Raising Your IoT Security Game

Author

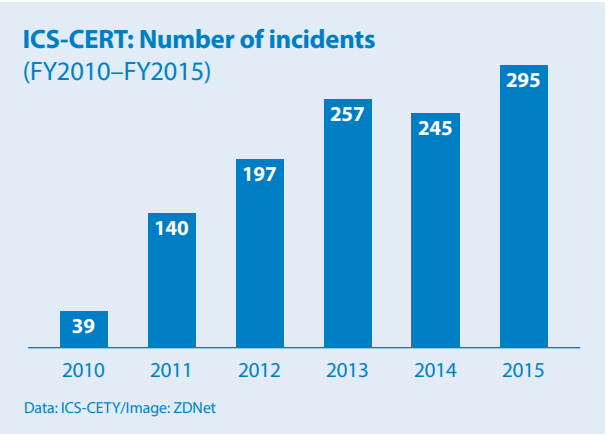
Satish Thiagarajan

Global Head, Cyber Security Practice, Tata Consultancy Services

The Internet of Things (IoT) opens up opportunities for companies to improve visibility of their operations and the products they make by collecting data from sensors attached to a range of machines, from controllers at factories to aircraft engines. But while many companies are embedding sensors and wireless communications devices into their industrial control systems and products, each implementation has the potential to open up their systems to hackers who can steal data or disrupt operations.

In the U.S., IoT incidents logged by the U.S. Department of Homeland Security rose more than seven-fold between 2010 (39 incidents) and 2015 (295).[56] Researchers project IoT will rise on the list of risks for chief information security officers (CISOs). Two-thirds of computer networks will see an IoT security breach by 2018, IDC researchers predict, adding that

[56] Charles McLellan, "Cybersecurity predictions for 2016: how are they doing?" ZDNet, September 15, 2016, accessed at http://www.zdnet.com/article/cybersecurity-predictions-for-2016-how-are-they-doing/.



by 2020, 10% of all attacks will target IoT systems. Gartner analysts say they expect IoT security costs will rise to 20% of annual information security budgets by 2020, up from a rounding error (less than 1%) in 2015 budgets.[57]

The risks of a breach in corporate networks incorporating IoT capabilities are real. Examples abound:

A regional water company saw its web-based payment system and operational technology system hacked, an event that led to unauthorized manipulations of its programmable logic controllers.[58]

Researchers have identified security flaws in the communications protocols used in medical devices such as implantable cardiac defibrillators that can be adjusted remotely without surgery.[59]

A demonstration by two hackers showed it was possible to gain control of a connected car with the knowledge of its IP address.[60]

[57] Gil Press, "Internet of Things Predictions from Forrester, Machina Research, WEF, Gartner, IDC," Forbes.com, January 27, 2016, accessed at https://www.forbes.com/sites/gilpress/2016/01/27/internet-of-things-iot-predictions-from-forrester-machina-research-wef-gartner-idc.

[58] Michael Hill, "Water Treatment Plant Hit by Cyber-attack," Information Security, March 24, 2016, accessed at https://www.infosecurity-magazine.com/news/water-treatment-plant-hit-by/.

[59] Lily Hay Newman, "Medical Devices are the Next Security Nightmare," Wired.com, March 2, 2017, https://www.wired.com/2017/03/medical-devices-next-security-nightmare/.

[60] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me in It," Wired.com, July 21, 2015, accessed at https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

The risks extend to consumer devices that interact with corporate networks. In 2016, malware called Mirai hijacked IoT devices such as closed-circuit video cameras and digital video recorders that used factory-default security settings. Those devices, in turn, attacked Dyn, an Internet infrastructure company that underpins top websites. The incident created problems for users at popular sites like Amazon, Twitter, Reddit, and Netflix.[61]

Such incidents demonstrate why companies must lock down their connected systems and networks, including the ones they use to design and manufacture their products and the connections they embed in their products.

The incidents show the vulnerability of interconnected systems that many parties have access to. And they point to the urgency that enterprise risk management leaders confront as they seek to maintain and improve existing defenses.

The Risks Embedded in IoT

The promise of IoT is that its technology can automate functions that are much more expensive to do manually. It's impractical to employ large operations teams to monitor all plant equipment 24x7. It's easy, and relatively cheap, to install sensors and connect them to a network that will alert managers to problems. It's now feasible to equip advanced engines with devices that provide ongoing measures of their mechanical health.

[61] Brian Krebs, "Hacked Cameras, DVRs Powered Today's Massive Internet Outage," Krebs on Security, October 21, 2016, accessed at https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.

But as IoT deployments have spread, risks have emerged. Manufacturers designed IoT devices with functionality in mind, not security. IoT devices are out in the field—attached to company products, in locations around the world—and are often not monitored centrally for attacks (unlike the corporate data center). As a result, practitioners see that attacks such as IoT botnets can spread quickly because many IoT devices are rarely patched or updated.[62]

In fact, the risks of IoT devices being hacked are far greater than they have been for any previous technology assets deployed by companies in at least three respects:

1 The large number of devices to monitor (millions, in the case of a large automaker instituting cloud-delivered infotainment systems or self-driving cars) makes the IoT a larger risk to manage than the thousands of laptops, desktops and mobile phones used by the employees of a major enterprise

2 The challenge is also more geographically dispersed due to IoT sensors embedded in products and machines installed or moving through corners of the world that are often far beyond where the company has offices and employees

3 The relatively new nature of the technology means there are heterogeneous platforms to manage. IoT devices are full of hardware and software from different vendors that make assessing vulnerabilities, patching software, and monitoring ongoing risks a multidimensional challenge

62 Verizon Security Solutions, 2017 Data Breach Digest, accessed at http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf.

Know What You're Dealing With

Addressing the IoT security challenge requires an understanding of your IoT landscape in detail. This includes analysis of what devices you have and at which point they may be vulnerable so that you can address critical security gaps. Companies must establish a group that will mitigate current problems and manage future risks. A comprehensive review requires eight steps:

1. Appoint a centralized team accountable for IoT security. A centralized team that includes the CISO must be accountable for securing the company's IoT devices—and ensuring the firm's ongoing compliance with risk management policies.

To establish this team, companies must evaluate the maturity (in terms of in-house skills and practices) of their IT organization and the operations technology (OT) organizations. In some companies, this exercise means confronting a cultural clash. While IT professionals typically have more experience managing information security based on experience and industry-established best practices, there nevertheless may exist a distrust between IT and OT based on each group's unfamiliarity with the other.

A common organization that combines experts in control systems for operations facilities, such as integrated control systems, and IT security can bridge this gap. In addition, standards organizations for IT and OT can serve as a resource for the centralized team applying the same principles to OT devices, such as the ISO 27001 standard[63] for information security management systems and the ISA/IEC-62443 standard to prevent cyber attacks on industrial operations.[64]

[63] International Standards Organization, document "ISO/IEC 27000 family—Information security management systems," accessed at https://www.iso.org/isoiec-27001-information-security.html

[64] Bill Lydon, "What Can We Do to Prevent Cyberattacks on Industrial Operations?" International Society of Automation Interchange blog, March 2014, accessed at http://automation.isa.org/2014/03/cybersecurity-strategy-and-actions/.

Once set up, the centralized team can:

- Monitor control-systems compliance with corporate policies for managing IoT devices
- Ensure that software patches are up to date for plant instrumentation, IoT devices, and infrastructure
- Run regular audits for security practices
- Conduct constant network monitoring

The team should also incorporate new best practices that emerge for IoT devices. For example, industrial service providers, including GE's Achilles program, certify devices and the organizations that implement them for compliance to the IEC-62443 standard.[65] Others provide IEC-62433 assessment services to organizations that deploy industrial systems. In addition, device manufacturers can provide maintenance and support remotely for their products. While a potential benefit to companies deploying IoT devices, such remote access must be controlled and secure.

2. Locate your company's critical IoT assets.
The first priority is to identify all the connected devices and sensors your company uses, and then determine which ones represent a significant security risk. Companies often discover assets about which they were previously unaware. You must also distinguish between those assets that signify important risks and those that do not. Not every asset is critical. In some cases, the risk of a breach occurring through a particular device is less urgent than the resources required to address the remote chance of a problem.

With all that said, these assets are likely to be distributed across enterprise networks and geographical locations, and may be found in isolated networks within industrial plants. They will be present in both IT systems and OT systems, including:

- End-point devices, such as PCs, laptops, smartphones, tablets, and other mobile computers
- Devices that move with transportation containers, trucks, and ships
- Industrial control systems managed by supervisory control and data acquisition (SCADA) systems, in factories and other facilities
- Legacy infrastructure, such as the controllers that utilities use to manage flows of electricity, water and natural gas

[65] GE Digital information sheet, "Achilles Practices Certification," accessed at https://www.ge.com/digital/sites/default/files/achilles-practices-certification-from-ge-digital-datasheet.pdf

3. Identify the software vulnerabilities in your IoT assets. Software vulnerabilities are the most significant risk facing IoT-connected devices. With an inventory of critical assets in hand, a company can assess which software governs the actions of each piece of hardware.

Different device manufacturers use their own conventions in software protocols, and each requires an assessment of its vulnerabilities. (For example, can a hacker exploit it remotely? How can such a weakness be fixed?) For some devices, changing the security settings in the product that was shipped can be enough to address a risk. For others, such as various generations of Windows devices, there may be known network vulnerabilities for which an immediate patch is available.

Failure to update software can leave systems susceptible to attacks, such as the one that occurred in May 2017 when a variant of the WannaCry ransomware program infected tens of thousands of computers worldwide.[66] It is imperative to maintain updated software patches on critical assets.

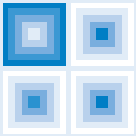
4. Discover devices that gain entry to your networks. As companies assess their own devices and software, it is important to understand when new devices—whether they are company-owned or devices used by customers, business partners, or contractors—access corporate networks. Where possible, use technology that can automate the discovery of new devices.

However, you must manually detect isolated networks at industrial sites that support your IoT devices. Assess the vulnerability of these devices and execute patches on them. If they are owned by external parties, require the parties to do the same.

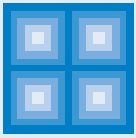
[66] Jeremy Ashkenas and Adam Pearce, "Animated Map of How Tens of Thousands of Computers Were Infected With Ransomware," New York Times, May 12, 2017, accessed at https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html.

5. Watch out for emerging threats.
Monitor all connected devices for evidence of new threats such as distributed denial of service attacks. Such attacks often arise from either a software developer error or the open source software community, as hackers seek to exploit uncovered vulnerabilities in software code. Isolate the devices that are the target of threats and apply software patches to them.

6. Inspect new devices before they connect.
Establish a process for ensuring that new devices, purchased or added, include security features in their hardware, software and network connection, and that the security features are updated.



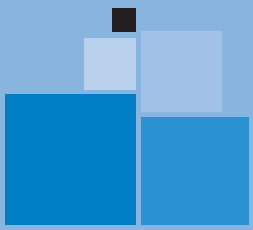
7. Demand best practices from your business partners.
Make certain that the business partners that have access to your networks also have strong security programs—and that they demonstrate compliance with your procedures. For example, a repairs contractor, which needs to access connected systems and devices must have implemented security measures such as software updates, and comply with your company's policies before it can enter your network.



8. Have backups ready.
A cyber security program for IoT systems fits into a broader corporate risk management program. Incorporate its elements into existing plans for disaster recovery and business continuity already established to deal with a system breach. Include information about IoT security in the company's incidents communications strategy.

IoT Security in Action: Three Cases

The experiences of three companies we have worked with show how IoT cyber security can work.

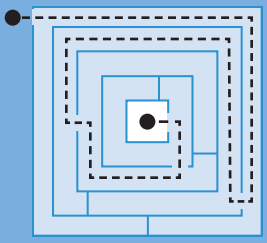


Manufacturing firm strengthens its OT security

Situation: At a manufacturing company, executives understood their plant floors had embedded software and Wi-Fi network connections in a typical mix of legacy equipment and newer devices. Such assets included programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems and human-machine interfaces (HMIs) to control industrial processes. The company had other connected devices including equipment for its field support crews, business continuity, and incident management programs.

Actions taken: The company deployed non-invasive software tools designed for IT systems and customized to work with OT network protocols, to scan all of its devices for vulnerabilities. The tools identified vulnerabilities, and the company then repaired them. After finishing this process at one factory, the company repeated the process at other factories.

Takeaway: By applying best information security practices developed for IT systems, this company was able to identify and remediate security risks in its operations. Building on its record, the company was able to monitor its devices and systems, and update its practices to address future vulnerabilities.



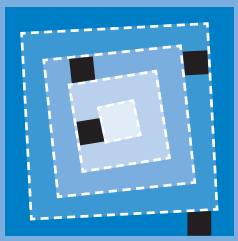
Utility establishes OT security roadmap

Situation: Concerned that its IoT devices presented a security risk, leaders at a utility company sought to identify problems and solutions.

Actions taken: The company began a 12- to 18-month assessment of its organization's security capabilities in addition to its security practices and controls, adapting the ISO 27001 IT standard developed for OT security. Assets evaluated will include controllers, HMIs, asset management systems, as well as equipment for the field service organization. The assessment also will examine how OT security should be included in its incident management plans and business continuity program.

The assessment will identify high-value assets that need immediate attention, as well as other measures the company must execute as part of a comprehensive OT security management plan.

Takeaway: By adapting best security practices for IoT devices, the company is strengthening its risk management posture.



Company establishes security governance program OT

Situation: After performing an IoT security assessment, executives at a utility company sought to develop capabilities to manage cyber security.

Actions taken: The company adapted IT best practices for its OT organization. It defined OT security policies. It established an OT security governance process with defined roles and responsibilities. It set metrics for governance procedures and security actions. It scheduled regular reports for the OT organization to update executives on the security status of its IoT assets.

Takeaway: An OT organization can establish strong information security governance to mitigate IoT security risks.

Manage Risks While Capitalizing on IoT Benefits

In the excitement to take advantage of IoT, companies today must assess the risks of a security breach or loss of control of important operational systems. Firms that demand secured technology will lay a strong foundation for ongoing risk management efforts.

Programs to prevent a security problem—such as updating and patching systems—and procedures to deal with any security disruption will enable companies to prepare for the worst as they seek to make good on the promise of this powerful technology.

Throughout these efforts, executives should ensure that IT and OT devote their experts' time to collaboration. The CISO should play a role while IT and OT leaders in a central group monitor conditions, follow best practices to mitigate risks that exist, and respond to incidents. A strong cyber security strategy includes continuous testing for, and addressing of, vulnerabilities in IoT devices.