Gartner

G00259020

What Securing the Internet of Things Means for CISOs

Published: 11 April 2014

Analyst(s): Earl Perkins

The Internet of Things redefines security by expanding the scope of responsibility into new platforms, services and directions. CISOs should focus existing security resources on specific use cases to identify new patterns for Internet of Things security solutions.

Impacts

- The power of an Internet of Things (IoT) object to change the state of environments — in addition to generating information — will cause chief information security officers (CISOs) to redefine the scope of their security efforts beyond present responsibilities.
- Most IoT devices and services may be Nexus of Forces-driven, but CISOs will be dealing simultaneously with all past eras of technology to secure the necessary scale and complexity that an IoT world demands.
- IoT security needs will be driven by specific business use cases that are resistant to categorization, compelling CISOs to prioritize initial implementations of IoT scenarios by tactical risk.
- The requirements for securing the IoT will be complex, forcing CISOs to use a blend of approaches from mobile and cloud architectures, combined with industrial control, automation and physical security.

Recommendations

- Deconstruct your current principles of IT security in the enterprise — the "information" mold and context of IT are too limiting. Expand technology security planning and architecture to include new (and old) technology and service delivery platforms and patterns.
- Evaluate incoming IoT security requirements that account for possible combinations of mainframe, client/server, Web, cloud and mobile security needs, which are impacted by operational technology (OT) and physical security in specific use cases.

- Do not overthink IoT security planning. Develop initial IoT security projects based on specific, even tactical, business risk profiles, then build on those experiences to develop common security deployment scenarios, core architectural foundations and responsibilities.
- Leverage current bring your own device (BYOD), mobile, cloud, OT, and physical security governance, management and operations for IoT use cases. Monitor adoption of key IoT-specific wireless-communication-, hardware-, connected-device- and cloud-based platforms.

Strategic Planning Assumption

IoT security requirements will reshape and expand over half of all global enterprise IT security programs by 2020 due to changes in supported platform and service scale, diversity and function.

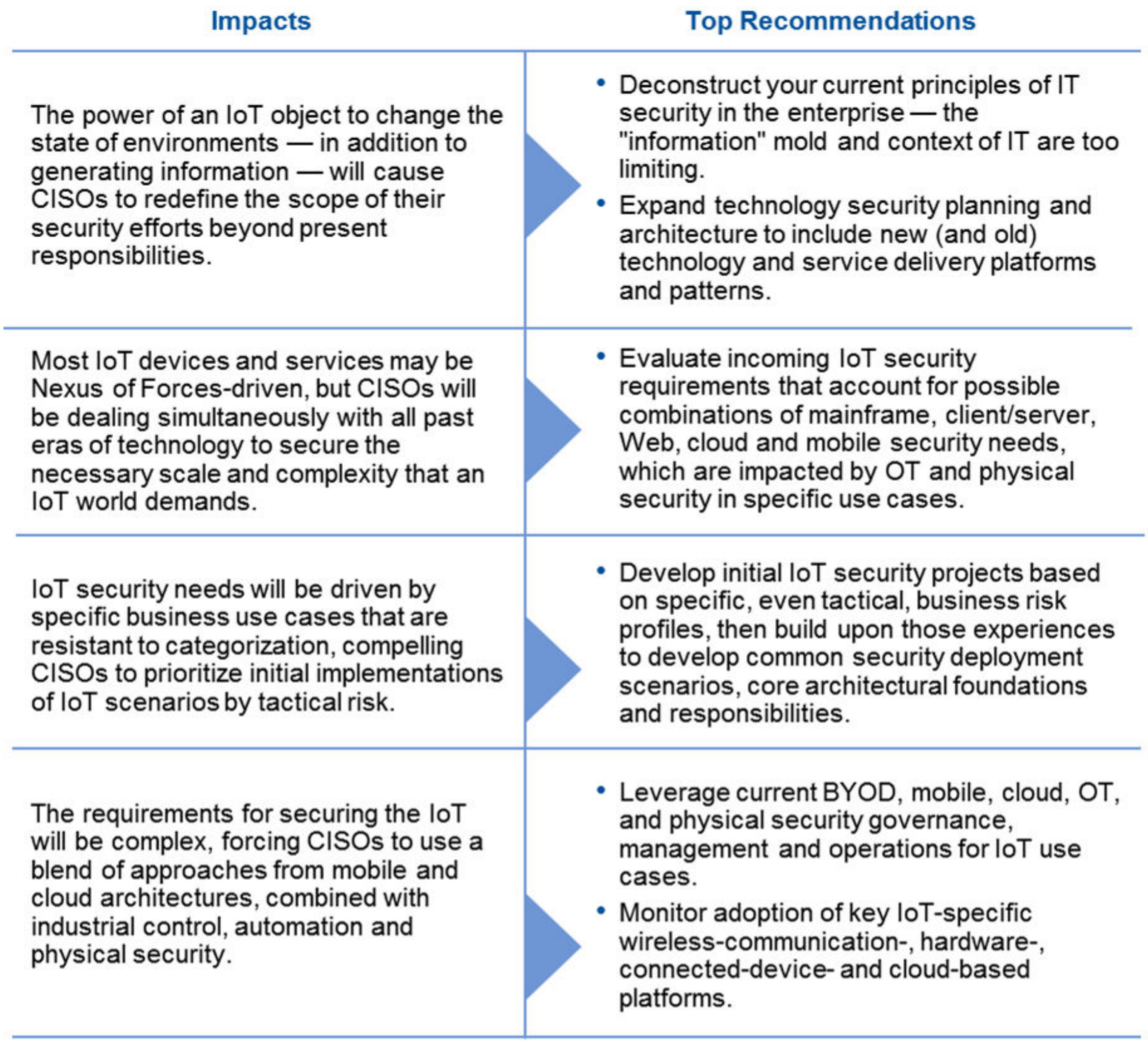
Analysis

In an IoT world, information is the "fuel" that is used to change the physical state of environments through devices that are not general-purpose computers but, instead, devices and services that are designed for specific purposes. The IoT is a conspicuous inflection point for IT security — and the CISO will be on the front lines of its emerging and complex governance and management. Gartner's Nexus of Forces — cloud, social, mobile and information — is driving early-state opportunities in the IoT. The IoT has a myriad of commercial and consumer technology use cases that range from connected homes and connected automobiles to wearable devices to intelligent medical equipment to sensor systems for smart cities and facilities management (see "The Potential Size and Diversity of the Internet of Things Mask Immediate Opportunities for IT Leaders"). The characteristics of intelligent, purpose-built devices that are networked to provide information and state changes for themselves or surrounding environments are increasingly used in OT systems, such as those found in industrial control and automation (sometimes referred to as the "industrial IoT"). But securing the IoT represents new CISO challenges in terms of the type, scale and complexity of the technologies and services that are required.

The IoT endpoints extend across the perimeter (and between third parties) to externally controlled appliances, customers and sensory-based technology that challenge traditional, layered-protection security management. In Gartner's security and risk management scenario for 2020 (see "Security and Risk Management Scenario Planning, 2020"), the target axis moves between the enterprise and the individual. Securing the IoT impacts both targets. It does not take much imagination to see the compromising impact of powering down or affecting millions of devices through a single IoT vulnerability — potentially resulting in physical damage to environments, injuries or death.

Although an IoT device may seem new and unique, a hybrid of old and new technology infrastructure enables the services that the device consumes to perform. Securing the IoT will force most enterprises to use old *and* new technologies from all eras (mainframe, client/server, Web, cloud and mobile) to secure devices and services that are integrated via specific business use cases. This also means that many of yesterday's problems will make their way into the IoT. CISOs will play an increased role in physical security responsibilities as present-day IT systems, legacy IT infrastructure, OT and the IoT become more automated and dependent on secure facilities to function. CISOs must balance specific business drivers with scalable security governance and management in a coming era that will be dominated by sensors, embedded systems, machine-to-machine (M2M) communications and purpose-built devices.

Figure 1. Impacts and Top Recommendations for CISOs



Impacts	Top Recommendations
The power of an IoT object to change the state of environments — in addition to generating information — will cause CISOs to redefine the scope of their security efforts beyond present responsibilities.	• Deconstruct your current principles of IT security in the enterprise — the "information" mold and context of IT are too limiting. • Expand technology security planning and architecture to include new (and old) technology and service delivery platforms and patterns.
Most IoT devices and services may be Nexus of Forces-driven, but CISOs will be dealing simultaneously with all past eras of technology to secure the necessary scale and complexity that an IoT world demands.	• Evaluate incoming IoT security requirements that account for possible combinations of mainframe, client/server, Web, cloud and mobile security needs, which are impacted by OT and physical security in specific use cases.
IoT security needs will be driven by specific business use cases that are resistant to categorization, compelling CISOs to prioritize initial implementations of IoT scenarios by tactical risk.	• Develop initial IoT security projects based on specific, even tactical, business risk profiles, then build upon those experiences to develop common security deployment scenarios, core architectural foundations and responsibilities.
The requirements for securing the IoT will be complex, forcing CISOs to use a blend of approaches from mobile and cloud architectures, combined with industrial control, automation and physical security.	• Leverage current BYOD, mobile, cloud, OT, and physical security governance, management and operations for IoT use cases. • Monitor adoption of key IoT-specific wireless-communication-, hardware-, connected-device- and cloud-based platforms.

Source: Gartner (April 2014)

Impacts and Recommendations

The power of an IoT object to change the state of environments — in addition to generating information — will cause CISOs to redefine the scope of their security efforts beyond present responsibilities

The IoT is redrawing the lines of IT responsibilities for the enterprise. IoT objects possess the ability to change the state of the environment around them, or even their own state (for example, by raising the temperature of a room automatically once a sensor has determined it is too cold or by adjusting the flow of fluids to a patient in a hospital bed based on information about the patient's medical records). Securing the IoT expands the responsibility of the traditional IT security practice with every new identifying, sensing and communicating device that is added for each new business use case, particularly if device operations have such impacts. Integrity (that is, correct functionality) is more critical for environment-changing systems that are people-impactful than it is for information alone. "Information" technology is now being supplemented by purpose-built, industry-specific technologies that are tailored by where and how a device is used and what function it delivers. Information remains a key deliverable — information is the fuel for IoT devices. Their ability to identify themselves (such as RFID tags that identify cargo), sense the environment (such as temperature and pressure sensors) or communicate (such as devices in ocean buoys that transmit environmental changes to the areas around them) requires information to be generated, communicated and/or used.

Although traditional IT infrastructure is capable of many of these functions, functions delivered as purpose-built platforms using embedded technology, sensors and M2M communications for specific business use cases signal a change in the traditional concept of IT and hence the concept of securing IT. For example, process, storage and power limitations on low-cost devices with minimal memory and processing power will curtail agent-based security solutions. Real-time, event-driven applications and nonstandard protocols will require changes to application testing, vulnerability, and identity and access management (IAM) approaches. Handling network scale, data transfer methods and memory usage differences will also require changes. Governance, management and operations of security functions will need to be significant to accommodate expanded responsibilities, similar to the ways that BYOD, mobile and cloud computing delivery have required changes — but on a much larger scale and in greater breadth. IT will learn much from its OT predecessors in handling this new environment. This is an inflection point for security.

Recommendations:

- Deconstruct your current principles of IT security in the enterprise by re-evaluating practices and processes in light of the IoT impact — the "information" mold and context of IT are too limiting.
- Expand IT security planning and architecture to incorporate new (and old) technology and service delivery platforms.

Most IoT devices and services may be Nexus of Forces-based, but CISOs will be dealing simultaneously with all past eras of technology to secure the necessary scale and complexity that an IoT world demands

Many CISOs mistakenly believe that the IoT consists of all new technologies and services. Although the business use cases being identified daily are indeed innovative and new, the technologies and services that deliver them are seldom new as well as seldom uniform in architecture and design. Each use case risk profile has specific requirements that may result in the use of old platform and service architecture with a new technology "overlay" to improve performance and control. This represents an interesting challenge for CISOs when delivering secure services for the IoT. In some cases, it may be a "past is future" exercise in evaluating mainframe, client/server, Web, cloud and mobile security options as part of an overall IoT business use case. Even out-of-maintenance systems such as Windows XP may still play a critical role for some industry infrastructure as part of an IoT security system. Security planners should not throw away their old security technology manuals just yet.

CISOs should not automatically assume that existing security technologies and services must be replaced; instead, they should evaluate the potential of integrating new security solutions with old. Many traditional security product and service providers are already expanding their existing portfolios to incorporate basic support for embedded systems and M2M communications, including support for communications protocols, application security and IAM requirements that are specific to the IoT. There are increasing options for delivering OT security to supplement IT security, focusing on areas such as threat detection and response and vulnerability management. In addition, solution providers for areas such as connected home, facilities management and physical access control are using IoT devices for physical security as well as providing security management and operations solutions for networks of the IoT. Unfortunately, there is equal opportunity for the security product and service industry to repeat undesirable history by inadequately incorporating security capabilities during the manufacturing and software development period.

Recommendation:

- Evaluate incoming IoT security requirements that account for possible concurrent combinations of mainframe, client/server, Web, cloud and mobile security needs, which are impacted by OT and physical security in specific use cases.

IoT security needs will be driven by specific business uses cases that are resistant to categorization, compelling CISOs to prioritize security implementations of IoT scenarios by tactical risk

At this time, there is no "guide to securing IoT" available that provides CISOs with a framework for incorporating IoT principles across all industries and use cases. Another unique characteristic of the IoT is the sheer number of possible combinations of device technologies and services that can be applied to those use cases. What constitutes an IoT object is still up for interpretation, so securing the IoT is a "moving target." However, it is possible for CISOs to establish an interim planning strategy, one that takes advantage of the "bottom up" approach available today for securing the IoT. Security leaders should not overthink IoT security by attempting to draft a grand strategy that encompasses all IoT security needs to this point in time. Lower the residual risk of the IoT by assessing whether your particular business use case provides better control and performance.

Enterprises can be considered part of the IoT if they are using devices that:

- Are networked for communication on private networks, public networks or the Internet
- Have some capacity to identify, sense and/or communicate information about a device itself or the state of the environment in which the device resides

CISOs will find that devices that use sensors, use some form of M2M communications for most functions, are built with embedded systems and have a means of being identified will appear increasingly in specific business use cases. CISOs must establish a presence in the early planning cycles for those use cases. Leverage planning results to identify any common security design components that can use existing security solutions or that require specialized technology or services to meet security policy requirements of the enterprise. After working with several use cases, a pattern of security requirements that is consistent with the specific industry of the enterprise should emerge to allow the CISO to develop core security services for safeguarding IoT in subsequent projects.

Recommendations:

- Do not overthink IoT security planning — patterns and solutions are still evolving. Start small.
- For now, develop initial security projects based on specific IoT interactions within specific business use cases. As a result, seek to define ownership and responsibility areas for security.
- Build on these use case experiences to develop common security deployment scenarios, core architectural foundations and a competency center for the future.

The requirements for securing the IoT will be complex, forcing CISOs to use a blend of approaches from mobile and cloud architectures, combined with industrial control, automation and physical security

Fortunately, many of the security requirements for the IoT will look familiar to the CISO. The technologies and services that have been used for decades to secure different eras of computing are still applicable in most cases. For example, past planning in mobile security and BYOD will be applicable because many of the IoT devices can be protected with mobile security solutions and IoT devices may be managed within BYOD frameworks (see "Securing Business Data on Bring Your Own PCs and Macs"). CISOs will also find that, even though there may be complexity that is introduced by the scale of the IoT use case or the unusual operating system, communications protocol or embedded firmware requirements, the core principles of data, application, network, systems and hardware security are still applicable. However, there will be differences in governance, risk, management and operations.

For enterprises with significant OT assets (such as manufacturing, energy and utilities, chemical, transportation or healthcare), there will also be additional complexity for the CISO. Many OT security requirements engage physical security practices, including health and safety systems, perimeter surveillance, physical access control and facilities management. IT planners have paid too little attention to the growth of these requirements. CISOs must be prepared for those use cases involving the IoT where OT and physical security requirements will be part of the end-to-end solution and coordinate accordingly. Enterprises with OT assets are increasingly converging, aligning and integrating their IT and OT security teams (see "How to Organize IT/OT Security for Success"), which will also impact governance and planning efforts for securing the IoT.

Recommendations:

- Leverage current BYOD, mobile, cloud, OT, and physical security governance, management and operations to consider the IoT use cases as your enterprise deploys them.
- CISOs should direct their staff members to monitor progress in the following technologies to ensure an understanding of security requirements:
  - Wireless technologies and standards, such as ZigBee and Modbus
  - Hardware platforms, such as Arduino and TMote Sky
  - Connected-device software platforms, such as TinyOS and Android
  - Cloud application software platforms, such as ThingWorx and Evrythng

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"How to Organize IT/OT Security for Success"

"The Potential Size and Diversity of the Internet of Things Mask Immediate Opportunities for IT Leaders"

"Forecast: The Internet of Things, Worldwide, 2013"

"Uncover Value From the Internet of Things With the Four Fundamental Usage Scenarios"

"Security and Risk Management Scenario Planning, 2020"

"The Impact of the Internet of Things on Data Centers"

"Securing Business Data on Bring Your Own PCs and Macs"

Evidence

O. Mazhelis and others, "Internet-of-Things Market, Value Networks, and Business Models: State of the Art Report," University of Jyväskylä, Department of Computer Science and Information Systems, 2013.

T. Brewster, "There Are Real and Present Dangers Around the Internet of Things," The Guardian, 20 March 2014.

S. Rodriguez, "Refrigerator Among Devices Hacked in Internet of Things Cyber Attack," The Los Angeles Times, 16 January 2014.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity."