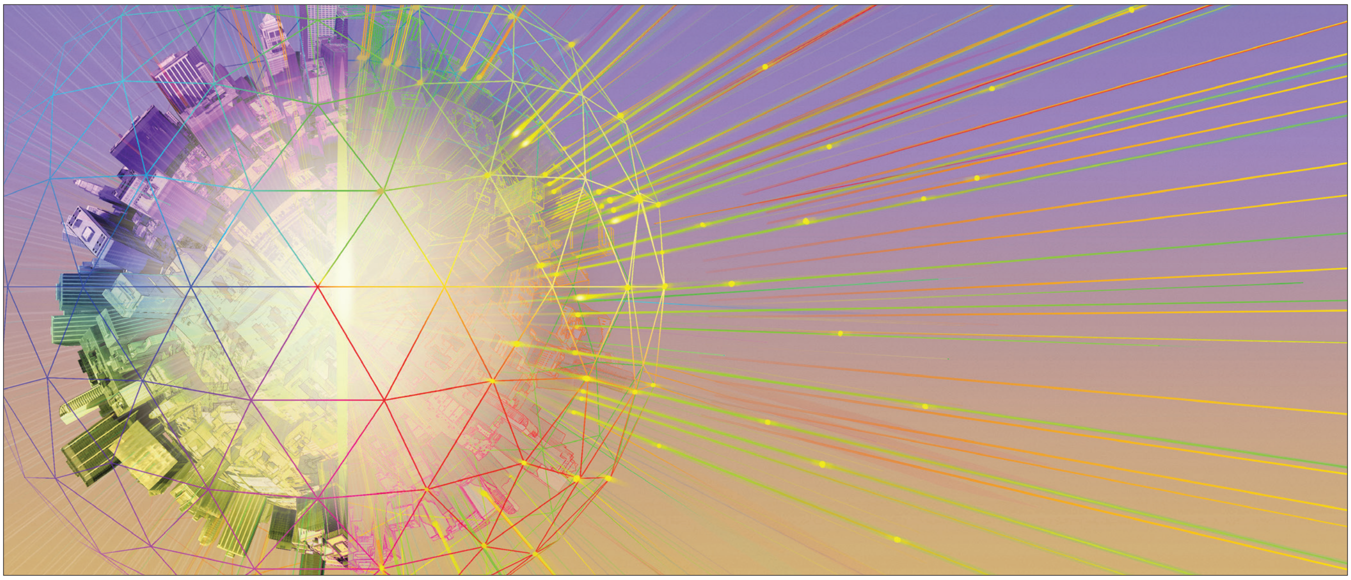
Deloitte Review

ISSUE 25, JULY 2019

COMPLIMENTARY ARTICLE REPRINT



Cyber, cyber everywhere: Is your cyber strategy everywhere too?

by Nick Galletto, Ed Powers, and Tim Murphy

ILLUSTRATION BY J. F. PODEVIN

Cyber, cyber everywhere

Is your cyber strategy everywhere too?

BY NICK GALLETTO, ED POWERS, AND TIM MURPHY

ILLUSTRATION BY J. F. PODEVIN

In the 21st century, the connective power of technology is giving rise to a wave of innovative products and services that are transforming the way people live and work. Consider Disney World Parks. Known for pushing the limits of its audience's imagination, Disney World combined sensor technology, cloud computing, and artificial intelligence (AI) to create connected, radio-frequency identification (RFID)-based wristbands that help create more immersive and enjoyable experiences for guests. These wristbands have helped Disney World both improve operations and better serve visitors, enabling organizers to—for instance—deploy special events to remove ride bottlenecks in real time (such as putting on Disney-character shows that hold guests' attention as they wait in long queues).

The technology has made it easier to create personalized guest experiences such as customized hotel accommodations and first-name-basis interactions with characters. And, not least, the wristbands, built with security as a top-of-mind design element, have helped Disney World cultivate safer digital and physical environments for its guests. For example, the wristbands are paired with multifactor identification mechanisms such as fingerprints and personal identification numbers to restrict park access and in-park purchases. And in a venue that caters to thousands of guests daily, the RFID-based wristbands can help security personnel quickly identify and reunite a lost child with his or her family.

To build innovative, connected experiences, businesses need a strong cyber program.[1] Every time a device is connected to a sensor that in turn connects to a network, a new cyber vulnerability emerges at each connection point. On a larger scale, connected technologies increasingly underpin the functioning of the nation's power grids, factories, entertainment venues, and communication and transportation infrastructures. Indeed, cyber vulnerabilities are seemingly *everywhere* these days, and they're only going to become more prevalent in the future.

Yet, just because cyber is everywhere, it doesn't mean that corporate strategies are necessarily following suit for addressing cross-enterprise risks. In Deloitte's 2019 *Future of cyber survey*, which polled more than 500 C-level executives on cyber issues, more than 90 percent of respondents suggested that less than 10 percent of their cyber budgets were allocated to digital transformation efforts such as cloud migration, AI-driven products, and software-as-a-service (SaaS)—all areas where cyber vulnerabilities are becoming more prevalent.[2]

The risk isn't just that cyber incidents will destroy value in the classical sense. The opportunity cost of what cyber vulnerabilities can *prevent* organizations from doing can be far greater. The specter of cybercrime and its fallout can cast a shadow over an organization's efforts to turn technology to better use, strangling innovation and slowing digital transformation efforts to a crawl. Though digital and connected technologies are an immensely fertile ground for innovation for organizations in all industries, their potential will go untapped if that ground is perceived to be too risky to be worth exploring.

Many executives are wrestling with this reality even now. In a recent global study on AI initiatives among businesses, 49 percent of respondents, a plurality, cited "cybersecurity vulnerabilities" as their top concern.[3] An earlier study polling US executives also revealed that 30 percent of respondents had slowed down an AI initiative to address cyber concerns, and another 20 percent had decided to not even start such initiatives due to their cyber implications.[4]

This is why cyber today is not purely a risk management issue, but is instead a core business enabler. For organizations to fully reap the benefits of new, digitally enabled technologies, they need to view cyber as a digital transformation priority. In an era when technological innovation underpins a business's marketplace performance, organizations that put cyber at the forefront should be better positioned to drive innovation and, consequently, bottom-line growth. Conversely, in the absence of a well-orchestrated cyber program, new products and services will be exposed to greater financial, brand, and regulatory risks, likely slowing their development and marketplace penetration.

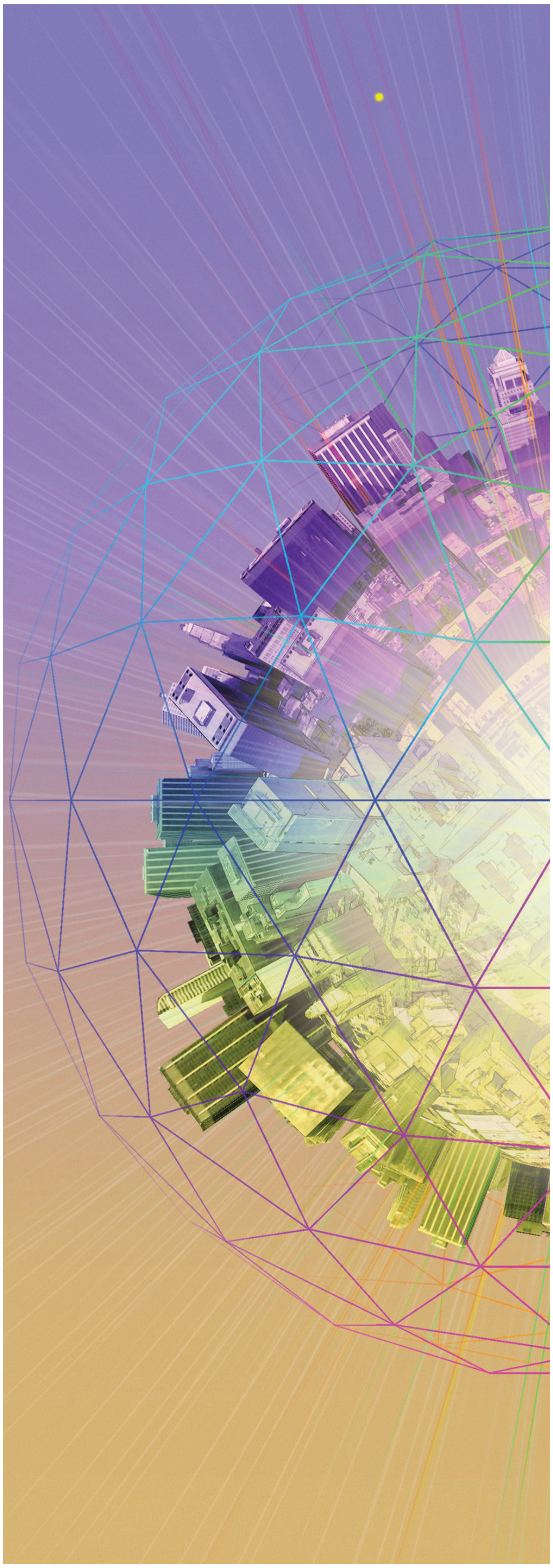
The good news is that, for those looking to redesign their businesses with cyber as a fundamental element, a host of new opportunities is emerging. While this is new ground for almost everyone, organizations can take action today to understand their cyber vulnerabilities, assess the risks, and put protections in place that make technology a safe space for innovation to grow the business.

Not just IT's problem any more

In the past, cyber was viewed as a means of protecting information—financial data, intellectual property (IP), or personally identifiable information. As such, cyber naturally found its organizational home within the information technology (IT) department, traditionally tasked with managing and protecting information.

For those looking to redesign their businesses with cyber as a fundamental element, a host of new opportunities is emerging.

But in today's "everything is connected to everything" environment, the implications of cyber go way beyond IT. A cyber adversary can strike wherever connected technology is deployed—whether it's to hack a server in a data center, an oil rig in the ocean, or a pacemaker implanted in a person—and this makes cyber not only an issue for protecting information, but also a necessity for protecting systems and people, both inside and outside the enterprise. Moreover, the proliferation



of use cases for connected digital technologies, even within a single enterprise—everything from, say, autonomous vehicles to medical implants to assembly-line robots—means that it's unrealistic to expect consistency across either cyber vulnerabilities or security solutions.

These factors have two important implications for an organization's cyber strategy:

- **The number of cyber stakeholders is expanding.** With IT, operational technology (OT), and the end user coming into the picture, cyber has to be an important consideration for executives from across the top ranks of management. It can no longer be relegated into an organization's sublayers, but instead should be represented in the C-suite so that the broader business can better understand the priority and importance of creating a cyber-secure enterprise. Included in the lengthening list of cyber stakeholders are individuals such as the chief supply chain officer (CSCO), the chief innovation officer, the chief marketing officer (CMO), the chief operations officer (COO), the chief risk officer (CRO), chief information officer, and chief information security officer (CISO), plus procurement, facilities managers, plant managers, and even (or especially) employees on the ground. A cyber governance model that starts and ends with the CISO under the confines of IT is no longer enough.

- **Standardization doesn't apply.** On the surface, most IT security solutions are fairly standardized, database structures are uniform, and firewalls still work broadly—regardless of industry or use case. However, how a hospital deploys robotics can be very different from the way a smart factory does. Nowadays, organizations combating cybercrime need to consider IT, OT, *and* customer product environments—all with have their own nuances that often lack a cross-organizational framework. Because of this, each cyber solution requires a level of bespoke customization that makes every solution set unique.

A cyber strategy that recognizes these principles can help organizations develop approaches to strengthening security that fuel—not throttle—the pace of innovation.

A stakeholder challenge: Getting people to step up

Since cyber is everywhere, cyber awareness needs to be embedded everywhere. That means that cyber must be part of everyone's job in a very literal sense. Converging cyber environments blur the lines of responsibility among stakeholders. No longer does the onus of cyber fall squarely on the CISO; rather, it is—or should be—a cross-functional endeavor.

Take the CMO, for instance. For the typical CMO, striving to build customer appeal and brand equity, cyber is new ground.[5] Yet CMOs are continually looking to digitize their efforts and enhance the customer experience through technology. To do this seamlessly—and safely—the CMO must incorporate cyber professionals, and their relevant expertise, into the development of customer-facing initiatives.

The CMO is only one of many people who need to be involved. To illustrate how cyber touches nearly everyone's role, consider the major stages of product development:

- **Innovation.** Chief innovation officers regularly look to advanced technologies to fuel new products. If cyber is not adequately considered, these innovations could be halted even before they begin. Or, worse, they could go to market with serious cyber vulnerabilities.

- **Sourcing.** As supply chains increasingly transition to digital supply networks, which transform linear supply chains into interconnected ecosystems,[6] CSCOs need to ensure that third-party vendors meet the company's required security standards. This is a regular issue for automotive original equipment manufacturers (OEMs), for instance. A vehicle's infotainment unit can consist of multiple components—navigation technology, USB drives, smartphone integration capabilities, and more—sourced from different vendors that may have inconsistent security protocols.

- **Manufacturing.** In today's converging environment, the plant manager's role is not limited to simply coordinating actions between humans and physical machinery. Plant managers are integrating robotics, sensor technology, and even augmented reality (for example, to assist in maintaining and repairing equipment) into their workflows.[7] Each of these technologies creates a new connective endpoint, each with its own cyber considerations.

- **End-product support.** The final product a customer buys represents a culmination of the first three stages. But cyber considerations don't necessarily end with the sale; many types of products need to be continually protected after they are launched. This may entail safeguarding both data and functionality—especially functions that are automated, such as customer-facing chatbots.

In practice, unfortunately, cross-functional collaboration on cyber issues rarely happens. In the aforementioned *Future of cyber survey,* only 30 percent of respondents indicated their organizations have integrated some form of cyber liaising into their core business functions to facilitate cyber awareness and readiness throughout the organization.[8] One big reason for this may be the relatively junior position of many CISOs in the executive suite. The study also highlighted that the CISO is often pushed down the organizational chart, even as the growing importance of cybersecurity would seem to call for the role to be elevated. For example, nearly 80 percent of responding CISOs report to the chief information officer or the chief security officer (CSO), despite the majority of CISOs saying that they were seeking greater access to the CEO (and, thereby, to the rest of the organization).[9] This poses a real problem for cyber-awareness. With the CISO's influence buried in the depths of the organizational hierarchy, it is difficult to cultivate a cyber-aware mindset across the rest of the C-suite.

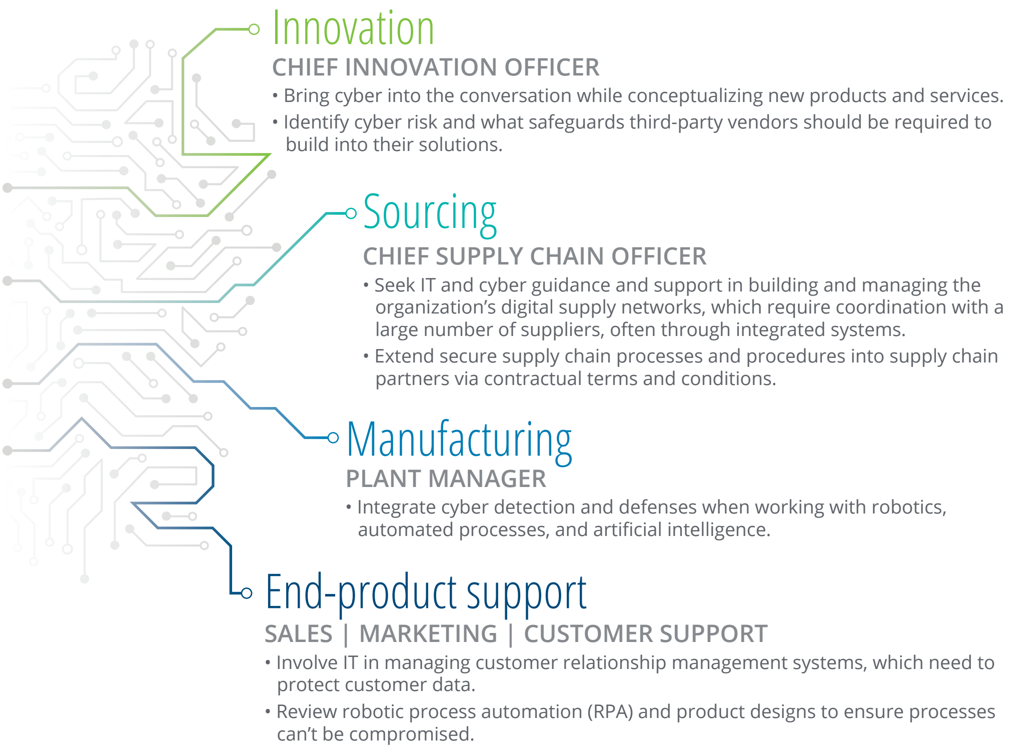
Figure 1 lists some steps that executives in various functions can consider to help achieve cyber awareness and action across the product life cycle.

The standardization challenge: Keeping up with the march of technology

As organizations' collective ambition has grown to push advanced technologies both across the enterprise and into consumers' hands, their cyber environments have expanded to include IT, OT, and customer-facing products and services. And with this expansion has come an ever-increasing variety of technology infrastructures and systems across which cyber must be maintained—and more

FIGURE 1

How leaders across the enterprise can build cyber into the business



Innovation

CHIEF INNOVATION OFFICER

- Bring cyber into the conversation while conceptualizing new products and services.
- Identify cyber risk and what safeguards third-party vendors should be required to build into their solutions.

Sourcing

CHIEF SUPPLY CHAIN OFFICER

- Seek IT and cyber guidance and support in building and managing the organization's digital supply networks, which require coordination with a large number of suppliers, often through integrated systems.
- Extend secure supply chain processes and procedures into supply chain partners via contractual terms and conditions.

Manufacturing

PLANT MANAGER

- Integrate cyber detection and defenses when working with robotics, automated processes, and artificial intelligence.

End-product support

SALES | MARKETING | CUSTOMER SUPPORT

- Involve IT in managing customer relationship management systems, which need to protect customer data.
- Review robotic process automation (RPA) and product designs to ensure processes can't be compromised.

Source: Deloitte analysis.

closely integrated. Yet, as organizations integrate IT, OT, and product environments, they are confronted with the reality that each environment has its own unique systems and processes that make finding a standardized solution difficult.

INFORMATION TECHNOLOGY: THE FIRST FRONTIER

As mentioned above, prior to the advent of connected sensors and cloud computing, almost all things cyber fell squarely in the realm of the IT department, which led the charge of protecting an organization's critical technology assets. These assets consisted primarily of core IT systems (for example, servers, networks, and applications) and information: IP, database schematics, and financial and customer data, to name a few.[10]

The advent and spreading use of cloud computing, advanced AI, and sensor technology shifted the IT landscape—and pushed organizations' cyber frontier beyond the bounds of the enterprise. New, more nimble competitors started forcing larger IT organizations to reprioritize and redesign their security solutions. Take financial services: Larger incumbent institutions are competing with new entrants that are using technology to change the service offering model by approving mortgage applications at a rate never seen before, for instance. To keep pace and accelerate development, IT functions are sacrificing control of their information to external partnerships and suppliers. Each partnership represents a new "building block" in the development of an IT solution. Thus, any IT solution can now consist of products and services from multiple suppliers.

OPERATIONAL TECHNOLOGY: A NEW AREA OF RESPONSIBILITY

At its core, OT monitors and manages physical devices and processes across a manufacturing operation. Until recently, since the Industrial Revolution, OT devices had traditionally been isolated from the IT function. But digital technology has changed that.

Consider automotive smart factories, which use sensors to not only measure plant humidity levels but also to redirect production processes when the humidity is too high.[11] To do this effectively, IT and OT systems need to integrate at various levels, including in their approach to cybersecurity: If a sensor reading is compromised, for instance, it can shut down the entire production process. Integrating cyber into the manufacturing process can help unlock new capabilities—but neglecting it can expose the production process to enhanced risks.

This issue isn't confined to the manufacturing industry. As another example, many hospitals are increasing the connectivity of clinical technology and medical devices such as in magnetic resonance imaging (MRI) machines. Many hospitals only have access to a single MRI setup, with demand constantly exceeding supply. Sensor technology helps alleviate bottlenecks by giving the hospital a better view of equipment downtime and availability. But like any connected device, medical devices—including MRI machines—are vulnerable to cyberattacks.[12] Without careful cybersecurity design and implementation, these devices can go down at time-sensitive moments—such as when a surgical procedure is contingent on an MRI result.

CONSUMER PRODUCTS: CONNECTIVITY LEADS TO NEW CYBER CONSIDERATIONS

Another major cyber frontier is the consumer environment. Many organizations view advanced technologies as a means to enhance the customer experience. In addition to the massive amounts of consumer information companies may hold, the proliferation of wearables and connected devices has blurred the lines between IT, OT, and the product environment.

The health care industry again provides an example. Many patients today are interacting firsthand with connected products. For instance, some pacemakers now come with software that enables them to be remotely monitored. Wireless technology in the pacemaker alerts both patients and physicians to any issues. Consequently, patients are engaging more with their health, and surviving longer.[13] However, if security is not designed into the device, cyber adversaries can go as far as buying equipment from third-party suppliers to remotely access and manipulate the data that informs patient treatments—thus negating the powerful benefits originally intended by the connected product.

Likewise, cyber considerations are affecting forthcoming innovations such as autonomous vehicles. To operate, each vehicle contains proprietary software with over 100 million lines of code.[14] As society collectively moves toward self-driving cars, the designers of those cars need to weigh the merits of each technological innovation against the possibility that someone with malicious intent could hack it. Although automotive regulatory bodies have yet to flesh out the cyber standards for vehicle technology, it's possible that forthcoming regulations—if regulators are forced to choose—may prioritize passenger safety and operating efficiency over cyber. Yet while autonomous vehicles may operate safely under ideal circumstances, a single cyberattack can turn a safely operating vehicle into a public hazard.

The convergence of the IT, OT, and consumer product environments pays dividends in terms of innovations to better serve the consumer—but also introduces intricacies that make products vulnerable throughout their life cycle. Moreover, the sheer variety of connected products, along with the proliferation of third parties that may have a hand in developing them, make it impossible to devise a one-size-fits-all solution. These factors make it that much more important for cybersecurity to be embedded into all facets of product development.

Navigating the new frontier

Stretching across environments and stakeholders alike, the scope of cyber is vast, complex, and difficult to coordinate. This growing cyber landscape requires a deliberate strategy and culture that accounts for organizational growth. Businesses evolve, meaning that the people responsible need to continually adjust practices, protocols, training, and contracts to manage risks both proactively and reactively. A leading practice for dealing with ongoing operations is to always be looking at the threat landscape to evaluate the organization's cyber risk posture in real time.

There are three concurrent paths that can be considered when developing solutions that cultivate an innovative—and secure—environment.

PATH 1: ESTABLISH A COORDINATED GOVERNANCE MODEL

While financing a cyberattack can cost as little as US$34, the cost of an incident to a company can reach into billions of dollars.[15] But even more costly, potentially, is the dampening effect a cyberattack can have on an organization's appetite for pursuing technological innovations. For both these reasons, corporate boards are becoming increasingly aware of the financial toll of cyberattacks. Yet cyber is on only 49 percent of boards' quarterly agendas, and only 4 percent of boards discuss the issue monthly.[16] This may change, however, as regulatory bodies are beginning to hold boards accountable for their knowledge of cyber issues and incidents. The pervasive impact of cyber throughout an organization's ability to execute its strategy shouldn't be underestimated. Boards can require management to provide key risk indicators that can enable them to quickly ascertain the state of cyber in the company.

Apart from raising the board's awareness, one way in which executives can work to raise cyber's profile across the organization is to establish an integrated governance model that is aligned with key business strategies and supported by consistent cyber frameworks. Such an integrated model seeks to break down silos between the IT, OT, and product environments so that security can be considered and implemented seamlessly across their boundaries.

We've seen this accomplished by a large oil and gas company.[17] While looking to update its remotely located refineries, where connectivity was a challenge, the organization brought together a diverse group of cyber professionals and business leaders to understand the overall business objectives, the refineries' workforce and their technical capabilities, and the limitations (such as sparse internet connectivity). Through bringing the cyber organization into the conversation, the company elevated cyber's importance and directly embedded the appropriate expertise into the work-design process. By diving into the business needs, the cyber professionals were able to identify security gaps and redesign the defenses to better align with the company's business objectives. Having cyber and business leaders work hand in hand also enabled both groups to effectively identify cyber vulnerabilities, and helped to alleviate the organizational knowledge gap where business leaders previously had little experience in navigating cyber design.

The effort netted promising results. First, the company recognized that many of its connectivity issues were due to outdated firewall configurations. By reconfiguring and standardizing the cybersecurity process, it was able to improve connectivity and decrease disruptions. Second, project leaders learned that much of the workforce regularly relied on paper forms and checklists. So, to effectively embed cyber considerations into employees' work, tasks such as monitoring and logging results were added to the refineries' regular checklists to prompt workforce adherence to strong security protocols. The value of the effort to company leaders speaks for itself: After the first successful integration, the company chose to repeat the

process at more than 100 refineries and field operations across the enterprise.

PATH 2: CULTIVATE COMMUNITIES OF LEARNING

Digital transformation, which relies on increasingly open environments, is forcing businesses to break down intra- and interorganizational silos to share both information and the underlying technical infrastructure that supports it. But organizations rarely undergo only a single digital transformation; many implement several transformations simultaneously. This creates new opportunities to spread cyber knowledge and information across groups.

Thanks to digital transformation, departments that previously had little interaction may now be required to work together. The cyber department, in particular, is likely to find itself pulled into a multitude of projects. Cyber professionals may work with marketing to revamp an e-commerce site, for instance, or with sales to enhance a customer-relationship management platform. By committing to greater knowledge-sharing, cyber organizations—armed with years of cyber experience—can help to better integrate and disseminate cyber learnings across the enterprise.

Digital transformations are also changing how organizations interact with—and learn from—outside partners and competitors. This is because they're increasingly relying on external parties to develop and support products. Beyond supplier relationships, we are even seeing companies that previously viewed each other as competitors become partners in certain areas.

Many such new partnerships are forming in the automotive industry. For instance, some automakers have gone from trying to develop their own smartphone integration software to partnering with technology companies to do so. These open environments are paving the way for sharing cyber practices and lessons learned across sectors. The emergence of Information Sharing and Analysis Centers (ISACs)—member-driven organizations dedicated to enhancing cyber protection—is a primary example of growing industry collaboration around cyber. They provide a forum for member companies to share security threats along with information on how to address them.[18]

By expanding the community of learning partners both within and outside the enterprise, organizations can increase their rate of adopting sound security practices that can help them address today's new and growing cyber threats.

PATH 3: INVENTORY THE ORGANIZATION'S CYBER

Hopefully, by now we've established that cyber vulnerabilities are embedded throughout the organization and (potentially) its products—typically not due to carelessness or accident, but simply because of their interconnectivity. A natural follow-up is to inventory critical assets, identify the risk, and pinpoint exactly where those cyber vulnerabilities exist, to the best of the organization's ability. Much of this comes down to "hand-to-hand combat" where leaders across the organization will need to wade through each of their assets to determine if and where potential cyber threats may exist. The good news is that strong governance and communities of learning can help.

A solid first step is to document the organization's critical assets. This can include taking stock of where data is stored, where single points of failure have occurred within supply chains, which processes are automated, and which devices are connected to which networks and servers. Of course, the proliferation of technology can make this an exhausting exercise. To prioritize efforts, leaders can start with identifying "crown jewel" assets. These might be assets that give the organization a competitive advantage (such as IP), help it achieve new efficiencies (such as warehouse robots), or in which safety is paramount (such as implanted medical devices).

Leaders in different industries and organizations with different objectives will likely, and appropriately, take different approaches to managing their cyber. For instance, established business-to-consumer organizations may want to focus their efforts mainly on products and supply chains. In contrast, a growing startup will most likely embrace a different cyber strategy, perhaps prioritizing creating employee-access protocols and training workers on leading cyber practices. For many startups, these are new areas of consideration that can make them especially vulnerable to attacks.[19] As the startup grows, it will need to establish more formal cyber programs around authentication, access, monitoring, and threat intelligence to match the organization's maturity.

As digital transformations increase in scope and scale, taking a cyber inventory needs to become a regular work process rather than a periodic event. This is because every new technology integration can give rise to new security considerations.

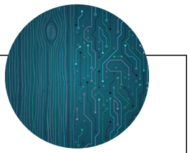
Protecting the ability to innovate

Technology permeates almost everything that organizations do and make these days, and the connectivity that technology creates means that cyber must be a constant and ubiquitous concern. Among other things, a strong approach to cyber entails collaborating, or at least coordinating, with organizationwide peers, external partners, and sometimes even competitors. But while doing this may be challenging, the payoff is considerable: a safe environment for innovation. If an organization's cyber practices are known to be strong, then its leaders can feel empowered to pursue technological innovations, confident in the knowledge that the cyber risks those innovations may create will be appropriately addressed. The imperative is clear: Implementing effective cyber risk management across internal and external organizational boundaries can neutralize cyber threats as an obstacle to innovation—and enable an organization to continue to find ways to turn technology to its own and its customers' better advantage. ●

NICK GALLETTO is the Global and Canada Cyber Risk Services leader. He is based in Toronto.

ED POWERS is the Deloitte Risk and Financial Advisory Cyber Risk Services leader in the United States. He is based in New York City.

TIM MURPHY is a researcher and analytical scientist with the Deloitte Center for Integrated Research. He is based in Milwaukee.



Cyber, cyber everywhere

page 62

1. In this article, we use the term “cyber” to convey the implications of connecting technologies. These can be the vulnerabilities and attacks that emerge, or the opportunities and solutions that strong cyber programs create.

2. Deloitte, *The future of cyber survey 2019: Cyber everywhere. Succeed anywhere.*, accessed May 6, 2019.

3. Jeff Loucks et al., *Future in the balance? How countries are pursuing an AI advantage: Insights from Deloitte’s State of AI in the Enterprise Survey, 2nd Edition*, Deloitte Insights, May 1, 2019.

4. Jeff Loucks, Tom Davenport, and David Schatsky, *State of AI in the Enterprise, 2nd edition: Early adopters combine bullish enthusiasm with strategic investments,* Deloitte Insights, October 22, 2018.

5. Deloitte, *Why CMOs should care about cyber risk*, accessed May 6, 2019.

6. Adam Mussomeli, Doug Gish, and Stephen Laaper, *The rise of the digital supply network: Industry 4.0 enables the digital transformation of supply chains*, Deloitte University Press, December 1, 2016.

7. Rick Burke et al., *The smart factory: Responsive, adaptive, connected manufacturing*, Deloitte University Press, August 31, 2017.

8. Deloitte, *The future of cyber survey 2019*.

9. Ibid.

10. Robin M. Ruefle, “Critical asset identification (part one of 20: CERT Best Practices to Mitigate Insider Threats Series),” Carnegie Mellon University Software Engineering Institute, April 12, 2017.

11. Brenna Sniderman, Monika Mahto, and Mark J. Cotteleer, *Industry 4.0 and manufacturing ecosystems: Exploring the world of connected enterprises*, Deloitte University Press, February 22, 2016.

12. BBC News, “Medical devices vulnerable to hackers,” September 29, 2015.

13. Ken Demith, “Remote monitoring proven to help prolong life in patients with pacemakers,” Heart Rhythm Society, May 8, 2014.

14. Leon Nash et al., *Securing the future of mobility: Addressing cyber risk in self-driving cars and beyond*, Deloitte University Press, April 4, 2017.

15. Deloitte, “Black market ecosystem: Estimating the cost of ‘Pwnership’,” December 2018.

16. Deloitte, *The future of cyber survey 2019*.

17. Deloitte analysis.

18. National Council of ISACs, accessed May 6, 2019.

19. Ralph Tkatchuk, “Seven things startups need to know about cybersecurity,” *CIO*, August 15, 2017.