IBM Security

IBM

Smart things call for smart risk management

Five indisputable facts to help you build in greater IoT security

Let's get started

IBM Security

IBM

Contents

Introduction

Consumers and businesses these days seem to be surrounded by "smart" things. Our cars, buildings and lives are increasingly becoming part of a complex, interconnected network of software, services and devices. In fact, Juniper Research has estimated that 38.5 billion IoT (Internet of Things) connected devices will be in operation by 2020—a nearly threefold increase from 13.4 billion in 2015.[1]

The "things" that are connected and represented by IoT can be anything from a wearable fitness tracker or a health device provided by a hospital, to a whole building with connected lighting, locks and automated systems. Connected cars and other vehicles are also considered IoT devices, featuring a traveling amalgamation of IoT devices and sensors working together to allow these smart vehicles to operate.

While IoT devices are improving the ways we work and live, they also present a growing security risk. And because IoT devices are both widely distributed and broadly connected, we believe it's important to recognize that the responsibility for ensuring security must be spread across device manufacturers, solution developers and users. Otherwise, it will be impossible to rely upon the systems, data and security of IoT solutions, which could ultimately impact return on investment and continued innovation.

To help reduce the potential security risks associated with continued IoT growth, IBM has identified five indisputable IoT security facts associated with building and deploying IoT devices and solutions. By understanding the risks implied by these five facts, users and manufacturers can take steps to help reduce the risks and increase the security of IoT devices and the data they both use and produce.

Five indisputable facts regarding IoT security

1. Devices may operate in hostile environments
2. Software security will degrade over time
3. Shared secrets do not always remain secret
4. Weak configurations persist
5. As data accumulates, exposure issues may increase

Understanding the roles of builders and buyers

In a simplified view, the IoT device lifecycle comprises two core constituents: builders and buyers, each with its own interests and goals.

Builders: This group includes hardware and software suppliers, along with the companies that unite them to create –and sometimes even operate—IoT devices. Builders may create all the components of the device themselves, or they may outsource all or part of the process. They tend to focus on a variety of critical security-related issues, including:

- **Cost**—While builders naturally strive to keep labor and component costs down, they must balance those cost considerations with the need to provide value, in terms of reliability, resilience and security in the final product.

- **Availability and scale**—Builders need to manage the supply of components to ensure manufacturing can keep up with market demands, often requiring complex supply chain management and sales channel monitoring to maintain product quality and reliability.

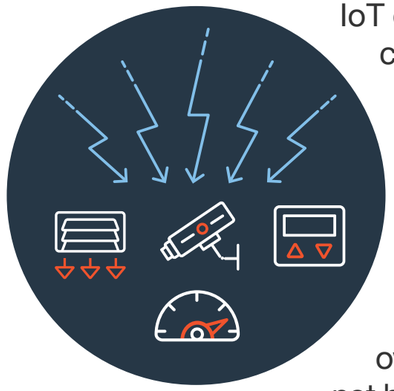
- **Identity**—Once IoT devices are shipped, analytics can make it possible for them to return value—provided that each device is equipped with its own identity. Builders need to determine how those analytics and identity management tools can be built into their devices to help optimize customer satisfaction and revenue.

- **Reputation**—If an IoT device or solution malfunctions, it doesn't matter to the user which component caused the failure. And if the impact of the failure is significant enough to generate media attention, the top-level brand associated with the device will be the one likely named in the news—and the one to potentially suffer the impact.

Buyers: This group is made up of the enterprises, consumers, users and operators who purchase and deploy IoT devices. They, too, are concerned with security—but for different reasons, including:

- **Cost**—While the marketplace generally favors the lowest possible price point, buyers are often willing to pay more for additional features and functions. But security features aren't always included in that calculation.
- **Reliability**—An IoT device or solution must perform reliably in order to be of value to the buyer, whether the device is a car, a refrigerator or an implantable medical device. When a device is found to be less than reliable, it can result in a loss of service or potentially a loss of life.
- **Privacy**—IoT devices can gather a great deal of information. Some of it is operational, and some is personal. But while builders may see the benefit and value in gaining customized behavior data and usage analytics, buyers may see it as a violation of their privacy.

Fact 1: Devices may operate in hostile environments



IoT devices typically act as computers when they're out in the world, handling information and connecting to networks. But they're not like traditional endpoints, such as mobile phones, tablets and desktops. An IoT device may not have a single human designated as its owner. In fact, many devices may not have a human associated with them at all. That means IoT devices need to be empowered protectors of their own realm, and therefore be resistant to physical tampering and extreme physical conditions, and able to recover from all types of malicious attacks.

What's more, since some IoT devices operate on a variety of networks and communicate via gateway devices, they may find themselves operating in "hostile" network environments. So they can't always rely upon those networks to provide security.

It's also important to be able to assess the risk of the deployment architecture and balance the prevailing risk, investment and potential exposures. For example, there's a vast difference between the risk and security considerations associated with a connected car and the ones associated with a connected consumer device—such as a baby monitor.

Recommendations for builders

- If a device will exist outside, provide tamper-proof access—such as physical locks for communication ports.
- House devices in climate-appropriate casings, to help make them waterproof or windproof, for example.
- Leverage tamper-resistant modules that will offer evidence of attempted physical attacks.
- Implement "fail-closed" behavior on modules—or entire systems—if tampering is detected.
- Build in remote monitoring and a capability for locking or wiping a device if failure or misuse is detected.

Recommendations for buyers

- Consider only those devices offered by reputable companies that build in security from the start.
- Look for a casing equipped with an alarm to help warn of potential weather damage or tampering.
- Place devices in protected spaces, such as inside a locked location instead of outdoors, if possible.
- Assume that all networks are hostile and provide end-to-end encryption with mutual authentication.

Physical threat considerations:

- Weather-related damage, including heat, cold, wind, rain, rot and rust
- Pests, including rodents, insects and birds
- Human tampering—including intentional breakage or sensor manipulation

Technological threats:

- Rogue access points and cell towers
- Open networks
- Interference or jamming

Fact 2: Software security will degrade over time

It's widely acknowledged today that all software in use should be kept updated. Of course that extends to IoT devices and solutions, as well. But when it comes to IoT sensors and devices, the patching process typically takes place across very distributed, highly uncontrolled environments—at an enormous scale. And while known vulnerabilities may be addressed with the initial update, it's a near certainty that new exposures and vectors for attack will be discovered over the lifespan of the device.

Technology advances over time, as do the tools and approaches attackers use to discover and exploit IoT vulnerabilities. Of course many IoT devices and solutions are expected to be in service for many years, making it even more important to acknowledge that the security of the software and firmware will degrade over time and require a secure and automated mechanism to update those devices and solutions.

What's more, the number and severity of threats are likely to increase with the length of time the equipment remains in service. That means system defenses will need to be updated regularly for the life of these devices, potentially impacting the supply chain for both software and equipment.

In the past, it was often considered safe to permanently install a device's software or firmware, assuming that it will be safe because it can't be changed. In practice, however, we all know that change will eventually become necessary. As new attacks emerge or the environment evolves, it will be important to respond and adapt to those changes. It's simply not possible to rely on a static set of security controls for the long term.

For example, it's already been demonstrated that connected cars can be vulnerable to attacks, even when they're moving.[3] The potential threat to human life—including drivers, passengers and pedestrians—makes it imperative that these types of IoT solutions be adequately secured for as long as the cars remain on the road. And that could be for decades after the cars have been manufactured and shipped.

While security attacks seem inevitable, safeguards are often missing

In a recent survey, **96 percent** of respondents said they expect to see an increase in security attacks on the Industrial Internet of Things (IIoT). Yet **51 percent** said they're not prepared for malicious campaigns that could exploit or misuse the IIoT. And that could have serious consequences. In many documented incidents, the failure to secure IoT devices allowed for significant damage and loss of privacy.[2]

Add to that the complicated update process. When vulnerabilities have been discovered in connected cars, they've often had to be brought back to the dealership or garage to be updated by a specialist. It can be a slow, expensive process that may need to be repeated within months or even weeks, as new vulnerabilities may be discovered and require new patches. The potential safety, business and liability risks of such a process are enormous. That's why some companies are now investigating and investing in more secure, over-the-air firmware updates, making physical access to the equipment unnecessary. Still, it's not enough to provide updates remotely, since that could open another potential avenue of attack. It's just as important to install the updates securely, which means verifying the authenticity of the update source—to help to prevent the updates themselves from being used as vectors for attack.

Recommendations for builders

- Build a system of self-checks and status monitoring into IoT software and components to periodically check in to verify correct operation and check for updates.
- Create a secure method for updating software over the air, ensuring mutual authentication and update media verification.
- Establish a secure distribution channel if physical updates are used (via USB, for example).
- Implement a secure software development life cycle program.

Recommendations for buyers

- Confirm that the IoT vendor employs some type of software development life cycle program.
- Look for solutions that offer over-the-air updates.
- Turn on and monitor automatic updates, if they're available.

Many IoT devices and solutions are expected to be in service for many years, making it even more important to acknowledge that the security of the software and firmware will degrade over time.

Software threat considerations

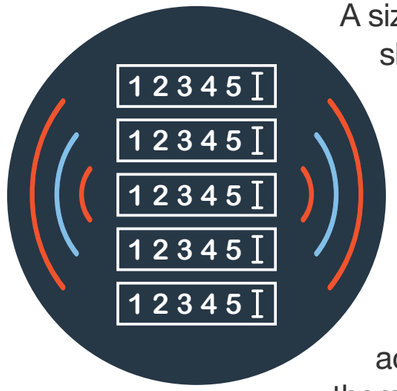
Pre-deployment:

- Well-defined security requirements
- Both static and dynamic testing
- Defined access control
- Partner and API integration

Post-deployment:

- Over-the-air updates in response to new vulnerabilities, threats and latent flaws
- Over-the-air feature and function upgrades
- Alerts for changes to partner ecosystems
- Continuous monitoring

Fact 3: Shared secrets do not always remain secret



A sizable number of IoT devices are shipped preloaded with identical credentials across multiple devices. Although these default credentials should be changed by users before the devices are made operational, they're often left as is. As we all know, however, default secrets aren't actually secret. Attackers can use them to take over those devices for unintended purposes, making them vulnerable to sabotage or disruption. But by delivering devices that prompt for a mandated password change upon first use, manufacturers can help ensure that default credentials are changed—and that secrets remain secret. Similar methods can be used for symmetric encryption keys, which present a different form of shared secrets.

So why do default credentials remain in use? Device manufacturers and solution implementers may face multiple challenges when it comes to production and deployment at a scale that can range into the millions. As a result, they often face pressure to keep prices as low as possible, sometimes dismissing security concerns altogether and preloading devices with default or burned-in keys, credentials, usernames and passwords. Reusing credentials across multiple devices adds to the convenience of mass production and bulk shipping.

What's more, identical or default credentials might make it easier for end users to deploy initially and set up those devices quickly. It could even help device and solution producers provide scripted responses for international help desk workers or remotely access and update devices with the same usernames and passwords. Of course once these credentials are exposed, they're easily shared online—sometimes with people who may have malicious intent.

The secrets we're discussing here could also be fixed symmetric keys used to set up a point-to-point encrypted communications link. They need only to be divulged once in order to reach a far wider user community. The same has been known to happen when multiple devices have been shipped with identical, but purportedly unique, identifiers.

The truth is, it might be helpful for organizations to assume that IoT devices—and the software associated with them—will be probed and penetrated for vulnerabilities. And if an IoT device is manufactured with secrets written into unprotected hardware areas, it's also safe to assume that those credentials will be compromised at some point.

IoT access considerations

- Reused passwords offer attackers easy access.
- Easy-to-remember passwords are also easy to discover and share.
- While users rarely change passwords—unless forced to do so, passwords for unattended, unmanaged devices will be changed even less frequently.
- Password themes (server1, sever2, and so on, for example) and schemas can be easily deduced—and broken.

Buy delivering devices that prompt for a mandated password change upon first use, manufacturers can help ensure that default credentials are changed—and that secrets remain secret.

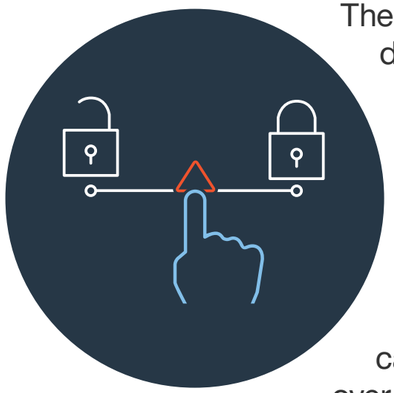
Recommendations for builders

- Make it a firm policy to ship devices with strong, unique initial passwords.
- Force device owners to always change passwords upon initial start-up.
- Require device buyers to use strong passwords.
- When working with high-security users, consider locking the system to operate in a "fail-closed" manner instead of reverting to a default password (which will never stay secret).
- Develop a trusted and secure management process and environment, in order to administer and update devices for the duration of their active lifespan.

Recommendations for buyers

- Always change the default password upon the first use of any device.
- Use strong passwords that are unique to each individual IoT device.
- Avoid using a predictable password pattern for IoT devices (Router1, Router2, for example).

Fact 4: Weak configurations will persist



The default configuration of an IoT device will usually remain in place because it is up to the users to change it. If the default settings for a given device have access control turned off, for example, it's left up to the owner to take measures to improve that security. Weak default settings can potentially lead to disaster over time.

A better approach might be to have security options enabled either by default or as part of an initial setup process, so that users are required to make a conscious decision to remove the default protections. This could lead to more secure configurations by default.

The expanding market for IoT devices and the growth of highly interconnected systems have both helped to create a new threat landscape. New devices are vulnerable to attack almost as soon as they're deployed. And in virtually no time at all, automated attack bots can strike. That's why manufacturers and solution deployment specialists need to ensure that devices are shipped and deployed as securely as possible.

While it may be convenient to produce IoT devices and solutions with weak configurations, the short term gains in manufacturing, set up and support costs are easily outweighed by the ease with which hackers could seize control of those devices and their data for malicious intent.

In the urgent rush to be first to market, solution developers and device manufacturers may operate under pressure to get everything out the door as quickly a possible. But as time and experience have demonstrated, it's better in the long run when security is built in and architected by design.

Recommendations for builders

- Ship devices with default "deny all" policies.
- Provide wizards to guide users through a secure setup process that includes architectural recommendations as needed.
- In high-security instances, enable roll-back control to a fully hardened state.

Recommendations for buyers

- Create unique user profiles for each device.
- Lock down configurations if a device is shipped without a secure configuration.
- Create a segregated network zone for devices that require open configurations for communication.

IoT configuration considerations

- All unnecessary services and communications ports should be shut off, disabled or removed.
- It's best to take a "deny all" approach and open ports only when necessary.
- Create and use access control lists with restricted access.
- Either require two-factor authentication for remote administration or turn it off.
- Implement a strong password policy.
- Turn on logging—and monitor the logs.

Fact 5: As data accumulates, exposure issues may increase

One of the key business drivers for IoT is the potential value of the data it generates, which puts a spotlight on data security. As data accumulates over time, connections between everything from audio recordings and transcripts to GPS locations and different, seemingly disparate datasets may emerge. And a sizable portion of that data—such as heart rate readings, for example—may be personal and sensitive. If the data isn't managed, secured and destroyed when it's determined to be worth less than the risk of holding onto it, the results may lead to loss of privacy and to issues regarding data ownership. That, in turn, increases the importance of partnering with IoT vendors and solution providers who can be trusted with your data.

Inevitably, IoT solutions, applications and the platforms that help harvest IoT data will become the targets of insider threats. The connectivity of IoT devices to the physical world, their links to critical infrastructure and the potential impact on human safety make it important to protect against such threats. It's likely that user behavior analytics will play an important role in providing visibility into the types of behavioral anomalies that might indicate the presence of insider threats. Organizations are now building solutions to uncover insights and gain business value from the data their IoT devices generate. That means the sensors and devices collecting the data need to be securely identified, maintained and protected. In addition, the raw data needs to be protected in transit and at rest. With the flow of data from multiple sensors and devices it's important to be able to identify personally identifiable information and manage it in accordance with international regulations and corporate guidelines.

If the data isn't managed, secured and destroyed when it's determined to be worth less than the risk of holding onto it, the results may lead to loss of privacy and to issues regarding data ownership.

IoT data accumulation considerations

- Can device data be aggregated across geographic, audio, video and voice-controlled input?
- How easy—or difficult—will it be to overlay GPS data with personally identifiable information and protected health information?
- How will third-party processing and storage impact data availability?

As data accumulates over time, connections between everything from audio recordings and transcripts to GPS locations and different, seemingly disparate datasets may emerge.

Recommendations for builders

- Create a data classification schema to manage your data more efficiently, enabling it to recall data for regulatory requirements, obfuscate sensitive data and delete redundant or obsolete data.
- Provide transparent terms of use to buyers.
- Understand and comply with all local privacy laws, recognizing that data privacy rules can change as data moves.
- Require buyers to sign off on terms of use before installing IoT devices and solutions.
- Allow for user data control where applicable.
- Implement processes to mask names and identifiers associated with personal data where and when appropriate.
- Build and manage a complete data lifecycle management program, managing the data from the time it's acquired to the time its's destroyed.
- Confirm that logging is being done in accordance with privacy terms.

Recommendations for buyers

- Read manufacturers' terms of service and use.
- Purchase from companies that are committed to protecting data privacy.
- Determine whether users are able to control how their data is used—if they can verify the accuracy of their information—and give them the right to have their data removed through a "right to be forgotten" mechanism.

Making a commitment to IoT security

Successfully mitigating the issues raised by the five indisputable facts regarding IoT security that we've discussed here will require making a serious commitment to stepping up your efforts in three key areas:

- **Device and data protection:** Begin by securing IoT devices and data according to the context within which they've been deployed. Work to ensure secure connectivity to IoT platforms, payload encryption and device identity using certificates and segregation, while encrypting data in transit and at rest.
- **Proactive threat intelligence:** Leverage network and solution monitoring tool to visualize and prioritize threats, allowing security and operations experts to focus their attention on real-time issues. Where appropriate, offer automated responses to provide proactive protection without impacting business operations.
- **Cognitive risk management:** Look toward cognitive computing to help you learn from the security intelligence gathered across your IoT landscape and provide the insights you need to deal with threats as they evolve. It's not likely that you'll be able to rely only on human response to situations involving enormous numbers of connected IoT devices. By enabling systems to detect and respond to situations as they're observed, cognitive computing will be able to provide valuable assistance in handling the complexity and scale of IoT security challenges.

These three efforts comprise a continuous cycle of learning and ongoing adjustments (see Figure 1). History has taught us that organizations must remain vigilant in addressing data safety, security and privacy.

A continuous cycle of commitment

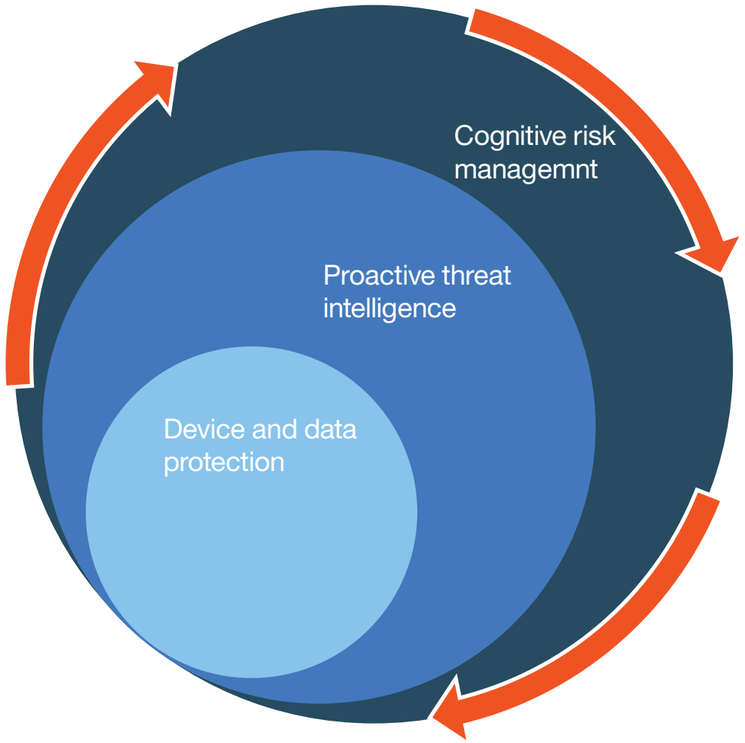


Figure 1. *Organizations need to make a commitment to improving IoT security, by continuously bolstering their efforts in three key areas: device and data protection, proactive threat intelligence and cognitive risk management.*

Why IBM

There's no doubt that the emergence of IoT devices and solutions will make an increasingly significant impact on the way both consumers and businesses function. And as the five indisputable facts regarding of IoT security point out, there are many security issues associated with IoT that need to be addressed now—before some of today's "worst practices" become standard operating procedures for the entire IoT industry.

IBM offers a comprehensive set of security solutions and services designed to help you manage your IoT journey, whether you're a builder or a buyer. Within that context, we deliver leading technology, best practices and, above all, flexibility. These capabilities and expertise are built on a heritage of enterprise security experience.

When you partner with IBM, you gain access to a security team of 8,000 people supporting more than 12,000 customers in 133 countries. As a proven leader in enterprise security, we hold more than 3,500 security patents. And with the recommendations discussed here, in addition to advanced cognitive computing, we let organizations like yours continue to innovate while reducing risk, so you can continue to grow your business—while securing your most critical data and processes.

For more information

To learn more about IBM Watson IoT global expertise and solutions, enabling organizations to securely embrace IoT through cognitive and cloud systems, visit:
ibm.com/Iot/security

To learn more about the IBM Security portfolio of solutions, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security

Additionally, IBM Global Financing offers numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition.
For more information, visit:
ibm.com/financing

IBM Security

IBM Security
75 Binney Street
Cambridge MA 02142

Produced in the United States of America
July 2017

WGB03038-USEN-00

[1] https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020

[2] https://www.tripwire.com/state-of-security/featured/90-pros-expect-attacks-risk-vulnerability-iiot-2017/

[3] https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/