IoT Security Primer: Challenges and Emerging Practices

Information Risk Research Team

Refreshed 6 January 2020
Published 15 July 2018

Gartner®

Gartner

IoT Security Primer: Challenges and Emerging Practices

Peer & Practitioner Research Refreshed 6 January 2020, Published 15 July 2018 - ID G00355851 - 27 min read

FOUNDATIONAL This research is reviewed periodically for accuracy.

Initiatives:Infrastructure Security

Organizations use the Internet of Things (IoT) to create value, reduce costs, or streamline operations. While IoT devices create business opportunities, they also create information risks. We examine IoT security practices and summarize how CISOs currently define, manage, and prepare for IoT risks.

Overview

Over 80% of organizations currently use The Internet of Things (IoT) to solve business use cases, yet less than one-third of CISOs are confident Information Security can reliably assess and mitigate IoT risk. CISOs must take steps to better understand and categorize IoT risk and then develop mitigation strategies that best serve their broader organizations.

Key Findings

- Almost 20% of organizations have already detected an IoT-based attack.
- Almost all organizations are exposed to IoT risk—even those that attempt to block IoT.
- Information Security's largest IoT challenge is poor visibility and understanding of IoT devices and how the organization uses them.
- Information Security functions have ambitious plans to adopt IoT-centric controls, processes, and governance over the next 12 to 18 months.

Recommendations

Leading CISOs take the following steps to define and build IoT risk management capabilities:

- Understand how the organization and its employees currently use and plan to use IoT to achieve business opportunities.
- Define and categorize the types of IoT risks the organization faces. These risks include external, buy-side, and sell-side IoT risks.
- Clarify Information Security's role in IoT risk management and work with other risk management functions (e.g., Legal, Privacy, Procurement) to define cross-functional roles and responsibilities.
- Recognize the IoT security challenges Information Security faces and develop a plan that addresses these challenges. The top IoT security challenges include poor visibility and understanding, lack of standardization, and poor vendor support and security practices.
- Develop a portfolio of IoT controls and mitigation strategies based on the advice and benchmarked plans of leading peers.

Introduction

The Internet of things (IoT) is now an Information Security priority. IoT adoption continues to grow exponentially, senior executives view IoT as an opportunity for digital transformation, and many organizations already detect IoT-based attacks.

The Internet of Things (IoT) is not a new concept, but until recently it was not a major concern for most Information Security leaders. Historically, IoT adoption was low, especially for critical enterprise applications. Furthermore, IoT devices were not viewed as attractive targets for adversaries; data breaches and DDoS attacks typically targeted traditional servers rather than new types of connected devices.

Internet of Things (IoT): The phenomenon of pervasive computing; the growing trend of embedding computational capability, data-collecting sensors, and internet connectivity into everyday objects

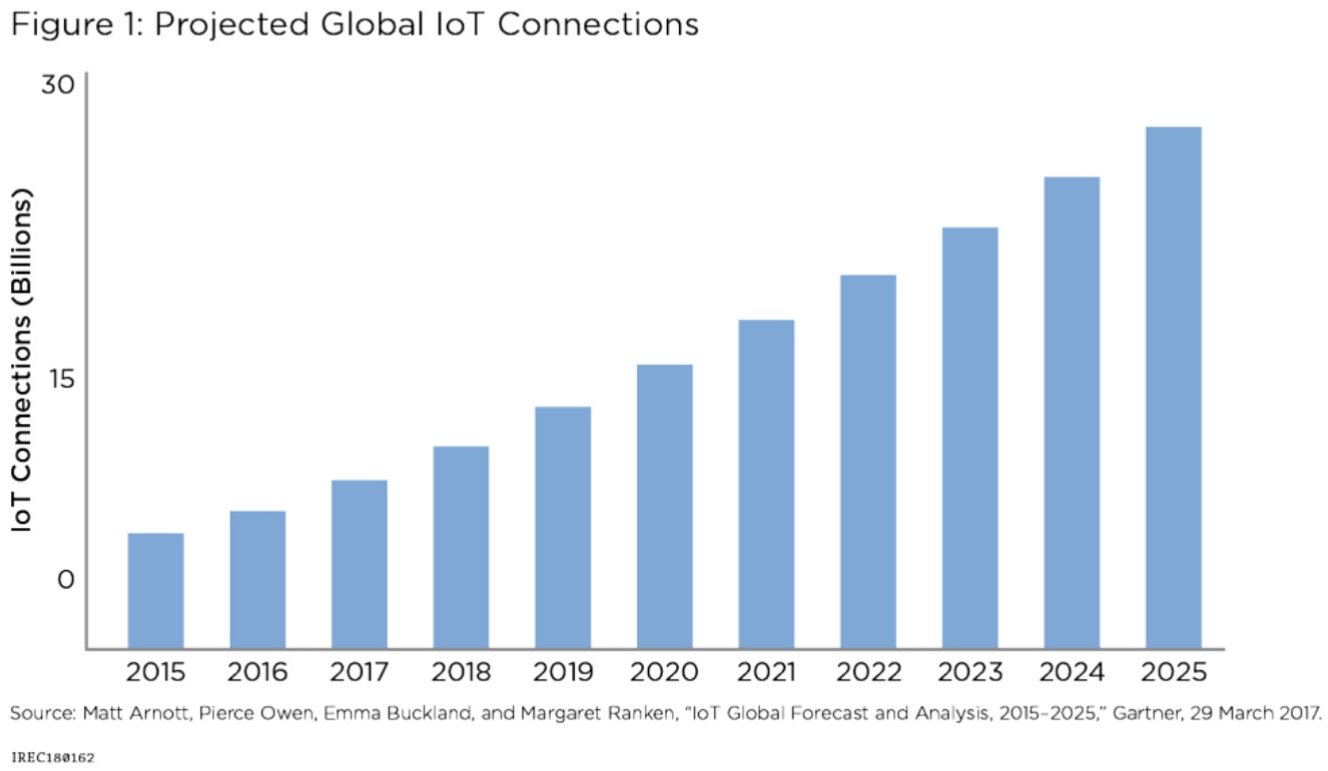
This is changing. Over 80% of organizations currently use IoT to solve business use cases, and almost 20% of organizations have already detected an IoT-based attack in the past three years.

Looking ahead, IoT risk is poised to multiply at most organizations. The number of global IoT connections continues to grow exponentially and will reach 25 billion by 2025. Yet less than one-third of Information Security professionals are confident in their function's ability to reliably assess or mitigate IoT risk.

Our research reveals three trends that make IoT security a key priority for CISOs in 2018 and beyond:

1. Exponential Growth in IoT Adoption by Organizations—The market for IoT devices will grow exponentially over the next decade. For example, projections estimate that the number of IoT connections will grow from 6 million in 2015 to a whopping 27 billion in 2025 (figure 1), which represents a 16% year-over-year growth rate over the next decade. Furthermore, we estimate that more than half of major new business processes and systems in 2020 will incorporate some element of IoT.[1] This growth means not only *more* IoT devices but also greater *variety* in the types of devices employees need to get work done and organizations use to grow.

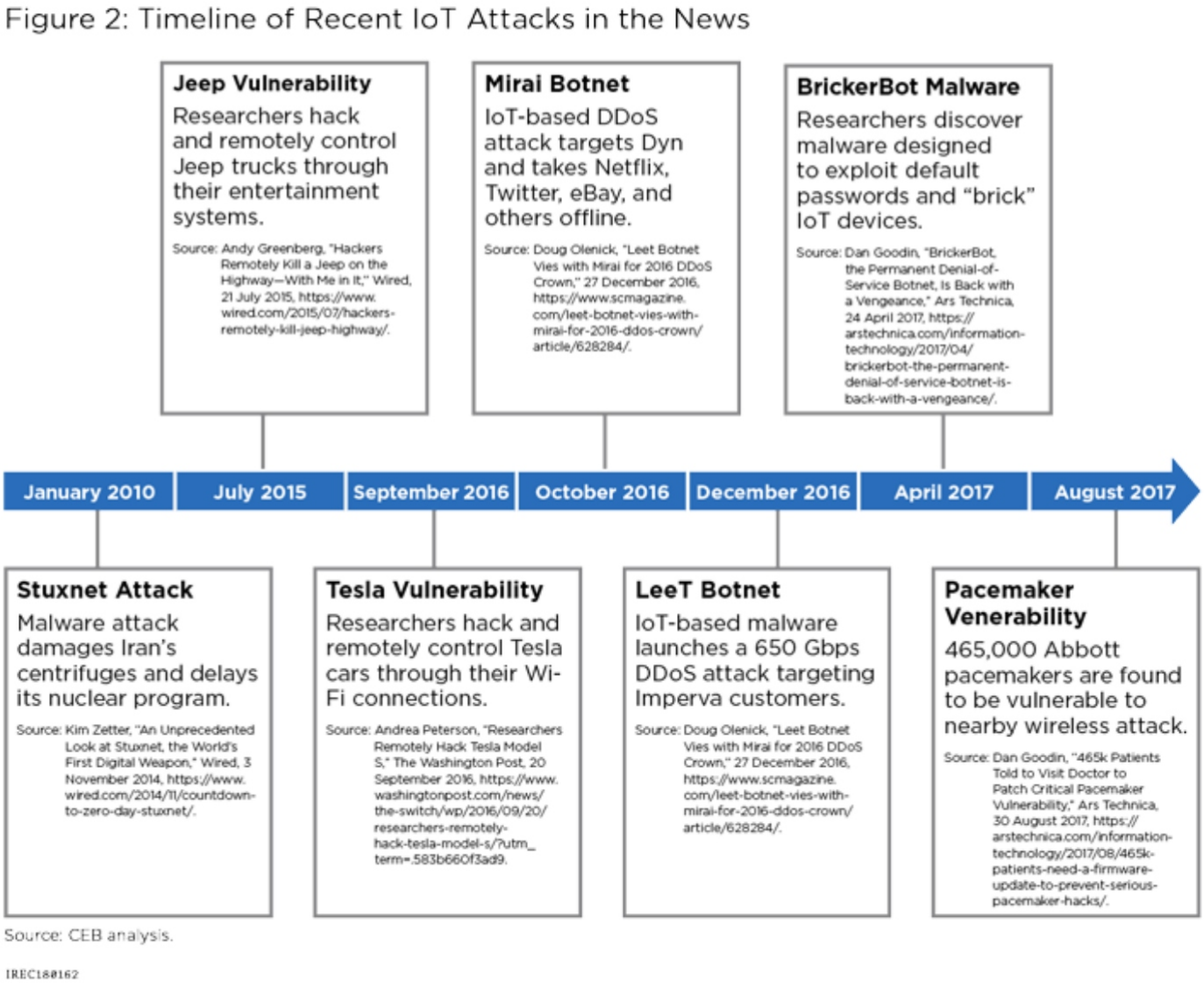
Figure 1: Projected Global IoT Connections



2. Increasing Board and C-Suite Interest—IoT garners C-suite and even board-level interest. CISOs tell us that business leaders recognize IoT's business opportunities—from product development and innovation, to operations, cost savings, and beyond—but are still in the early stages of defining and implementing such opportunities. Fifty-four percent of CISOs discuss IoT risks and opportunities with their C-suite at least twice a year, and two-thirds of CISOs discuss IoT with the board at least once a year. In addition, over two-thirds of CISOs expect C-suite and board-level IoT discussion to be more frequent over the next 12 to 18 months. Leading CISOs routinely tell us Information Security plays an important role in ensuring IoT adoption promotes growth while mitigating risks.

3. Growing Evidence of Real IoT Threats—Recent events show that IoT risks are real and routinely realized by adversaries (figure 2). And it's not just examples from the news—20% of organizations already observed at least one IoT-based attack in the past three years. Furthermore, IoT devices can present new-in-kind risks—such as physical attacks that harm or even kill individuals via medical devices or self-driving cars.

Figure 2: Timeline of Recent IoT Attacks in the News



Our research examines how leading CISOs and their teams currently view, assess, and manage IoT risk. This includes insight on:

- The current state of IoT adoption,
- IoT risk and Information Security's role,
- Information risk management challenges posed by IoT, and
- Emerging IoT security practices.

Current State of IoT Adoption

Most organizations already use IoT and have ambitious plans to expand adoption over the next 12 to 18 months. Organizations are also exploring industry-specific uses for IoT, such as for manufacturing, utilities, and shipping.

Information Security functions cannot afford to “wait and see” in IoT risk management because the risks are real and the technologies are already in use (figure 3):

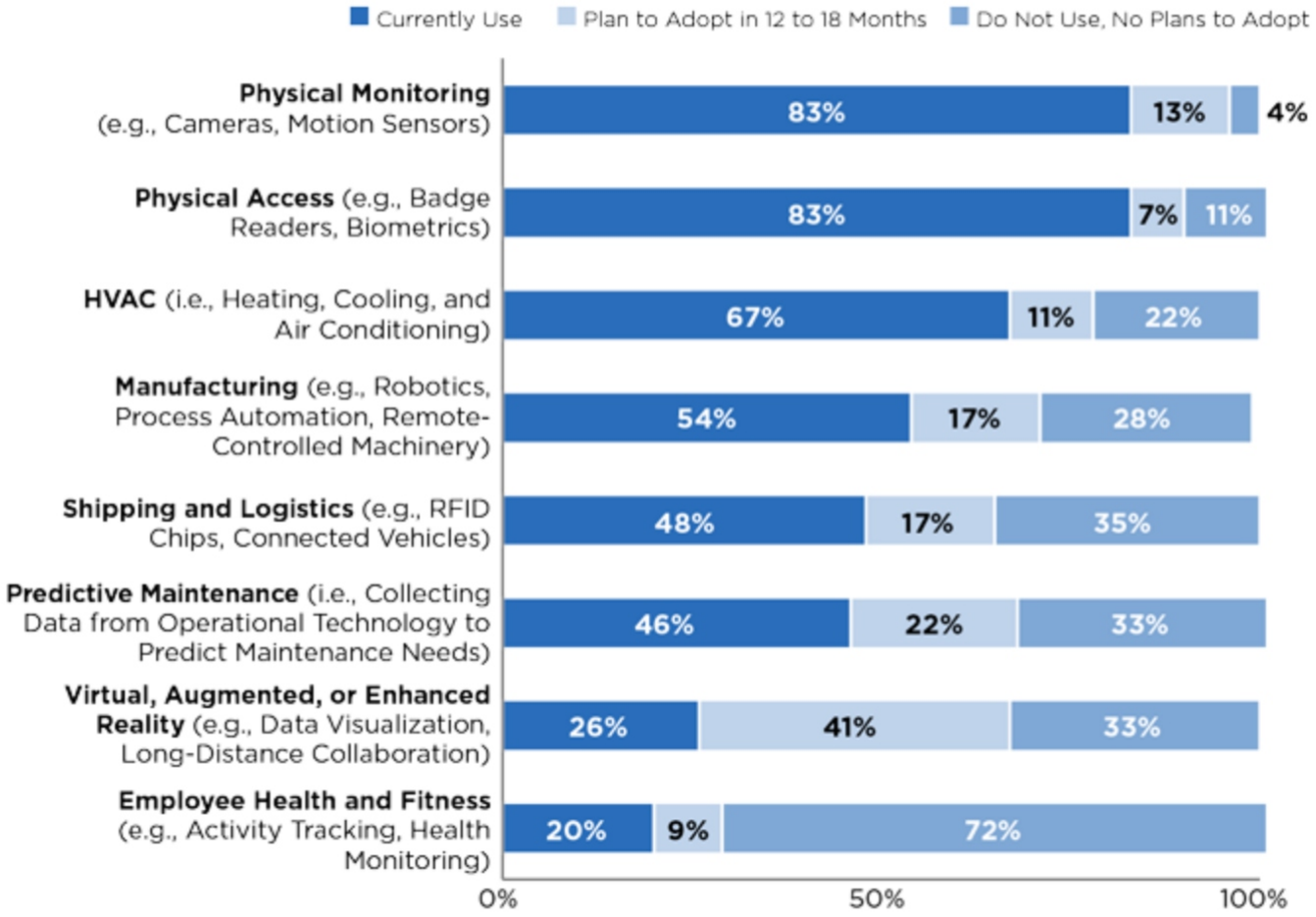
- Over 80% of organizations have adopted physical access and monitoring IoT use cases.
- Over three-fourths have adopted HVAC use cases.
- Over half have adopted manufacturing use cases.

Organizations also have ambitious plans to expand IoT adoption over the next 12 to 18 months:

- 41% of organizations plan to adopt virtual, augmented, or enhanced reality.
- 22% plan to adopt predictive maintenance.
- 17% plan to adopt manufacturing and shipping and logistics use cases.

Figure 3: Current and Planned IoT Use Cases

Figure 3: Current and Planned IoT Use Cases
Percentage of Organizations



n = 46.
Source: CEB 2017 IoT Security Survey.
Note: Totals may not equal 100% due to rounding.

IREC188162

Organizations we surveyed also note the following IoT use cases:

- **Currently Use**
  - Industrial control systems (ICS) and SCADA
  - Precision agriculture (precision AG)
  - Personal assistant devices
  - Smart power grids
  - Wearable glasses (for picking parts in a factory)
  - Telematics gateway (for managing connected vehicles)
  - Office equipment

- **Plan to Adopt in the Next 12 to 18 Months**
  - Expanded sensor deployments

- Increased power grid automation
- Advanced distribution management systems
- New mobility solutions
- Centralized notifications and alerts from distributed devices

Clearly, IoT is widely used by organizations—a trend that will only increase over the next few years. Information Security must prepare now for IoT or risk falling behind as adoption grows.

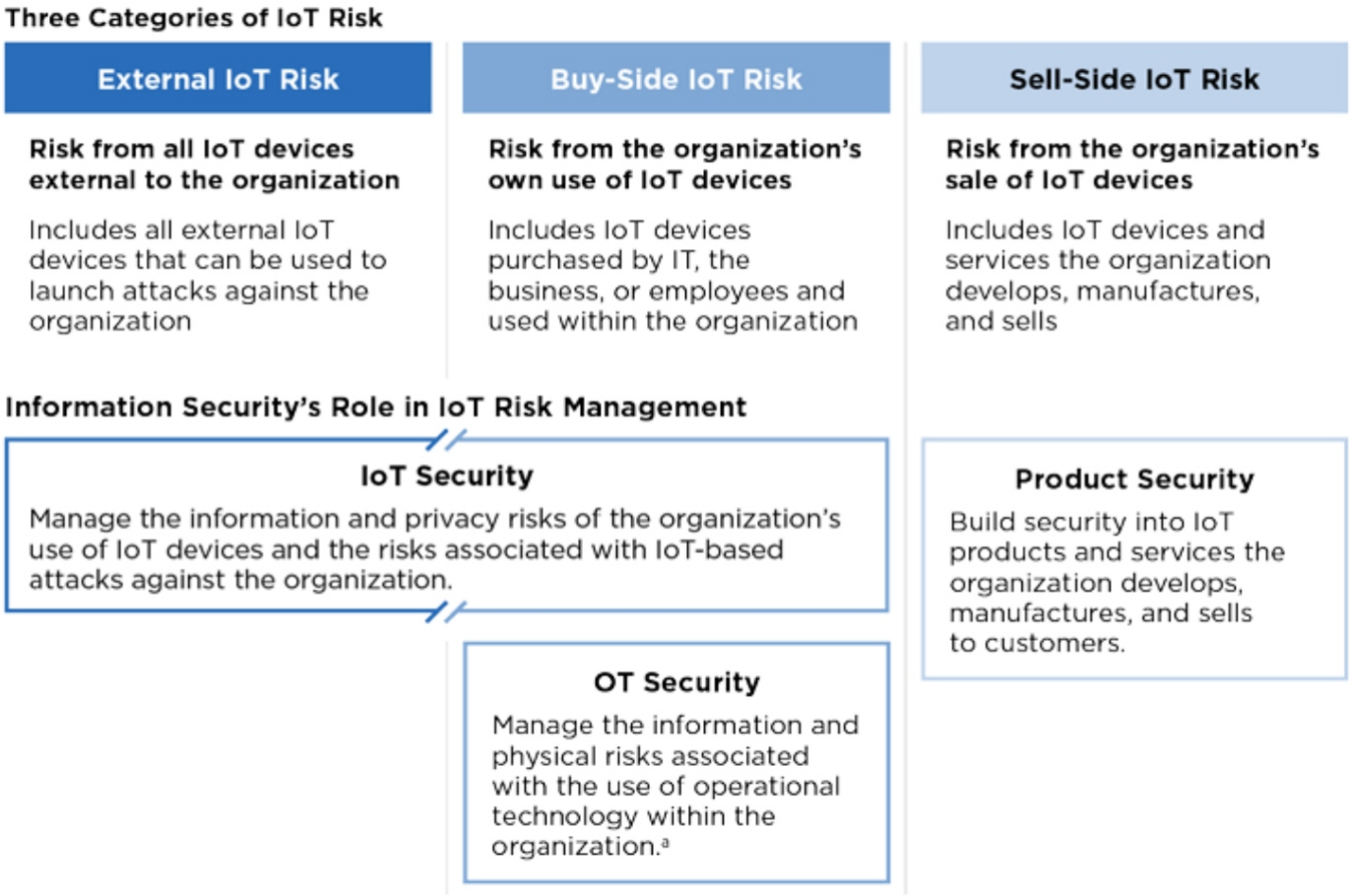
Clarifying IoT Risk and Information Security's Role

Information Security must first define and categorize IoT risk, then define the function's role in IoT risk management. Doing so clarifies the risks facing the organization and Information Security's role in mitigating these risks.

Information Security often plays multiple roles when managing risks associated with IoT devices. These roles depend on the types of IoT risk the organization is exposed to (e.g., external, buy-side, and sell-side) (figure 4).

Figure 4: Three Categories of IoT Risk

Figure 4: IoT Risk Management



Source: CEB analysis.

[a] Examples of operational technology include programmable logic controllers (PLCs), ICS and SCADA systems, computer numerical control (CNC) machines, and smart telematics gateway systems.

IREC180162

Three Categories of IoT Risk

Conversations with leading CISOs reveal three broad categories of IoT risk: external, buy-side, and sell-side. Organizations must understand these categories before defining Information Security's roles in IoT risk management:

1. External IoT risk (affects all organizations)—IoT devices external to the organization can be exploited to launch attacks against the organization. Examples include DDoS attacks, man-in-the-middle exploits, and third-party breaches. These risks face all organizations and cannot always be directly managed because the exploited devices lay outside the organization's purview. Instead, organizations must develop compensating controls where possible to identify and manage external IoT risks.

2. Buy-side IoT risk (affects almost all organizations)—Most organizations buy and use IoT devices in some capacity—even if Information Security is unaware of these purchases. In particular, CISOs commonly cite three ways Information Security misses IoT purchases:

- Procurement may not be aware that certain purchases carry information risks and thus fail to

involve Information Security. This issue is particular common where traditionally unconnected products (e.g., machinery, appliances, vehicles) are now connected in ways Procurement does not realize or understand.

- IoT devices are often acquired via business-led purchases outside IT, Procurement, or Information Security's purview altogether.
- Employees at almost all organizations bring their own personal IoT devices into the workplace, regardless of IoT policies, security controls, or formal procurement procedures.

These realities mean almost all organizations are exposed to—and must manage—IoT risks, even at organizations that attempt to block or sharply curtail IoT purchases.

3. Sell-side IoT risk (affects some organizations)—Organizations that develop and/or sell IoT devices or services are exposed to the risk that these devices will be exploited to harm customers or the organization itself. This includes customer data theft, service disruptions, privacy issues, and even life safety implications. Organizations exposed to sell-side IoT risk must devise ways to build sufficient security into their IoT products and services.

Factors That Influence Information Security's Role in IoT Risk Management

We found there is no one-size-fits-all approach to defining Information Security's role in IoT risk management. Rather, every Information Security function should take an approach that works best for the broader organization.

CISOs often consider the following factors when defining the function's role in IoT risk management:

- **Type(s) of IoT Risk Exposure—**The types of IoT risk exposure (i.e., external, buy-side, and sell-side) applicable to the organization affect Information Security's role in IoT risk management. In particular, organizations not exposed to sell-side IoT risk may not have or need product security capabilities.
- **Information Security's Mandate—**Information Security's mandate, organizational structure, and reporting lines, as well as those of other risk management functions in the organization, influence Information Security's role in IoT risk management. For example, an Information Security function that reports outside IT may write IoT policies, define IoT controls, and oversee IT's implementation and adherence to IoT policies and controls, whereas an Information Security function that reports within IT may own more day-to-day IoT security operations.
- **Industry—**An organization's industry plays a significant role in determining Information Security's role in IoT risk management. Some industries (e.g., utilities, manufacturing) may make larger use of Internet-connected operational technology (OT), and IoT risk management practices and norms may vary by industry. Industry groups (e.g., ISACs) and peer networks are good resources for understanding, sharing, and even establishing IoT risk management practices.

Information Risk Management Challenges Posed by IoT Devices

Information Security often struggles to manage IoT risk. The top challenge CISOs cite is poor visibility and understanding of IoT devices and how the organization uses them.

Leading CISOs and their teams cite the following IoT risk management challenge areas: poor visibility and understanding, lack of standardization, poor vendor support and security practices, physical risk implications, and regulatory compliance and privacy implications (figure 5).

Figure 5: Top IoT Risk Management Challenges

Our conversations with security leaders further reveal specific concerns within each challenge area:

Poor Visibility and Understanding

- **IoT devices are difficult to anticipate and discover in the network.** Security often struggles to discover and classify IoT devices employees introduce to the network. This challenge is exacerbated as IoT device variety increases over time. Furthermore, employees may not consider the security implications when existing devices (e.g., HVAC systems, security systems, appliances) are upgraded to connected versions.

- **IoT devices are "black boxes" that cannot always be fully understood or evaluated for risk.** IoT devices—from sensors to software—cannot be penetration-tested or hardened. This contrasts with the past, when Information Security managed a more limited and known set of devices that could be more deeply understood and evaluated for risk.

> **"IoT devices are black boxes. For example, there's often no admin login or patch statuses, and you don't even know what the OS is. Even if the vendor answers your questions, there's not much you can do to the device itself to improve its underlying security. IoT takes all the security challenges we face with the fractured Android world and multiplies them."**
>
> *— Paul Beckwith, Chief Security Officer, Progressive Casualty Insurance Company*

- **IoT devices often create data without a clear understanding of how it's used or stored.** IoT devices typically create and store data, which creates potentially unknown risk. Information Security often lacks knowledge of where IoT devices store data (e.g., public cloud, private cloud, locally), how the data is stored (e.g., unencrypted, encrypted, tokenized), who has access to the data, and how the data is analyzed, aggregated, and reported. This lack of understanding exposes the organization to unknown and unmitigated risk, privacy, and compliance issues.

Lack of Standardization

- **IoT devices often cannot conform to existing security standards or policies.** IoT manufacturers often prioritize speed, cost, and convenience over transparency and security—especially during software development. Therefore, IoT devices often use old (e.g., Windows XP, outdated versions of Linux) or proprietary firmware that is prone to vulnerabilities and cannot be modified, updated, or otherwise protected. Furthermore, firmware varies more among IoT devices than among traditional form factors (e.g., smartphones, laptops, tablets) where operating systems, vulnerability disclosures and patches, and version control are more standardized and transparent. As a result, Information Security cannot expect IoT devices to easily conform to existing security standards, policies, or practices.
- **There are no widely adopted IoT security standards that device manufacturers can adhere to.** The IoT landscape is too nascent and splintered to have clear security standards and norms. Currently, a lack of standardized IoT development and manufacturing practices (e.g., platform development, test, and evaluation, connectivity and communication) means IoT vendor security

practices vary widely. This lack of standardization makes it more challenging for Information Security to define IoT policies, assess IoT risks, and communicate IoT standards to other risk management functions in the organization.

> **"I find that Procurement prioritizes IoT device price over value. Therefore, our organization often purchases the cheapest IoT solution as opposed to one that balances price, functionality, and security. The current lack of IoT standards makes it harder to make the case to Procurement that it sometimes makes sense to spend more on IoT devices with better security. Right now we operate on a case-by-case basis."**
>
> — *CISO, Fortune 500 Financial Services Company*

Poor Vendor Support and Security Practices

- **Companies lack incentives to update and maintain software on the IoT devices they sell.** IoT vendors often lack financial incentives to patch vulnerabilities and update firmware—in part because such updates are rarely tied to a revenue stream. Therefore, IoT software is often static and vulnerabilities remain unknown and unmitigated.
- **Startups and small IoT vendors typically lack robust product security practices.** IoT devices often bring innovative functionality at the cost of robust security. This trade-off is especially true of small, young IoT vendors that lack the funding, expertise, and time to develop robust security in their devices. Furthermore, IoT vendors often lack financial incentives to improve security, as corporate customers (e.g., Procurement) are not yet willing to pay more for better security.

> **"Few IoT companies have adequate cybersecurity practices, assurance practices, or test and validation processes. Overall, I think IoT companies simply don't face enough economic incentives yet to build better security into their devices."**
>
> — *Bill Boni, VP Information Security, T-Mobile USA*

Physical Risk Implications

- **IoT devices add safety challenges to the "CIA" triad.** Traditionally, Information Security functions consider risk from data confidentiality, integrity, and availability. However, IoT devices can pose personal safety issues (e.g., from medical devices or vehicles) that force Information Security to add personal safety to its core mission. Many Information Security functions may be initially ill equipped to assess and manage personal safety risks, as this is a new terrain.
- **New risks (e.g., life-safety hazards) emerge as IoT devices become more autonomous.** IoT devices vary significantly in their degree of autonomy. For example, some devices may only create and send data in one direction, others may receive instructions remotely, and still others may use AI to make autonomous decisions. In general, IoT devices become harder to control—and their risks more challenging to assess and anticipate—as they grow more autonomous. In particular, IoT devices such as connected vehicles, medical devices, and industrial machines will create new life-safety risks as they grow more autonomous.

We view autonomy along the following scale, from least to most risk:

- *'Get data' devices send but do not receive data. These devices pose the lowest risk.*
- *'Analyze data' devices send data that is then used for analytics and other data services. This risk is that customers and employees do not trust the integrity of collection data.*
- *'Two-way data' devices both send and receive data. The risks are much more pronounced, as human error, malicious insiders, or malicious adversaries could remotely control connected machines in ways that (physically) harm individuals.*
- *Lastly 'autonomous machines' make their own decisions using AI and Machine learning. These devices, such as self-driving vehicles, pose the most significant and challenging risk.*

CISO
Fortune 500 Financial Services Company

Regulatory Compliance and Privacy Implications

- **IoT devices create greater, deeper privacy concerns.** IoT devices often introduce or magnify privacy issues. Sensors (e.g., GPS trackers, cameras, microphones, medical sensors) embedded in devices potentially collect private and personal information. These concerns are further magnified when IoT devices store data remotely or combine data in ways that generate personally identifiable information (PII). Such regulatory concerns can blindside organizations when historically "dumb" devices are upgraded to connected versions without proper scrutiny from Procurement.

> **"We recently ran an internal employee fitness competition that used GPS tracking devices to count steps. We ended up spending a lot in unplanned expenses building controls to anonymize employee location data. Had we not caught this in time, we would have inadvertently exposed the company to regulatory compliance issues."**
>
> — *Per Anders Eriksson, CISO, ICA AB*

Prepare for the Future: Emerging IoT Security Practices

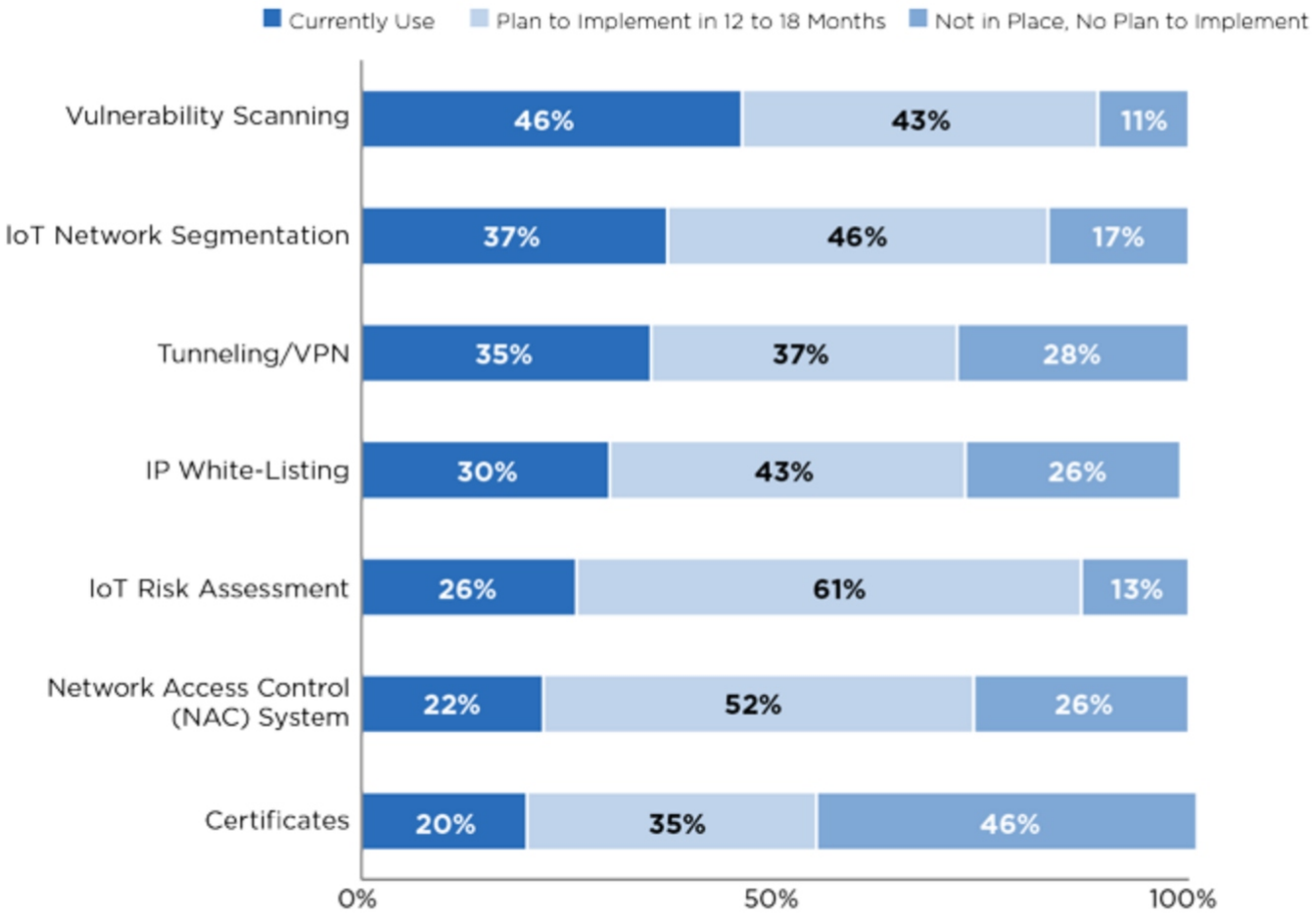
Many organizations already have IoT controls in place, and most organizations plan to expand their IoT controls portfolio over the next 12 to 18 months.

We've found that IoT security efforts are nascent at most organizations. In many instances, Information Security functions are just starting to grapple with how to approach IoT risk management and what governance and controls need to be expanded, modified, or created to mitigate this risk.

Unsurprisingly, there are no perfect answers. Rather, we find that leading organizations take several approaches (figure 6), and in almost every case IoT controls continue to evolve as the IoT landscape takes shape.

Figure 6: Current Adoption of IoT Risk Assessment and Technical Controls

Figure 6: Current Adoption of IoT Risk Assessment and Technical Controls
Percentage of Organizations



n = 46.
Source: CEB 2017 IoT Security Survey.
Note: Totals may not equal 100% due to rounding.
[REC188162]

Leading Information Security functions we spoke with currently use or are exploring the following IoT governance and controls:

IoT Governance

- **Information Security's Mandate**—Update Information Security's mandate, as necessary, to include IoT risk management. In particular, Information Security may want its mandate to explicitly cover:
  - **Cross-functional roles, responsibilities, and expectations** related to IoT risk management;
  - **The extent of Information Security's authority** to compel business units and other corporate functions to adopt IoT-specific controls; and
  - **The types of IoT risks** (e.g., external, buy-side, or sell-side) Information Security is responsible for managing.

- **IoT Security Policies**—Create IoT-specific security policies that outline how the organization defines and manages IoT security risk. An IoT security policy serves as a first step in

documenting and communicating high-level IoT security guidance. An IoT security policy may include:

- **Guidance for assessing or categorizing risks** associated with different IoT devices,
- **Requirements for procuring or reporting new IoT devices** to Information Security, and
- **IoT-specific control requirements** or recommendations based on associated risk.
  IoT security policies may be based on existing BYOD or mobility policies. However, it is important to consider how IoT may present new and unique risks or challenges not covered by existing policies. For example, IoT devices may pose:
- **New-in-kind risk of physical harm** not previously seen with more traditional mobile devices (e.g., smartphones, tablets),
- **New attack vectors or techniques** specific to IoT devices or exacerbated by an influx of IoT device volume and complexity, or
- **New sources of information risk** where it did not previously exist (e.g., adding new sensors to previously unconnected objects).

- **Cross-Functional Collaboration—**Design cross-functional processes and workflows that enable Information Security to work better with other functions in order to manage information risks associated with IoT devices. Cross-functional collaboration partners may include:
  - **Procurement—**Procurement can help Information Security discover new IoT devices before they are purchased, assess IoT risks during procurement, and apply security policies to make better-informed trade-off decisions—where they exist—between IoT device cost, functionality, and security. In particular, Information Security should teach Procurement how to identify IoT devices and define when to involve Information Security. Information Security should also gauge Procurement's appetite for spending more on IoT devices that have better security (i.e., Information Security should shift Procurement's focus from price to value).
  - **Physical Security—**IoT devices blur the line between physical and information (or "cyber") risk. This is particularly true in cases where physical access (e.g., doors, turnstiles) and monitoring devices (e.g., cameras, microphones, motion detectors) connect to the Internet. Information Security should work closely with Physical Security to assess the information risks associated with connected devices. These risks include the collection and storage of sensitive employee information, the regulatory implications of collecting employee PII, and the potential for attackers to cause disruptions or gain physical access by targeting connected devices. Some organizations may consider combining Information and Physical Security given the blurring lines between these risks.
  - **Facilities/Maintenance—**Facilities and Maintenance functions likely are or will be working with IoT devices (e.g., HVAC, fridges, thermostats, doors, manufacturing robotics) used in the organization's workspaces. Information Security must work with these functions to detect and manage IoT devices. In particular, these functions should understand how to detect when

previously unconnected devices are now connected (a potential blind spot for Information Security) and should take appropriate ownership of controls that mitigate IoT risks.

- **Lobbying and Industry Collaboration—**Look for opportunities to join industry groups or conduct lobbying to help define IoT security standards. IoT standards are most likely to emerge from either government action (e.g., laws, regulations) or large industry groups that define IoT requirements across large industries. CISOs should explore industry-wide collective action to push IoT vendors toward new and emerging standards.

IoT Process Controls

- **Information Risk Assessment—**(Re)define the information risk assessment process to accommodate IoT devices. In particular, Information Security should formally define criteria used to assess and categorize IoT risks. These criteria may include:
  - **Data**
    - **Data Creation:** What data does the IoT device create? How sensitive is this data?
    - **Data Storage:** Where and how does the device store data (e.g., locally, public cloud, encrypted)? Can data storage be controlled or monitored?
    - **Regulatory Implications:** Does the IoT device create, store, or process data that is regulated? (Consider both local and international laws and regulations.)
    - **Privacy Implications:** Does the IoT device create, store, or process data that could trigger privacy implications? (Consider both local and international privacy laws and norms.)
  - **Hardware**
    - **Sensors:** What sensors does the IoT device have (e.g., cameras, microphones, motion sensors)?
    - **Storage:** How much data can the IoT device store? (This has data exfiltration and command and control implications.)
    - **Processing power:** How much processing power does the IoT device have? (More processing power can provide greater opportunity to use the device to launch attacks.)
  - **Software**
    - **Operating System:** What operating system and version does the IoT device run?
    - **Certificates:** Can the IoT device accommodate secure certificate solutions? (Device certificates help with IoT device detection, authentication, and trust.)
    - **Autonomy or Remote Control:** To what degree can this device be controlled remotely or act autonomously? What specific actions can the device take autonomously or via remote

control? What types of remote control input(s) does the IoT device accept (e.g., voice commands, remote web interface commands)?

- **Physical**
  - **Life Safety:** To what degree could the IoT device cause bodily harm or death to employees, customers, or bystanders?

- **Vendor**
  - **Support:** Does the vendor offer ongoing support for the IoT device (e.g., patching, updates)? If so, how long does this support last?
  - **Lifespan:** What is the vendor's intended lifespan for the IoT device?
  - **Supply Chain:** What suppliers and components does the IoT vendor use in its IoT device?

Technical IoT Controls

- **Network Segmentation**—Segment IoT devices onto one or more dedicated networks within the organization to isolate IoT risks.
  Considerations:
  - Network segmentation requires an ability to accurately detect and correctly segment IoT devices onto the correct network. Some IoT devices may be inadvertently connected to the wrong network or may jump networks in unintended ways that allow attackers to move laterally within the organization. You may consider building IoT device detection before embarking on a major network segmentation project.
  - Network segmentation isolates IoT risk, but attackers may still have ample opportunities to steal data or breach devices within the IoT network. Furthermore, imperfect segmentation may allow lateral movement across networks.
  - Network segmentation may consolidate significant, unknown risk into a single network that attackers can easily target. For example, grouping IoT devices that pose life safety risks may actually create a concentrated area of risk, even if these devices are separated from other networks. Always consider how risk is reduced or magnified by network segmentation.
  - Some IoT devices' communication with devices on other networks can allow attackers to move laterally from network to network. Thus, even network segmentation that is correctly implemented as intended may be vulnerable to lateral movement.
  - Creating multiple network segments for different types of IoT devices (with different risks) adds greater granularity to this control but also creates additional complexity and exacerbates the challenges of getting devices onto the correct network segments. When devising an IoT network segmentation strategy, consider how best to balance control granularity, feasibility, and risk mitigation.

- **IP Allow-Listing—**Pre-define which IP addresses IoT devices can communicate with to protect against malicious connections to these devices.
  Considerations:
  - IP allow-listing may be overly restrictive, as it can limit (or break) IoT device functionality, slow the organization's experimentation with IoT, and position Information Security as an IT roadblock. For this reason, Information Security should work with business and IT partners to understand when IoT IP allow-listing is appropriate.
  - IP allow-listing is fairly manual and hard to scale as IoT device volume and variety expand. Therefore, IP allow-listing cannot typically be applied to all IoT devices. Consider developing criteria that define when IP allow-listing is an appropriate IoT control.
  - IP allow-listing does not necessarily prevent attackers from accessing IoT devices via allow-listed IP addresses or reconfiguring compromised IoT devices.

- **Tunneling/VPN—**Create private, secure network connections that let IoT device traffic travel in secure tunnels.
  Considerations:
  - Tunneling is particularly useful when transmitting IoT traffic between disperse physical locations (e.g., between corporate offices, from a customer location).
  - Tunneling can sometimes inadvertently break IoT device functionality by preventing the device from accessing servers required for the device to function properly. For example, some IoT devices must connect to the vendor's servers to fully function. Such traffic may be blocked by traffic tunneling.

- **Certificates—**Embed electronic certificates into IoT devices to improve device trust, identification, and authentication.
  Considerations:
  - IoT devices do not always support secure certificate solutions. Such support typically must be embedded by IoT vendors at additional cost and is not always available.

- **Security Analytics—**Use analytics-based threat detection (e.g., behavioral analytics, network monitoring) to identify new or suspicious network activity associated with IoT devices. Analytics can be used to identify new IoT devices and detect suspicious activities associated with malicious or inadvertently risky activity.
  Considerations:

- Security analytics can be costly to implement and, in some cases, may fail expensively when results do not match expectations.
- Suspicious activities discovered by analytics typically have to be individually examined and investigated by Information Security personnel, which is an expensive and tough-to-scale endeavor.
- Security analytics has the benefit of focusing on data flows as opposed to devices themselves. This means Information Security can detect suspicious IoT behaviors even if the devices themselves are unknown or not well understood.

- **Network Access Control (NAC) Systems—**Use a NAC system to detect and categorize new devices connecting to internal networks.
  Considerations:
  - NAC systems are useful in categorizing common devices (e.g., Windows, Linux, iOS, and MacOS machines) but may struggle to identify and categorize less common IoT devices.
  - NAC systems can be useful in enforcing and scaling network segmentation rules.

- **Vulnerability Scanning—**Routinely scan devices for known vulnerabilities, and use this information to guide patching efforts and other mitigating controls on IoT devices.
  Considerations:
  - IoT devices running proprietary or obscure software or operation systems may not be scannable.
  - Vulnerabilities on IoT devices may not be patchable depending on vendor and technology constraints, so discovered vulnerabilities may require more complicated compensating controls.

Conclusion

IoT-based attacks are already a reality, yet most Information Security functions are just starting to think about how to manage IoT risk. Leading CISOs and their teams must work more broadly in the organization to understand IoT use cases, educate and categorize IoT risks, and adopt emerging IoT security practices. With time, Information Security functions will need to advance their IoT risk management practices as IoT security standards emerge, best practices develop, and the vendor landscape matures.

Recommended by the Authors

- Use our 2018 Survey Report: State of IoT Security to benchmark IoT risk management practices against leading peers.

About This Research

This research draws upon extensive qualitative and quantitative research conducted with leading CISOs at Fortune 500 organization. We interviewed over 30 CISOs and their direct reports, collected survey data from over 45 unique organizations, sourced practitioner-tested ideas and emerging practices, and reviewed external literature on IoT and IoT security.

Recommended For You

2018 IoT Security Survey Report

Security Considerations and Best Practices for Securing Serverless PaaS

Protect Your Legacy and Technical Debt

Control Network Security Complexity, Inefficiencies and Security Failures by Minimizing Firewall Diversity

Designing Security for Remote-Work-First Enterprises

Helping leaders leverage IoT to tap in new business opportunities
gartner.com/en/information-technology/insights/internet-of-things

Become a Client

Get access to this level of insight all year long — plus contextualized support for your strategic priorities — by becoming a client.

gartner.com/en/become-a-client

U.S.: 1 800 213 4848

International: +44 (0) 3331 306 809

About Gartner

Gartner is the world's leading research and advisory company and a member of the S&P 500. We equip business leaders with indispensable insights, advice and tools to achieve their mission-critical priorities today and build the successful organizations of tomorrow.

Our unmatched combination of expert-led, practitioner-sourced and data-driven research steers clients toward the right decisions on the issues that matter most. We are a trusted advisor and an objective resource for more than 15,000 enterprises in more than 100 countries — across all major functions, in every industry and enterprise size.

To learn more about how we help decision makers fuel the future of business, visit gartner.com.

Gartner®