

Risk Practice

# Cybersecurity: Linchpin of the digital enterprise

As companies digitize businesses and automate operations, cyber risks 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.<sup>1</sup> 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.

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

---

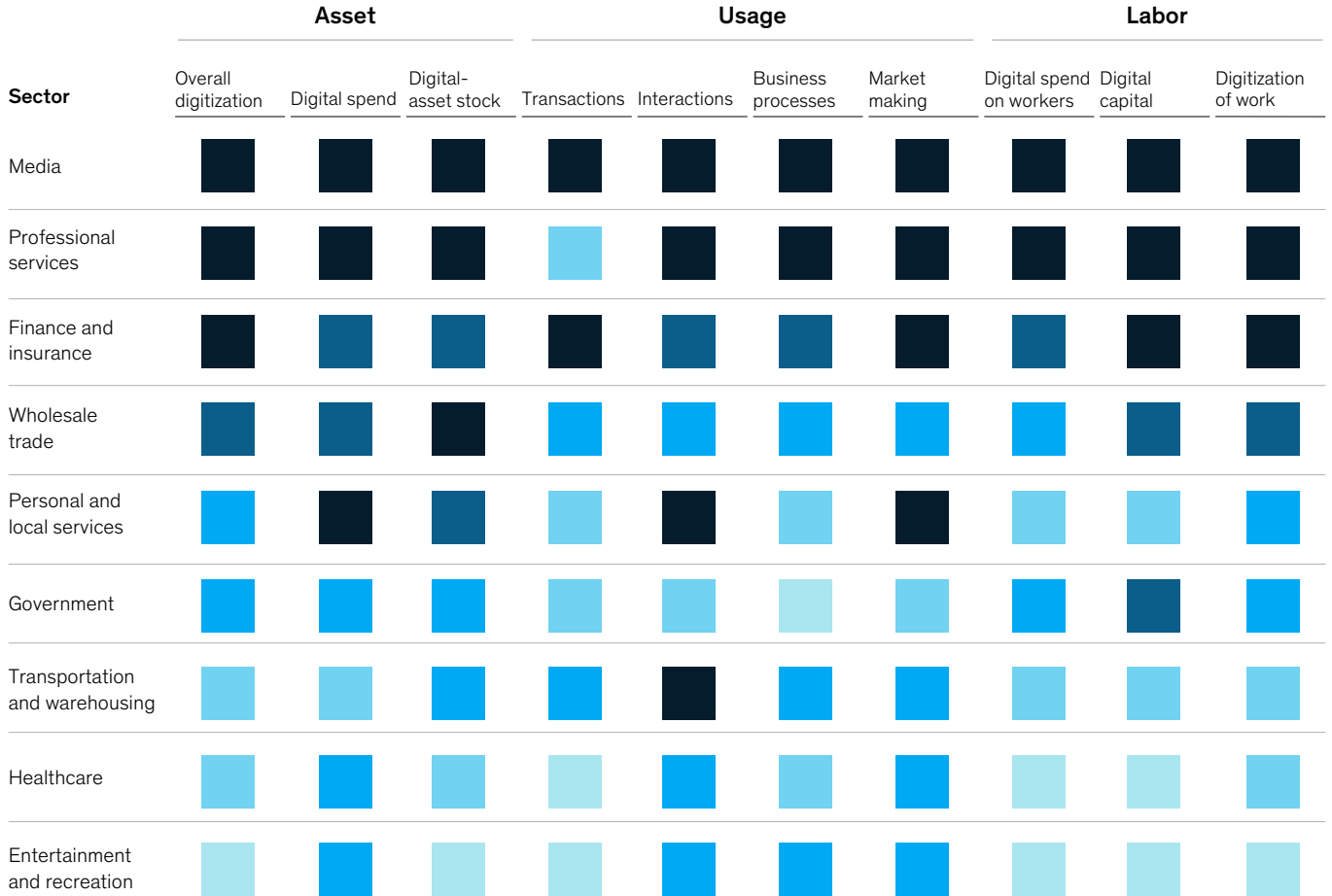
<sup>1</sup> An API is software that allows applications to communicate with each other, sharing information for a purpose.

Exhibit 1

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

**Digitization levels**

Low digitization High digitization



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

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 for the vulnerability scan required to promote

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).

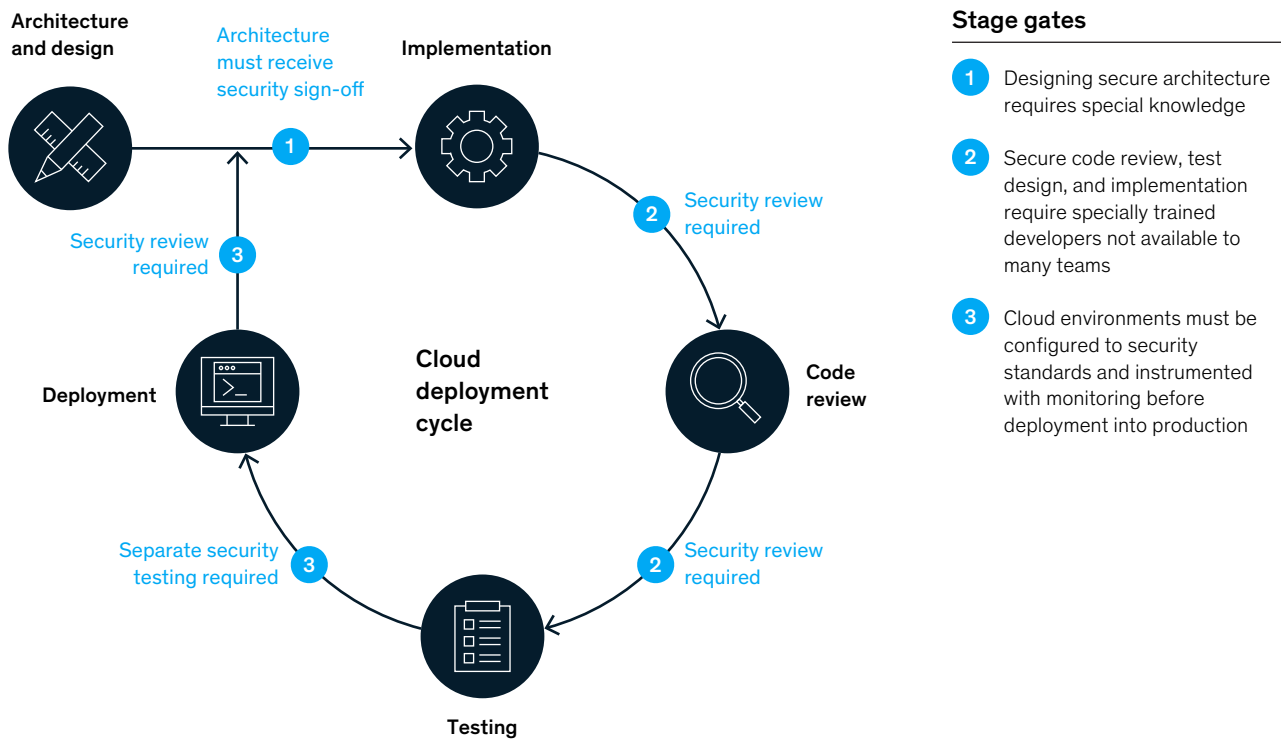
The misalignment between development and cybersecurity teams leads to missed business opportunities, as new capabilities are delayed in reaching the market. In some cases, the pressure to close the gap has caused increased vulnerability, as development teams bend rules to work around security policies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



#### Activities

Architecture and design	Implementation	Code review	Testing	Deployment
<ul style="list-style-type: none"> <li>Analyze resource availability from cloud service provider</li> <li>Analyze capacity requirements</li> <li>Develop initial solution design</li> <li>Design interfaces</li> </ul>	<ul style="list-style-type: none"> <li>Instantiate development and testing environments</li> <li>Begin solution implementation</li> </ul>	<ul style="list-style-type: none"> <li>Review code</li> <li>Conduct automated code scanning</li> <li>Accept code into code base</li> </ul>	<ul style="list-style-type: none"> <li>Develop test cases</li> <li>Do continuous testing</li> <li>Fix bugs and errors; make changes</li> <li>Do regression testing</li> </ul>	<ul style="list-style-type: none"> <li>Instantiate cloud infrastructure</li> <li>Establish cloud services</li> <li>Deploy production application</li> <li>Do final testing</li> </ul>

### Using quantitative risk analytics for decision making

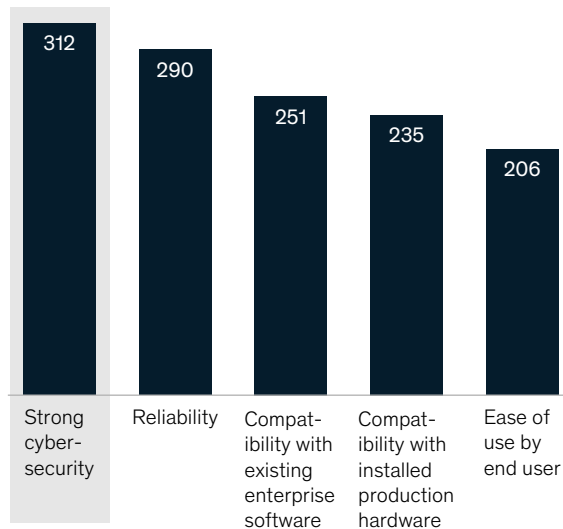
At the core of cybersecurity are decisions about which information risks to accept and how to mitigate them. Traditionally, CISOs and their business partners have made cyberrisk-management decisions using a combination of experience, intuition, judgment, and qualitative analysis. In today's digital enterprises, however, the number of assets and processes to protect, and the decreasing practicality and efficacy of one-size-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. It

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,<sup>1</sup> number of survey responses



<sup>1</sup> 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.

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 auto-parts 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-to-end 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

Exhibit 4

## How to embed security into a product-development process.

### From treating security and privacy as afterthoughts ...

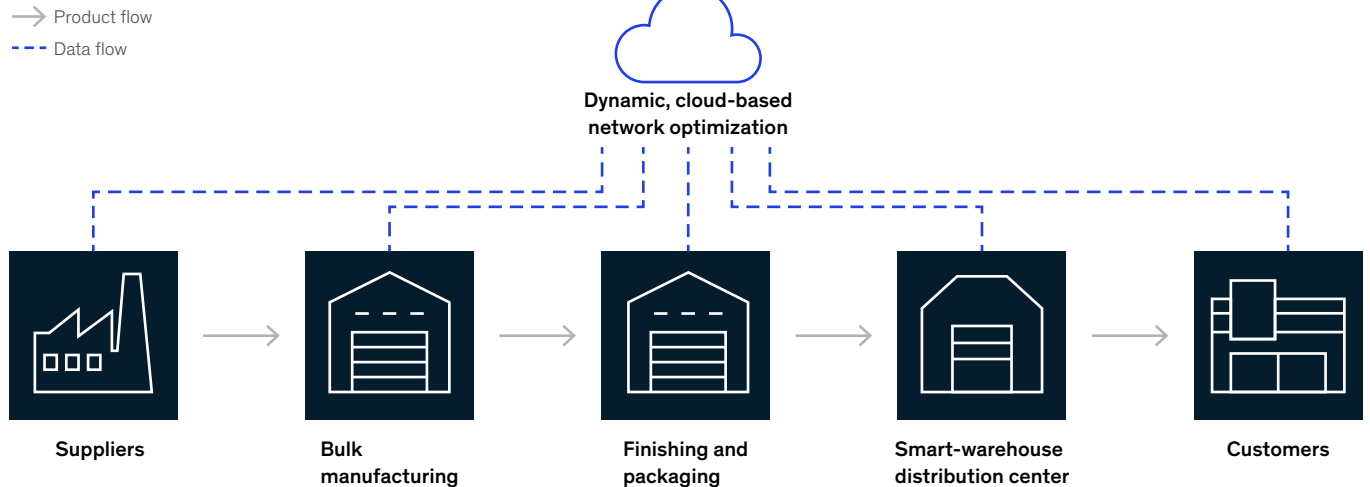
### ... to incorporating them by designing and building an agile security-and-privacy model

Developers are unclear when security and privacy requirements are mandatory	Product owners don't consider security and privacy tasks during sprint planning	<b>Requirements</b>	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
		<b>Design</b>		
Unclear how to handle distribution of tasks within development team	Chief information-security and privacy officers (CISPOs) have limited capacity to support development teams	<b>Development</b>	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		<b>Testing</b>	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	<b>Deployment</b>	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	<b>Throughout process</b>	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.**

**Supply chain**



● Advanced business capability

● Resulting cyberrisks

**Suppliers**

- Predictive supplier risk protection
- Risk of exposed vendor details and trade secrets

**Bulk manufacturing**

- Yield optimization through advanced analytics and digitized operations
- Hacking of legacy equipment
- Unauthorized changes in safety or compliance regulations
- Loss of intellectual property and competitive advantage

**Finishing and packaging**

- Fully integrated and automated production
- Attack on process, leading to shutdowns or errors
- Transition from closed to open systems prompts new security risks

**Customers**

- No-touch order management
- Leak of customer data, leading to loss of customer trust and competitive data

**Overarching technologies**

- Machine-learning forecasting and integrated production planning
- Inaccurate business decisions and bad-actor access
- Real-time monitoring
- Unauthorized monitoring of processes and leakage of business decisions

as suppliers and customers negotiate liability and 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).

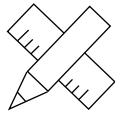
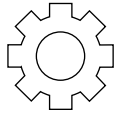

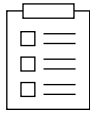
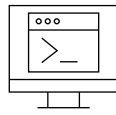
- Organize security teams into agile scrum or scrumban teams that manage developer-recognizable services, such as identity and access management (IAM) or DLP. Also, recruiting development-team leaders to serve as product owners for security services can help, just as business managers are product owners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

Exhibit 6

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

### Automation opportunities in a notionally secure DevOps model

	 <b>Architecture and design</b>	 <b>Implementation</b>	 <b>Code review</b>	 <b>Testing</b>	 <b>Deployment</b>
<b>App application programming interfaces (APIs)</b>	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
<b>Process APIs</b>	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
<b>Infrastructure APIs</b>	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



## 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.

in integrative problem solving, automation, and development—as well as security technologies.

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.

Designed by Global Editorial Services  
Copyright © 2019 McKinsey & Company. All rights reserved.