Preparing for planet-scale security

Getting it right in electronics

IBM Institute for Business Value

Securing electronics

Despite the business-transforming upsides of data from the Internet of things (IoT), there’s a downside: security. Porous networks and lax users offer tantalizing access for hackers. Although most security spending is at the enterprise level, a shift is needed to secure IoT applications and provide improved governance and accountability. Electronics companies must create secure environments that safely collect, consume, share and store data on their networks. But they also must go beyond devices and consumers to close holes to factory, ecosystem and partner networks.

Add it up: Know who owns each element of the security equation

Data drives the insights that can keep your company competitive, but it has intrinsic value as a business asset as well. Like any asset, data requires protection. Electronics companies need to protect and secure fast-growing data, but security is complex in this industry because it crosses so many organizational domains. IoT combines operation technologies (OT) and information technologies (IT). Each area has specific design, management and decision criteria. The focus of OT is safety. It combines the hardware and software that collects information. Because IT works across people-centric computer and information systems, it should own privacy. The question is: does IoT security belong to IT? IoT creates an intersection that needs to cover safety, security and privacy across devices and networks that may be loosely controlled and not well-secured over the longer lifecycle of OT.

A recent study from the Ponemon Institute notes that the organizational functions most responsible for mobile and IoT security are often located outside of the IT security team.[2] With IoT applications, only 5 percent of respondents say the Chief Information Security Officer is primarily responsible.[3] Instead, respondents say that the head of product engineering and lines of business own the solution, and implicitly, the security of the solution.[4] That dividing line between development and long-term delivery support must be reconciled for success.

With only slight hyperbole, *The New York Times* named the 2016 Dyn security incursion, which used millions of IoT-connected devices to cause a massive web outage, a "weapon of mass disruption."[1]

Examine security at every level

Five indisputable facts about IoT security

1. Devices will operate in hostile environments. IoT devices often operate without human supervision, so they must be both rugged and resistant to physical tampering.
2. Software security will degrade over time. As the amount of time a device is in service increases, so does the risk of attack.
3. Shared settings don't remain secret. Default settings are prevalent and attackers can use them to take over devices for unintended purposes.
4. Weak configurations will persist unless users are required to make a conscious decision to remove the default protections.
5. As data accumulates, exposure risks will increase. If data isn't managed, secured and destroyed appropriately, the results may lead to loss of privacy and to issues of data ownership.

Cross-functional policies and appropriate usage guidelines are imperative. As the division between physical computers and the virtual world has blurred, system security must extend from the smallest remote equipment to the largest, most private and protected computing systems. According to the IBM Institute for Business Value report, "Securing the C-suite," 94 percent of CxOs said it's probable their companies will experience a significant cybersecurity incident in the next two years.[5] To them, the question is not if an incident will happen, but when. Executives must understand how the business might be harmed and how the damage can be mitigated.

As consumers add new devices to IT networks, protocols from industrial systems are often repurposed to drive these home appliances. Although the enterprise may have rigorous controls in place, these controls often don't exist at the consumer level. Attacks may come in the form of tampering, which includes data changes, delays or replacement. Exhaustive attention is needed at the device level as every sensor can be considered an extension of the enterprise. Endpoint devices from simple sensors to programmable logic controllers and cloud servers may be part of a complex network. Or they may be part of multiple networks, which makes determining potential points of attack challenging. As cloud is the primary platform for almost all electronics companies, evaluating the cloud providers that offer carrier-class IoT security should be a top priority.

In the electronics industry, potentially thousands of devices communicate across cloud systems and store data. Soon, these devices are expected to communicate directly with one another. You need to examine all of your communications streams, including the devices involved in routing traffic to, from and within a cloud infrastructure for potential security holes. You also need to check any dedicated, shared or virtualized hardware. The entire infrastructure needs to be frequently reexamined to account for updates from hackers and other “dark players.”

IoT systems can be deeply interconnected and all of these interfaces carry risks. For example, if you’re using third-party cloud service providers, you want to keep the information flowing into these systems safe from attack. Risk prevention and mitigation on IoT devices and connections should be included in device and data protection policies. As data moves across the networks and is collected analyzed and stored, security measures must be taken.

Consider adapting advanced security technology, such as physical unclonable functions (PUF). With shared systems, attacks on other cloud customers or the platform can propagate and affect your company too.

Data is also subject to deletion and theft for ransom. It’s important to consider how your data is connected, communicated and used, now and in the future. Evaluate the potential risks and costs of tampering and misuse. Are you protected from ransomware holding your data hostage? What about data breaches where sensitive corporate data may be released? Where are your weakest points, and are they strong enough? Assess the likelihood of incursion, the degree of damage and prioritize appropriately.

According to the Ponemon Institute, the more records lost, the higher the cost of the data breach.[6] In 2017, the average total cost ranged from USD 1.9 million for incidents with less than 10,000 compromised records to USD 6.3 million for incidents with more than 50,000 compromised records.[7]

Resolve the ethical implications

Are you ready to fortify your security footing?

- What is your planned response if a cybercriminal stole financial information from customers who purchased your IoT devices?
- Imagine if a hacker gained access to control systems of high profile rides at a theme park?
- Who's responsible when a USB key logger is used to steal personal health records and sensitive data from a hospital using a port on one of your firm's medical devices?
- What if an IoT camera on a device made in one of your plants was used to record unauthorized video which was then ransomed or posted to the internet?
- What if a malicious intruder were able to tamper with lightly-secured IoT heat sensors in a dryer to burn down a house?

Regulatory compliance is another issue complicating security strategy. In the European Union, the General Data Protection Regulation (GDPR) goes into effect on May 25, 2018 and companies will have to comply with the law's far-reaching data privacy provisions. US legislation related to IoT may also be on the horizon.[8]

Security goes beyond hardware. Whenever you're tracking personal information, privacy concerns exist. The data may seem harmless, such as how many times someone opens the refrigerator door. However, when combined with other data, it may reveal more about people than you initially intended. Attention is needed on the ethical implications of the data being collected. Many countries have published or are developing guidelines, standards and regulations to protect personally identifiable information and the personal health information of their citizens. These regulations include GDPR in the EU, and HIPAA, COPPA and PIPEDA in North America.

In the electronics industry, privacy risks increase as industrial systems are interconnected with other systems that contain sensitive data. Once the data is collected, how and where will it be used? Are there privacy issues involved? What data will be kept and for how long? Where will the data be stored and how will it be transferred? What are the implications for connecting, communicating or correlating information across devices?

For example, if data from a person's fitness tracker system is integrated with a design system shared across the ecosystem, information about the person's health could be revealed through a security breach of either system. Other risks may arise if the data is shared or distributed by third parties, such as a partner who manufactures an add-on product, an application interface or report.

Contain your risks

You need to think about the point at which obtaining information about people goes beyond assisting customers and turns into surveillance or invasion of privacy. Where do you draw the line? If a speaker is always on, could it be brought into court as evidence in a case? Will these devices be treated similarly to home security systems? What happens when wearable tech can detect pregnancy before users might be aware? Although the specific answers to these questions depend on the company, having a defined and frequently examined policy will help protect your company, your customers and your industry partners.

Security for electronics is only going to become more complex going forward. Everyone from the CEO on down must be informed and accountable for implementing and executing practices and policies regarding data, device, security and privacy.

Here are some key questions to improve security and privacy approaches now:

What is your policy for IT, OT and IoT? You need to create a policy about data, devices and the information derived from them. Also, examine security at the device level and at sufficient fidelity. Look at all systems and platforms, particularly any endpoints that are extensions of the enterprise, such as cloud providers.

Who owns and interacts with your data and customers? How well do you understand your partners' data practices and when they're reusing your customers' data? Clearly spell out how data will be collected, used, shared, validated and secured.

How informed are your customers? Develop and share specific, plain-language, customer-facing recommendations and guidelines. Be clear, specific and direct in your terms of service, so customers and users/consumers understand how their data will be used.

Experts on this topic

Tim Hahn

IBM Distinguished Engineer,
Internet of Things Security,
IBM Master Inventor
https://www.linkedin.com/in/hahnt
hahnt@us.ibm.com

Hiroshi Yamamoto

IBM Distinguished Engineer, Global
Electronics Industry CTO, IBM Member of
Academy of Technology
https://jp.linkedin.com/in/hiroshiyamamotoibm
hiroshiy@jp.ibm.com

About ExpertInsights@IBV reports

ExpertInsights@IBV represents the opinions of thought leaders on newsworthy business and related technology topics. They are based upon conversations with leading subject matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

New Orchard Road
Armonk, NY 10504
Produced in the United States of America
September 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

The data used in this report may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an "as is" basis and IBM makes no representations or warranties, express or implied.

GBE03875USEN-00

Notes and sources

1 David E. Sanger and Nicole Perlroth. "A New Era of Internet Attacks Powered by Everyday Devices." *New York Times*. October 2016. https://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html

2 "2017 Study on Mobile and IoT Application Security." Independently conducted by Ponemon Institute LLC, Sponsored by IBM & Arxan. January 2017.

3 Ibid.

4 Ibid.

5 "Securing the C-suite: Cybersecurity perspectives from the boardroom and C-suite." March 2016. https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03738USEN

6 2017 Cost of Data Breach Study Global Overview Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC. June 2017.

7 Ibid.

8 Mark R. Warner, US Senator from Virginia. "Senators Introduce Bipartisan Legislation to Improve Cybersecurity of "Internet-of-Things" (IoT) Devices." https://www.warner.senate.gov/public/index.cfm/2017/8/enators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices