The CEO's Guide to Securing the Internet of Things

Executive Abstract | AT&T Cybersecurity Insights | Volume 2

AT&T's State of IoT Security study finds that 85% of global organizations are at least considering a strategy for the Internet of Things (IoT), with one-quarter of those cited 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.

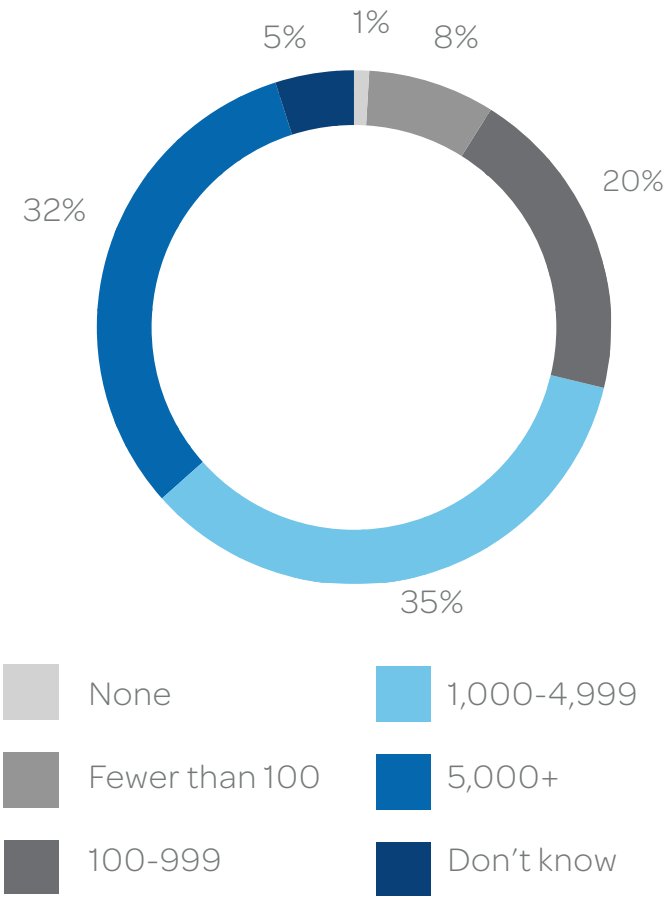
More IoT devices are coming online each and every day. Through connected devices, health care is improving patient care; for example, a diabetic patient's blood sugar level can now be monitored remotely, enabling a quick response to a possible life-threatening situation.

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.

This new generation of connected, intelligent devices dramatically increases the complexity of information security. Cybersecurity is already top of mind for many organizations, as threats grow from a broad collection of adversaries. But IoT deployments make it much tougher for C-suite executives to answer the question that corporate boards are asking with growing frequency and urgency: Has the IoT increased our exposure to cyberthreats?

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

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

The challenge: Security trails development

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.

"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 the enterprise network with any degree of confidence," says Brian Rexroad, executive director, technology security, AT&T.

The IoT attack surface is magnified by scale, distribution, and the broad spectrum of IoT endpoints, from the very simple to the highly sophisticated. The stakes climb even higher as these devices are interconnected by the thousands — and begin to bridge the digital and physical worlds.

The magnitude of the IoT is so significant, organizations need to anticipate security needs, not react to new devices as they are deployed.

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

"It's essential to architect IoT devices with security in mind," says Chris Penrose, senior vice president, IoT solutions, AT&T. "To minimize exposure to risk, it is important to isolate critical IoT devices and data from other communications."

The solution: A strategic framework for securing the IoT

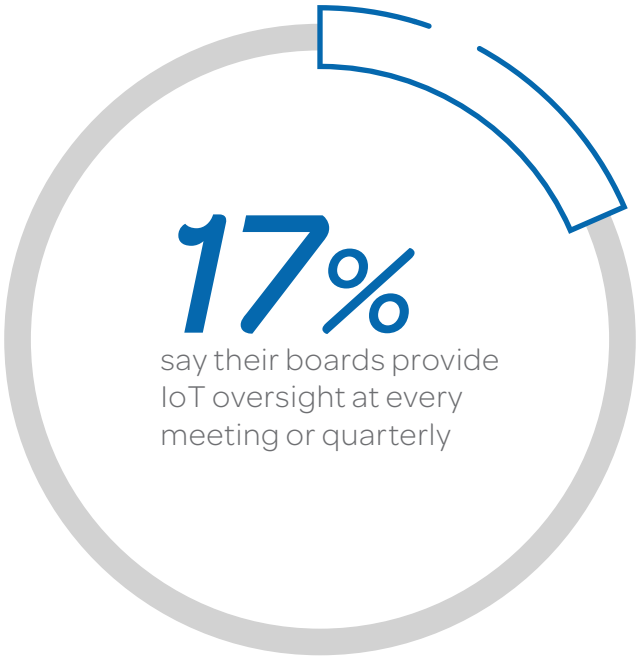
A more disciplined approach to IoT initiatives gives organizations an opportunity to implement security strategies ahead of the IoT wave. The approach requires collaboration among manufacturers, software developers, consultants, and other partners, because IoT security is only as strong as the weakest device, sensor, operating system, or application across the ecosystem.

Here's a four-part framework to help 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. Each IoT initiative takes on a security profile of its own.

A comprehensive risk profile, therefore, requires identifying and assessing every IoT device and its security vulnerabilities and mapping out worst-case scenarios for each device. You'll want to isolate IoT systems, wherever possible, to limit exposure to "crown jewel" databases. The level of IoT security should be commensurate with the level of risk identified.

2. Secure both information and devices. Data being transmitted to and from IoT devices and systems — particularly highly sensitive information — should be safeguarded with existing cybersecurity controls such as data



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

encryption, network monitors, firewalls, and other familiar tools.

Beyond data protection, however, IoT deployments introduce the need to consider device-related risks and security. Because IoT devices may interact in new ways with the physical world, such as controlling the flow of water or electricity, you must consider operational security threats as well as information security concerns.

3. Align IoT strategy and security. 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 of 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.

The level of board involvement appears to influence 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.

4. Identify legal and regulatory issues. Most companies already understand the liability risks they face from a data breach. But the physical and operational parameters of IoT devices can bring new — and potentially more damaging — types of corporate responsibility and liability into play.

In addition, the multilayer/multivendor characteristic of most IoT implementations require you to assess more than just your own IoT security needs and capabilities. You need to establish clear guidelines and levels of accountability among all business partners or product and service providers that connect to your IoT infrastructure.

Bottom line: Securing the IoT with confidence

A strategic approach to IoT security will help you to more confidently begin capturing new IoT opportunities — while keeping potential risks in check.

Read the full report at att.com/cybersecurity-insights

IoT security: Critical considerations

As organizations move into the brave new world of the IoT, following core security principles and practices will help reduce the risks and maximize the benefits of utilizing new types of connected devices. Here are the most important IoT security considerations:

Adopt a risk-driven approach. Identify the types of risks that each IoT deployment introduces and apply commensurate security controls.

Assess IoT device security characteristics. Every connected device — regardless of function — should meet certain security requirements.

Look beyond IoT device security. Secure not just device-based data and operations, but also IoT-related networks and applications.

Utilize existing security solutions. Many IoT security needs can be addressed by in-place security controls and procedures, though new controls may be required for unique IoT devices or applications.

Consider the entire IoT ecosystem. Companies must establish clear lines of responsibility with IoT product and service providers as well as business partners.

Automate security, where possible. IoT deployments are driving the need for increased automation in data monitoring, threat identification, policy management, and other facets of security.

MOBILIZING **YOUR** WORLD℠

Download the full report at att.com/cybersecurity-insights