DXC.technology

White Paper

10 steps to securing the internet of things

Support IoT and digital change with cyber resilience across the enterprise

Security
April 2018

Table of contents

10 steps to securing the internet of things

Support IoT and digital change with cyber resilience across the enterprise

New opportunities, new risks

The internet of things (IoT) system is just the latest development in an ongoing transformation that started with the disruption to business models caused by widespread use of the internet.

The internet enabled the real-time collection and transmission of data from any device or system connected to it. IoT systems harness the data from those devices, enable automated decisions and predictions, and help enterprises respond more rapidly and efficiently to business changes and operational demands. At its core, the IoT is a way of instrumenting, sensing and controlling connected physical devices by embedding IT in them.

The IoT is already driving change across industries, including improved equipment maintenance and asset management, connected products with new insights into consumer behaviors, supply chain automation, and new forms of human and machine collaboration.[1]

However, the IoT also presents a heightened security challenge. Security organizations must protect significantly more endpoints across the enterprise, and an IoT security breach could lead to immediate damage to IT and physical systems.

IoT underscores the need for today's enterprises to focus on cyber resilience — the ability to keep transforming efficiently and effectively in the face of increased threats from nation-states, criminals, competitors and insiders. These risks include:

- The increasingly widespread use of IoT technologies both within the enterprise and by connected stakeholders, resulting in little or no control of data security
- Continued reduction in the size of IoT devices, making them more difficult to identify and police
- Vulnerabilities in interconnected IoT devices that could result in interception of data or damage to data integrity
- Attacks that could interrupt key business systems and disrupt operations

[1] World Economic Forum, Industrial Internet of Things: Unleashing the Potential of Connected Products and Services, January 2015.

Cyber resilience in an IoT environment is critical because failures are potentially far more serious than in conventional IT systems. When operational assets are integrated into digital business processes, a security incident can interrupt not only the enterprise's operations but also those of suppliers and customers. In October 2016, the largest distributed denial-of-service (DDoS) attack ever was launched on service provider Dyn by using an IoT botnet. This led to huge portions of the internet going down, including Twitter, *The Guardian*, Netflix, Reddit and CNN.

This IoT botnet was made possible by malware called Mirai. Once infected with Mirai, computers continually search the internet for vulnerable IoT devices and then use known default usernames and passwords to log in, infecting them with malware. These devices were such things as digital cameras and DVR players.

Due to the physicality of such systems, there are physical security and safety implications. A breach could damage business partners and, in extreme cases, cause injury to workers or even loss of life. For example, an innocuous fitness app, Strava, which posted heat maps of users' exercise routes online, inadvertently revealed the location and layout of U.S. military bases in North Africa.[2] And where business ecosystems are integrated across the entire value chain, an IT security breach could have far more serious consequences.

In an IoT world, cyber resilience involves physical and organizational aspects as well as technical security. Now more than ever, cyber resilience in IoT is a governance issue that affects not just IT but the whole enterprise.

IoT and governance

In a 2016 report,[3] the World Economic Forum (WEF) pointed out that it is critical for boards of directors to understand emerging technology issues with potential to affect the cyber resilience of their business — and to take responsibility for implementing an appropriate strategy.

The report calls out IoT as such a technology, but quotes a WEF survey of business leaders indicating that 88 percent felt businesses are not currently ready for the IoT challenge.

The report described four case studies in the healthcare, transportation, automotive and critical infrastructure sectors in which IoT risks have already been identified. The inference drawn by the WEF is that it is vital, when considering IoT, for boards to consider the 10 principles of cyber resilience governance described in the report. In particular, boards should implement Principle 4 — integration of cyber resilience — making sure that all IoT systems are secure by design as they are integrated into the organization's business model.

[2] Richard Pérez-Peña and Matthew Rosenberg, "Strava Fitness App Can Reveal Military Sites, Analysts Say," *New York Times*, Jan. 29, 2018.

[3] Cyber Resilience Principles and Tools for Boards, *World Economic Forum*, 2016 (published Jan. 18, 2017).

IoT cyber resilience standards

Currently there are no standards, regulations or laws specifically aimed at securing IoT. This is unsurprising, given the multiplicity of components involved in IoT and the lack of coherence around the scope.

In August 2017, a bipartisan group of U.S. senators introduced a bill that proposed baseline security standards for any internet-connected devices that are to be purchased and used by the U.S. government.

One of the key goals of the proposed legislation is ensuring that security is designed into all new systems from the outset. This is likely to be a feature of much of the future legislation and regulation relevant to IoT currently being considered by a number of governments worldwide.

Therefore, it is important to watch this issue — making sure that new legislation and regulation do not catch organizations unaware.

While Europe does not currently have any specific legislation relating to IoT security, there are a number of European Union (EU) directives that are relevant — most notably the Network Information Security Directive,[4] which obligates operators to manage risks posed to the security of networks and information systems that they control and use in their operations.

Securing IoT now and in the future will also require the application of standards relevant to the scope of the business that any particular IoT application supports. For example, use of IoT solutions in healthcare should consider the nonbinding recommendations issued by the U.S. Food and Drug Administration on management of cyber security in medical devices.[5] Similarly, any IoT transport application in Europe will need to consider Directive 2010/40/EU on the protection of in-vehicle communications.[6]

In general, the main security risks to any IoT application are likely to be mitigated by common security controls such as network segmentation, asset and configuration management, and risk management.[7] As a result, organizations are advised to consider the use of widely used information security standards, such as the international standard for information security management systems (ISO/IEC 27001:2013).

[4] Directive (EU) 2016/1148 of the European Parliament, EUR-Lex, 2016.

[5] U.S. Department of Health and Human Services, Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff, December 2016.

[6] Evaluation of the Intelligent Transport Systems (ITS) Directive, *European Commission*, 2017.

[7] European Union Agency for Network and Information Security, Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures, November 2016.

IIoT: Emerging threats to industrial controls

The fast-growing industrial internet of things (IIoT) is a crucial technology for many industries, including utilities, manufacturing, pharmaceuticals, chemicals, and oil and gas. Operational technologies (OT), which include industrial controls systems (ICS) designed to monitor and control a wide array of industrial machines, switches and pumps, are harnessing IIoT sensor data, analytics and machine-to-machine automation to increase efficiency and reduce downtime.

Industry groups have been warning for years that these systems are vulnerable to attacks because of lax controls, such as using default usernames and passwords, and failure to patch with the latest software and firmware updates. Threats from hackers are growing. In December 2017, Schneider Electric announced a new vulnerability to millions of its Triconex controllers used in safety systems around the world by HatMan malware. According to the National Cybersecurity and Communications Integration Center, HatMan surpasses malware such as Stuxnet and Industroyer/CrashOverride with the ability to directly interact with, remotely control and compromise a safety system.[8]

To secure IIoT systems, enterprises must focus on both cyber security and physical security (see **Figure 1**). For example, IIoT devices should never be connected to the public internet unless absolutely necessary. Passwords should be unique per device, with clear policies on permissions, privileges and access controls. Additionally, physical controls should be in place to prevent unauthorized access to the plant, controllers should be secured in locked cabinets, and devices should be set to display an alarm in the control room when they are remotely accessed.

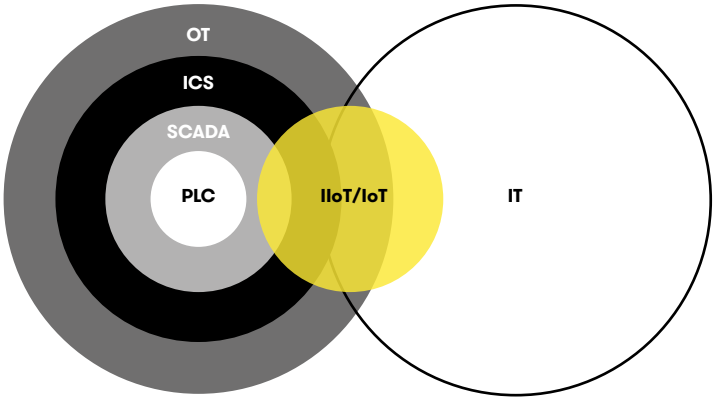

Figure 1. IT and OT systems overlap in industrial processes that rely on a series of control systems including industrial control systems (ICSs), supervisory control and data acquisition (SCADA) systems and programmable logic controllers (PLCs).

[8] National Cybersecurity and Communications Integration Center, Malware Analysis Report, Dec. 18, 2017.

How to approach IoT security

To achieve IoT cyber resilience, enterprises must begin with a thorough assessment, identifying all IoT-related assets that already exist within operations, focusing on identity and access management tools and practices, managing IoT devices across their entire life cycle, and providing proactive incident response and ongoing monitoring.

Risk assessment

As part of the risk assessment, organizations should consider how an IoT security incident would affect the business. An appropriate response plan can then be created that takes into account the policies and processes needed to detect, respond to and remediate incidents. Assess whether your IoT incident response capability is fit for purpose — if not, seek an expert partner or upskill rapidly. Conduct a crisis response simulation to understand your ability to respond to an IoT attack.

The fact that IoT device failures can have the potential to put health and safety at risk must be taken into account when determining response time frames. The plan should also ensure that business continuity and disaster recovery objectives are defined and met to enable required levels of cyber resilience. Review your disaster recovery plans to minimize damage during an IoT compromise.

Asset identification and management

Asset management must begin by understanding the system to be managed. The first step in securing IoT, therefore, is to discover and map the IoT devices on the network. In view of the ubiquity of IoT devices, bear in mind that any such an inventory may inevitably be on a larger scale than any previously conducted.

Discovery can be performed in a number of ways:

- Socially, by interviewing key stakeholders, in both lines of business and corporate functions, to understand their IoT-related projects
- Through the use of forensic accounting: analyzing capital and operating expenditures
- Technically, through active or passive (the latter is the DXC Technology preferred method) network analysis
  - Active analysis relies on software to scan the various subnets and enclaves of the network. However, such scans may cause unexpected failures in devices and may not respond as expected, so they are not generally recommended.
  - Passive analysis relies on the installation of network probes in well-architected network choke points. These will provide both device identification and information about network usage patterns.

When an inventory of IoT devices has been completed, a scope can be defined for the risk assessment. Once the assessment is complete, appropriate policies and processes can be designed and funded to manage and mitigate the risk, in accordance with the organization's risk appetite. It is important that this not be a one-off activity, but an iterative process that ensures the risks to new systems can be detected and managed.

Auto-updates: Mitigation or attack vector?

While automated patch deployment can be a great aid to reduce the vulnerability exposure window by speedily patching systems, it can open up a new vector for attack. As we saw with the CCleaner compromise[9] in 2017, a trusted means of deploying assumed to be safe executable code within the organization can also be exploited to efficiently deploy malicious executable code in a widespread fashion.

It is therefore essential to understand what update mechanisms may be used within an organization and what assumptions are made of the trustworthiness of the end-to-end process.

Identity and access management

Increased use of IoT implies increases in user-to-machine and machine-to-machine interactions. Organizations will need greater focus on identity management and strong identity assertions. Networks containing both users' personal devices and other things will be forced to rely on mutual authentication rather than default usernames and passwords. Hardware-backed security credentials should be used to limit the risk of devices being compromised and therefore of impersonation.

Such changes will require scaling of public key infrastructures to cope with increased demand. Due to the inherent nature of IoT, a convergence of physical access control, offered by building management systems, and computer access control is advised. The correlation of actions and behaviors between physical and virtual environments will help ensure that only authorized users are allowed physical access to devices.

Network access control and good architectural design, such as network enclaves and flow-based software-defined networking, should also be considered. These will limit an IoT device's interactions with the network. They will also provide an interactive means of elevating a device's access permissions as needed.

Lastly, a secure and auditable log of actions by devices and users should be maintained for operational and information security purposes. This provides a means of understanding the actions that have been taking place on the network.

Life-cycle and supply chain management

IoT systems will potentially last for many years. While it is tempting, therefore, to treat such systems as "install and forget," in practice they will require continuous support and maintenance. This is especially relevant to their security.

At the point of purchase it is important to select IoT devices that are, as far as possible, secure from known attacks, free from vulnerabilities and have state-of-the-art defenses. However, risks change constantly, so it is also important to select devices that can be updated.

Update mechanisms must themselves be secure and easy to use. They must also be integrated into your organization's operations so updates can be carried out when needed. Simple aspects of design can eliminate whole classes of vulnerabilities. Update mechanisms will also give a quick feel for whether the supplier understands the need for security — for example, by ensuring that the device forces users to set a strong password during configuration.

Once in operation, the device's behavior must be observable. Systems will therefore be needed to carry out and interpret those observations. If the device's embedded operating system allows remote connections for administration purposes, for example, it must also be able to log that information to a central system for analysis.

[9] Pieter Arntz, [Updated] Infected CCleaner downloads from official servers, Malwarebytes Labs, Sept. 18, 2017.

At the end of an IoT device's life, it may contain information that should be erased prior to disposal. Such information, for example, could be the keys for your WiFi network, or the last set of data sampled by the device. Information of this kind would be of great use to a potential attacker.

It is therefore important to choose suppliers that focus on security and will continue to do so throughout the life cycle of the installation. By definition, IoT devices collect data and communicate it. You must therefore be sure that your supplier has trustworthy manufacturing partners, that they produce firmware that collects only the data you want and sends it only to you.

Incident response

Within the enterprise, safety and availability are crucial in IoT systems. Incident responders must consider whether an attacker may be able to cause a failure that results in threat to life, or whether a critical service — such as energy production — could be halted, resulting in mass disruption to clients.

The quality of any response to an IoT disruption or attack is directly correlated to the comprehensiveness of the enterprise's preparation for that response. IoT safety preparation should be treated in that same way that the business prepares for fire safety. Documentation, drills and disaster recovery all need to be considered in advance of the incident.

Therefore, DXC's preferred approach is analogous to firefighting. Three core priorities are critical during incident response:

- **Stop the spread.** Prevent the attack or disruption from compromising further machines. Take proactive steps to anticipate the trajectory of the attack, and disable systems or connectivity as required.
- **Prevent damage.** Safety must remain the highest priority, while stopping the attacker from communicating with compromised systems and executing dangerous commands.
- **Extinguish the threat.** Remove the cause of the attack or disruption and implement defensive measures to prevent further compromise.

Enterprises need to consider whether they have capable forensic resources to deploy at a moment's notice and the information needed to make those forensic efforts effective. IoT systems offer forensic investigators a number of unique challenges, such as:

- **Legacy systems.** Extended refresh cycles mean that equipment may be decades old and ill-suited for forensic analysis.
- **Custom-built architectures.** Many IoT systems are tailored to each implementation. Given its esoteric nature, the architecture is often understood only by a select few in the enterprise. With high staff turnover, knowledge is often lost — making investigation and remediation challenging.
- **Physical access.** IoT systems will be of varying sizes, from the tiny to the very large and widespread, some perhaps even being mobile — so gaining physical access may prove challenging.
- **Absent or unhelpful logging.** Typically designed by engineers rather than security experts, IoT logging, if available at all, is often of limited use to security professionals.
- **Proprietary protocols.** While protocol standardization in the IoT world is taking place, it is by no means complete — often few can understand the exchanges that occur between machines, making network communications analysis complex.
- **Inability to rebuild.** Reimaging IoT components, such as programmable logic controllers, is often impossible — therefore recovery from attack, if it can be achieved, is a time-consuming and highly specialized process.

None of these challenges is insurmountable. However, they can only be overcome if appropriate preparations are made in advance. Attempting to do so when machinery has been shut down, or when thousands of clients have been left without a vital service, is destined for failure.

Security monitoring

Security is a dynamic situation. One of the lessons from decades of general-purpose computing is that installing a system, setting it up correctly but then just leaving it does not ensure a secure solution. Apart from updating the system as vulnerabilities are discovered, it is necessary to monitor the system to detect issues and respond to them to address problems and disrupt adversaries. This lesson applies to IoT as well.

Historically, technology deployed in industrial control environments tended to be heavily monitored for availability and to ensure the correct functioning of the systems that it monitored and controlled. However, the behavior of the devices themselves was less closely instrumented and monitored, leading to security gaps. Lack of ability to oversee device behavior meant there was no way to respond to insecure activity.

Effective monitoring and response in an IoT environment is not yet a fully established discipline, but it is a necessary one. It must be considered in any new IoT system design and deployment. Fortunately, many IoT devices are designed as single-purpose systems with relatively simple, well-defined behaviors. This means that, once monitoring has been established, it is far easier to identify anomalous behavior than it is for general computing devices.

However, because many IoT devices have inherent safety imperatives, security responses require far shorter decision cycles than those of traditional IT security operations. Historically, these have meant mean times from occurrence to remediation lasting hundreds of days.

A safety-first secure system, on the other hand, may require subsecond response times. Companies should pursue early detection through well-instrumented systems, and implement rapid response via orchestration. More aggressive responses may be required, with “safety first” being the default — for example, quickly removing a device’s access to the system without waiting for a decision from the device owner.

It is clear that as IoT gains momentum there will be a dramatic increase in the scale of what enterprises will need to secure and monitor. Failure to build cyber resilience into IoT installations could have serious consequences. But if companies take a proactive approach, they can achieve cyber resilience for IoT, and the business can reap the benefits.

What steps should the CISO take?

Here are the 10 most important actions that a chief information security officer (CISO) can take to mitigate risk to IoT systems.

1. Make sure the board of directors understands the security risks associated with IoT systems and is prepared to fund measures to mitigate and manage them, particularly by ensuring that security is designed into all new systems.
2. Apply well-established international standards (such as ISO 27001) and sectoral guidelines (such as those issued by the U.S. Food and Drug Administration) and keep watching for new legislation and regulation in this area.
3. Identify your IoT systems and assets and inventory them.
4. Assess the risks to your inventoried IoT systems and establish appropriate policies and procedures to mitigate them.
5. Ensure that IoT devices can be identified on the network and that means are in place to manage and control their access permissions.
6. Use only those IoT devices known to be secure and ensure that these are updated regularly to meet changing risk profiles.
7. Use only trustworthy suppliers that will support your IoT systems throughout their life cycles.
8. Ensure that you have an IoT incident response plan in place — and that it is reviewed and tested regularly.
9. Ensure that your IoT devices are visible to your monitoring systems and that anomalous behavior can be detected.
10. Ensure you have a "safety first" attitude when responding to IoT incidents and are able to take rapid and effective action when needed.

Learn more at www.dxc.technology/security

Authors

Luc Manfredi
Security Principal
DXC Technology

Lukas Hatala
IoT and Analytics Consultant
DXC Technology

Simon Arnell
Security Chief Technologist
DXC Technology

Rhod Davies
Security Customer Advocate
DXC Technology

Jeremy Ward
Cyber Security Solution Specialist
DXC Technology

About DXC Technology

DXC Technology (DXC: NYSE) is the world's leading independent, end-to-end IT services company, helping clients harness the power of innovation to thrive on change. Created by the merger of CSC and the Enterprise Services business of Hewlett Packard Enterprise, DXC Technology serves nearly 6,000 private and public sector clients across 70 countries. The company's technology independence, global talent and extensive partner network combine to deliver powerful next-generation IT services and solutions. DXC Technology is recognized among the best corporate citizens globally. For more information, visit www.dxc.technology.

MD_7950a-18. April 2018