean labor. Enterprise chief information security officers (CISOs) must manage myriad cybersecurity threats, automation, regulatory compliance, and ever-evolving technologies. Jason Witty, global CISO, JPMorgan Chase, discusses his role and these challenges with McKinsey's James Kaplan.

This interview is part of a series of interviews on the evolving relationship between the CISO and CIO. (See "Protecting the business: Views from the CIO's and CISO's offices," on McKinsey.com.)

James Kaplan: How do you define the role of a CISO?

Jason Witty: A CISO drives and controls an agenda, and building trust is critical in implementing that agenda, because trust is a force multiplier. As a CISO, my priorities are to protect the firm, enable the firm to drive growth, and make this growth as seamless as possible from a security standpoint.

Being a successful CISO these days involves wearing many hats, from business to risk to technology to software engineer. You must be aware of the threat landscape and understand human behavior. You also have to know how to work with regulators and gain trust from multiple stakeholders.

Doing those things gives you a firmwide view of what's going on in the business, what's going on in technology, what's going on in risk, and what's going on in the legal and regulatory landscape. This allows you to connect the dots in a way that other roles simply do not provide.

You must constantly be shifting, adapting, and learning. I spend about two hours every morning just digesting what's changed since I went to bed, be it new threats, bad actors, or vulnerabilities. Then you need to translate this into digestible content for a nontechnical audience, which requires good soft skills as well.

James Kaplan: How do you manage the complexity of an institution the size of JPMorgan Chase?

Jason Witty: You manage scale. You build trust. You have command of the details without getting bogged down. You also have to have very strong leaders under you that you can trust. I am fortunate to have a fantastic team.

James Kaplan: How are you addressing security concerns amid increasing automation and continuous controls monitoring?

Jason Witty: We put a lot of effort around controls as code, or policies as code, ensuring the ubiquity of modern software engineering practices across the firm. All of our applications are in the process of being rearchitected to support a modern software environment, with automated, self-evidencing controls built in.

We have hundreds of engineers on the security side dedicated to automation, such as by making controls seamless and integrating security tools within the product, platform, and service pipeline.

It's all about data and code now. This ensures strong integration and collaboration with the businesses as well. Security is thought of as a part of each technology capability or product rollout, which is a tremendous advance compared to a decade ago, when security was viewed as a hindrance.

James Kaplan: In years past, security was fragmented. How have the organizational structure and lines of responsibility evolved?

Jason Witty: DevOps has significantly changed the way that IT in general thinks about product management, application development, and production support. Site reliability engineering (SRE) is a big focus, along with our product journey. It's a change in traditional telemetry management from years ago, when it was very fragmented and siloed. Our software environment provides transparency, which enables people to respond quickly to issues.

We're simultaneously integrating core functions with SRE, as well as modernizing the environment. This means more colocation and cocreation, which spur both product and security innovation. We're completely aligned on the customer and client experience.

James Kaplan: How are new technologies like cloud impacting the institution?

Jason Witty: Today's modern software environment is faster from a business-capability standpoint. You have more incremental change and faster release cycles; you can also know earlier when something goes wrong, which means you can respond faster.

James Kaplan: There's often an overlap between infrastructure and security engineering. How have you addressed this collaboration?

Jason Witty: The product model supersedes departmental silos. When you have multiple teams working on the same set of issues, it completely transcends organizational boundaries. If everyone involved understands the end objectives and how they are measured, then they're all pointing the needle in the same direction. It's a combination of site reliability engineering and product that makes the process more seamless.

James Kaplan: As the product model becomes more pervasive, how does the role of the CISO change over time?

Jason Witty: The role of the CISO has already changed. It's about measured risk taking, not risk elimination. This measured risk taking must also evolve with the availability of new technologies. You must constantly adapt, train, and educate so that you can adjust the control environment to enable the things the business is trying to accomplish.

James Kaplan: Talk about the collaboration around regulatory compliance.

Jason Witty: We take compliance very seriously. We are constantly mapping and cross-mapping international regulations to our control environment and legal obligations. We're always looking for better ways of automating that process. We're adopting the Bank Policy Institute's Financial Services Sector Cybersecurity Profile as our framework of frameworks in 2020 and encouraging regulators to start auditing against the profile, which has the potential to be an industry-wide game changer.

James Kaplan: Are you experiencing the talent or skills gap that we hear about in the cybersecurity space?

Jason Witty: Yes. We have myriad ways we try to address that. We have programs specifically focused on bringing in non-computer-science talent, who we put through coding boot camps and upskill. We also have a Cyber Kids school program that goes into schools and provides basic skills training on internet safety and security. We hope to help spur interest in STEM-related activities and careers. We also recruit talent from the military and affinity groups to attract the best talent available. We were a founding sponsor of the Financial Services Information Sharing and Analysis Center's (FS-ISAC's) scholarship program for female university students looking to pursue a career in cybersecurity. Recruiting the right people is critical, but retaining them is also important, hence our emphasis on upskilling, training, and continuing education.

James Kaplan: If you look down the road for the next three or four years, what keeps you up at night?

Jason Witty: "Deepfakes" are a concern, so having the ability to prove that who you are talking to is actually the person you think you are talking to is vital. Artificial-intelligence (AI) and natural-language-processing algorithms are also advancing rapidly, posing new reputational and financial threats in addition to opening new doors for business growth.

Safely enabling AI and maintaining our ability to keep up with the velocity of automated attacks is also something being much discussed. We'll continue to modernize software engineering around the cloud to ensure security and resiliency and to further unlock its business value. Finally, we're looking into crypto-agility and decoupling the encryption process from the software-development process.

James Kaplan is a partner in McKinsey's New York office.

The benefits of a CISO background to a business-unit CIO

A deep understanding of cybersecurity is a competitive advantage.

Although chief information security officers (CISOs) focus on technology and chief information officers (CIOs) concentrate on the business, their missions are inextricably linked. A CIO with a foot in each world enjoys a unique perspective that can only enhance effectiveness and better serve the enterprise. Rohan Amin, CIO, Consumer & Community Banking, JPMorgan Chase, explains to McKinsey's James Kaplan how his CISO background prepared him for the CIO role.

This interview is part of a series of interviews on the evolving relationship between the CISO and CIO. (See "Protecting the business: Views from the CIO's and CISO's offices," on McKinsey.com.)

James Kaplan: What was it like making the transition from CISO to business-unit CIO? What was unexpected once you moved into the CIO role?

Rohan Amin: I had the technical background, but the main learning curve was getting much closer to the technology that supports the business – and, of course, the business processes – itself. I'm thankful I get to work with an incredible team, and they have been very supportive of me in my new role. In a CISO role, you can be a step removed, so it's been a great learning experience for me.

James Kaplan: Where has the learning curve been the fastest? Where has it been the steepest?

Rohan Amin: I began my career as a software engineer and have led large development teams, so that was a more comfortable part of the transition. The greater learning curve has been around the business itself and the business strategy. In my previous CISO role, the primary set of relationships I had were mostly with the technology risk-and-controls community. While I did have a presence at the business table, most day-to-day interaction was with our technology teams. In my current CIO role, I am balancing across two senior teams, so my interaction with different stakeholder communities has increased dramatically.

James Kaplan: How long did it take you to get up to speed on the consumer banking side of the business?

Rohan Amin: I'm still getting up to speed! It is a behemoth of a business, with more than 52 million digitally active consumers. I have never been the CIO of a consumer bank. That I am, I think, is a testament to how the organization thinks about talent development and mobility. Second, I wanted to do something where I was forced to learn a lot of new things and was intellectually stimulated and fully engaged. I got all of that.

James Kaplan: Having been a CISO provides an interesting background for a CIO role. Was there anything about your CISO experience that made you a more effective business-unit CIO?

Rohan Amin: When we think about what matters most to our customers, running a disciplined environment with stability, resiliency, controls, and data privacy are non-negotiables. Being in the CISO role obviously instilled a lot of that in me.

The other aspect that's helpful in having a CISO background is a deep understanding of non-functional requirements and how to make them easier to adopt. For example, modernizing our applications and striving for platform-centric thinking help to focus our engineers on the most relevant business functions, which are the features and value for customers.

As a CISO, you have a global view of risk and what the issues are and how you think about enterprise management in the application-development context. Some CISOs are policy and governance focused only, while others have a stronger technical and business background. Having a technical background and being able to effectively communicate complex issues to the business have served me well.

James Kaplan: What advice do you have for CISOs who may aspire to someday become CIOs?

Rohan Amin: In the CISO role, you get a deep appreciation for the importance of the control environment and security. You learn that everyone understands the importance of controls but wants control adoption to be more seamless and part of the engineering process.

Security-and-controls teams face a continuous challenge to figure out how to make this stuff simple and easy to use. This requires the engineering work to make it easy to adopt, easy to innovate on the platform, and easy for engineers to do the right thing. People can't be forced to read thousands of pages of policy to figure out the right thing to do. The right thing to do should be easy and baked into the platforms and enabled via software, so that something as simple as "you should encrypt your data" isn't something every engineering team has to figure out for itself. Make security the easy answer, not the hard answer.

James Kaplan: Do you think the skill sets of CISOs and CIOs will converge over time?

Rohan Amin: To some degree, yes. If you want to help the builders, you have to know how to build. As a CISO, if you are not close to the modernization agenda – modern architectures, cloud, data, machine learning, and so on – then it's hard to effectively guide an organization in the right direction. That said, the risk-and-controls discipline is also rapidly evolving, with increasing focus on data governance, privacy, and operational resiliency in a world powered by the cloud and machine learning.

James Kaplan: What advice would you have for a business-unit CIO who's never been a CISO about establishing an effective relationship with a CISO?

Rohan Amin: Take the time to understand in detail what those teams are seeing. Because when you're on the outside of that, it's sometimes difficult to appreciate the full extent of the problem they're trying to solve. It's unlike other aspects of the technology organization. Understand the challenges those teams face as they try to keep the bank and the firm safe. That's an eye-opener in terms of thinking through how you build software and the values that you instill in the organization.

James Kaplan: Is there any advice you would give to folks newly entering the security domain?

Rohan Amin: Spend time with the folks in the business who have to use the stuff you're creating. If your objective is to help the business – which is what it should be – then you need to spend time in the business to understand what it takes to deliver something to a customer. If you spend time only in security land, you really don't understand the complexities the builders go through to deliver. Knowing what I know now, building simplicity into security-control adoption is where I'd recommend they focus.

James Kaplan: What do you know now that you wish you had known a year or two ago?

Rohan Amin: I have a much greater appreciation for our engineering and development teams and the challenges they face in trying to do the right thing. There are so many things hitting them at once – modernization, cloud, data security, controls, resiliency, regulatory, and, of course, business functionality. I would have had a far greater sense of urgency about what a difficult environment we create for builders if we're not putting them first and thinking about them as customers. That's a different mindset, one I would have acted on faster if I'd had the insights into their challenges that I do now.

James Kaplan: How do you advance the skill sets of development teams?

Rohan Amin: Your development teams' training should be balanced with what you ask those development teams to focus on. You can't train for everything, and the evolving complexity demands that we make this easier for engineers. For example, typically you run your software through a scanning tool designed to highlight vulnerabilities, and typically, the security tool reports thousands of things you need to fix. But when you go through data sets and reports, there's simply too much to handle. A good security team will say, "Here are the discrete actions you need to focus on and take," as opposed to, "Here are 5,000 things that you need to figure out the importance of addressing."

James Kaplan: How do you address security training for developers?

Rohan Amin: Increasingly, we're baking those requirements into the software-development life cycle itself, so you don't deploy software that has issues. That, to me, is the ultimate way to solve this problem. You need the training, but you also have the tool chain and the telemetry. Enforce what you want through a controls-and-security perspective. With cloud applications, these platforms are automatically enforcing the control environment.

So if you're not compliant, your workload won't get deployed or run in production. That's a big change in mindset. And to be clear, I'm referring to cloud generically – private or public.

James Kaplan: Authentication is an incredibly important part of the consumer-banking experience. What are your thoughts about managing that?

Rohan Amin: Authentication is often the first experience a consumer has with an organization, so we're working on the authentication strategy of the future. Previously, authentication was thought about as a channel-specific thing, meaning how do we authenticate you in the branch? How do we authenticate you when you call in? How do we authenticate you online or on mobile?

We're working to bring these experiences together in a secure and more integrated manner. We're thinking about ways of putting the customers at the front of the design and about the multichannel ways people interact with us differently than in the past.

James Kaplan is a partner in McKinsey's New York office.

Robust cybersecurity requires much more than great technology

Security is increasingly an interdisciplinary capability.

It's easy to view the 21st-century "threatscape" through a purely technological lens. But today's chief information security officers (CISOs) and chief information officers (CIOs) need to understand and appreciate the people and process elements as well. George Sherman, CIO of Global Technology Infrastructure, JPMorgan Chase, discusses his multiprong outlook on information security with McKinsey's James Kaplan.

This interview is part of a series of interviews on the evolving relationship between the CISO and CIO. (See "Protecting the business: Views from the CIO's and CISO's offices," on McKinsey.com.)

James Kaplan: How does your security background shape your approach to your current role?

George Sherman: I use my technical-security skills on a daily basis. With new technology and connectivity platforms, many of our older security paradigms are being stressed. In the past, you could get away with not having the most robust identity or authorization constructs and authentication and authorization metrics. This is no longer the case, as the dynamic nature of these modern technologies requires dynamic management of the trust chain.

If you add to this the complexity of the multivendor cloud environments connecting into our companies, you must have a strong understanding of the "threatscape" and how you deal with cybersecurity issues. Everyone within the organization must understand that cybersecurity is non-negotiable. We have to get it right all the time. The bad actors only have to get it right once.

James Kaplan: What makes for a good CISO?

George Sherman: I think the best CISOs are the ones who have learned about policy and controls but at their core are very strong technologists. The CISO role must evolve with the threat landscape and technologies. You must understand the technical side of cybersecurity. But information security and protecting against cyberthreats are also about people and process, not just technology, so you have to understand all three dimensions in order to fully appreciate what you have to do to protect the firm.

Sometimes you have to go slow to go fast. It's the old race-car analogy. You can go really fast in a race car because you're wearing a fireproof suit, you're in a protective cage, you have an automatic fire-extinguishing system, and you were trained. This allows you to drive superfast. But getting to that point can feel slow. CISOs who "get it" spend a little bit more time up front being thoughtful about their execution.

James Kaplan: Does that need to understand the technology environment holistically at every layer in the stack provide a good background for a future business-unit CIO?

George Sherman: We are unique and fortunate in that three of our CIOs are former CISOs. This makes the CISO's life much easier, specifically as it relates to how you design, deliver, and execute the business-process automation efforts. Thanks to our security background, we tend to think about data protection and security earlier in our processes and require that security and controls be embedded into all the technology we deliver.

James Kaplan: Given all that's changing, particularly around cloud and digitization, how different will the skill set of a CISO be in a decade?

George Sherman: You can go back a decade and see how much has changed. Everything seemed much simpler. The successful CISOs of the future can't be process managers. They must have a deep understanding of technology. Imagine leading thousands of software engineers but never having actually written a line of code. At some point, you have to ask yourself how you can relate to that community. And how will that community relate to you? Those questions are just as relevant to today's and tomorrow's CISOs.

Also, the technology is going to become more segmented but also more hyperconnected. You can see that in the evolution of the private, public, and hybrid cloud, and with a combination of infrastructure-as-a-service, platform-as-a-service, and software-as-a-service providers clamoring to support new growth. But with this hyperconnectivity comes hypercomplexity, and with that comes fragility. Fragility leads to reliability and security issues. The enemy of a good security program is complexity. If we're not careful in our execution, CISOs could end up with a "least common denominator" problem where their environments are only as secure as their weakest controls.

James Kaplan: CISO and infrastructure responsibilities often overlap – for example, in patch management. How do you deal with this?

George Sherman: Having clear lanes of responsibility is important. If you view patching and life-cycle management as a tax or a duty, then you really don't understand the need to keep software current and manage it in a near-real-time way. This mindset translates into your organization's view of these functions as a burden. A CIO has the responsibility to design and direct their organization to understand that this isn't a burden but instead a core part of their team's job. Protecting the firm, keeping it patched and updated, is everyone's responsibility.

James Kaplan: Where does security fit into people's roles in IT?

George Sherman: Resiliency, availability, and security are everyone's responsibility, regardless of whether you're involved with infrastructure, applications, or both. Everyone must believe that operational risk and information security are core requirements of their role, so you need to invest in training and move this to the forefront of your team's minds, or you will end up with yet another remediation program.

Secure by design is critical. You can build systems that are reliable and available, but they may not necessarily be secure. But when you build secure systems, you often end up with ones that are both reliable and available. The disciplines around security tend to lend themselves to the same disciplines as resiliency and availability or operational efficiency and effectiveness.

James Kaplan is a partner in McKinsey's New York office.

Enterprise-wide security is both a technology and business issue

CISOs have important skills that can position them for the CIO role.

A chief information security officer (CISO) focuses on creating a secure operating environment, while a chief information officer (CIO) strives to deliver value to the business. But if you don't get the former right, it becomes impossible to do the latter. Anish Bhimani, CIO, Commercial Banking, JPMorgan Chase, has filled both roles. He discusses how they interact – and how they are evolving – with McKinsey's James Kaplan.

This interview is part of a series of interviews on the evolving relationship between the CISO and CIO. (See "Protecting the business: Views from the CIO's and CISO's offices," on McKinsey.com.)

James Kaplan: Tell us about your cybersecurity journey.

Anish Bhimani: I joined JPMorgan Chase in 2003, nominally as the CISO. I say "nominally," because when I got here, we were heavily outsourcing our cybertechnology. My role was largely a policy-vetting job, and I had 12 people working for me.

Everything changed dramatically when we merged with Bank One. The role became much more technology oriented and transformed into execution as well as policy. We were initially responsible for issues such as threat response, vulnerability management, security infrastructure, and so on. At that point, we didn't have a CISO, so the challenge was getting the right level of buy-in from the CIOs, and we were pushing hard to get people to pay attention to cybersecurity matters.

In 2009, the role was made into a proper CIO-level role, as it is today. It was at that point that cybersecurity had more visibility. Cyber became visible across the entire organization, with leadership driving the tone. It felt like a remediation exercise. We began to see an increase in denial-of-service attacks and malware, and leadership said, "This is more than a technology problem; it's a business problem. Let's fix it."

James Kaplan: What happened when internal stakeholders realized that cybersecurity was a business-critical issue?

Anish Bhimani: We began putting the right resources behind it. Businesses were trying to find a balance between security and the growth of new digital platforms. And as regulatory scrutiny intensified around technology, we paid more attention to technology control than to security. Since then, our level of focus on cybersecurity in the entire organization has been fantastic.

James Kaplan: Are there things you know now that you wish you had known then in your CISO role that could have made you more effective?

Anish Bhimani: What I realize now is that a lot of the things we try to do centrally have a tremendous impact on people. I can now set and drive the tone for the organization so that we get in front of security issues, remediate, and move on to the next challenge. I also did not fully appreciate the transition from developing policy to implementing policy. Finally, we probably should have pushed business leaders harder much earlier by stressing that security was not just a technology issue, but a business issue as well.

James Kaplan: Technology has changed. In years past, it was a 15-minute conversation in passing. By the early 2000s, you'd have a daylong strategy session. How is the topic being addressed at the highest levels of the organization?

Anish Bhimani: I used to go to the board of directors and the audit committee annually for about 20 minutes. We now meet with the board eight times a year for at least an hour each time.

James Kaplan: Discuss your transition from CISO to CIO.

Anish Bhimani: I spent my entire career aspiring to be the CISO of a large bank, and when I got the job, it was a significant accomplishment in my career. When I then became a CIO, it meant shifting to more of an implementation approach, and I was eager to work with the business. But despite my excitement, I was clear that job number one is having a secure and resilient operating environment. If you don't do job one, you don't earn the right to do job two, which is to deliver value to the business.

James Kaplan: What do you miss about your CISO role?

Anish Bhimani: You always miss the cat-and-mouse challenge, the game theory, as well as the

problem solving and intellectual curiosity. There is also a very active peer and industry community for best-practice sharing, since everyone is facing many of the same challenges. It's amazing how the CISO role has evolved.

James Kaplan: How do you see the CIO role evolving?

Anish Bhimani: The ongoing debate is where security should report. Some say security can't report to IT, because it's a conflict of interest. Others say there's no way you can get the job done reporting outside of IT. I think that, in years to come, security will become more embedded within the IT fabric of any organization as standard operating practice.

There is also the client impact. As we become better at securing systems, the point of vulnerability moves from the system to the person. Security becomes every employee's responsibility. Cyber organizations are now building frameworks, working across infrastructure with developers on systems such as cloud. So the architecture of how the CIO goes about implementing infrastructure and security policies will evolve with the role itself. A security organization will always attempt to be agile, but it's very challenging when you're moving at the speed of light.

James Kaplan: Do you see the CISO and CIO roles integrating?

Anish Bhimani: Every CIO should spend time in a security role, since it makes you think differently. Regardless of your role, you're never out of security. With new technologies, including automation, security is a layered process. It's built into the fabric of the organization, from process to people.

James Kaplan: What advice can you offer on breaking down silos and managing talent?

Anish Bhimani: Understand how to navigate the organization. Manage conflicts. Keep your objectives in mind while managing these conflicts. Understand your business's priorities. One of the things I am most proud of is the professional development of my direct reports. During my time as CISO, 21 of the people I managed went on to serve as CISOs elsewhere. So you must develop the people, not just their roles.

James Kaplan: It sounds like one of the biggest priorities is security remediation.

Anish Bhimani: It's less remediation and more about how you proactively build controls. For example, several years ago, when we found a serious issue with some systems, we would run a remediation program that took days or weeks. Now, a similar incident is opened and fixed before people go home.

James Kaplan: Talk about the movement to cloud applications.

Anish Bhimani: When moving to the cloud, the first priority is figuring out your technology and business priorities and then striking a balance. Services and architecture templates need to be validated and automated for cloud configuration. Second, cloud security can be a business enabler, and we know that businesses need to grow and thus must move fast.

Why do you have brakes on a car? It's not just to stop. It's so you can go fast, secure in the knowledge that you can stop whenever you want or need to. Security done right enables businesses to go at the speed they want while being able to manage risk appropriately.

James Kaplan: What type of advice would you offer someone who is just beginning their career in cyber?

Anish Bhimani: My first advice is that life never moves in a straight line. You need to be able to adapt to constantly changing circumstances. Well-roundedness is critical, and everything you do should get you a step closer to your goals. Rotations are valuable in gaining experience in security and infrastructure.

James Kaplan is a partner in McKinsey's New York office.

Securing software as a service

Here is how SaaS providers can meet the security needs of their enterprise customers.

by Rich Cracknell, James Kaplan, Wolf Richter, Lucy Shenton, and Celina Stewart

Companies are rapidly adopting software as a service (SaaS) in place of purchasing commercial off-the-shelf software (COTS). Companies using SaaS rely on SaaS vendors to host their applications in the cloud instead of running them in their own data centers. Industry analysts estimate that the SaaS market will grow by more than 20 percent annually, reaching nearly $200 billion by 2024, a level that would represent nearly one-third of the overall enterprise-software market. With enterprise values for SaaS businesses reaching approximately seven times forward revenue, software companies are racing to convert from on-premises to SaaS-based delivery models.[1]

Most companies, therefore, will eventually confront the cybersecurity risks inherent in the SaaS approach. These are different risks from those posed by on-premises COTS. In building COTS, the vendor takes responsibility for removing security vulnerabilities from the application code. The customer, however, installs the software, configures it, and takes responsibility for running it in a secure infrastructure. For SaaS offerings, the vendor takes on many of the security responsibilities previously assumed by the customer.

Companies do not always feel comfortable with the indirect relationship to cybersecurity risk that SaaS presents, mediated as it is through vendorbased protections. More important, SaaS vendors have not always ensured that their products meet their customers' security requirements. That is the story that emerged from our survey of cyber professionals from companies seeking to adopt SaaS solutions.[2] Their responses also provide insights into how enterprises should think about security in an SaaS world and important clues for SaaS vendors on how to earn the confidence of their enterprise customers.

The security challenges of software as a service for adopting companies

Our survey polled chief information-security officers (CISOs) and other cybersecurity professionals from more than 60 companies of varying size in a range of industries. We wanted to understand how companies experienced SaaS offerings and how they responded to security challenges. Almost universally, respondents confirmed what we had suspected: they have increased their focus on security for SaaS offerings, emphasizing capabilities at the intersection of the vendor's and their own security environments. They expressed a fair amount of frustration with shortcomings in vendors' cybersecurity capabilities, which often caused delays in contracting and implementation. In their view, SaaS vendors need to take a much more customer-centric approach to security, making it easier to understand their products' security capabilities, easier to integrate them with the rest of the enterprise-security environment, and easier to configure them in a secure and compliant way.

All the companies we spoke with had already begun to make the transition to SaaS offerings. About half had used products from 20 or fewer SaaS vendors, about a quarter from more than 80. Almost all companies surveyed were deploying SaaS offerings in at least one major area, especially office automation, IT-service management, and niche business applications (Exhibit 1).

Many security executives said that their organizations were not ready to use SaaS in some critical domains, however, because of the potential risks. These include enterprise-resource-planning applications, where downtime can prevent the entire business from functioning. Similar concerns were raised for engineering- or manufacturer-related applications. For health-related applications and applications that may contain M&A information, the biggest barriers to SaaS adoption concern data confidentiality.

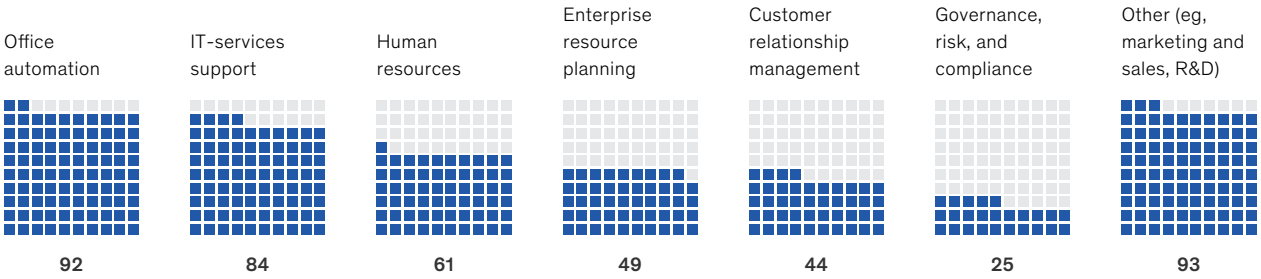
[1] KBV research cited in "Software as a service (SaaS) market to reach a market size of $185.8 billion by 2024: KBV Research," PR Newswire, December 19, 2018, prnewswire.com; Enterprise software market research report – global forecast 2023, Market Research Future, May 2019, marketresearchfuture.com; "Just where are SaaS companies priced after the 2018 correction?," Tomasz Tunguz, December 26, 2018,tomtunguz.com.

[2] 2019 McKinsey Customer Perspectives on SaaS Survey of chief information-security officers (and managers responsible for cloud security or vendor security) from more than 60 organizations. More than half of the participants were from companies in financial services, insurance, pharma, and health services, with the rest spread across the government, industrial, and tech sectors. Each third (approximately) of the responding companies had respective annual IT budgets of $500 million and above, $50 million to $500 million, and less than $50 million. Most respondents were from companies based in the United States. Differences in size, geography, and sector apart, however, the companies largely expressed similar concerns.

Exhibit 1

Surveyed enterprises most commonly used software as a service for office automation, IT-services support, and niche business applications.

Level of SaaS[1] adoption by usage type, % of respondents (n = 61)



[1] Software as a service.
Source: McKinsey Customer Perspectives on SaaS survey

Priorities in attempting to secure software as a service

In their relationships with SaaS vendors, most respondents use questionnaires to gauge security capabilities but criticize the approach as imprecise, incomplete, and overly time consuming. Security executives tend to focus on four key issues when confronting SaaS capabilities: encryption and key management, identity and access management (IAM), security monitoring, and incident response (Exhibit 2). Notable is that each of these issues has more to do with the interface between the customer and the SaaS provider than with the providers' intrinsic technical protections, such as code security and endpoint protection.

Encryption and key management

Applications running in the cloud and data stored there are not protected by a traditional corporatesecurity perimeter of firewalls and the like. As a result, security becomes essentially reliant on encryption and management of the keys that provide access to encrypted data. Our interviews revealed that most companies, especially large ones, do not entrust SaaS providers to host and manage their security keys. The majority prefer to hold their keys on premises through a hardware security module, retain management control of cloud-hosted keys, or use a combination of methods (Exhibit 3). These approaches allow companies to control access to sensitive information. It also ensures that government agencies cannot gain access to and unencrypt their data without contacting them first.

The survey further revealed that companies want a degree of sophistication in key management so that they can grant access to data for a certain period of time or revoke access quickly. This preference again emphasizes that most respondents want to exercise full control over their sensitive information.

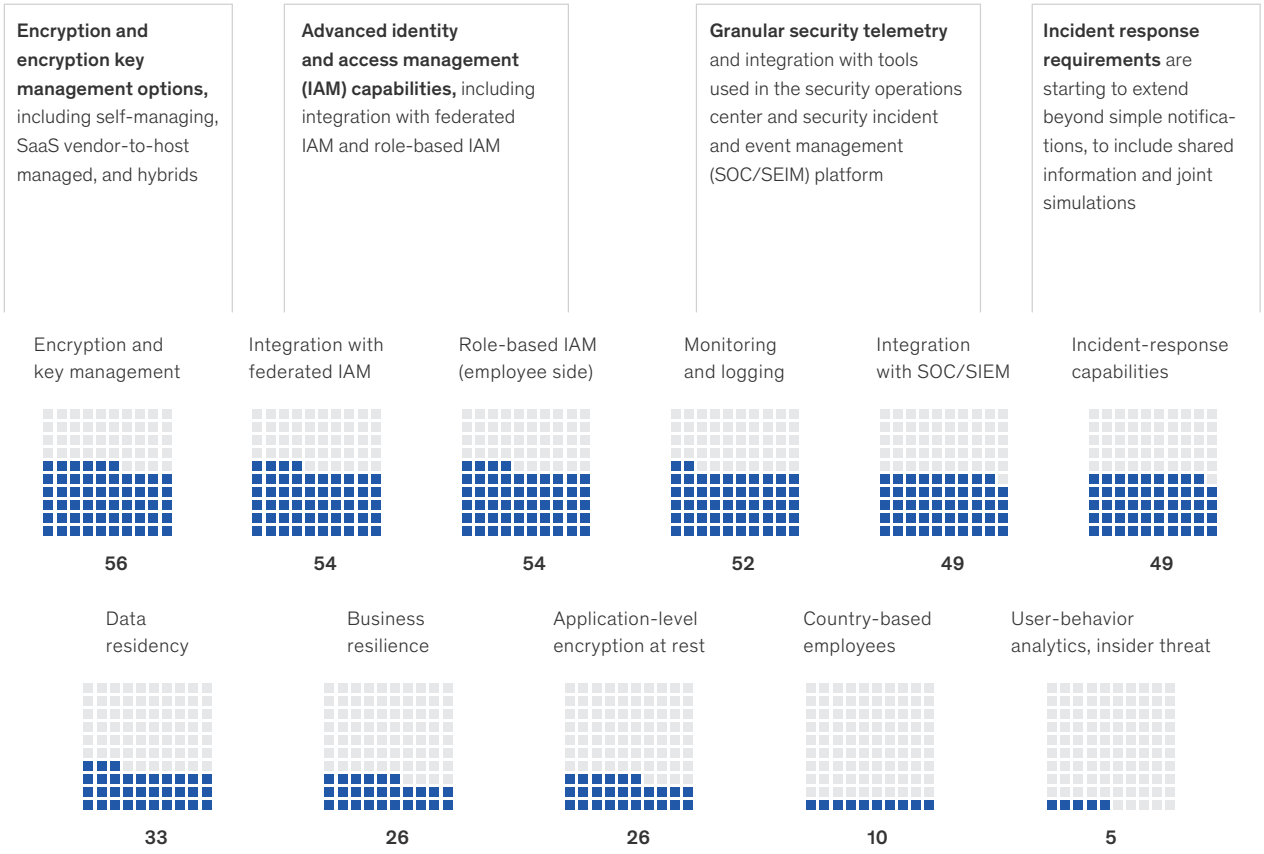
Identity and access management

Identity management is the act of confirming that each user is the person he or she purports to be. Access management is the determination that a user does or does not have legitimate rights to retrieve data or use an application. As important as both identity and access management are on company premises, they are even more important for cloud-based applications.

Exhibit 2

Enterprise customers focus on the interface between software-as-a-service providers and their own security environments.

Capabilities that respondents would like to see from SaaS[1] vendors, % of respondents (n = 61)



[1] Software as a service.
Source: McKinsey Customer Perspectives on SaaS survey and interviews with more than 60 industry leaders

Security executives emphasized that two IAM capabilities are especially important to them. First, they want tight, easily implementable integration between SaaS applications and widely adopted enterprise IAM tools. Companies deploy hundreds or thousands of applications, dozens of which are SaaS applications. They cannot expect users to memorize yet another password for each new SaaS offering that is adopted. They want to allow users to sign into SaaS applications via enterprise-wide IAM platforms, which will provide additional features like two-factor authentication. Second, they need sophisticated, role-based access management, including the ability to provide selected people with the authority to access certain data or undertake certain transactions within an application.

Security telemetry and monitoring

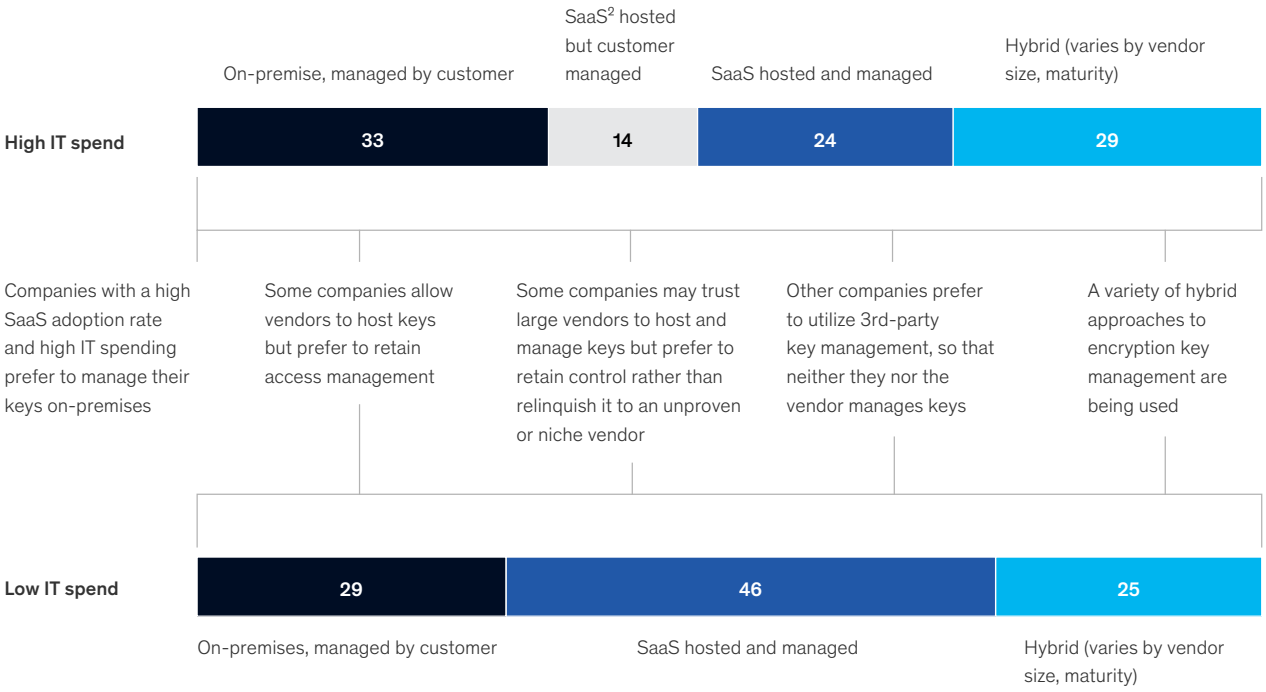
Increasingly, CISOs acknowledge that they cannot prevent every instance in which security is compromised. They therefore want the necessary transparency to identify and assess emerging security risks quickly and thoroughly. As companies adopt SaaS offerings, data from SaaS providers about usage patterns become critical to this analysis.

Security reporting is the baseline capability CISOs demand. They want a clear view – usually consolidated in a dashboard – of the users that have been accessing their data and what they have done with it. Without this kind of transparency, implementing even the best security concepts can be a "nightmare," as one security executive remarked.

Exhibit 3

Most enterprises do not fully entrust software-as-a-service providers with hosting and managing encryption keys and so use different control methods.

Preferences for hosting and managing encryption keys, by level of estimated IT spending,[1] % of respondents (n = 44)



[1] All IT-spending estimates rely on information from "IT key metrics data 2019: Executive summary," Gartner, December 17, 2018, gartner.com.
[2] Software as a service.
Source: McKinsey Customer Perspectives on SaaS survey and interviews with more than 60 industry leaders

Many security teams seek to integrate data on SaaS usage with external-threat intelligence and information from the rest of their technology environment to determine the actions they must take to protect their company. To accomplish this, the security teams need SaaS providers to offer application programming interfaces (APIs), which will allow them to pull data into their security operations centers (SOCs) and security-incident and event-management platforms (SIEMs). As a health-services CISO explained, "On-premises security controls are getting extended into the cloud. Only a few SaaS providers allow us to pull logs to go into our SIEM." A banking CISO said, "I want to integrate with SOC/SIEM. I want something flexible enough to work with hardened SIEM tools, and something capable of integrating as well." In other words, CISOs want their vendors to make it easier to use APIs for integration. They also want timely service provision as well as accurate security information from their SaaS providers included in service-level agreements (SLAs).

Incident response

Every company can be breached. Therefore, security teams must implement tools and practices for managing, mitigating, and resolving incidents. Naturally, security monitoring plays a significant role in this, as greater transparency enables better incident response.

Most organizations focus on SOC and SIEM integration. The more sophisticated security organizations we spoke with have dramatically broadened their incident-response requirements to include joint simulations, joint forensic activity, and intelligence sharing. One company even secured the right from one provider to send personnel to the provider's SOC in the event of a major breach.

Broader security concerns and pain points

CISOs also stated broader concerns with SaaS vendors' security capabilities. These include a lack of readiness of many SaaS offerings for integration with the company's larger security environment, as well as insufficient transparency on whether SaaS products meet local data-privacy requirements. A further concern surrounds the experience of SaaS sales forces, which CISOs say can be ill informed and sometimes even outwardly deceptive about security-related issues.

Integration is challenging

Nearly two-thirds of companies express frustration with the process of integrating SaaS products with the rest of their security environments. The trouble spots cited are as follows:

- Lack of preexisting connectors to commonly used IAM and SIEM platforms
- Insufficient functionality of APIs for obtaining the information required, especially log visibility at the platform level
- Poor API documentation, confusing API-usage semantics, and a shortage of relevant code samples
- Differently designed APIs for products from the same vendor
- Lack of trained vendor personnel to assist in using APIs.

CISOs complained of APIs that are not delivered, integration that is not achieved, even when the road map is followed, missing documentation, a lack of active support, and no vendor response when a problem develops. A biotech CISO emphasized "the lack of security monitoring: [SaaS vendors] forget about the confidentiality and integrity aspects of the monitoring."

Limited focus on data privacy

As major data breaches proliferate and regulatory attention mounts, data privacy is becoming an issue in the decision-making process for SaaS contracting and implementation. Security teams, meanwhile, find vendors scrambling to provide adequate clarity on the data-privacy protections in their offerings. One medical-products CISO pointed out that SaaS providers struggled to fulfill data-residency requirements – identifying the countries where the data are stored. Companies need to know the residency to meet local data regulations.

CISOs often cannot tell whether SaaS products properly meet new data-privacy mandates, including the European Union's General Data Protection Regulation (GDPR), Brazil's General Data Protection Law, and the California Consumer Privacy Act. Companies need to know this information to configure critical features, like encryption, data purging, and data logging, as they ensure compliance.

Respondents say that the claims SaaS providers make about product compliance are often overstated, so they don't necessarily trust them. A technology company's CISO said, "For things like GDPR, everyone is trying to figure it out; if anyone claims that they are mature in their process around GDPR, I would question this. I would prefer a sense of openness [and] honesty around what SaaS providers are doing and why they believe they are compliant."

Uninformative sales interactions

Security executives assert that their interactions with SaaS-provider teams on security issues are difficult and frustrating. They say that sales reps make security claims that don't appear to be backed up by fact, and that vendors don't have security experts they can talk to. Such experts, who would know the technical specifications of the offerings, are needed to help companies decide how to configure SaaS offerings in a secure way. More than 70 percent of respondents said that uninformed or misleading claims about security capabilities were a cause of dissatisfaction. Reportedly, some sales representatives even misrepresent certifications or customer references. One manufacturing company's CISO said, "I am sick of receiving glossy marketing materials, which are essentially snake oil when it comes to security features . . . many, many vendors will claim their security features are better than

[what] a very simple assessment will reveal." Another pointed out examples where simply checking a reference proved that the referenced company had not used security features in the way the sales team had described.

Implications on software as a service purchasing and contracting

SaaS vendors' shortcomings in security capabilities are shaping the ways enterprise customers contract for and use SaaS products. Negotiations about security terms and conditions (T&C) can add weeks or months to contracting processes. Survey respondents said the most challenging issues debated included financial liability for breach events, required cyber-insurance policies, and preferred location for legal proceedings.

Security issues often disqualify providers from consideration. For those that are considered, security remains a major concern; a few of our respondents told us that they had reverted to a provider's on-premises solution because they could not become comfortable with the security provisions of the SaaS offering. When deploying SaaS offerings, security executives cited the cost and complexity of the compensating controls they had to put in place to manage the accompanying risk. Many decide to invest in specialized third-party tools to manage encryption keys, ensure compliance with corporate policies, analyze vulnerabilities, enhance encryption, or track data usage for SaaS offerings. CISOs also say that they must expend scarce talent and resources in configuring and managing security offerings to meet their standards.

In a few reported cases, large companies called off planned migrations from an on-premises platform to an SaaS offering for security reasons. In one case, the vendor failed to meet commitments to make the APIs mature for IAM and SIEM integration. After the company had devoted significant resources to use the required APIs, it gave up and reverted to the existing version of the application in order to ensure required performance. In another example, new charges for security-related features were significant enough to sour the business case for adoption of a SaaS offering, causing the company to continue using the on-premises version.

Actions software-as-a-service providers can take to meet the security requirements of their enterprise customers

For all the value that SaaS promises, security concerns limit enterprise customers seeking to make the transition from on-premises solutions to SaaSbased ones. Fortunately, providers can take the following steps to remove barriers to SaaS adoption.

1. Build agile security capabilities

Every company surveyed expected its SaaS providers to have a robust solution in place, including a secure development life cycle and a secure stack for hosting its application in production. However, changes in software-delivery models have disrupted existing security practices and architectures. As established software vendors adopt agile development methods to improve time to market, earlier practices supporting a waterfall development process – sometimes put in place over decades – are becoming increasingly irrelevant. Since software companies provide their applications via their cloud but also host them on infrastructure provided by hyperscale cloud companies, years and decades of experience designing secure on-premise infrastructure stacks also become less relevant. Finally, the security organization can no longer "inspect for security," since this delays the process.

Security issues often disqualify providers from consideration.

SaaS providers must take a number of steps to build agile security capabilities. They must design and build security into their agile development processes. This includes automating security into the development tool chain, placing security champions on scrum teams, and training every developer on secure coding. They must furthermore build an infrastructure-operating model with a clear understanding of security ownership, determining what their cloud-infrastructure provider for security will do and what they must do themselves. A secure system configuration in the cloud will be especially critical here. Finally, underpinning all this, SaaS providers must build an agile security organization, one that enables the business by providing automated security services, rather than slowing it down with inspections and rework.

2. Adopt a multilevel model for addressing security-related customer inquiries

When asked about the characteristics of best-in-class SaaS vendors on security, 70 percent of cyber professionals cited transparency on security capabilities. They said that in selling, vendors can distinguish themselves by giving informed, straightforward responses regarding security capabilities and aftersales onboarding. They also said that vendors should provide transparency regarding updates and expected implications for customer systems. Software vendors can meet these expectations with a multilevel model for addressing security-related customer inquiries.

Level 1. Partner with third-party security assessment vendors to make data about security capabilities easily available at a low cost. Some third-party platforms capture more than 1,200 data points about each vendor's security capabilities. SaaS providers have no reason to refrain from sharing this information with potential customers.

Level 2. Train the sales force in the basic security features of the offerings and ensure that they respond to security inquiries accurately and intelligently. In addition, vendors need to provide incentives to sales people that encourage them to ask for expert help rather than provide incorrect or incomplete information.

Level 3. Create a specialized team to respond to sales-force inquiries, supported by a robust knowledge base to help answer more complicated questions. Given the importance of API-based integration, this group should act as a developer-support function in many respects. It should also invest in developing code samples and other artifacts that will make it easier for the customer's security teams to implement the vendor's products.

Level 4. Provide a clear escalation path to security engineers who can answer the most complicated questions about IAM, telemetry, key management, and other issues.

Level 5. Prepare for customer T&C requests. Customers will ask about the assumption of liability, preferred legal venues, and other issues. Vendors need to develop protocols for the circumstances under which they will accept requests, such as which requests will be accepted and from whom. Just as enterprise customers seek to assign prices to security risk, vendors may want to assign costs to special T&C requests. Even if they cannot pass that cost along to the customer, this type of accounting tool can provide an indication of whether a deal is worth making.

3. Aggressively facilitate integrations

The day of the stand-alone, monolithic application ended years ago, for security features as well as for the enterprise-technology environment. SaaS vendors should thus make it easier to integrate their offerings with the rest of their customers' security environments. This requires several actions.

Build a comprehensive set of connectors to relevant security tools. Major SaaS providers need to have pre-wired integration capabilities for every major enterprise IAM platform, cloud IAM platform, privileged-access-management platform (PAM), and SIEM platform. So equipped, providers will enable customers to implement their products more quickly, less expensively, and with greater confidence that they are not introducing new security vulnerabilities.

Invest in building better APIs. Too often, SaaS vendors pay little attention to security APIs. Instead, they should create a consistent security-API model across the products they offer. They should work with customers' security teams to provide the granular capabilities required in the areas of encryption, key management, and telemetry. They should deploy simple, easy-to-understand API semantics backed up by documentation.

Enhance security-related customer-success teams. Nearly two-thirds of security executives said that leading vendors were distinguished by the superior technical expertise of their support organizations. This means that vendors should enhance the security skills of the teams that help customers implement their products. In addition to improving customer outcomes, enhanced customer support could lead to more sales.

4. Help customers address data privacy
With expanding market and regulatory demands for data privacy, CISOs believe that SaaS vendors have not demonstrated sufficient leadership in this area. They need these vendors to research thoroughly the regulatory expectations in the markets they participate in and identify the specific actions required to comply. They need vendors to invest in the encryption, key-management, logging, data-tracking, and data-purging capabilities necessary for compliance. They should also guide CISOs on how to implement their products to minimize regulatory risk.

Over time, SaaS will largely replace traditional on-premises COTS applications, with enterprises benefiting from faster innovation, reduced complexity, lower operating costs, and massively reduced management spending on obsolete technologies. However, SaaS disrupts the traditional relationship between vendors and customers on security. With the vendor taking on much more security responsibility than before, the security team is put right in the middle of SaaS-adoption decisions. Moreover, companies cannot accept SaaS products as security "black boxes." As we have emphasized, they must be able to determine how to integrate them into the rest of their security environments.

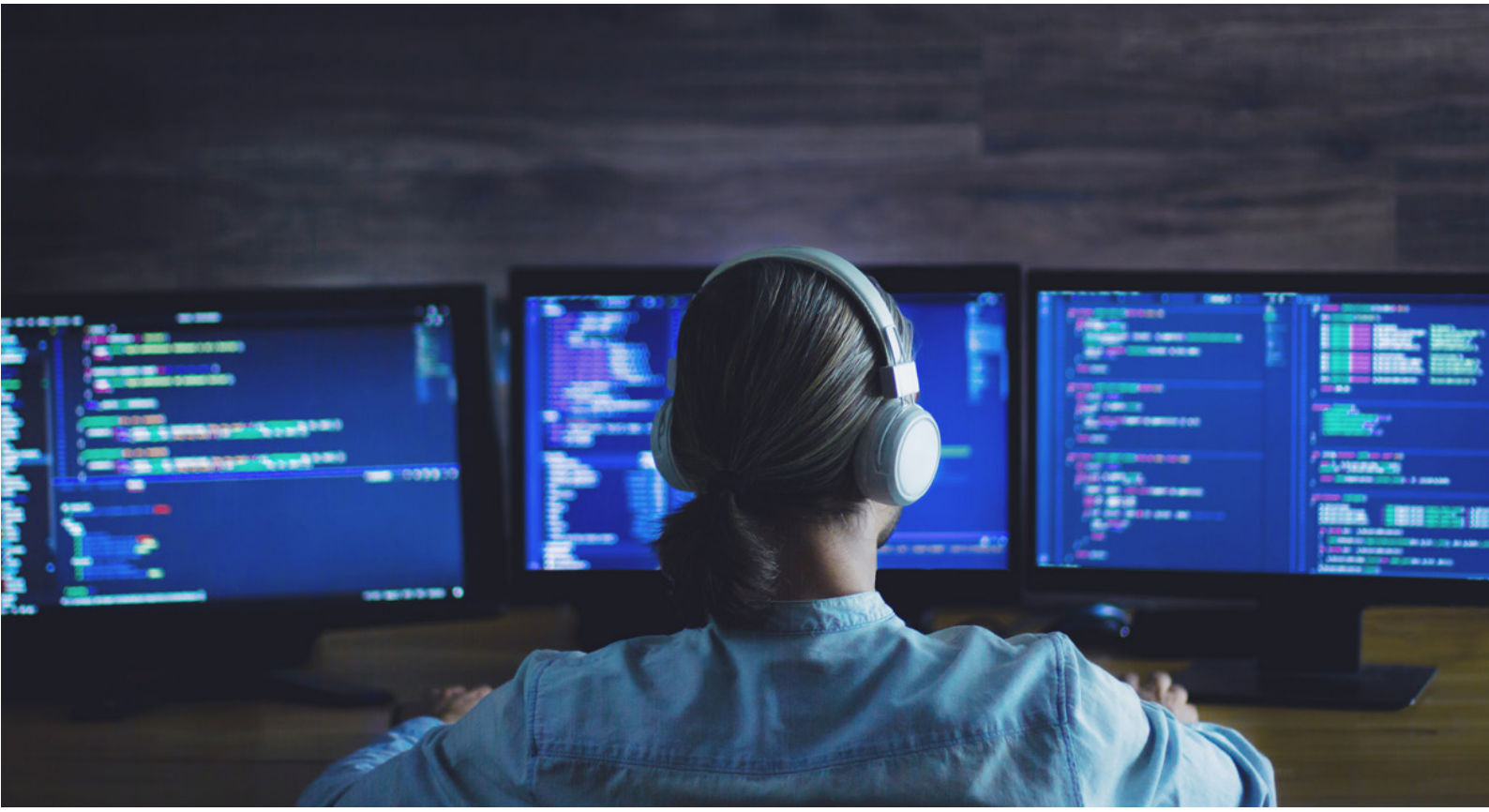
Our survey indicates that many SaaS vendors have yet to understand this new reality. They do not communicate well with customers on security; their products are hard to integrate with the rest of the customers' security environments; and they have not taken the lead in helping customers comply with data-privacy expectations. Security issues are causing companies to eliminate certain vendors from consideration, extending procurement processes by weeks and months, and adding significant cost and complexity to SaaS deployments. By actively addressing these issues, providers will speed the ongoing migration from traditional on-premises applications to SaaS.

Rich Cracknell is a manager of solution delivery in McKinsey's Silicon Valley office; **James Kaplan** is a partner in the New York office, where **Celina Stewart** is a cyber solutions senior analyst; and **Wolf Richter** is a partner in the Berlin office, where **Lucy Shenton** is a cyber solutions specialist.

Agile, reliable, secure, compliant IT: Fulfilling the promise of DevSecOps

By integrating security into DevOps, companies can step up the speed and frequency of software releases without compromising controls or increasing risk.

by Santiago Comella-Dorda, James Kaplan, Ling Lau, and Nick McNamara



As digital technologies transform industry after industry, businesses are increasingly adopting modern software-engineering practices pioneered by tech companies. Agile, DevOps, and other methods enable organizations to test, refine, and release new products and functionality more rapidly and frequently than ever before. However, the speed and frequency of releases can come into conflict with established methods of handling security and compliance. How can organizations resolve this tension?

We think the answer lies in DevSecOps, a method for integrating security into agile processes and DevOps efforts across the whole product life cycle. Properly implemented, DevSecOps (literally, development, Ssecurity, operations) offers enormous advantages.

Companies can increase the frequency of software releases from quarterly to weekly, or even daily, without compromising their risk posture. They can cut mean time to remediate vulnerabilities from weeks or months to hours as well as eliminate delays, cost overruns, product defects, and vulnerabilities. Last, but not least, getting security and compliance right from the outset is imperative as companies' growing dependence on digital technologies makes them more vulnerable to cyberattack, especially in the wake of the uncertainty and confusion wrought by the coronavirus pandemic.[1]

In our experience, the companies that are most successful at extracting the full value from DevSecOps commit to managing technology differently. They have an integrated operating model made up of teams of people – including those from security and compliance – with the full range of necessary capabilities, make practical use of automation, develop secure modular services that are easy to use, and conceive of and build digital products that are secure by design.

What is DevSecOps?

Pioneered by digital-native companies, DevSecOps is based on the principle of integrating development, security, infrastructure, and operations at every stage in a product's life cycle, from planning and design to ongoing use and support (exhibit). This enables engineers to tackle security and reliability issues more quickly and effectively, making organizations more agile and their digital products and services more secure and reliable. Security, reliability, and compliance considerations are built into every agile sprint rather than being handled separately or left until the end of the development process.

Adopting a DevSecOps approach has implications for each stage of the product life cycle:

— **Planning.** From the inception of a new product, teams are aware of their security and reliability responsibilities and trained to handle them. For significant efforts, teams start by quickly modeling threats and risks and then identifying and prioritizing backlog[2] items needed to make the product secure, reliable, and compliant. Where possible, teams take advantage of existing architectural designs that have been developed in collaboration with security and reliability experts, thereby ensuring that best practices are observed, as well as speeding up planning and design.

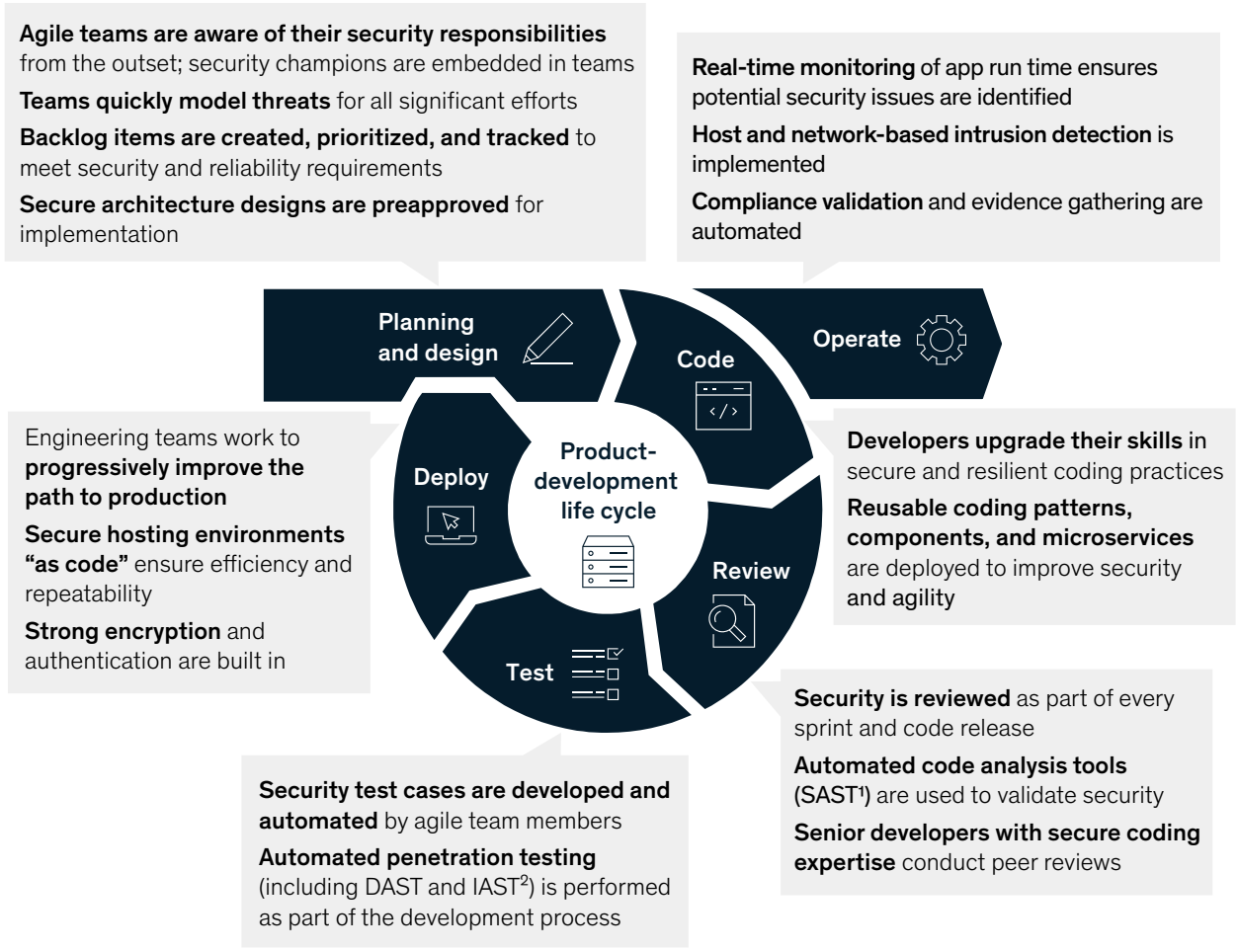
— **Coding.** To improve code quality, developers constantly develop and update their knowledge of secure and resilient coding practices. They take full advantage of reusable coding patterns, components, and microservices to quickly build the functionality and services needed to meet common security and resiliency requirements for encryption, authentication, availability, and observability.

[1] See Jim Boehm, James Kaplan, and Nathan Sportsman, "Cybersecurity's dual mission during the coronavirus crisis," March 2020, McKinsey.com.

[2] A backlog is a prioritized list of the features that an agile product team is planning to build and work on.

Exhibit

Security is integrated into every step in the product-development life cycle.



[1] Static application security testing.
[2] Dynamic application security testing and interactive application security testing.

— **Reviewing.** Instead of having a specialist group scrutinize a product for security vulnerabilities and resiliency issues once it emerges from months of development, teams review code as often as every two weeks as part of regular agile sprints, using both automated and manual checks. After automated code-analysis tools such as SonarQube and Fortify have looked for known vulnerabilities and issues, senior developers conduct peer reviews to discuss the results and ensure the software meets appropriate standards.

— **Testing.** Engineers create automated security tests to be run alongside automated functional and performance tests. This not only ensures that testing is consistent and efficient but also makes security requirements explicit, so that developers don't waste time puzzling over how to satisfy ill-defined policies laid down by separate groups. Common security tests, such as penetration tests that look for security holes in systems, are conducted automatically as part of every sprint and release cycle.

— **Deployment.** Code is delivered to production hosting environments, not through manual processes itemized in checklists, but via well-engineered automated processes that ensure the right software is built and that it is deployed securely and reliably. In addition, best-practice companies have secure production hosting environments that can be rapidly invoked through application programming interfaces (APIs), eliminating wait times and reducing risk.

— **Operations.** Once software is in production, automated processes – including real-time monitoring, host- and network-intrusion detection, and compliance validation, and evidence attestation – are used to increase efficiency and detect vulnerabilities. If defects or vulnerabilities are discovered, resolutions are identified, prioritized, and tracked to make sure product reliability and security are constantly improved.

Adopting DevSecOps principles

Capturing the potential of DevSecOps isn't easy. It relies on tight collaboration both within IT and across IT, security, compliance, and risk. To get it right, companies need to make four shifts in the way they manage technology: create a more integrated operating model, build secure "consumable" services, automate development and release processes, and evolve product architectures.

To illustrate what these shifts look like in practice, we'll draw on examples from two organizations that have recently adopted DevSecOps principles: a global software-and-services company and a large financial-services provider. The software-and-services company was already using agile methods to develop digital products and manage infrastructure, but it was striving to improve the resiliency of its products while making its internal processes more efficient. By contrast, the financial-services firm still relied on traditional waterfall methods to deliver its projects, and it saw DevSecOps as a way to improve performance, accelerate software releases, and streamline controls without increasing risk.

Organization and talent: Integrated cross-functional teams

When organizations struggle with the tensions between being agile and maintaining security, reliability, and compliance, it's often because the skills and accountabilities for developing, operating, and securing products and validating compliance are split between different groups. The answer is to break down these silos by setting up integrated agile teams charged with solving all the requirements of the products in their scope, regardless of any functional, security, reliability, or compliance issues they may pose. These teams should be staffed not with specialists but with well-rounded "full-stack" engineers who can work across disciplines and pick up new skills quickly. Every team member must be responsible for the security and reliability of the code they create, whether it's for customer-facing products or internal shared services.

The software-and-services company mentioned earlier reconfigured its product-development teams to own their code bases from end to end instead of relying on separate teams to address maintenance and defects. The company also set up site reliability engineering (SRE) teams to help improve the way products were developed and operated. The two teams worked closely together, shared objectives and key results (OKRs), and took part in joint agile events to stay aligned on

how to improve the security and reliability of the company's products.

The financial-services firm took a slightly different approach, embedding SREs in product-development teams instead of having them in a separate team. But similar to the software-and-services company, it introduced security and reliability OKRs for those product teams as well as common service metrics to drive alignment and accountability.

Consumable services: Developer-owned operations

In the past, the accountability for a digital product's functionality, operations, reliability, security, and compliance was split. A development team created an application, an infrastructure team operated it, and a maintenance team took care of reliability. With a DevSecOps approach, on the other hand, a single team is given as much accountability and ownership as possible for all aspects of a product.

In this approach, central enablement teams build shared consumable services for development, infrastructure, and security. They equip these services with guardrails and transparency so that subsequent product developers can use them safely, securely, and efficiently in their operations. Central checks and validations are still performed to ensure that correct procedures and best practices are implemented, but the goal is to make teams accountable for the products they own. This involves providing them with the tools they need to meet their responsibilities – tools that are convenient to use and designed to ensure that the easiest path for developers is also the most secure and reliable route.

Building these consumable services takes time, so companies need to prioritize those with the greatest impact and assign agile teams to build and own them. The software-and-services company decided to prioritize two key services: life-cycle management for its on-premise hosting environments (including provisioning, patching, and so on) and continuous integration and continuous delivery (CICD) pipelines for getting code safely and securely to production. Thanks to these efforts, it managed to cut setup times for hosting environments from three months to 15 minutes, as well as automating deployments that previously required eight hours of manual release work.

Similarly, the financial-services firm focused on creating a secure CICD pipeline, which had to be able to handle the high level of controls needed to satisfy regulatory requirements. Implementing the pipeline cut software release times by half. By introducing mechanisms such as automated security test cases, the firm also streamlined controls by 50 to 80 percent without increasing risk.

Development and release: Automated pipelines with built-in security controls

The traditional path to production for software code was lengthy and prone to error. Developers wrote code, and then quality-assurance engineers tested it – usually manually and in settings that bore little resemblance to the environment in which it would eventually be used. Shepherding code through these processes involved many manual steps. Most testing took the form of basic functional and regression tests. Some defects and vulnerabilities slipped through and were caught only after the software was released.

Over the past decade, the DevOps movement has striven to make the path to production more efficient and more effective at catching defects as early as possible, when they are cheaper to address. Leading companies have adopted CICD pipelines to automate workflows and enable best engineering practices to be followed in the writing, reviewing, testing, and deployment of code. In addition to this, DevSecOps companies need to go further by integrating an extra layer of testing into their CICD pipelines to analyze code for potential security issues, run security test cases, and conduct light penetration tests.

To improve their development and release processes, the software-and-services company and the financial-services firm adopted similar approaches. In designing and implementing automated CICD pipelines for deployments to both the cloud and on-premise environments, they took care to involve their security and compliance specialists to ensure that controls would not be compromised in any way. They also used OKRs and metrics dashboards to encourage adoption of the pipelines and increase the levels of automated test coverage.

Product architecture: Secure by design
Traditionally, applications have been built from scratch, with all capabilities locked inside a single code package and security not usually tackled until late in the development process. Adding a new feature required extensive testing across the whole system, making upgrades slow and complex to execute. Since applications were seldom designed to scale in a linear fashion as additional load was put on the system, maintaining reliability was often a challenge.

With DevSecOps, by contrast, digital products are conceived and built from the ground up to be secure by design. Security requirements and best practices are factored into all elements of a product, from the code itself to the infrastructure it runs on. Engineers take advantage of existing components built by enablement or shared-service teams, such as container templates and standardized monitoring APIs. They also draw on open-source libraries released by web-scale industry leaders – such as Netflix's Hystrix library for improving fault tolerance – to incorporate best-practice resiliency patterns. Following a "systems of systems" approach, they integrate pre-engineered microservices via loosely coupled interfaces based on well-maintained APIs. All of this improves agility as well as security. Instead of struggling to build their own code, waiting for reviews by security and compliance teams, and iterating until they pass audit checks, product teams reuse code built with expert input and oversight.

Both the software-and-services company and the financial-services firm had legacy systems they needed to support, and both pursued an evolutionary approach to modernizing their application landscape. They used their new processes to build new "greenfield" digital products and incrementally adapted older products to support DevSecOps best practices, including the use of microservices, unit tests, security test cases, static code analyses, and resiliency patterns.

Common pitfalls to avoid

The best path for an organization to take in adopting DevSecOps depends on many factors, ranging from its size to its familiarity with agile and DevOps methods. But regardless of their starting point, all organizations should take care, as they set out on their transformation journey, to avoid a few common pitfalls.

Pitfall 1: Focusing on tooling alone
Companies should beware of assuming they can realize the potential of DevSecOps merely by implementing tools such as a CICD orchestration system or a static code analysis tool. To capture the full benefit, they need to make the four shifts described earlier. Without that broader transformation, new tooling is unlikely to be used effectively or consistently across the organization.

Pitfall 2: Failing to secure leadership buy-in
If teams are to change their way of working, the leaders of the technology organization must play an active part in steering the transformation. In turn, development leaders must model and reinforce target behaviors and equip their teams to deliver on their new objectives. Finally, security and compliance leaders need to be fully involved to ensure that greater agility doesn't come at the cost of higher risk. To help gain leadership buy-in, successful companies develop a baseline understanding of their agile and DevSecOps maturity and communicate the business case for improvement. Adding key stakeholders to the team leading the transformation is another way to make leaders feel accountable for ensuring its success.

Pitfall 3: Focusing only on greenfield development

Though DevSecOps principles are easiest to adopt in new development efforts, applying them more broadly can deliver significant value. For instance, secure CICD pipelines can support larger, more monolithic applications, which can in turn be gradually broken down into loosely coupled microservices. Organizations should constantly explore where they can best deploy DevSecOps to increase agility, security, and reliability.

Pitfall 4: Taking too long to deliver value

In successful DevSecOps transformations, value is captured from an early stage. Leaders quickly identify any changes that need to be made to product teams and decide which consumable services they need to launch. When rolling out changes, they prioritize products and services that will drive the highest impact or reduce the most risk. By identifying quick wins in the first two or three months, they showcase the value of the transformation and gain support from engineers and the broader organization.

Pitfall 5: Overlooking capability building and culture

Engineers operating in traditional technology organizations are likely to find adopting DevSecOps a challenge. As well as developing new capabilities, they need to make a major cultural shift by learning to take ownership for their product's security, reliability, and compliance, no matter which team they are on. At the same time, they need to acquire knowledge and skills in creating and operating resilient products to meet their new objectives. Culture and capability building can reinforce one another: when engineers know that the teams they work with expect them to have particular skills, they will be more motivated to develop them.

In addition to avoiding these pitfalls, best-practice organizations ensure they pursue a structured approach to change management. They use dedicated change-management and capability-building workstreams as part of the transformation ,and roll teams out in waves that allow enough time for training, team alignment, and planning activities, such as agile sprint 0s.[3]

Once a niche practice confined to Silicon Valley start-ups, DevSecOps has matured to become a priority for traditional enterprises, too. Adopting the principles outlined in this article will help companies not only acquire the agility to stay current but also strengthen their security to withstand exposure to cyberattacks in the future.

Santiago Comella-Dorda is a partner in McKinsey's Boston office, **James Kaplan** is a partner in the New York office, **Ling Lau** is a partner in the New Jersey office, and **Nick McNamara** is an associate partner in the Chicago office.

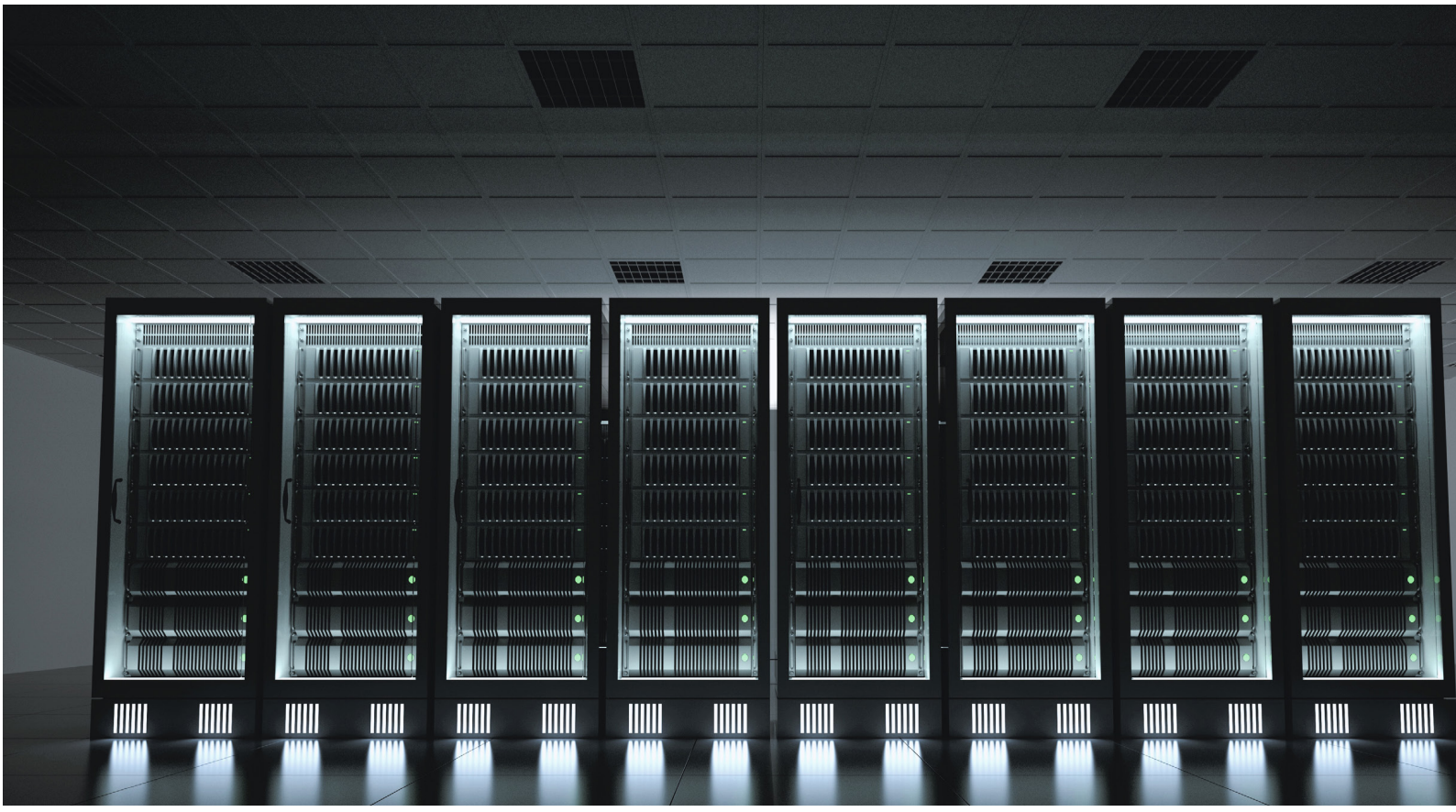
The authors wish to thank Nagendra Bommadevara, Daniel Brosseau, Alharith Hussin, Steve Jansen, Jesus Mathus Garza, Mark Mintz, Thomas Newton, Jan Shelly Brown, Marc Sorel, Kevin Telford, and Charles Wisniewski for their contributions to this article.

[3] Agile sprint 0s are short efforts before a team starts working together, used to create a common vision, align on team norms, and create a product backlog for what they plan to build.

Cybersecurity's dual mission during the coronavirus crisis

Chief information-security officers must balance two priorities to respond to the pandemic: protecting against new cyberthreats and maintaining business continuity. Four strategic principles can help.

by Jim Boehm, James Kaplan, and Nathan Sportsman



The extraordinary efforts of many organizations to protect workers and serve customers during the COVID-19 pandemic have also increased their exposure to cyberthreats. Large-scale adoption of work-from-home technologies, heightened activity on customer-facing networks, and greater use of online services all present fresh openings, which cyberattackers have been quick to exploit.

The overarching challenge for chief information-security officers (CISOs) and cybersecurity teams will be protecting their institutions while enabling operations to go on without interruption. For example, cybersecurity teams at companies that provide web-based services to consumers must adjust their security programs to match scaled-up operations while securing a massive shift to work-from-home tools. At the same time, CISOs must make it possible for security-team members to look after themselves and their families during a health crisis.

Addressing these diverse and sometimes competing needs at once won't be easy. But recent conversations with cybersecurity leaders suggest that some governing principles are helping them meet the challenge. This article recommends four such principles: focusing on critical operating needs, testing plans for managing security and technology risks, monitoring for new cyberthreats, and balancing protection with business continuity.

How the response to COVID-19 has increased cyberrisk

As organizations and people have curtailed travel and in-person gatherings, they have shifted a great deal of activity into the digital realm. Workers and students are staying home, using videoconferencing services, collaboration platforms, and other digital tools to do business and schoolwork. In their free time, they are going online to shop, read, chat, play, and stream. All these behaviors put immense stress on cybersecurity controls and operations. Several major vulnerabilities stand out:

— **Working from home has opened multiple vectors for cyberattacks.** A broad shift toward work-from-home arrangements has amplified long-standing cybersecurity challenges: unsecured data transmissions by people who aren't using VPN software, weak enforcement of risk-mitigating behaviors (the "human firewall"), and physical and psychological stressors that compel employees to bypass controls for the sake of getting things done. The more that homebound employees struggle to access data and systems, the more they will attempt to use risky work-arounds (exhibit). Cybersecurity teams will need to secure work-from-home systems and test and scale VPNs and incident-response tools. In addition, they may wish to revisit access-management policies so that employees can connect to critical infrastructure via personal devices or open, internet-facing channels.

— **Social-engineering ploys are on the rise.** In social-engineering gambits, attackers attempt to gain information, money, or access to protected systems by tricking legitimate users. Companies have seen more malware-laced email-phishing campaigns that borrow the identities of health, aid, and other benevolent organizations. Scammers posing as corporate help-desk teams ask workers for their security credentials using text phishing ("smishing") and voice phishing ("vishing"). Email fraudsters have tried to get executives to move money to fund vendors, operations, and virus-related-response activities.

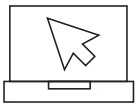
— **Cyberattackers are using websites with weak security to deliver malware.** With the creation of new domains and websites to spread information and resources to combat the coronavirus, attackers are exploiting the weak security controls on many of these sites to spread malware via drive-by downloads. A common approach hides readily available malware (such as AZORult) inside coronavirus heat maps or early-warning

Exhibit

Shifting to work-from-home arrangements can open multiple vectors for cyberattacks.

Changes in app-access rights

- Under existing policies, access to apps differs based on criticality and cyberrisk appetite (eg, data infiltration, data-protection loss), from less critical apps accessible from almost anywhere (eg, public network) to apps accessible through extranet, apps accessible only through VPN, and, ultimately, critical apps accessible only on site (eg, trading, treasury)
- Remote working can require organizations to widen access rights by enabling off-site access to some of the most critical apps, which can increase cyberrisk
- Some users might not have strong multifactor authentication, because their access rights are usually limited; change in access rights, combined with weak authentication, constitutes a further threat



Use of personal devices and tools

- Some employees may have been enabled to work from their own personal devices, but because these devices are not centrally controlled (for patching, network-access control, and endpoint data-protection systems), they can introduce cybersecurity vulnerabilities
- To get work done, many employees use consumer-grade tools, accounts, and devices and share data over nonsecure and noncontrolled channels

Lack of social control

- Click-through rates for phishing emails and success rates of fake call-center agents can increase if employees no longer maintain a "human protection shield" by asking coworkers about suspicious emails or calls

applications. In one instance, a threat actor targeted a public-sector entity by embedding malware in a pandemicrelated document and disguising it as an official communiqué from another part of the government. Once installed, such a malicious application steals a user's confidential data (for example, personal information, credit-card information, and bitcoin-wallet keys). Some malware applications launch ransomware attacks, which lock a user's system until they pay a certain amount of money to the attacker.

— **Public-sector organizations are experiencing acute pressure.** A large government entity in North America suffered from a distributed denial-of-service attack aimed at disrupting services and issuing misinformation to the public. A major hospital in Europe was hit with a cyberattack that forced it to suspend scheduled operations, shut down its IT network, and move acute-care patients to another facility. And a department of a local government had its website encrypted by ransomware, preventing officials from posting information for the public and keeping employees from accessing certain files.

As the COVID-19 outbreak progresses and alters the functioning of our socioeconomic systems, cyberattackers will continue their efforts to exploit our fears and our digital vulnerabilities. To remain vigilant and effective, CISOs will need new approaches.

Employees on the front line will play an especially important role in keeping the organization safe as normal on-premise security measures become less relevant.

How to address the challenge: Strategic practices for chief information-security officers

While many CISOs and other executives have drawn on their experiences with past crises to respond to the early stages of the COVID-19 outbreak, the pandemic's vast scale and unpredictable duration are highly unusual. There is no playbook that CISOs can open for guidance. Nevertheless, the CISOs and senior cybersecurity managers we have spoken to have found it especially helpful to follow four practices:

— **Focus.** Security- and technology-risk teams should focus on supporting only those technology and security features, capabilities, and service rollouts that are critical to operations. Examples of focus areas that may justify a surge in capacity over the coming weeks include maintaining security operations, mitigating risks of remote access to sensitive data and software-development environments, and implementing multifactor authentication to enable employees to work from home. Organizations should also reiterate to employees their safe remote-working protocols and their procedures for threat identification and escalation. Employees on the front line will play an especially important role in keeping the organization safe as normal on-premises security measures become less relevant.

— **Test.** If your organization has security- or technology-risk plans of any kind – such as plans for incident response, business continuity, disaster recovery, talent succession, and vendor succession – then test them right away. If your organization doesn't have adequate plans in place, create them and then test them. You must determine whether your organization's riskresponse approach is effective and efficient. Eliminating risk events is impossible, but you can reduce the exacerbated risk associated with a poor response.

— **Monitor.** Consider mustering all available resources to help with monitoring, which enables risk response and recovery to begin. Areas for stepped-up monitoring can include remote monitoring of collaboration tools, monitoring networks for new and novel strains of malware, and monitoring employees and endpoints to catch data-related incidents before they result in operational risk.

— **Balance.** Cybersecurity teams are likely to receive a flood of urgent requests for cybersecurity-policy exceptions that will allow teams elsewhere in the organization to get work done (for example, to approve the installation of new apps and allow the use of USB drives). While CISOs might be inclined to deny such requests for the sake of preventing undue risk, they must also bear in mind the importance of maintaining business continuity during a fluid and challenging time for their colleagues. To support continued operations, CISOs may need to tolerate slightly higher risk in the short term by granting waivers or temporarily relaxing some controls. An accommodating

approach will encourage colleagues to make intelligent risk trade-offs. That said, CISOs shouldn't allow these exceptions to weaken an organization's risk posture permanently. If CISOs grant waivers or relax controls, they should establish formal evaluation and review processes and implement time limits to force periodic reevaluation or limit the exceptions to particular user groups.

The COVID-19 crisis is a human challenge above all else. Everyone is juggling professional responsibilities with important personal ones. The coming weeks and months are likely to bring more uncertainty. By adhering to the practices we described – focus, test, monitor, and balance – CISOs can fulfill their responsibilities to uphold their institutions' security and maintain business continuity while also meeting their obligations to their teams.

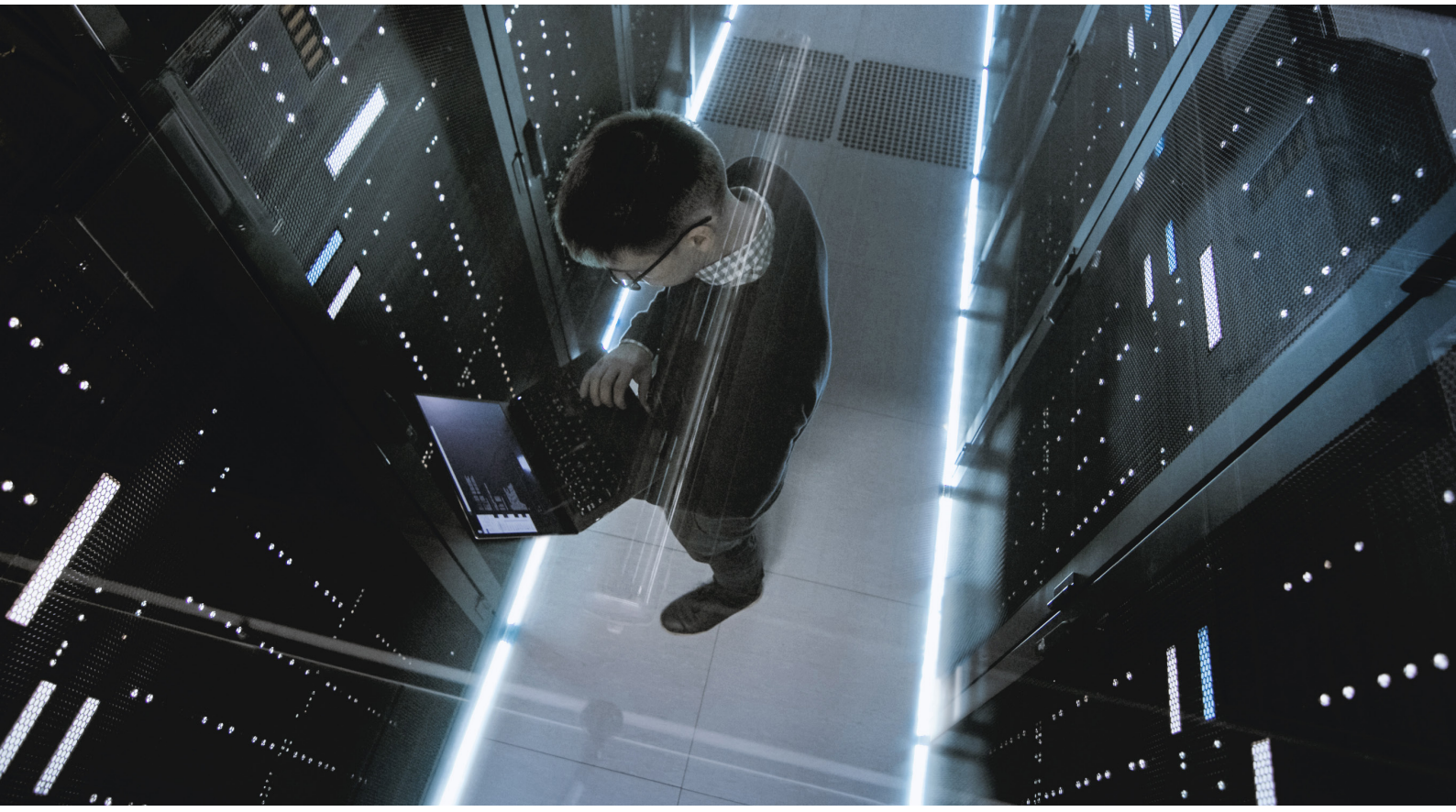
Jim Boehm is a partner in McKinsey's Washington, DC, office. **James Kaplan** is a partner in the New York office, and **Nathan Sportsman** is the founder and CEO of Praetorian.

McKinsey and Praetorian have entered into a strategic alliance to help clients solve complex cybersecurity challenges and promote innovation. As a part of this alliance, McKinsey is a minority investor in Praetorian.

Cybersecurity tactics for the coronavirus pandemic

The pandemic has made it harder for companies to maintain security and business continuity. But new tactics can help cybersecurity leaders to safeguard their organizations.

by Jim Boehm, James Kaplan, Marc Sorel, Nathan Sportsman, and Trevor Steen



The COVID-19 pandemic has presented chief information security officers (CISOs) and their teams with two immediate priorities. One is securing work-from-home arrangements on an unprecedented scale now that organizations have told employees to stop traveling and gathering, and government officials in many places have advised or ordered their people to stay home as much as possible. The other is maintaining the confidentiality, integrity, and availability of consumer-facing network traffic as volumes spike – partly as a result of the additional time people are spending at home.

Recent discussions with cybersecurity leaders suggest that certain actions are especially helpful to fulfill these two priorities. In this article, we set out the technology modifications, employeeengagement approaches, and process changes that cybersecurity leaders have found effective.

Securing work-from-home arrangements at scale

The rapid, widespread adoption of work-fromhome tools has put considerable strain on security teams, which must safeguard these tools without making it hard or impossible for employees to work. Conversations with CISOs in Asia, Europe, and North America about how they are securing these new work-at-home arrangements highlight the changes these executives are making in three areas: technology, people, and processes.

Technology: Make sure required controls are in place

As companies roll out the technologies that enable employees to work from home and maintain business continuity, cybersecurity teams can take these actions to mitigate cybersecurity risks:

— **Accelerate patching for critical systems.** Shortening patch cycles for systems, such as virtual private networks (VPNs), end-point protection, and cloud interfaces, that are essential for remote working will help companies eliminate vulnerabilities soon after their discovery. Patches that protect remote infrastructure deserve particular attention.

— **Scale up multifactor authentication.** Employees working remotely should be required to use multifactor authentication (MFA) to access networks and critical applications. Scaling up MFA can be challenging: the protection it will add calls for a surge in short-term capacity. Several practices make the rollout of MFA more manageable. One is to prioritize users who have elevated privileges (such as domain and sys admins, and application developers) and work with critical systems (for instance, money transfers). Targeting those users in pilot rollouts of modest scale will allow cybersecurity teams to learn from the experience and use that knowledge to shape more extensive implementation plans. Cybersecurity teams can also benefit from using MFA technologies, such as the application gateways offered by several cloud providers, that are already integrated with existing processes.

— **Install compensating controls for facility-based applications migrated to remote access.** Some applications, such as bank-teller interfaces and cell-center wikis, are available only to users working on-site at their organizations' facilities. To make such facility-based applications available to remote workers, companies must protect those apps with special controls. For example, companies might require employees to activate VPNs and use MFA to reach what would otherwise be facility-based assets while permitting them to use MFA alone when accessing other parts of the corporate environment.

— **Account for shadow IT.** At many companies, employees use so-called shadow IT systems, which they set up and administer without formal approval or support from the IT department. Extended work-from-home operations will expose such systems because business processes that depend on shadow IT in the office will break down once employees find themselves unable to access those resources. IT and security teams should be prepared to transition, support, and protect

business-critical shadow assets. They should also keep an eye out for new shadow-IT systems that employees use or create to ease working from home, to compensate for in-office capabilities they can't access, or to get around obstacles.

— **Quicken device virtualization.** Cloud-based virtualized desktop solutions can make it easier for staff to work from home because many of them can be implemented more quickly than on-premises solutions. Bear in mind that the new solutions will need strong authentication protocols – for example, a complex password, combined with a second authentication factor.

People: Help employees understand the risks

Even with stronger technology controls, employees working from home must still exercise good judgment to maintain information security. The added stress many people feel can make them more prone to social-engineering attacks. Some employees may notice that their behavior isn't monitored as it is in the office, and therefore choose to engage in practices that open them to other threats, such as visiting malicious websites that office networks block. Building a "human firewall" will help ensure that employees who work from home do their part to keep the enterprise secure.

— **Communicate creatively.** A high volume of crisis-related communications can easily drown out warnings of cybersecurity risks. Security teams will need to use a mix of approaches to get their messages across. These might include setting up two-way communication channels that let users post and review questions, report incidents in real time, and share best practices; posting announcements to pop-up or universal-lock screens; and encouraging the innovative use of existing communication tools that compensate for the loss of informal interactions in hallways, break rooms, and other office settings.

— **Focus on what to do rather than what not to do.** Telling employees not to use tools (such as consumer web services) they believe they need to do their jobs is counterproductive. Instead, security teams must explain the benefits, such as security and productivity, of using approved messaging, file-transfer, and document-management tools to do their jobs. To further encourage safe behavior, security teams can promote the use of approved devices – for example, by providing stipends to purchase approved hardware and software.

— **Increase awareness of social engineering.** COVID-19-themed phishing, vishing (voice phishing), and smishing (text phishing) campaigns have surged. Security teams must prepare employees to avoid being tricked. These teams should not only notify users that attackers will exploit their fear, stress, and uncertainty, but also consider shifting to crisis-specific testing themes for phishing, vishing, and smishing campaigns.

— **Identify and monitor high-risk user groups.** Some users, such as those working with personally identifiable information or other confidential data, pose more risk than others. High-risk users should be identified and monitored for behavior (such as unusual bandwidth patterns or bulk downloads of enterprise data) that can indicate security breaches.

Processes: Promote resilience

Few business processes are designed to support extensive work from home, so most lack the right embedded controls. For example, an employee who has never done high-risk remote work and hasn't set up a VPN might find it impossible to do so because of the in-person VPN-initiation requirements. In such cases, complementary security-control processes can mitigate risks. Such security processes include these:

— **Supporting secure remote-working tools.** Security and IT help desks should add capacity while exceptionally large numbers of employees are installing and setting up basic security tools, such as VPNs and MFA. It might be practical to deploy security-team members

Even with stronger technology controls, employees working from home must still exercise good judgment to maintain information security.

temporarily at call centers to provide added frontline support.

— **Testing and adjusting IR and BC/DR capabilities.** Even with increased traffic, validating remote communications and collaboration tools allows companies to support incident-response (IR), and business-continuity (BC)/disaster-recovery (DR) plans. But companies might have to adjust their plans to cover scenarios relevant to the current crisis. To find weak points in your plans, conduct a short IR or BC/DR tabletop exercise with no one in the office.

— **Securing physical documents.** In the office, employees often have ready access to digital document-sharing mechanisms, as well as shredders and secure disposal bins for printed materials. At home, where employees might lack the same resources, sensitive information can end up in the trash. Set norms for the retention and destruction of physical copies, even if that means waiting until the organization resumes business as usual.

— **Expand monitoring.** Widening the scope of organization-wide monitoring activities, particularly for data and end points, is important for two reasons. First, cyberattacks have proliferated. Second, basic boundary-protection mechanisms, such as proxies, web gateways, or network intrusion-detection systems (IDS) or intrusion-prevention systems (IPS), won't secure users working from home, off the enterprise network, and not connected to a VPN. Depending on the security stack, organizations that do not require the use of a VPN or require it only to access a limited set of resources may go largely unprotected. To expand monitoring, security teams should update security-information- and-event-management (SIEM) systems with new rule sets and discovered hashes for novel malware. They should also increase staffing in the security operations center (SOC) to help compensate for the loss of network-based security capabilities, such as end-point protections of noncompany assets. If network-based security capabilities are found to be degraded, teams should expand their IR and BC/DR plans accordingly.

— **Clarify incident-response protocols.** When cybersecurity incidents take place, SOC teams must know how to report them. Cybersecurity leaders should build redundancy options into response protocols so that responses don't stall if decision makers can't be reached or normal escalation pathways are interrupted because people are working from home.

— **Confirm the security of third parties.** Nearly every organization uses contractors and off-site vendors, and most integrate IT systems and share data with both contract and noncontract third parties, such as tax or law-enforcement authorities. When organizations assess which controls must be extended to employees to secure new work-from-home protocols, they should do the same for third-party users and connections, who are likely to

be managing similar shifts in their operations and security protocols. For example, ask providers whether they have conducted any remote IR or BC/DR tabletop drills and, if they have, ask them to share the results. Should any third parties fail to demonstrate adequate security controls and procedures, consider limiting or even suspending their connectivity until they remediate their weaknesses.

— **Sustain good procurement practices.** Fast-track procurement intended to close key security gaps related to work-from-home arrangements should follow standard duediligence processes. The need for certain security and IT tools may seem urgent, but poor vendor selection or hasty deployment could do more harm than good.

Supporting high levels of consumer-facing network traffic

Levels of online activity that challenge the confidentiality, integrity, and availability (CIA) of network traffic are accelerating. Whether your organization provides connectivity, serves consumers, or supports transactions, securing the CIA of network activity should be a top priority for any executive team that wants to protect consumers from cyberbreaches during this period of heightened vulnerability. Much as organizations are stepping up internal protections for enterprise networks, security teams in organizations that manage consumer-facing networks and the associated technologies will need to scale up their technological capabilities and amend processes quickly.

Technology: Ensure sufficient capacity

Companies that make it possible for employees to work from home must enable higher online networktraffic and transaction volumes by putting in place technical building blocks such as a web-application firewall, secure-sockets-layer (SSL) certification, network monitoring, anti-distributed denial of service, and fraud analytics. As web-facing traffic grows, organizations should take additional actions to minimize cyberrisks:

— *Enhance web-facing threat-intelligence monitoring.* To anticipate threats and take preventive measures, security teams must understand how heightened consumer traffic changes the threat environment for web-facing enterprise activities. For example, to find out if attackers are becoming more interested in an organization's web-facing technologies, organizations can conduct increased passive domain-name scans to test for new malicious signatures tailored to the enterprise domain or for the number of adversarial scans targeting the enterprise network, among other threats.

— **Improve capacity management.** Overextended web-facing technologies are harder to monitor and more susceptible to attacks. Security teams can monitor the performance of applications to identify suspected malware or low-value security agents or even recommend the removal of features (such as noncritical functions or graphics on customer portals) that hog network capacity.

Processes: Integrate and standardize security activities

Customers, employees, and vendors all play some part in maintaining the confidentiality, integrity, and availability of web-facing networks. Several steps can help organizations to ensure that the activities of these stakeholders are consistent and well integrated:

— **Integrate fraud-prevention capabilities with the SOC.** Organizations that support the execution of financial transactions should consider integrating their existing fraud analytics with SOC workflows to accelerate the inspection and remediation of fraudulent transactions.

— **Account for increased costs.** Many SOC tools and managed-security-service providers base charges for monitoring on usage – for example, the volume of log records analyzed. As usage increases with expanded network traffic, organizations with usage-based fee arrangements will need to account for any corresponding increase in costs.

— **Help consumers solve CIA problems themselves**. For media providers, enabling customers to access content without interruption is essential, but increased usage levels can jeopardize availability. Companies may wish to offer guides to show users how to mitigate access problems, particularly during periods of peak use.

Securing remote-working arrangements and sustaining the CIA of customer-facing networks are essential to ensure the continuity of operations during this disruptive time. The actions we describe in this article, while not comprehensive, have helped many organizations to overcome the security difficulties they face and maintain their standing with customers and other stakeholders.

Jim Boehm is a partner in McKinsey's Washington, DC, office. **James Kaplan** is a partner in the New York office, and **Marc Sorel** is a partner in the Boston office. **Nathan Sportsman** is the founder and CEO of Praetorian, where **Trevor Steen** is a senior security engineer.

The authors wish to thank Wolf Richter and Mahir Nayfeh for their contributions to this article.

McKinsey and Praetorian have entered into a strategic alliance to help clients solve complex cybersecurity challenges and secure innovation. As a part of this alliance, McKinsey is a minority investor in Praetorian.

Contacts

Asia

Aman Dhingra, Associate Partner
Aman_Dhingra@mckinsey.com

Juan Hincapie, Expert Associate Partner
Juan_Hincapie@mckinsey.com

Patrick Nagel, Expert Associate Partner
Patrick_Nagel@mckinsey.com

Europe

Vito Di Leo, Expert Associate Partner
Vito_Di_Leo@mckinsey.com

Peter Merrath, Senior Solution Leader and Associate Partner
Peter_Merrath@mckinsey.com

Thomas Poppensieker, Senior Partner
Thomas_Poppensieker@mckinsey.com

Wolf Richter, Partner
Wolf_Richter@mckinsey.com

Gundbert Scherf, Partner
Gundbert_Scherf@mckinsey.com

Latin America

Julen Baztarrica, Partner
Julen_Baztarrica@mckinsey.com

Cristian Berner, Partner
Christian_Berner@mckinsey.com

Elias Goraieb, Partner
Elias_Goraieb@mckinsey.com

Beltran Simo, Partner
Beltran_Simo@mckinsey.com

Middle East

Ayman Al Issa, Senior Expert
Ayman_Alissa@mckinsey.com

Mahir Nayfeh, Partner
Mahir_Nayfeh@mckinsey.com

North America

Bharath Aiyer, Expert Associate Partner
Bharath_Aiyer@mckinsey.com

Venky Anant, Partner
Venky_Anant@mckinsey.com

Tucker Bailey, Partner
Tucker_Bailey@mckinsey.com

Jim Boehm, Partner
Jim_Boehm@mckinsey.com

Kevin Buehler, Senior Partner
Kevin_Buehler@mckinsey.com

Rich Isenberg, Partner
Rich_Isenberg@mckinsey.com

Piotr Kaminski, Senior Partner
Piotr_Kaminski@mckinsey.com

James Kaplan, Partner
James_Kaplan@mcKinsey.com

Merlina Manocaran, Partner
Merlina_Manocaran@mckinsey.com

Marc Sorel, Partner
Marc_Sorel@mckinsey.com

David Ware, Partner
David_Ware@mckinsey.com

Digital McKinsey and Global Risk Practice
June 2020

Designed by Visual Media Europe

www.mckinsey.com