www.pwc.com/cybersecurityandprivacy

Converging cyber risks in a digital world

pwc

Converging cyber risks in a digital world

How the fusion of information, operational, and consumer technologies is transforming the security landscape for businesses, individual consumers, and society at large.

Highlights

The convergence of internet-enabled information, operational, and consumer technologies is generating sweeping business opportunities as well as increasing product and system vulnerability to cyberattacks.

Operational technologies (OT) such as systems that control manufacturing processes are becoming more interconnected with other technology domains, increasing the risk of disruption and the integrity of products and services.

Consumer technologies (CT)—end-user products and services that include home automation and sensor-enabled automobiles—are becoming more connected with other technologies, introducing new, potentially dangerous privacy and safety concerns.

Recent global cyberattacks have produced significant financial impact on multinationals. The stakes of cyber insecurity are rising. In our 2018 Global State of Information Security® Survey (GSISS), we asked leaders about the biggest potential consequence of a cyberattack on business systems that use automation or robotics. Forty percent of survey respondents cite the disruption of operations as the biggest potential consequence of a cyberattack, 39% cite the compromise of sensitive data, 32% cite harm to product quality, 29% cite damage to physical property, and 22% cite harm to human life[1]. Yet despite this awareness, many companies at risk of cyberattacks remain unprepared to deal with them. Forty-four percent of the 9,500 executives in 122 countries surveyed by the 2018 GSISS say they do not have an overall information security strategy.

Cybersecurity is no longer only an IT issue but interconnects with manufacturing, production, sales, logistics and other business operations that are enabled by digital technologies. We live in a hyper connected world in which consumer devices, buildings, vehicles, businesses, and critical infrastructure and cities are increasingly tied together via the internet. These interconnected systems encompass building automation, manufacturing plants, automobiles, aircraft, oil and gas production, personal medical devices, virtual assistants, and automated homes. But the unprecedented conveniences enabled by this interconnectivity come with a significant caveat. For corporate leaders, the convergence of everything digital—including information technologies (IT), operational technologies (OT), and consumer technologies (CT)—can present an immense security challenge.

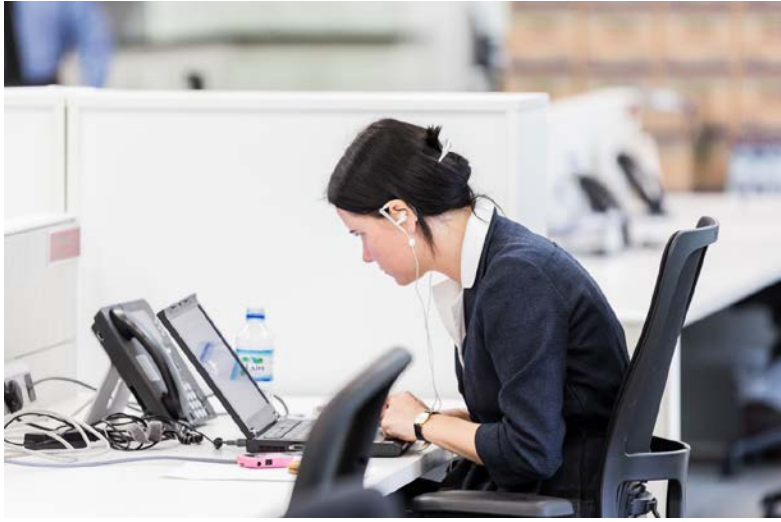
On one hand, enhanced connectivity and the monetization of data offers numerous business opportunities. Interconnectivity has enabled technological innovations that have improved operations, redefined consumer relationships and interactions, and enabled business innovations. Among consumers, this digital convergence has brought unprecedented lifestyle conveniences, improvements in healthcare, and enhanced features in homes and automobiles.

[1]PwC, CIO and CSO, *The Global State of Information Security® Survey 2018*, October 2017

But these innovations have also created significant cybersecurity and privacy challenges. Unaddressed, these challenges can represent disruptive threats that may require robust risk management. For industrial control systems that support critical infrastructure, the consequences of a cyberattack can be especially significant.

Cyberattacks can cause unprecedented disruption to expansive areas. For example, 230,000 Ukrainian residents lost power in a December 2015 cyberattack on a power grid[2]. One year later, malware dubbed "Crash Override" used malicious code to scan, infiltrate and disable electrical grid components, also in Ukraine. Researchers have said these methods and techniques could easily be adapted to attack other utilities with multiple cyber-physical systems[3]. The number of malicious attacks worldwide that utilize malware to disrupt interconnected systems is growing quickly. In fiscal year 2016, the US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 290 incidents, including 63 in the critical manufacturing sector, 62 in the communications sector, and 59 in the energy sector. Hackers used spear phishing to gain unauthorized access to systems in 26% of these incidents, making this tactic the leading access vector for the 2016 incidents, according to ICS-CERT[4].

[2]SANS Industrial Control Systems Security, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, March 2016
[3]Wired, *'Crash Override': The Malware That Took Down a Power Grid*, June 2017
[4]ICS-CERT, *FY2016 Incident Response Fact Sheet*



New opportunities for hackers

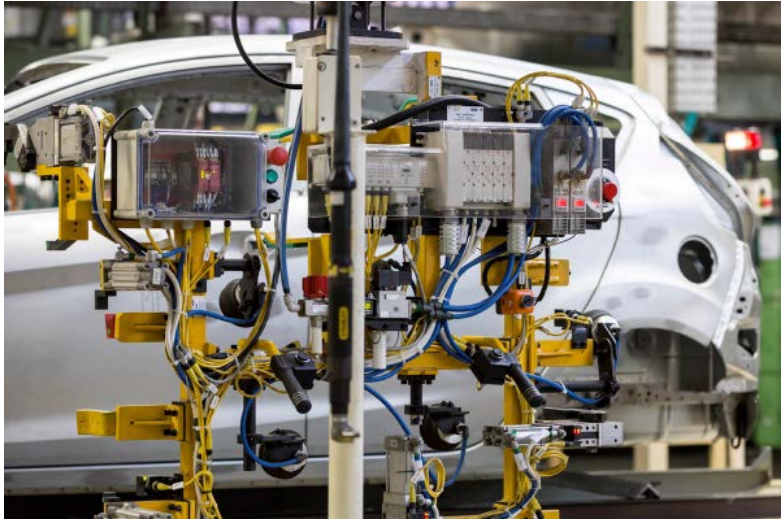
On a much larger scale, the infrastructure of the internet itself--the glue that holds together regional and global connectivity—is also vulnerable to disruption. Hackers have repeatedly exploited weak security on devices such as video recorders and routers to take control of these commodities in mass quantities, wielding the combined power of the systems to create malicious robotic networks dubbed “botnets.”

According to the internet firm targeted by the Mirai botnet on Oct. 21, 2016—up to 100,000 malicious endpoints associated with the botnet unleashed a sophisticated distributed denial of service (DDoS) attack that significantly disrupted consumer access to prominent US websites. The incident, which spurred an electronics maker to plan a product recall, was the “highest throughput DDoS attack seen to date,” according to the Electricity Information Sharing and Analysis Center [4] . This type of threat to internet infrastructure is particularly pernicious because it can serve as a beachhead to connected IT and OT systems, introducing new categories of risk with potentially serious implications for security, business reputation, and public safety.

As interconnectivity expands, the cyberattack surface—the points on which adversaries attempt to access data, applications, and systems—will likely continue to expand exponentially, moving beyond the traditional information security scope to encompass disparate asset types associated with operational and end-user products and services.

[4] E-ISAC, *Internet of Things DDoS White Paper*, October 2016

Danger on wheels



Defining the basic technology domains

Information technology traditionally encompasses the resources and connectivity needed to process and manage the data that supports business functions and transactions. IT processes aim to ensure the confidentiality, integrity, and availability of data and systems. IT-enabled solutions include enterprise resource planning, HR management, customer service, transaction processing, financial reporting, and corporate collaboration.

Operational technology (OT) includes a company's systems and related automation assets that monitor and control physical equipment and events or support the creation and delivery of products and services. For example, a company's OT assets may include environmental control, plant management, integrated facility management, electricity smart grids, air traffic control, and automated logistics operations. Maintaining physical control of proprietary assets such as monitoring whether a valve in a manufacturing plant remains open or closed) is an important responsibility of OT. Historically, organizations have managed and maintained their operational systems separate from their IT systems. That's changing as businesses begin to connect their OT and IT assets via internal networks or the internet.

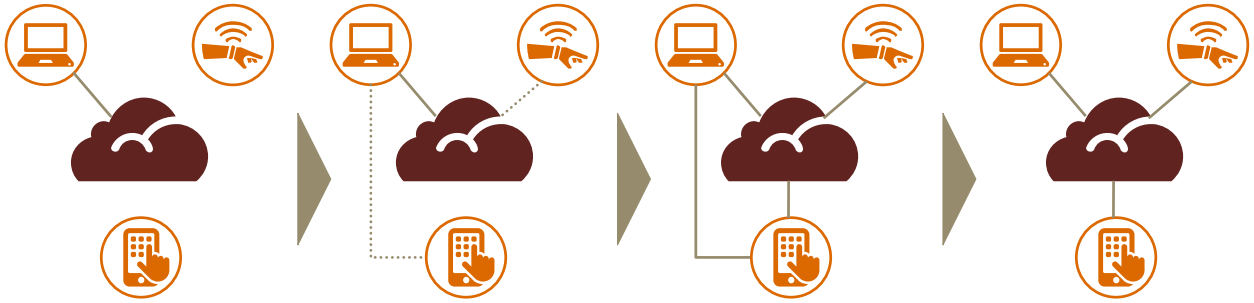
Consumer technologies include the products and services companies provide to end users, such as smartphones, tablets, health and fitness monitoring devices, location-aware services, and gaming networks. Ubiquitous connectivity and advanced mobility, combined with the boom in cloud-based services, has fueled the demand for and production of technology-based consumer products. New technologies such as near field communication, radio frequency identification, and Bluetooth Low Energy are enabling a new wave of products such as digital wallets and personal health monitors.

Consider, for example, the increasing number of wireless, internet-enabled, interconnected technology assets embedded in today's automobiles. New automobiles may contain dozens of these assets, giving hackers new opportunities to potentially assume control of the brakes, steering wheel, and even the engine of individual vehicles.

Further compounding the risk, some interconnected automobiles automatically link to manufacturers' IT and OT systems to perform firmware updates, maintenance monitoring, and real-time communications. And behind the scenes, automakers continue to integrate and automate their operational plant manufacturing systems with their IT environment and back-office business systems. This pervasive interconnectivity has created an environment in which individual automobiles, IT systems, and operational machinery are increasingly vulnerable to cyber threats.

In this scenario, yesterday's security practices cannot effectively address the elevated risks of technology convergence that come with today's automobiles. A strategic approach to cybersecurity—one that encompasses the security requirements unique to information, operational, and consumer technologies—is required.

A concise history of digital convergence



1980s

- IT, OT and CT operate in different environments and on different platforms
- OT and CT are based on proprietary platforms
- Data is not shared between technologies
- OT and CT face little to no cyber risk since they are not connected to a network

1990s

- OT is networked to allow centralized operation
- CT remains in a separate environment
- OT becomes vulnerable due to the connection, but is partially protected by the obscurity of proprietary solutions

2000s

- OT connects to IT using standardized IT channels to reduce costs and increase compatibility
- Boundaries between IT and OT start to blur
- CT connects to IT through pur- pose built channels
- OT is no longer protected by obscurity and CT is now vulnerable. Traditional IT security does not cover either

2010s

- The technology underlying IT has become ubiquitous across OT and CT
- The combination of these three represents the integrated technology ecosystem
- IT, OT and CT are all vulnerable to cyber threats. Businesses should adapt their security model to include the full scope of technologies

Information Technology

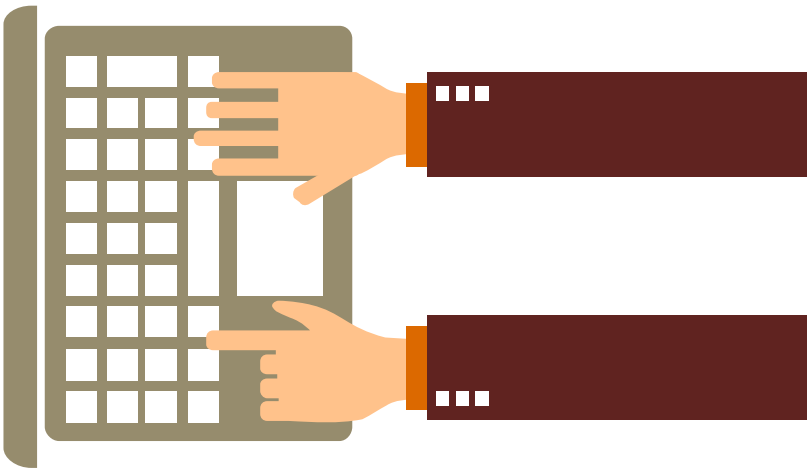
Operational Technology

Consumer Technology

Internet

Proprietary Connection

IT Protocol Based Connection



New technologies create new vulnerabilities

Despite the increasing interconnection of information, operational, and consumer technologies, most organizations still treat the security of these domains separately, maintaining individual security practices for each of them.

IT systems are one exception. While a legacy of IT hacks has led most organizations to implement mature security processes for their IT systems, the same cannot be said for companies' operational and consumer technologies. This has inevitably resulted in gaps in basic security processes such as user access, patch management, and third-party risk assessment.

Insufficient patch management can in particular make organizations vulnerable to cyberattacks. While most businesses have policies and processes for ensuring that the operating systems and firmware for their IT assets are up to date, few apply the same rigor to patching their OT and CT technologies. Updating software on operational systems, in particular, can present considerable challenges. In many industries, OT assets are outdated and may run discontinued operating systems that cannot be patched. These unpatched systems can result in significant vulnerabilities that put businesses at increased risk as cyberattacks that target OT systems continue to proliferate.

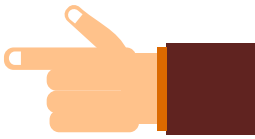
Of course, interconnectivity adds to that vulnerability, as was evident with the outbreak of the NotPetya malware[5], a tool of political warfare. Collateral damage was suffered by hospitals that were unable to treat and assess patients and automobile and pharmaceutical manufacturers that were unable to maintain their production lines.

The problem is compounded when organizations fail to ensure the security capabilities of third-party vendors. Our 2018 Global State of Information Security Survey found that 19% of incidents are attributed to third parties[6].

As more devices produced by more manufacturers flood our increasingly interconnected ecosystem, it is critical that organizations carefully assess the security capabilities of business partners to ensure they comply with current standards. Doing so, however, may stretch the capabilities of many IT and security departments. Already, security personnel are so overwhelmed with frequent, but relatively minor, vulnerabilities that they can fail to address emerging risks that may have significant consequences.

[5]. PwC, *Strategically managing emerging cyber risks*, June 2017
[6]. PwC, *The Global State of Information Security® Survey 2018*, October 2017

Areas leading to new cyber risks: Operational and consumer technologies across key industries



Sector	Operational technology examples	Consumer technology examples
Automotive	Automated manufacturing & logistics	In-vehicle communications & navigation systems, remote diagnostics & maintenance, Highway of the Future
Consumer products	Automated manufacturing & logistics	Home automation & security, smart appliances, wearable devices, smartphones & tablets
Energy & utilities	Generation & transmission, smart grid, intelligent asset management, automated meter reading	Smart meter apps, smart thermostats, digital communications with utilities
Entertainment, media, & communications	Cable distribution networks, broadcasting equipment	Set-top boxes, on-demand services, video streaming
Financial services	ATMs, branch equipment, transaction & payment processing	Online banking, alternative currencies, digital wallets
Healthcare provider/payer	Automated pharmacy dispensing systems, RFID real-time location	Wearable fitness devices, remote-patient monitoring, e-doctor services, patient portals & apps
Pharma and Lifescience	Automated manufacturing & logistics, environmental management	Medical devices, diagnostic tools
Retail & consumer	Point-of-sale systems, RFID inventory management, location-based advertising	Shopping apps, in-store Wi-Fi, digital wallets, e-commerce
Technology	Data centers, cloud services, communications protocols, product life cycle management	Embedded technology & connectivity, consumer cloud services, social networking

Business strategies that can increase security risks

New vulnerabilities also can arise from business strategies that leverage technology advancements to drive innovation and competitive advantage.

Consider, for example, the introduction of implantable patient devices such as pacemakers and glucose monitors. These devices monitor and wirelessly report patient health status to doctors and hospitals. Hackers have demonstrated that they can infiltrate these connected consumer devices, a capability that could result in not only serious health and safety risks, but also data privacy concerns and subsequent legal exposure. In many cases, these types of technologies are deployed before their risks are completely understood, and few healthcare providers are prepared to manage these risks, as indicated by the FDA warning letter[7].

Business strategies that embrace growth via mergers, acquisitions, and joint ventures can also increase the risk inherent in combining technology assets and integrating them under the same security safeguards. In many cases, businesses cannot thoroughly assess the implications of converging the technology assets of multiple organizations in the initial phases of a merger, nor can they immediately understand how to limit access to connected technologies by newly acquired personnel.

The Food and Drug Administration (FDA) has ongoing effort calling for more effective cybersecurity to govern the medical devices that are increasingly connected to the Internet, hospital networks, and to other medical devices to exchange the electronic health information[8]. Similarly, the National Highway Traffic Safety Administration has issued a best practice guidance with layered solutions to ensure modern vehicle systems are designed to take safe actions even when an attack is successful[9].

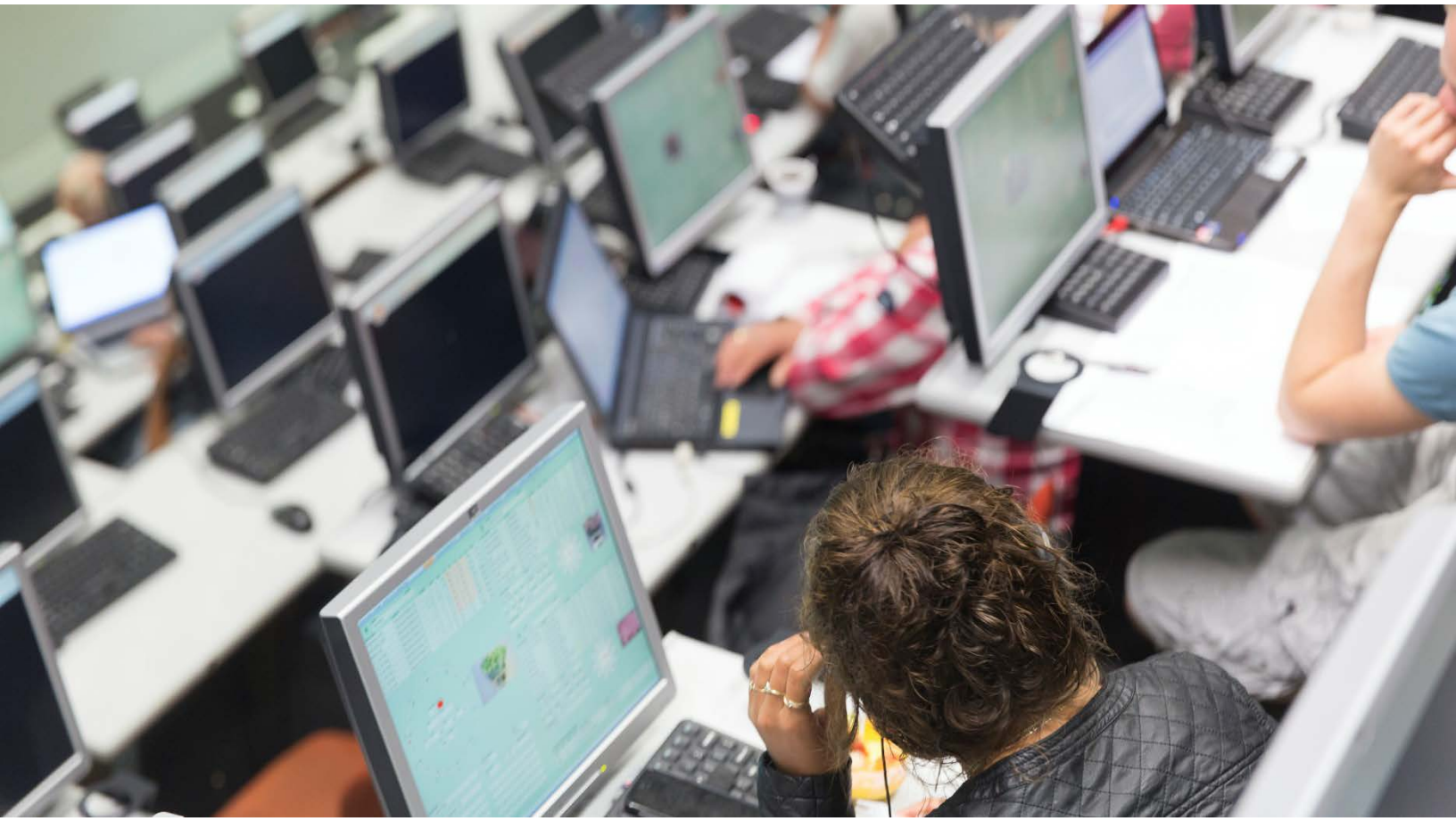
[7]. US Food and Drug, Abbott (St Jude Medical Inc.), April 2017

[8]. Food and Drug Administration, The *FDA's Role in Medical Device Cybersecurity; Postmarket Management of Cybersecurity in Medical Devices*, December 2016;

[9]. National Highway Traffic Safety Administration, *Cybersecurity Best Practices for Modern Vehicles*, October 2016

Given these vulnerabilities, it is inevitable that new regulatory scrutiny and responsibilities will accompany digital convergence. For example, the US National Institute of Standards and Technology (NIST) has developed a Cybersecurity Framework of standards that aims to reduce cyber risks related to critical infrastructure[10]. This framework provides risk-based cybersecurity guidelines that, while voluntary, could increasingly shape expectations for cybersecurity programs in the context of business, as well as in future legal and regulatory investigations. It is now used by a wide variety of public and private companies and organizations, from retail chains to state governments. As a result, security organizations may need to adapt to new regulatory, compliance, and safety requirements. This will be a challenge for many organizations that do not have a holistic view of threats and an integrated approach to managing risk in the operational and consumer environments.

Today's hyperconnected business ecosystem will continue to grow even more intertwined as organizations grow and seek data from their suppliers, customers and partners. Concurrently, the ongoing convergence of IT, OT and CT will continue to propagate throughout your organization's environment and business offerings, adding a plethora of new capabilities to explore and utilize, data to mine and analyze but also can create complex security challenges.



[10]. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, February 2014

Call to action

To meet those challenges head on organizations should take a methodical approach to understanding what their IT, OT, CT environment looks like, what new risks impact their business, how they can work to mitigate those risks, and importantly what steps they can take to make ongoing risk management maintainable. Organizations should:

Understand the risk exposure in your converged environment:

A fundamental step to success is understanding the overall scope of the challenge that the new environment presents. Although organizations have traditionally focused on perhaps just one or two of the IT, OT or CT environments, a more holistic approach to risk assessment is now required. Care should be taken to consider assets from all domains, map interdependencies, and determine the criticality of assets from the perspective of each stakeholder. Such a risk assessment should explore how technology convergence will affect the organization, and then establish an initial set of goals for securing information and operations for future convergence. It is also important to understand what services are being rendered and how, the assets used to render those services, who their owners are and what practices maybe already in place to secure those assets. Without this basic understanding organizations fight an uphill battle against an ever expanding environment and associated attack surface.

Develop an integrated approach to security:

Understand who the stakeholders are across the enterprise, make them aware of the risk and assign responsibility and ownership. Working in tandem with these stakeholders, craft a roadmap to holistically integrate security activities and initiatives across all domains and functions. Such a plan should incorporate and account for the NIST CSF[11] functions of *identify*, *protect*, *detect*, *respond* and *recover*. Given the asymmetric nature of attacks against such converged environments, it will be critical to ensure that forensics and incident-response capabilities are in place to quickly address security incidents that may span multiple technologies and platforms.

Apply appropriate risk based mitigation strategies:

Operational and consumer technologies typically do not lend themselves well to traditional IT centric security approaches for a variety of reasons ranging from different uptime/runtime needs or being of differing asset classes to lacking computing power and residing beyond the corporate edge of an enterprise. Working with assets that cannot be controlled with tried and true IT-centric methodologies often creates unique challenges. These challenges should be *addressed* through a combination of risk management approaches tailored to meet the needs of the organization. At leading organizations, this has taken the form of combining traditional IT security practices with a focus on security beyond the enterprise (such as supply chain security) and leading edge techniques such as Zero Trust Networking, machine learning based network monitoring and advanced network analytics.

[11]. NIST, Cybersecurity Framework, February 2014

Incorporate cybersecurity early into future business planning and development activities: Partnering your enterprise security team and business stakeholders to help understand and manage future business risk can pay dividends in reduced Total Cost of Ownership. Leaders can empower their organization to proactively manage risk (and reduce future costs) by allowing their security professionals to appropriately guide decisions before embarking on costly mistakes.

Continuously monitor and address the risks of change: Design an internal centralized process for monitoring the future integration of the organization's technology or operations against the continually evolving threat landscape, and holistically update security practices across all domains to manage risks that may result from these changes.

To recap, businesses should develop a holistic, cross-functional approach to security that identifies and manages risks across all technology domains. Taken together, the five steps outlined above will set organizations down the path of managing the risks against this converged environment. At the same time, it will likely represent a considerable challenge for many businesses. The advantage will go to those that take action now to build a holistic security model for the convergence of information, operational, and consumer technologies.

www.pwc.com/cybersecurity

Contacts

To have a deeper discussion about security related to the convergence of information, operational, and consumer technologies, please contact:

Michael Compton
Principal, Cybersecurity and Privacy
Email: michael.d.compton@pwc.com

Shafeeq Banthanavasi
Managing Director, Cybersecurity and Privacy
Email: shafeeq.b@pwc.com