
www.pipelinepub.com
Volume 20, Issue 9

# Enhancing IoT Security in Critical Infrastructure

By: Andrea Carcano, Michael Dugent

As global digitalization continues in virtually all aspects of society, seemingly millions of new devices are connected to corporate networks and the internet on a daily basis, creating a much larger attack surface for nefarious actors to take advantage of. Cybersecurity researchers note that numerous attacks nowadays are driven by a desire for control and destruction, placing critical infrastructure environments squarely in the crosshairs of hackers. Critical infrastructure systems -- the assets and networks, be they physical or virtual, underpinning the functioning of an economy and society -- determine the security, prosperity, well-being, and resilience of an entire nation.

A recent report focused on Operational Technology (OT) and Internet of Things (IoT) security, revealed that threat actors are not only escalating their attack frequency but also honing their tactics and identifying new entry points. In 2023, cyberattacks fueled by nation-state actors affected 120 countries, with over 40 percent targeting critical infrastructure.

Nowadays, cyberattacks on critical infrastructure represent a global risk, demanding heightened attention and deeper understanding of activities that pose a potential threat. Attacks on critical infrastructure environments often include targeting IoT environments first, as these devices are often easier to compromise and monitoring of these environments is still limited. In this regard, IoT is an important concept embedded within a larger spectrum of networked products and digital sensors that has caused an explosion of applications, marking a fundamental shift in the way human beings interact with the Internet, amplifying both opportunities and challenges surrounding critical infrastructure across the globe. The question arises: why do threat actors target IoT environments?

# IoT in Industrial and Critical Infrastructure

In October 2016, the most significant **DDoS attack** in history left a large portion of the East Coast of the United States without internet. The following year, hackers accessed sensitive personal and financial data from a **North American casino.** In March 2021, a security camera company was attacked, **exposing live feeds from 150,000 surveillance cameras in hospitals**, manufacturing facilities, prisons, and schools. The common thread among these three attacks was that the perpetrators targeted the IoT environments of these companies to gain access to their internal systems.

The Internet of Things, known as IoT, is a system of interconnected computing devices. The definition of what constitutes an IoT device varies widely and includes everything from biomedical implants to sensors on manufacturing and electrical equipment. An industrial ecosystem can encompass many different smart devices that collect, send, and act on data from their environments. Sometimes, these devices even communicate with each other and act on the information they get from one another.

Over the last 10 years, industrial and critical infrastructure operators have rapidly deployed billions of devices to optimize their automation processes using the data provided by these "things." Unfortunately, this trend has created new cybersecurity risks, as these devices are open to networks, both public and private. These endpoints have become low-hanging fruit for attackers who want to compromise operational processes and maximize the economic benefits of a cyberattack.

As digital transformation leads to an increase in unmanaged devices across industrial environments, the importance of a robust IoT security program to safeguard critical infrastructure from cyberattacks cannot be overstated. But what makes IoT security such a challenge for companies?

# Keep in Mind: IoT Security Challenges

First of all, IoT devices are often unmanaged and inherently insecure. Once deployed, the software on these devices is seldom updated, especially firmware where many vulnerabilities exist. As a result, these devices remain susceptible to attacks that could easily be prevented on other managed devices. Secondly, the use of default passwords and weak authentication procedures makes these devices easier to compromise than managed IT devices. Attackers frequently exploit default and predictable passwords to access smart devices, which can then be used to target other critical devices and networks. **Recent regulations** announced by the UK Government aim to address this issue by banning manufacturers from using weak, easily guessable default passwords. But while this is a significant step towards eliminating "insecure by design" devices, it is not enough to protect IoT environments from penetration.

Another reason for IoT environments having weak resilience is that IoT devices typically connect to an ecosystem that includes business applications, data centers, IT infrastructure, and the cloud. Their inherent lack of robust cybersecurity controls makes them attractive targets for hackers seeking entry into broader networks. Moreover, large-scale industrial IoT deployments do not easily accommodate the level of network segmentation required to mitigate cyber threats or prevent malware spread. Most IoT devices also lack the capacity to host software security agents due to their limited processing and communication capabilities, as well as insufficient space for such software.

Finally, IoT devices are often deployed without the involvement of IT or cybersecurity teams. This can lead to devices being placed in sensitive or insecure areas of the network, making them easier to compromise due to the absence of additional cybersecurity layers.

# Keep in Mind: Security Guidelines

First, it's essential for companies to understand the types of IoT devices used within their organization and the associated risks, and to make sure that every device is accounted for. This involves identifying all the devices communicating on the network (including devices connected wirelessly), understanding the data these devices collect and transmit, and understanding the potential impacts of a cybersecurity incident. An integral part of this step is implementing an asset management mechanism that can track every connected device with real-time data.

Second, organizations should take steps protect their networks from threats by deploying suitable security controls. This includes measures capable of isolating or terminating connections linked to malware or other anomalies. It also encompasses network segmentation, multi-factor authentication (MFA), and encryption. Companies should establish a process to understand the most critical assets and to prioritize patching the highest risk and most vulnerable assets first to reduce overall risk exposure and increase resilience.

Implementing monitoring and detection mechanisms is another crucial step for companies to identify potential cybersecurity threats and vulnerabilities. These mechanisms could involve network monitoring, log analysis, and security incident and event management (SIEM) systems. Utilizing an industrial network monitoring solution that integrates with network access control (NAC) products can expose significant potential risks in real-time.

Next, companies need to develop a plan for responding to cybersecurity incidents. This includes procedures for isolating affected devices and systems and communicating about the incident to relevant parties. Comprehensive incident response playbooks and forensic analysis tools can aid in achieving this swiftly and efficiently. Finally, planning and practicing business continuity strategies for recovering from cybersecurity incidents is vital. This includes procedures for restoring affected systems and processes and mitigating any potential impacts.

In addition to these steps, companies should collaborate with industry partners and government agencies to share information about cybersecurity threats affecting IoT devices. Regularly reviewing and enhancing cybersecurity procedures to ensure they remain effective against the evolving threat landscape is also recommended. Critical infrastructure organizations should prioritize proactive defense strategies that include network segmentation, asset discovery, vulnerability management, patching, logging, endpoint detection, and threat intelligence. There is also a growing need for actionable asset and threat intelligence that can be used by different stakeholders within an organization such as IT teams, compliance officers, and risk managers who may have different perspectives on security issues.