The CEO's Guide to Securing the Internet of Things

Exploring IoT Security

AT&T Cybersecurity Insights | Volume 2

90%

of organizations lack full confidence in their IoT security.

Source: AT&T State of IoT Security survey, 2015

Contents

For more information:

Follow us on Twitter @attbusiness

Visit us at

securityresourcecenter.att.com

Executive summary

The rapid rise of a new generation of connected, intelligent devices — collectively known as the Internet of Things or IoT — is more than just the latest digital disruption to impact businesses of all sizes. The IoT presents vast opportunities for organizations to improve internal efficiencies, serve customers better, enter new markets, and even build new business models.

More IoT devices are coming online each and every day. Through connected devices, health care is improving patient care; for example, a diabetic patient's blood sugar level can now be monitored remotely, enabling a quick response to a possible life-threatening situation.

The way we drive is also being transformed with advances that enhance safety through features such as hands-free communication or automated response to potentially dangerous situations. For industry and manufacturing, connected devices are being used to create more efficient, productive systems that can track shipments of grain across oceans or monitor oil well pumps, among other capabilities. Even if you are not utilizing the IoT today, you soon will be — and your suppliers and customers will be as well.

As IoT devices become crucial for keeping up with fast-evolving markets, business and technology leaders must be mindful of the security implications of this new technology. The scale of connected devices greatly increases the volume of data and the complexity of cybersecurity. The challenge grows further as IoT devices are deployed to control infrastructure, such as factory operations and supply chains.

Cybersecurity is already top of mind for many organizations. But IoT deployments make it much tougher for C-suite executives to answer the question that corporate boards are asking with growing frequency: Has the IoT increased our exposure to cyberthreats?

Building security from the start into IoT devices and their connecting networks is key to protecting a growing IoT infrastructure. This proactive approach will set the foundation for a strategy that integrates IoT security with existing cybersecurity policies and systems. Such a strategy will also encompass the entire IoT ecosystem — not just your own devices, data, and applications, but those of your partners and customers as well.

In this second installment of Cybersecurity Insights, we help you understand the IoT opportunity, as well as the inherent risks. Most important, we'll provide a strategic framework for securing the IoT, crafted from the work we're doing with customers across many industries — as well as with our own IoT deployments.

The CEO's framework to help secure the Internet of Things

1. **Assess your risk**
2. **Secure both information and devices**
3. **Align IoT strategy and security**
4. **Identify legal and regulatory issues**

See page 14 for more detail

In this report, we define the Internet of Things (IoT) as the digitization of elements of the physical world, in which products and other "things" are outfitted with intelligent sensors and tags that let them communicate across the Internet without human intervention.

IoT evolution: Security trails deployment

5,000+ One-third of organizations surveyed say they have more than 5,000 connected devices.

In this section:

85% of organizations are considering, exploring or implementing an IoT strategy.[1]

88% of organizations lack full confidence in the security of their business partners' connected devices.[2]

Bottom line: The IoT's potential impact on your business is significant — as is the risk.

In 1999 Kevin Ashton, an assistant brand manager at Procter & Gamble, delivered a presentation about wireless connectivity with an intriguing title: "Internet of Things." Sketching out a futuristic scenario in which computers "knew everything there was to know about things," Ashton predicted that the IoT "has the potential to change the world, just as the Internet did. Maybe even more so."[3]

A decade and a half later, the digital shift that Ashton imagined is well underway. Organizations are using the IoT to glean new

operational insights, grow revenues, reduce costs, and increase productivity.

This extensive ecosystem of interconnected devices, operational tools, and facilities holds much promise for connecting people, processes, and assets in ways that profoundly impact how we live and work.

For example, in the transportation sector, companies are using sensors to monitor movements of cargo, inventory, and delivery vehicles to improve efficiencies and reduce costs. Using information collected from bar codes, RFID tags, or other embedded sensors, businesses can manage and optimize delivery routes and track vehicle performance. Sensors also enable business to react quickly to environmental or other threats, such as a dramatic temperature change in a refrigerated truck.

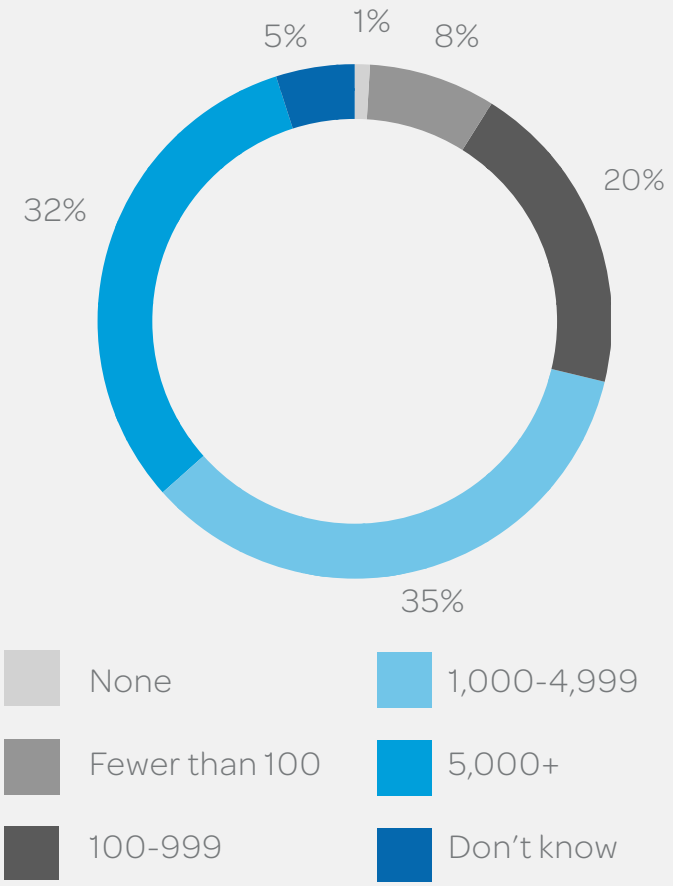
B&P Enterprises — an emergency response specialist that operates 200 vehicles and over 400 other pieces of construction and marine equipment across the United States — used a fleet management solution to decrease DOT violations by 80% and save $86,000 annually on insurance.[4]

In the agriculture sector, OnFarm, a California-based startup, has built an IoT platform that collects data from multiple types of farm equipment. Using IoT-connected equipment, such as irrigation systems, OnFarm has been able to help growers improve crop management.[5]

AT&T's State of IoT Security survey finds that 85% of global organizations are considering or exploring an IoT strategy, with one-quarter already piloting or implementing IoT-related projects. Connected devices now number in the thousands for two-thirds of the respondents, and almost one-third say they have more than 5,000 connected devices across their organization.

IoT deployments are on the rise

How many connected devices do you have in your organization?



Source: AT&T State of IoT Security, October 2015

These deployments are contributing to a rapidly growing number of connected devices that is expected to swell to anywhere between 30 billion[6] (excluding smartphones) and 50 billion[7] (including smartphones) by 2020.

The impact is already being felt across industries and with consumers alike. Organizations are widely deploying the IoT to become more efficient in customer-facing, back-office, and supply chain operations.

Beyond cost savings, businesses are beginning to tap into the IoT for new revenue models, often from products, platforms, and services that enable smart homes, offices, and supply chains. For example, by automating and streamlining common tasks performed by security systems, thermostats, electric meters, and lighting, devices for the digital home are already replacing many labor-intensive chores and offering unprecedented convenience.

458%

AT&T has logged a 458% increase in vulnerability scans of IoT devices in the last two years.

"Organizations need to infuse security expertise early into the process so that the IoT is architected for security. We've already seen the consequences when that doesn't happen."

Jason Porter
Vice President, Security Solutions
AT&T

A lack of foundational security increases risk

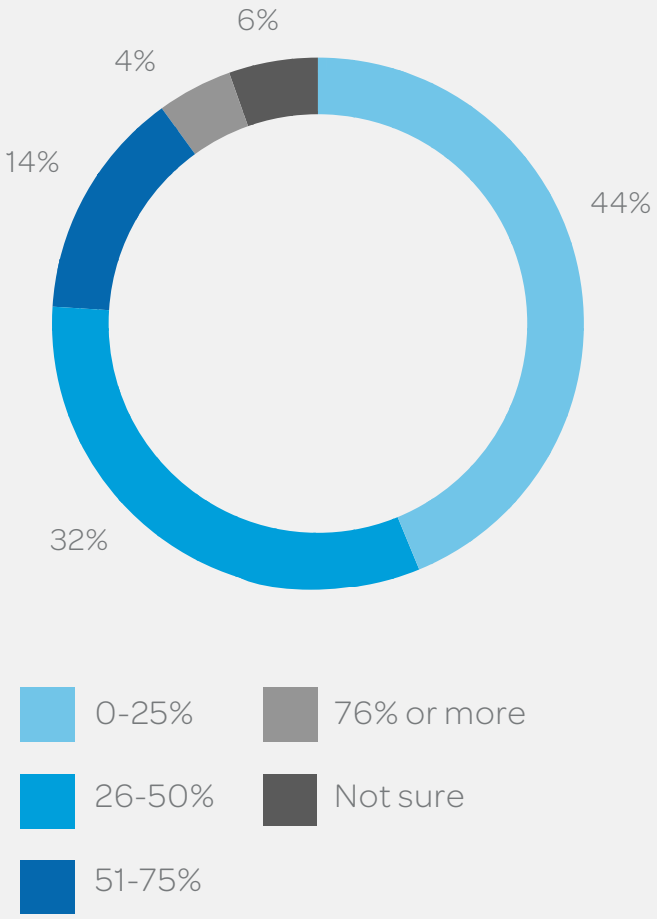
As IoT deployments increase in both number and scope, one concern rises to the top of the CEO's agenda: security. Just 10% of respondents to the AT&T survey are fully confident that their connected devices are secure, and only 12% are highly confident about the security of their business partners' connected devices.

Given that backdrop, it's no surprise that more than two-thirds (68%) of the respondents say their companies plan to invest in IoT security in 2016. Half of those organizations are earmarking at least one-quarter of their security budgets toward the IoT.

Even though these organizations plan to invest in IoT security, they may have some catching up to do. At many organizations, IoT devices are being deployed without proper security measures. This shortcoming is in part because many vehicles, shop-floor equipment, and other increasingly IoT-enabled devices were not built with Internet connectivity — or the requisite security — in mind.

IoT grabs a share of IT security budgets

How much of your security budget is allocated toward IoT security?



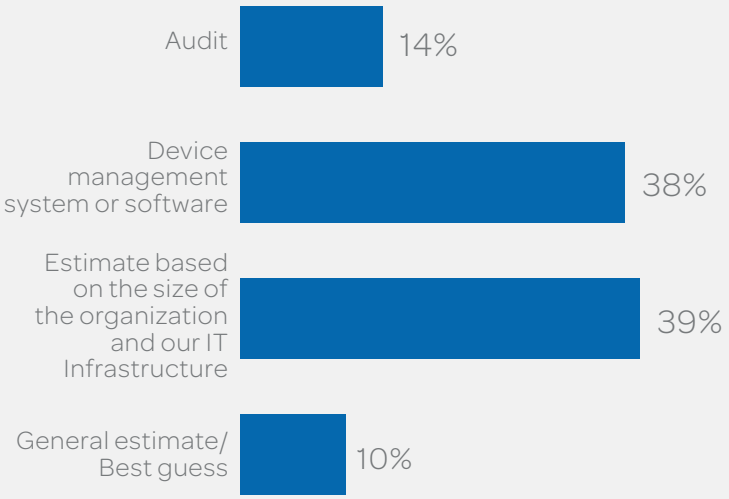
Source: AT&T State of IoT Security, October 2015

For this reason, the IoT ecosystem has become a digital Petri dish for hackers and other cybercriminals eager to probe for new weak spots. Over the past two years, AT&T's Security Operations Center has logged a 458% increase in vulnerability scans of IoT devices.[8]

In many cases, IoT exploits mimic traditional cyberattack methods. In New Zealand, hackers

Methods for identifying connected devices vary

How do you determine the number of connected devices in your organization?



Source: AT&T State of IoT Security, October 2015

reverse engineered the firmware of a popular line of home security cameras, accessed the cameras' IP addresses from a file-sharing website, and commandeered the cameras' streaming video links. The company that made the device allowed its customers' login credentials to be transmitted unencrypted over the Internet, leading to hundreds of camera feeds being accessed and posted online.[9]

The IoT attack surface is magnified by scale, distribution, and the broad spectrum of IoT endpoints, from the very simple to the highly sophisticated. It's possible that some of these devices are not even being monitored. Nearly half of the AT&T survey respondents admit they are merely estimating the number of connected devices they have. Just 14% have a formal audit process in place, while an additional 38% use device management systems or software to identify connected devices.

The stakes climb even higher as these devices are interconnected by the thousands — and begin to bridge the digital and physical worlds.

The business community is all too familiar with the financial and reputational damage that a cyberattack on corporate databases can cause. With IoT devices, however, those risks can be transferred into the physical realm. The ability to compromise or manipulate devices that control critical systems carries far more severe consequences. For example:

- Cyberattackers inflicted "massive damage" on a blast furnace at a German steel mill in late 2014 after a phishing attack allowed them to steal employee login information. Germany's Federal Office for Information Security says the attackers exploited that information to access the plant's office network and production systems. They subsequently disrupted operations to such a degree that a blast furnace could not be properly shut down.[11]

"With the IoT, the information associated with an individual device may not be as important as the role the device plays in the IoT ecosystem. If the device were to fail or be manipulated, what are the impacts?"

Jen Morovitz
Director, Technology Security
AT&T

Security spotlight: Connected car

What it is: IoT-connected cars bring value by improving safety, reducing operational costs, and streamlining traffic flow. A variety of in-vehicle IoT sensors gather performance data to monitor maintenance schedules, troubleshoot problems, and analyze usage. Other sensors, paired with voice controls and mobile apps, add functions such as navigation and a variety of infotainment features.

AT&T has alliances with nine top automakers. More than 10 million connected cars are expected on the AT&T Network by the end of 2017.

Security implications: The potential for a hacker to unlock and enable a car's ignition or remotely take over mission-critical systems — brakes, steering, transmission — has caught the attention of consumers, manufacturers, and legislators.

With the added possibility for the loss of personal information, such as current location or driving history, automakers and their partners are doubling down on efforts to improve security at all entry points.

Potential security safeguards: Look at all devices and sensors within the vehicle and identify possible weak points. Separate critical safety systems and engine control units so that they cannot be accessed through infotainment and tethered device connections. Build in multiple layers of security controls, including encryption, to protect mission-critical functions.

Restricting the interdependence of connected systems will help reduce cascading errors that can create a multitude of unrelated and potentially hazardous vehicular issues.

Telling stat: Reduced rates of collisions and theft thanks to in-vehicle IoT devices could lower insurance premiums by as much as 25%.[10]

"It's essential to architect IoT devices with security in mind. To minimize exposure to risk, it is important to isolate critical IoT devices and data from other communications."

Chris Penrose
Senior Vice President,
Internet of Things Solutions
AT&T

• The U.S. Government Accountability Office warned in a 2015 report that someone could potentially use a laptop to access aircraft avionics systems and take control of an aircraft's on-board computers.[12] At around the same time, a cybersecurity researcher admitted to the FBI that he had hacked into in-flight entertainment systems aboard aircraft 15 to 20 times between 2011 and 2014 — at one point, issuing a climb command to the aircraft on which he was traveling.[13]

Security must be the bedrock of IoT development

The risk to human safety adds an entirely new level of complexity to your information security strategy. That's why security must be the bedrock of IoT development and deployment, not an afterthought. The magnitude of the IoT is so significant that it's important to anticipate security needs and not react to new devices as they're deployed.

This approach will likely require rethinking traditional security governance models. In the AT&T survey, nearly two-thirds of respondents say IoT business strategy is shared across IT and business units, but IoT security at the majority of organizations (55%) is still managed through the IT department. Just as the business strategy is shared, so must security responsibilities be extended beyond the IT team.

Operational improvements are needed as well. Three-quarters of survey respondents say they analyze security logs and alerts from connected devices at least daily, with 34% doing so in real time. Real-time analysis will become increasingly important, but harder to achieve, as the volume of connected devices and machine-to-machine data grows. Companies will need to determine the right frequency for monitoring device activities based on their function and value.

Many different standards initiatives are underway for IoT security, governing everything from application development to device identity verification. Although it's important to engage with the associations representing your specific industry, you can't afford to wait for standards to take hold. The steps you take now to secure IoT devices will have a direct impact on your ability to do business with customers and partners in the IoT economy.

"When you're making health care decisions based on analytics coming from connected medical devices, corruption of that data could lead to catastrophic consequences."

Todd Waskelis
Executive Director,
Security Consulting Services
AT&T Consulting

Know the term:

Machine-to-machine (M2M)

Any direct interaction over any network of electronically enabled devices, with no human involvement in the communications loop.

Security spotlight: Industrial/manufacturing

What it is: The value IoT-connected devices offer industry and manufacturing is the improvement of overall production and efficiency. The proliferation — and connection — of sensors, actuators, and other devices on industrial machinery is at the heart of a transformation sometimes labeled industry 4.0 or smart manufacturing.

Connected IoT devices transmit data, such as equipment operations, environmental conditions, and maintenance needs. Sensors measure and report machine tool tolerances, fluid temperatures, and other critical data. They can also warn when equipment is moving close to operational parameters, prompting preventive maintenance or shutdowns to avoid costly repairs and unanticipated disruptions.

AT&T connects more than 25 million connected devices worldwide.

Security implications: Care must be taken to protect data about manufacturing operations and to prevent unauthorized access to interconnected networks. Industrial sabotage, the targeted disruption of processes or damage to products by competitors, often has strong financial backing and is technologically sophisticated. Cybercriminals also can operate as modern-day burglars by hacking into systems to unlock a facility and steal property.

Of particular concern: threat scenarios where IoT-connected robots or other remotely actuated machines are compromised, potentially resulting in manufacturing errors, equipment or parts damage, or even employee harm.

Potential security safeguards: Understand what IoT-connected devices are doing and how they are communicating. Partition the networks of major industrial processes to isolate and prevent a cyberattack spreading throughout the organization. Establish authentication/authorization controls throughout the ecosystem, with steps to securely patch and update software and firmware. Implement detective controls to identify and contain security breaches as they occur — rather than six months after a pernicious attack.

Telling stat: 35% of U.S. manufacturers are using data generated by smart sensors to enhance their manufacturing or operating processes.[14]

A strategic framework for securing the IoT

A comprehensive
risk assessment
is a critical first step.

In this section:

If you approach IoT security proactively and strategically, you can help manage complexity and reduce risk.

A critical first step is conducting a comprehensive risk assessment that incorporates the IoT into your overall risk profile.

Bottom line: Following core security principles and practices will help reduce the risks and maximize the benefits of utilizing new types of connected devices.

The fundamental objective of every IoT security initiative must be to build in security at the ground floor. A more disciplined approach to IoT initiatives gives you an opportunity to implement security strategies in front of growing the IoT wave, rather than after you've been swamped by it.

The approach requires collaboration among manufacturers, software developers, consultants, and other partners, because IoT security must be robust across every device, sensor, operating system, and application in the ecosystem.

Here's a four-part framework to help you identify IoT-related risks and put the proper controls in place.

1. Assess your risk

The first item on your to-do list is to conduct a comprehensive risk assessment that incorporates the IoT into your overall risk profile. It may seem trite to say "every IoT implementation is unique," but that statement is indisputably true from a security perspective. Even two companies that set up similar smart systems to make their buildings more energy efficient will need to blend those new IoT solutions into their existing — and unique — IT security infrastructures and processes. Add to the mix different IoT use cases, vertical sector regulatory demands, and other variables, and it's easy to see how each IoT initiative takes on a security profile of its own.

An IoT risk assessment should comprise these primary steps:

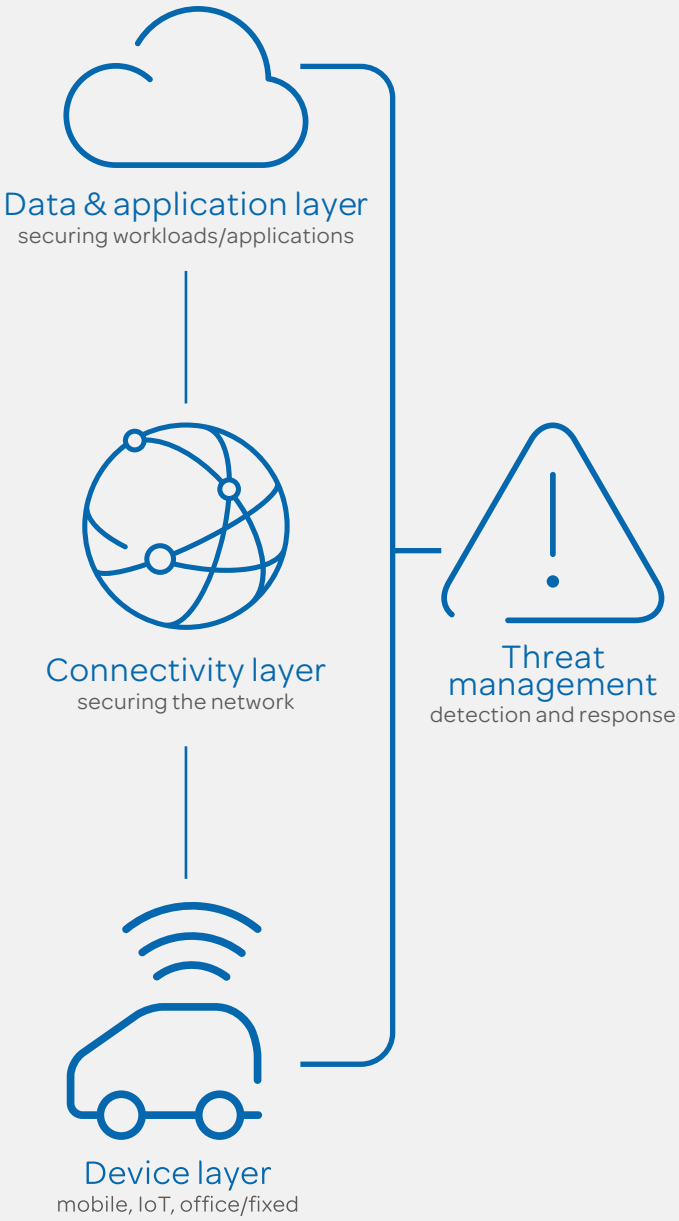
Track your IoT solutions. A thorough audit includes devices, communication protocols, networks, and applications. It's telling that 10% of the AT&T survey respondents cited the "best guess" estimate as their method for tracking the number of IoT devices at their organization.

Assess the security vulnerabilities of each IoT element. Beyond the devices themselves, consider the communication protocols and networks involved in the solution, the applications and databases, and any other IoT networks with which your solution may interact.

Map out worst-case scenarios. What happens if an IoT device fails or if it is compromised and manipulated? For example, whether your IoT devices are controlling a nuclear power plant or dispensing insulin in a diabetic patient, the ramifications of a malfunction or breach are much greater than compromising a smart watch to steal personal data.

IoT security requires a multilayered approach

Multiple threat types across IoT devices, data, and networks require a variety of cybersecurity methods — including a proactive approach to identifying and responding to threats.



Determine whether IoT devices and data can be isolated. Some IoT operations and traffic can be managed through separate networks or systems, but some will have to integrate with existing IT networks. For example, HVAC sensors and systems can typically function on networks completely separated from your firm's core IT networks and applications. You want to minimize IoT exposure to your "crown jewel" databases.

Gauge the value of the data from individual IoT devices. It's important to determine the sensitivity of data that IoT devices generate, communicate, and aggregate. (More discussion on this below.)

Only after completing such a risk assessment can you intelligently tackle the IoT security challenge. As has always been the case when it comes to IT security, the level of IoT security should be commensurate with the level of risk identified. That said, you still need to understand that IoT deployments introduce some new twists when it comes to the types and scale of risks posed.

2. Secure both information and connected devices

Traditional IT security solutions deal primarily with protecting sensitive information — the lifeblood of any organization — from theft, exposure, or corruption. Depending on the nature of an IoT solution, however, securing information may not be your primary concern.

For example, the data sent by an RFID tag on a package in transit may have little value to an outsider, and therefore has little need for rigorous security protections. Even when the data from hundreds or thousands of these devices are aggregated, the consequences of compromise may remain minor.

By contrast, if a sensor is part of a health monitor worn by a patient or a device is tracking an extremely valuable asset, such as a piece of art, the data can be highly sensitive — and desirable to criminals. In these cases, it's vital to help protect the data using existing controls, such as data encryption, network monitors, firewalls, and other familiar tools.

Beyond data protection, of course, IoT deployments introduce the need to consider device-related risks and security. By definition, IoT devices don't just generate data, but also interact in new ways with the physical world, such as controlling the flow of water or electricity. As a result, you must consider operational security threats, as well as information security concerns.

It's easy to identify nightmare scenarios for some types of IoT devices should they be compromised. People could be harmed if someone commandeers the IoT controls of a car traveling down the highway or a robotic arm in a factory. Even seemingly innocuous IoT endpoints can potentially pose significant physical risks. How much damage

might result, for example, if an office's smoke detectors are disabled and a fire occurs, or if they are falsely triggered and set off a soaking from the sprinkler system?

Given the immediate and significant risks associated with some IoT device scenarios, you may not have the luxury of analyzing archived IoT data monthly, weekly, or even daily. Many IoT deployments will require real-time analysis and response, which necessitates automated processes that have little or no human involvement. In the AT&T survey, 47% of respondents say their organizations analyze connected device security logs and alerts no more than once a day — a pace that will need to quicken as the risk profile rises.

3. Align IoT strategy and security

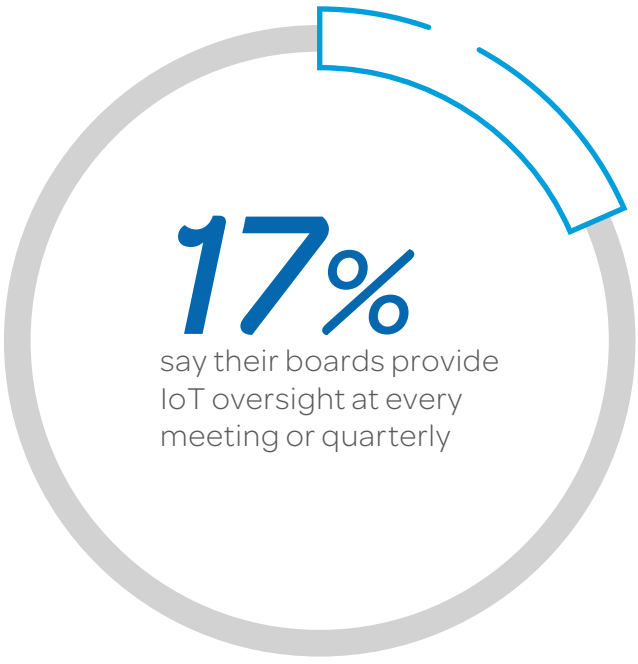
In recent years, organizations of all types have bought into the notion that IT and business strategies must be tightly integrated and complementary. This IT-business union seems to be holding true when it comes to IoT initiatives. Among decision-makers in the AT&T survey, 65% say their IoT business strategies involve collaboration between IT and business units.

When it comes to IoT technology strategy, nearly as many respondents (60%) say IT and business units both contribute to the effort. This type of cross-organization, cross-functional collaboration is critical, regardless of the thoroughness and timeliness of an IoT security-risk analysis.

The effectiveness of an IoT deployment can be undermined if your organization isn't fully engaged in the effort from the top down. The scope, speed, and potential impact from the IoT's emergence demands the attention of not just your IT security team and business units, but also your executive officers and board of directors.

On this last point, the AT&T survey provided some encouraging data. More than 90% say their boards have at least some level of involvement in providing oversight of connected devices or IoT data.

Still, the survey results suggest board involvement, overall, has room for improvement. Just 17% say their boards provide IoT oversight at every meeting or quarterly.



Security spotlight: Health monitoring

What it is: The value of IoT-connected health care devices lies in their ability to allow physicians to efficiently monitor patient health, while improving communication between physicians and patients.

Some devices measure and transmit data about different physical conditions, such as heart rate or respiratory rate. Others can dispense drugs or perform actions in response to those measurements. The various types of devices perform functions that measure common health markers in the form of wearables or are smart versions of traditional devices, such as pacemakers or insulin pumps.

AT&T has solutions for remote patient monitoring that help to ensure security for cloud-based data, as well as the device itself.

Security implications: Patient information is already a favorite target of cybercriminals. As noted in our first Cybersecurity Insights report, a health record is 50 times more valuable to a cybercriminal than a Social Security number. Data exposure and device failure can open manufacturers to compliance violations such as HIPPA and other regulatory guidelines.

Beyond data vulnerability, the risk of outsiders taking control of some devices has critical health implications and is of particular concern.

Potential security safeguards: Examine the function of connected devices — not just the vulnerabilities — and build more protections into connected things that could impact physical health and safety. Traditional cybersecurity solutions — threat detection and analysis, authorization/authentication, encryption, and the ability to securely patch vulnerabilities — are key to preventing connected-device breaches and tampering.

Security standards should become a part of an ongoing effort to protect against an ever-developing threat environment. Before production, all IoT-enabled devices should meet those security standards. In general, cybersecurity must be a consideration throughout the lifecycle of the product.

Telling stat: Only 11% of health care/life sciences providers are extremely confident in the security of their connected devices, and 30% are analyzing the logs and alerts of connected devices in real time.[15]

The level of board involvement matters, in part, because it impacts the confidence level that a company's decision-makers have in the security of their organization's connected devices. Specifically, there was a 300% increase in the number of organizations showing full confidence in the security of their connected devices when their board was highly involved.

Corporate boards and C-suite executives may well find they need to modify corporate policies and standards to see that IoT deployments meet both business and security requirements. To assess and address these needs, your organization's chief security officer must occupy a central and influential seat at the IoT strategy table.

Especially at this early stage of the IoT revolution, it's important for your organization to have clear lines of responsibility for IoT security, as well as consistent security systems and procedures throughout the organization. Even if individual business units are permitted to pursue their own IoT initiatives, they should be required to do so only in tight consultation with your organization's IoT security experts.

4. Identify legal and regulatory issues

As you explore the risks and security demands associated with IoT deployments, you must also consider your organization's legal and regulatory requirements and exposures. Most companies already understand the liabilities they face if, for example, they allow the theft of Social Security numbers or medical files.

Beyond information thefts or breaches, the physical and operational parameters of IoT devices can open new types of corporate responsibility and liability. The consequences of an IoT device that is manipulated to cause

Know the term:

SOTA/FOTA

Software-over-the-air/firmware-over-the-air, in which updates, settings, and other digital programming are transmitted wirelessly to networked devices.

physical harm, for example, will quickly surpass those associated with many information breaches.

The use of multiple vendors in most IoT deployments requires that you assess their level of IoT security.

Here again, board involvement can play a significant role, as our survey shows. As is the case with an organization's own connected devices, confidence levels in the security of their business partners' connected devices are lower when boards are less involved in IoT oversight.

Basic requirements for secure connected devices

As illustrated throughout this report, the IoT is in part defined by a dizzying variety of IoT device types and characteristics. But the IoT is also united in its reliance on certain requirements to help secure every connected device. They include:

Software/firmware update capability: Every network-connected device should have a means for authorized operators to update the device's software and firmware (e.g. software-over-the-air/SOTA and firmware-over-the-air/FOTA). Ideally, the updating process will be highly automated while still providing cryptographic checks to allow updates from an authorized source.

System reset: Every device should include a way to reset it to its original manufactured clean state.

No default password: Rather than permitting an easy-to-hack default password, each device should require the user to define a unique and reasonably secure password for access from a network interface.

No ancillary services: A device should not offer any services to the network that it does not require to support its core functions.

No backdoors: A device should not have hidden or known entry points that can be easily exploited by the device vendor or others.

Device support: Device makers should provide online access to operators' manuals, access to updates, and updated instructions. Support information should include a clear explanation of the product's support lifecycle.

Contact information and support forum: Vendors should provide contact details or a support forum to which organizations can report any problems with the device or its software.

Basic support label: Each device should carry a label that helps the authorized operator identify it and find support information.

Conclusion: Your call to action

It's easy to feel overwhelmed by the scope and complexity of the fast-materializing IoT era. You can, however, begin to reduce that complexity, first by understanding the security implications that connected devices introduce and then by building a framework for securing your IoT ecosystem.

As your organization inevitably moves into the brave new world of the IoT, we'll leave you with four questions — based on our framework for securing IoT deployments — that every CEO should ask his or her team about securing the IoT.

1. Have we done an all-inclusive risk assessment that considers the IoT as a part of our overall risk? Identify the types of risks — data and physical/operational — that every IoT deployment introduces. This will help you to apply security controls that are commensurate with each level of risk. Regardless of the device type, every connected device should meet baseline security requirements.

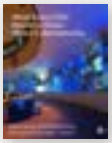
2. Are our data and connected devices secure when deploying new IoT solutions? Whenever possible, isolate IoT data and networks from existing IT systems. This will help to reduce an attacker's ability to launch broader cyberattacks on mission-critical systems. And given the massive increase in connected devices and data volumes, consider adding automated processes to monitor data and identify threats.

3. Are we aligned, from leadership to the front line, on IoT security and strategy? Communicating often with your board of directors will help ensure that corporate leaders clearly understand the opportunities and risks of IoT deployments. It's also critical that every business unit understands the unique security considerations that IoT devices introduce.

4. Have we defined legal and regulatory guidelines covering new IoT devices and deployments? It's important to evaluate the security capabilities and responsibilities of your business partners, customers, and IoT product and service providers. Establishing clear security protocols — and lines of accountability — is critical to minimizing weak-link scenarios.

The IoT era is just beginning, and many aspects of securing it remain a work in progress. Organizations in every industry are already reaping the benefits of IoT implementations. By approaching the IoT strategically, and with security at the core of every connected device, your organization can begin to capture new business value — while keeping potential risks in check.

Additional reading



- Cybersecurity Insights, vol. 1: What Every CEO Needs to Know About Cybersecurity, www.corp.att.com/cybersecurity/archives/
- Know the Terms glossary www.corp.att.com/cybersecurity/terms/
- More resources available at securityresourcecenter.att.com

About our survey

To gain a better understanding of the current state of the Internet of Things in large businesses and the current thinking behind security issues related to IoT, AT&T commissioned a survey of business and IT decision-makers in October 2015. Respondents to the State of IoT Security survey had to be director-level or above at companies with at least 1,000 employees. The self-administered survey returned more than 500 responses globally, covering a mix of functional areas and roles within the organization.

End notes and sources

1 State of IoT Security, AT&T, October 2015

2 ibid

3 "That 'Internet of Things' Thing," RFID Journal, July 1999, http://www.rfidjournal.com/articles/view?4986

4 "Things Are Getting Interesting," AT&T, January 2016 [unpublished draft of companion IoT report]

5 "How Smart, Connected Products are Transforming Competition," Harvard Business Review, November 2014, https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition

6 "Worldwide Internet of Things Forecast," 2015-2020, IDC, May 2015, http://www.idc.com/infographics/IoT/ATTACHMENTS/IoT.pdf

7 "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco, April 2011, https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

8 "What Every CEO Needs to Know About Cybersecurity," AT&T, September 2015, http://www.corp.att.com/cybersecurity/

9 "FTC Approves Final Order Settling Charges Against TRENDnet, Inc." FTC, February 2014, https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc

10 "The Internet of Things: Mapping the Value Beyond the Hype," McKinsey Global Institute, June 2015, http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

11 "Hack Attack Causes 'Massive Damage' at Steel Works," BBC, December 2014, http://www.bbc.com/news/technology-30575104

12 "FAA Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NextGen," U.S. Government Accountability Office, April 2015, http://www.gao.gov/products/GAO-15-370

13 "FBI: Hacker Claimed to Have Taken Over Flight's Engine Controls," CNN.com, May 2015, http://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/

14 "The Internet of Things: What It Means for U.S. Manufacturing," PwC, February 2015, http://www.pwc.com/us/en/industrial-products/next-manufacturing/big-data-driven-manufacturing.html

15 State of IoT Security, AT&T, October 2015

"If you don't have the ability to patch vulnerabilities or don't know if a device has been scanned for vulnerabilities, you can't connect it to your network with any degree of confidence."

Brian Rexroad
Executive Director,
Technology Security
AT&T

att.com/cybersecurity-insights