CyberTalk.org

What Security Leaders Need to Know About IoT Regulations

IoT DEVICES ARE EVERYWHERE, BUT ARE THEY SAFE?

As your organization's cyber security executive, you have witnessed firsthand the unprecedented growth of the Internet of Things (IoT) devices in your organization. They are everywhere these days. Although slowed by chip shortages and supply chain issues, global IoT connections still grew by 8 percent in 2021 to 12.2 billion active endpoints, and they were projected to grow 18 percent to 14.4 billion devices in 2022.[1] IoT spending is expected to reach US $1.1 trillion in 2023.

> "Cyber attackers are increasingly weaponizing OT environments to attack hardware and software that control industrial processes and secure OT networks. Skilled workforce shortages and overlapping IT and OT environments can make cyber incident containment difficult."
>
> *— Ramsey Hajj, Deloitte US, and global cyber OT leader*

Organizations, large and small, have integrated IoT devices onto network infrastructures, allowing new ways to use and manage collected data. Both consumer and business users have seen a huge influx of IoT devices. Consumer IoT devices can include smart home monitoring, cameras, routers, printers, televisions, among many others. Business uses for IoT vary widely, including keeping track of customers, inventory, and the status of important components. Industrial IoT devices have been widely used in industries such as oil and gas, agriculture, automotive, transportation, and others. The diagram below provides a sample of typical uses for consumer and industrial IoT:

IoT Use Cases

[1] "State of IoT 2022: Number of connected IoT devices growing to 14.4 billion globally," by Mohammed Hasan, IoT Analytics, May 18, 2022

IoT: UNDERSTANDING THE RISKS AND REWARDS

The ubiquitous deployment of IoT does come at a cost. For many of these devices, security of the device and its data are nowhere to be found, promoting active security risks, including Denial of Service attacks, malware, ransomware, and DNS spoofing. IoT are attacked to take advantage of username and password, and bypass code security issues. Per intelligence analysis at Google, "We have already seen large-scale attacks using IoT, in the form of IoT botnets. In that case, actors leveraging unpatched vulnerabilities in IoT devices used control of those devices to carry out denial of service attacks."[2]

Additionally, the automation found with many critical infrastructure projects can render networks vulnerable to cyberattacks. Realizing IoT security can be lacking, governments are on the move to introduce regulations aimed at improving the security of IoT devices. In this paper, we provide a brief review of current regulations.

IoT CYBER SECURITY REGULATIONS IN THE US AND EU

In 2017, ENISA, published a study recommending baseline security recommendations for IoT.[3] It has served as an important reference point for relevant forthcoming initiatives and development. One such attempt to regulate IoT appeared with the California IoT law, a mandatory privacy provision first created in 2018 and enacted on January 1, 2020.[4] This privacy law requires manufacturers of connected devices to equip the device with a reasonable security feature or features and sold in the state. Oregon has also followed suit.

Elsewhere in the US, the IoT Cybersecurity Improvement Act was passed in 2020, and the National Institute of Standards and Technology (NIST) was tasked with creating a cybersecurity standard for IoT devices. In May 2021, the Biden administration released an Executive Order to improve national cybersecurity, and in October 2022, the White House released a Fact Sheet, including the use of labels for IoT devices indicating their level of cybersecurity. It starts with routers and home cameras.

The creation of these laws was spurred by government realizing that IoT devices are highly vulnerable, and the manufacturers failed to adopt security capabilities, or any security recommendations were treated a voluntary regulation. Purchasers and users of these connected devices saw them as instrumental to normal business operation and used them without security precautions. Only when IoT devices became targets of significant cyberattacks did the awareness grow that manufacturers have a responsibility to provide cybersecurity with their IoT products.

---

[2] "The dark web's criminal minds see Internet of Things as next big hacking prize," by Elizabeth Macbride, CNBC, January 9, 2023
[3] "Baseline security recommendations for IoT," ENISA, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
[4] "IoT Manufacturers – What You Need to Know About California's IoT Law," by The National Law Review, January 28, 2020

In the European Union, the European Parliament has introduced the Cybersecurity Act and the Cyber Resilience Act, which impose several requirements for manufacturers to meet before a product can receive the CE marking and be placed on the European market. This includes stages of assessment and reporting and managing cyber-attacks or vulnerabilities throughout the product lifecycle. The General Data Protection Regulation (GDPR) also applies to companies operating within the EU and requires them to implement appropriate technical and organizational measures to protect personal data. The Data Act that was adopted by the Commission in February 2022 ensures fairness by setting up rules regarding the use of data generated by Internet of Things devices.

One research report states that one in seven cyberattacks in the UK in 2022 sought to gain control of devices connected to IoT.[5]

In a separate action, the UK enacted the Product Security and Telecommunications Infrastructure Act 2022 in December 2022. Manufacturers, importers, and distributors of internet/network-connectable products for UK consumers and some businesses must comply with relevant security requirements, provide a product "statement of compliance regarding security requirements, investigate potential compliance failures, among other specified duties.

It is important to note that other countries around the world are adopting or in the process of enacting IoT security regulations. Such regulations could call for mandatory compliance in the manufacture and use of IoT devices, both consumer and industrial.

[5] "Business Cyber Threat Report 2022," Beaming, https://beaming.activehosted.com/social/67f7fb873eaf29526a11a9b7ac33bfac.60
[6] "Baseline security recommendations for IoT," ENISA, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

KEY ELEMENTS OF IoT SECURITY REGULATIONS

To comply with the regulations, manufacturers must implement the following key elements:

1. **Software Updates:** Manufacturers must provide the option for firmware updates and ensure the validity and integrity of updates, particularly for security patches.

2. **Data Protection:** Regulations follow the concept of "minimization of data", collecting only necessary data with user consent and securely handling and storing sensitive data in an encrypted manner.

3. **Risk Assessment:** Developers must follow a risk management process during the design and development phase and throughout the product's life cycle, including analyzing Common Vulnerabilities and Exposures (CVEs) and releasing patches for new vulnerabilities.

4. **Device Configuration:** Devices must be released with a security-by-default configuration and have dangerous components removed, interfaces closed when not in use, and a minimized attack surface through the "principle of least privilege" for processes.

5. **Authentication and Authorization:** Services and communication must require authentication and authorization, with protection against brute force login attacks and a password complexity policy.

6. **Secured Communication:** Communication between IoT assets must be authenticated and encrypted, using secured protocols and ports.

NAVIGATING REGULATIONS WITH CHECK POINT QUANTUM IoT PROTECT

Complying with these regulations can be challenging due to their complexity. To make the process easier, various certifications and standards such as UL MCV 1376, ETSI EN 303 645, ISO 27402, and NIST.IR 8259 have been introduced to break down the regulations into practical steps.

Check Point has introduced Quantum IoT Embedded to help manufacturers secure their devices with minimal effort. The solution includes a risk assessment service and a Nano Agent® that can be embedded into an IoT device to provide on-device runtime protection against cyberattacks. The Nano Agent® is a standalone solution that can be added to a product without intrusive code change and requires only minimal resources. Benefits include:

- On-device runtime protection blocks known and unknown (zero-day) cyberattacks
- Access control and Login protection against brute force attacks
- Password complexity policy enforcement
- Data Protection with top industry encryption
- 100% firmware coverage including 3rd party components
- Lightweight, non-intrusive architecture with minimal impact on the device performance
- Consolidated management, visibility and logging available with Check Point Infinity Portal or API
- Comply with top standards and regulations for IoT security (NIST, UL, ETSI, and more]

Quantum
IoT Protect

For more information, head to https://www.checkpoint.com/quantum/iot-protect/iot-device-security/