www.pwc.com

The convergence of everything digital

How the fusion of information, operational, and consumer technologies will transform the security landscape—for businesses, government, and society

January 2014

Highlights

- Convergence of information (IT), operating (OT), and consumer (CT) technologies will generate sweeping business opportunities—as well as a host of unforeseen security risks. Businesses must balance opportunities with risks, and plan for a dramatically expanded attack surface.
- Operational technologies will continue to converge with IT and CT systems. Security flaws could lead to downtime, theft of IP, or outages of critical infrastructure services.
- Connected consumer technologies, such as home automation, health-monitoring devices, and sensor-based automobiles, are proliferating. As these products and services begin to converge with IT and OT, businesses must plan to deliver consumer technologies in a reliable and secure manner.
- The convergence of three diverse technology ecosystems will create a multifaceted security challenge as the number of attack vectors multiply and interconnect. Companies should understand that all data cannot be safeguarded at the highest level, and be ready to identify and manage new risks.
- Taken together, the risks associated with digital convergence will demand a new, holistic approach to security.

pwc

It goes by many names: The Internet of Things, Machine to Machine Technology, the Internet of Everything, and the Industrial Internet.

Whatever nomenclature ultimately sticks, the convergence of everything digital—information technology (IT), operational technology (OT), and consumer technology (CT)—will unleash a profound force of industrial and personal change, challenge, and opportunity.

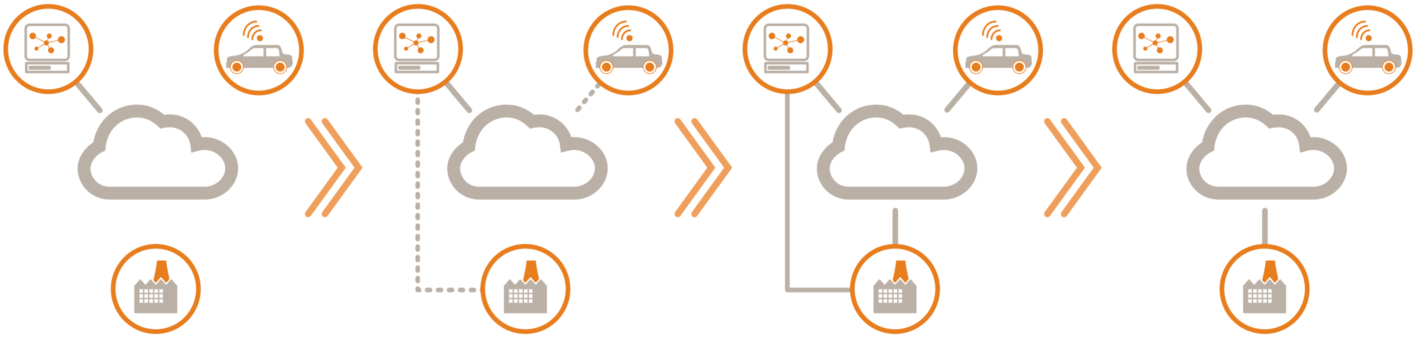
In the near future, converged ecosystems will create a universe of intelligent devices that are interconnected, indirectly or directly, via the Internet. Today, these connected objects include building HVAC systems, manufacturing plants, automobiles, oil and gas production assets, personal medical devices, and automated homes. Tomorrow, they will likely encompass entire cities.

This sweeping metamorphosis is well under way. An estimated 10 billion devices are now connected directly or indirectly to the Internet—and the research firm IDC forecasts an installed base of 212 billion connected devices will be on line by the end of 2020.[1]

Digital convergence is rooted in decades-long technology advances that have fused connections between businesses, operations, data, and people. (Figure 1) In recent years, the unstoppable proliferation of wireless networks, smart phones and tablets, mobile apps, and cloud computing has profoundly enhanced employee productivity, e-commerce capabilities, and consumer lifestyles. At the same time, increasingly inexpensive and miniaturized embedded microprocessors, sensors, and robotics have been deployed across industries to link production and manufacturing assets with industrial control systems, enabling businesses to efficiently manage plants, remote assets, and physical processes.

The convergence of these technologies will create a wealth of business opportunities and ultimately transform relationships with consumers. And it will do so in a very big way: IDC forecasts that the technology and services spending related to digital convergence will generate global revenues of $8.9 trillion by 2020, growing at a compound annual growth rate of 7.9%.[2]

Figure 1:
A concise history of digital convergence



1980's

- 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

1990's

- 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

2000's

- 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 purpose built channels
- OT is no longer protected by obscurity and CT is now vulnerable. Traditional IT security does not cover either

2010's

- 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 must adapt their security model to include the full scope of technologies

Information Technology
Operational Technology
Consumer Technology
Internet
Proprietary Connection
IT Protocol Based Connection

[1] IDC, *Internet of Things (IoT) 2013 to 2020 Market Analysis: Billions of Things, Trillions of Dollars,* October 2013

[2] Ibid.

The downside? Pervasive convergence will introduce a new world of security risks for businesses. The attack surface—the points in which cyber adversaries attempt to access data, applications, and systems—will expand exponentially, moving beyond traditional information security targets to encompass disparate assets associated with operational and consumer technologies.

Consider, for instance, the automobile. Cars today contain dozens of computers that are often connected to the Internet via cellular technology. Hackers have proved they can infiltrate these embedded computers to take control of the brakes, the steering wheel, and even the engine. What's more, some connected cars automatically link back to the manufacturer's IT and OT systems for actions like firmware updates, maintenance monitoring, and real-time communications. Behind the scenes, automakers are beginning to connect OT plant-manufacturing systems to their IT environment to integrate with enterprise requirements planning and supply chain management solutions. The result? Individual cars, IT systems, and OT machinery are increasingly vulnerable to attack as they are interconnected via the Internet.

As the risks of convergence multiply across a sprawling ecosystem of connected technologies, one thing is certain: Yesterday's security practices cannot effectively address even today's threats, much less the elevated risks of tomorrow. In this converging environment, safeguarding all data at the highest level is no longer realistic or even possible; rather, organizations should anticipate threats and resiliently identify and manage the associated risks. What is needed is a new model of security, one that is based on a disciplined approach to identifying and managing risks across assets in information, operational, and consumer technologies.

Prepare for new threats and broader security impacts

The convergence of information, operational, and consumer technology ecosystems will transform the very nature of security risks. It will also open new opportunities for cyber attack that may have serious consequences to security, business operations, and public safety.

Today's interconnected global business ecosystem, which often comprises partners, suppliers, supply chains, and customers, is increasingly vulnerable as an ever-greater volume of data flows through digital channels. As noted, this has expanded the attack surface and profoundly elevated the threat environment, trends that will broaden as operational and consumer technologies become more intertwined with IT. (Figure 2) In a converged ecosystem, for instance, adversaries may leverage IT vulnerabilities as a means to compromise operational and consumer technology processes, and vice versa.

As the attack surface expands, so too will security incidents. This year, for instance, the number of detected incidents increased by 25% over 2012, according to The Global State of Information Security® Survey 2014, a worldwide study of more than 9,600 executives conducted by PwC, *CIO* magazine, and *CSO* magazine.[3]

We believe that operational technologies, such as process automation systems that run a plant, may be vulnerable to the most serious security risks. Increasingly, functions in industrial businesses rely on process automation, and as these systems are connected to the Internet they may elevate risks of operational downtime, theft of intellectual property, and supply chain disruption, to name a few.

An additional OT risk: Unpatched software on far-flung or inaccessible embedded devices. In some industries, these OT assets

Defining the basics of convergence

Information technology traditionally comprises resources and connectivity for processing and managing data to support business functions and transactions. Its goal is to ensure the confidentiality, integrity, and availability of data and systems. IT includes systems such as enterprise resource planning, HR management, customer service, and corporate e-mail.

[3] PwC, *The Global State of Information Security® Survey 2014,* September 2013

Operational technology is typically defined as systems and related automation assets that monitor and control physical equipment and events. Physical control of an object, such as shutting off a valve in a manufacturing plant, is key to OT. Historically, operational systems have been managed and maintained separately from IT. That’s starting to change, however, as businesses begin to mesh OT and IT and connect the two via internal networks or the Internet. OT includes systems such as manufacturing plant machinery and HVAC for large corporate facilities.

Consumer technology encompasses the explosive adoption of smartphones, tablets, health- and fitness-monitoring devices, location-aware services, and gaming networks, to name a few. Ubiquitous connectivity and advanced mobility, combined with the boom in cloud-based services, has further fueled the surge of consumer products. Today, manufacturers continue to add features to their products and services to deliver greater choices and convenience for tech-obsessed consumers. Technologies such as near field communication (NFC), radio-frequency identification (RFID), and Bluetooth Low Energy are enabling a new wave of products like digital wallets and wireless audio speakers.

are outdated and may run discontinued operating systems that cannot be patched. What’s more, field devices are often deployed in remote—and often rugged—geographic locations, further complicating firmware patches.

Unpatched systems may put businesses at serious risk as cyber attacks targeting OT systems continue to proliferate. This is a particular concern among industries that provide critical infrastructure services such as transportation, energy, telecommunications, and defense. As Stuxnet, the 2010 worm that targeted Iran’s nuclear facilities, so conclusively proved, cyber adversaries are targeting industrial control systems to monitor and take control of manufacturing processes.[4]

Compounding matters, the addition of consumer technologies to the mix will introduce new categories of risk with potentially serious implications for security, business reputation, and public safety. Hackers have demonstrated, for instance, that they can compromise connected consumer devices such as pacemakers implanted in heart patients, which could result in potentially deadly health and safety risks. And as utilities implement smart grid technologies and enable customers to access usage data from their smartphones, they may open new avenues of attack on the power grid.

Figure 2:
The impact of digital convergence across industries

Sector	*IT*	*OT*	*CT*	***Examples of OT/CT***
Automotive	✓	✓	✓	Automated manufacturing processes Automobiles
Consumer products	✓	✓	✓	Automated manufacturing End products
Power generation/ utilities	✓	✓	✓	Equipment (generation and transmission) Smart meter apps
Energy/oil & gas	✓	✓		Equipment (drilling, refining, transportation)
Entertainment, media and communications	✓	✓	✓	Broadcasting equipment Set top boxes, handsets
Financial services	✓	✓	✓	ATMs, branch equipment Online and mobile banking
Healthcare provider/ payor	✓	✓	✓	Networked equipment, paperless medical records, embedded medical devices, patient portals and apps
Retail and consumer	✓	✓		Point of sale systems, online shopping
Technology	✓	✓	✓	Datacenters/cloud services Software, home networking equipment
	WAS USED	BEING USED		

[4] Symantec Corp., *W32.Stuxnet Dossier,* Feb. 2011

Already, the world's cybercriminals are starting to write malware designed to compromise consumer devices as a means to gain a beachhead to connected OT and IT systems. Symantec recently identified a new worm called Linux.Darlloz that targets connected devices such as security cameras and home routers running the Linux operating system.[5] This type of threat is particularly pernicious because many consumers are unaware of security risks, even as the volume of malware continues to multiply. In fact, computer security firm Kaspersky Lab detected 315,000 new malicious files a day in 2013, up from 200,000 a day the year before.[6]

Certain consumer technologies, when linked to IT and OT systems, will also elevate data-privacy concerns. In a healthcare ecosystem, for instance, an attack on embedded monitoring systems that report patient health status to hospitals and doctors may expose personal data and compromise privacy regulations.

Indeed, digital convergence will inevitably lead to new regulatory risks and responsibilities. Already the US Food and Drug Administration (FDA) has called for more effective cybersecurity to govern connected medical devices and the electronic exchange of health information. Similar regulations are likely in other industries. State legislatures, for instance, are considering rules for self-driving cars and the National Highway Traffic Safety Administration has issued a preliminary policy.[7]

Managing the security challenges of convergence

61%

of global organizations have deployed asset-management tools.

In a converged—and connected—ecosystem, the security function will no longer be defined by information, and security objectives will differ among technologies. Consequently, a connected ecosystem will require an integrated approach to security, one that is predicated on holistic thinking, preparedness, and contingency planning.

This new model of security will require that differing security objectives for each type of technology are carefully assessed according to business needs and risks. Information security, for instance, focuses on data confidentiality, integrity, and availability. Operational security is primarily concerned with reliable and efficient operations of manufacturing systems, as well as health, safety, and environmental issues. Consumer security centers on public safety and privacy concerns.

Rethinking security strategy to address all these objectives will be an ambitious agenda.

As the category and number of these assets multiply, asset identification and management will become increasingly important. Today, many organizations do not adequately manage their IT assets, much less disparate and undefined operational and consumer assets. In fact, our research shows that only 61% of global organizations have deployed asset-management tools.[8]

An effective asset-management program will require that businesses look beyond traditional IT equipment and fully scrutinize every asset required to deliver a service, including intangibles such as third-party relationships or Internet connections. Once identified, it is imperative that businesses ensure that management of assets and risks is carried out with disciplined standards across all divisions.

[5] Symantec Corp., *Linux Worm Targeting Hidden Devices,* Nov. 27, 2013

[6] Kaspersky Lab, *Number of the year: Kaspersky Lab is detecting 315,000 new malicious files every day,* Dec. 10, 2013

[7] http://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action#cite_note-0

[8] PwC, *The Global State of Information Security® Survey 2014,* September 2013

A further challenge lies in the paucity of security and interoperability standards among the three technology ecosystems. We are seeing new calls for security standards, but they do not yet address the convergence of information, operational, and consumer technologies.

The responsibility for driving and managing convergence initiatives will likely fall to the CIO. Gartner forecasts that by 2015, more than 70% of CIOs will oversee connected performance of all digital technologies.[9] Already, many CIOs are adding OT responsibilities to their portfolio as operational technology is increasingly connected to corporate IT. In the future, the CIO may be expected to lead more processes, information resources, and relationships across more areas of the enterprise.

And that may warrant a restructuring of the IT organization to align operational and consumer technology stakeholders. An integrated security function will enable IT personnel to collaboratively work with OT and consumer technology divisions as a team, formally or informally. We believe that effective communications among these groups and a common culture among IT, engineering, operations, and marketing teams will be critical to the success of the security program.

Why holistic security matters more than ever

As billions of connected devices converge across information, operational, and consumer ecosystems, businesses should assess their mix of technologies and craft an integrated, holistic strategy to secure them.

We believe that businesses should disregard concerns about organizational structure and start by creating a steering committee headed by an enterprise-wide chief security officer. This committee should comprise, at a minimum, leaders from IT security, physical security, operational technologies, and consumer products.

These committees should define ownership of security risk and accountability for information, operational, and consumer technologies. It also will be necessary to align standards and processes of these technologies, as well as ensure workable relationships and roles between the IT and OT groups, in particular. Incident response should be an integral part of the security practice, one that is regularly updated and practiced.

At the same time, it is increasingly critical that business leaders view cyber threats as enterprise risk-management issues that could severely impact their business objectives, operational stability, reputation, and ultimately public safety. Security must become a foundational component of the business strategy, one that is championed by the CEO and board, and adequately funded.

As technologies converge, knowledge demands will increase. Organizations should understand the new threats they face, as well as the goals of adversaries and the evolving techniques they may employ. In addition, the security function may be asked to help protect consumers' data on mobile apps and devices, and to help ensure the safety of customers who use the company's consumer products.

Doing so will require a new commitment to collaboration, internally and externally, to share security intelligence and threat awareness. Our research shows that 50% of companies currently collaborate with others to improve security.[10] That's a good start, but the convergence of digital ecosystems will require a deeper commitment to knowledge sharing.

Finally, no security strategy will succeed without employee security awareness and training programs. Convergence will bring new threat vectors and new risks, and it is critical that all employees receive on-going training on current threats and best practices for security.

50%

of companies currently collaborate with others to improve security

[9] Gartner, *Top 10 Strategic Technology Trends for 2013,* October 2012

[10] PwC, *The Global State of Information Security® Survey 2014,* September 2013

It’s time to act

The convergence of information, operational, and consumer technologies is unstoppable. The potential benefits to businesses and consumers alike are simply too great to ignore.

So, too, is the need for a new approach to security.

One of the first steps will be to create an asset-management program that extends beyond IT to all relevant areas of the enterprise. As operational and consumer technologies are added to the ecosystem, it will be necessary to meticulously explore the technology environment and identify new assets. These assets should be managed using standard risk-management processes across all business units.

A comprehensive asset-management program will enable businesses to fully understand the features, functions, and security risks of all devices across the extended ecosystem. Beyond that, it will be necessary to identify processes the each asset supports, to which assets the device connects, and the context and location in which they operate.

A complete self-assessment of connected assets will require a very broad view, particularly when assessing operational technologies. It is critical that organizations fully understand the potential impact of an OT-related incident on business operations, consumer safety, critical infrastructure, and the environment.

Only then can they begin to apply traditional security concepts, business process controls, and technology safeguards to all assets and devices cross the ecosystem. Doing so will demand a disciplined assessment and alignment of current and future business objectives.

It will also require an unflagging commitment to collaboration among business units. Each division will have specialized knowledge of security processes and technologies that will be key to an integrated program. The NIST cybersecurity framework, in fact, encourages collaboration among internal and external stakeholders to share information on evolving risks, best practices, and incidence-response tactics.

It is imperative that organizations establish appropriate, effective requirements for governance, procurement, and the supply chain—and that security is built into these functions. When purchasing equipment from third-party suppliers, for instance, ask for written details explaining the security risks and capabilities of each device. Because security personnel will not be involved in all purchases, it may be beneficial to provide procurement teams with written guidelines for evaluating devices.

Careful planning and implementation notwithstanding, no security program is foolproof. Forensics and incident-response capabilities are absolutely critical to address attacks that may span multiple technologies and platforms. An integrated security incident-response program should be implemented and regularly tested across divisions.

Finally, it’s important to note that creating a security framework for the convergence of everything digital will not succeed without support of the C-suite and Board. We believe that security professionals are uniquely qualified to champion a new model of security and ensure that digital convergence becomes an integral part of the business agenda.

5 questions you should be asking now

1. How does your process to identify and manage assets integrate nontraditional assets such as operational and consumer technologies?
2. Do you fully understand the features, functions, and security risks of existing information, operational, and consumer technologies?
3. How will you integrate digital convergence and security with current and future business objectives?
4. Is your approach to governance and security built on proactive collaboration between stakeholders in information, operational, and consumer divisions?
5. Do you have a full understanding of the impact of an OT-related incident in your environment?

Contacts

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

David Burg
Principal, PwC
(703) 918-1067
david.b.burg@us.pwc.com

Michael Compton
Principal, PwC
(313) 394-3535
michael.d.compton@us.pwc.com

Peter Harries
Principal, PwC
(213) 356-6760
peter.harries@us.pwc.com

John D Hunt
Principal, PwC
(703) 918-3767
john.d.hunt@us.pwc.com

Gary Loveland
Principal, PwC
(949) 437-5380
gary.loveland@us.pwc.com

Joseph Nocera
Principal, PwC
(312) 298-2745
joseph.nocera@us.pwc.com

David Roath
Partner, PwC
(646) 471-5876
david.roath@us.pwc.com

PricewaterhouseCoopers has exercised reasonable care in the collecting, processing, and reporting of this information but has not independently verified, validated, or audited the data to verify the accuracy or completeness of the information. PricewaterhouseCoopers gives no express or implied warranties, including but not limited to any warranties of merchantability or fitness for a particular purpose or use and shall not be liable to any entity or person using this document, or have any liability with respect to this document. BS-14-0228-A-12.13