McKinsey & Company

Risk Practice

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

© Milko Marchett/Getty Images

April 2019

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

[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.

sensitivity of the targets, this has quickly 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]

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 while they

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

tend to have a good handle on IT assets managed 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

[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

	Led by a CISO,[1] whose location will vary, typically within IT, risk, or security department												Led by a CSO[2]			
	No clear direction of OT[3] so defaults to operations				CISO advises and has oversight, operations directs				CISO is accountable, but not responsible for execution in OT				Single accountability for IT, OT; cyber is part of risk agenda			
OT security functions	CISO	Ops	IT	CRO[4]	CISO	Ops	IT	CRO	CISO	Ops	IT	CRO	CSO	Ops	IT	CRO
Policy setting		●			○	○			●				○			○
Standards creation		●							●				●			
Security architecture and engineering		●				●			○	○			○	○		○
Execution deployment		●				●				●					●	
Operations/maintenance (within perimeter)		●				●				●					●	
Operations/maintenance (perimeter/IT interface)		○	○			○	○				●				●	
Operations/maintenance (physical security)		●				●				●			○			○
Adherence		●			○	○			○	○		○	○			○
	— Earliest stages of maturity; OT cybersecurity ownership defaults to business units — Decentralized policy and standard setting				— CISO advises on security policy, but has little influence over operations — Execution, operations, and maintenance with operational units				— CISO determines policy and standards centrally — Operational units responsible for execution and operations				— CSO spans IT and OT; owns security end to end — Collaboration between security and CRO for policy setting, architecture, adherence			

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

between the OT and IT networks enable companies to inspect the traffic 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.

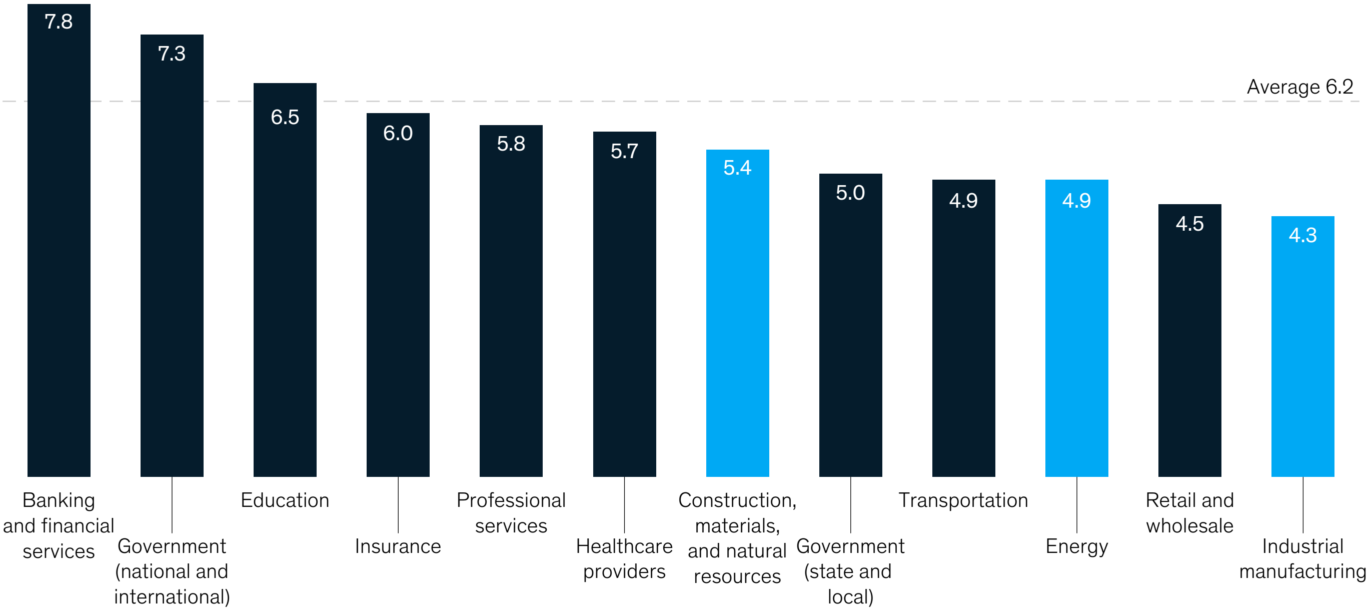
Greater industry-wide collaboration

Knowledge-sharing initiatives have started to emerge across heavy industrial sectors, but much more can be done. Some good examples come

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 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.