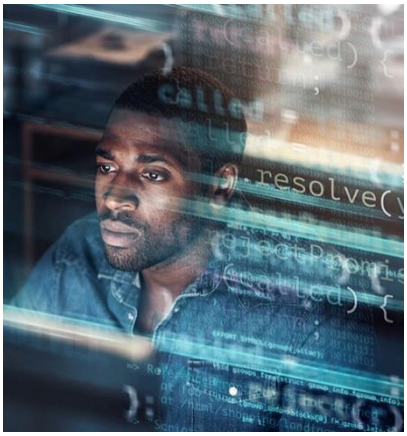
www.pipelinepub.com
Volume 18, Issue 9

IoT Device Security for the Future of Cyber Resilience

By: Dennis Mattoon



We are living in an increasingly digital world with the Internet of Things (IoT) playing a huge role in how we live and work. A wide range of IoT devices can be found in the home, from smart lightbulbs and refrigerators to doorbells and cameras, and in factory or office environments, too. In industrial settings, many machines and devices are connected to streamline processes, enable remote operation, and boost efficiency. But with IoT devices nearing 27.1 billion in 2021, according to Cisco, security must be a key consideration in their development and manufacturing.

Sophisticated attacks

In recent years, we have seen numerous attacks across many industries and environments, including critical infrastructure, which have caused significant damage. Attacks on the systems, assets, facilities, and networks that society relies upon for public health, safety, and security can cause widespread levels of disruption on a national or even global scale. If critical infrastructure is compromised or taken down, it does not take long for the impacts to be felt beyond governments and corporations to ordinary citizens. The attack on the Colonial Pipeline, the largest fuel pipeline in the U.S, is a recent example of this type of attack. The system was shut down for six days in response to a cyberattack, increasing average gasoline prices in affected areas.

The level of sophistication shown by cyber criminals is growing, while the rising number of connected devices implemented across industries is also opening the door to more attacks. The rise in IoT devices is often driven by industrial digital transformation and the benefits that come with it. Increasing automation, enabling remote operations, increasing efficiency, and

streamlining operations are just a handful of benefits. Security is not usually a driving force here, as it can often be considered as an unnecessary added expense.

As all IoT devices need to be connected to a network to function, however, we need to view each connected device as an entry point, allowing access to that network and all the sensitive data generated, stored, and communicated. This is why security must be at the top of the agenda when these billions of devices are created on the factory floor: manufacturers and developers must start taking a security-first approach if we want to stay ahead of cyber criminals.

Proactive IoT device security solutions

We need to place an emphasis on security right at the start of a device's creation. Security must be a key consideration as prevention methods built in at this stage will protect it throughout its entire lifecycle. It is important that a device has the ability to protect itself, respond to attacks, and recover. Cost is often used as a justification for not prioritizing and funding security measures properly but implementing the steps that allow a device to do this will actually save time, resources, and costs in the years to come.

For this to happen successfully and universally, the implementation of cyber resilient architectures is key. The three primary principles for resilience are: protecting updatable persistent code and configuration data, detecting when vulnerabilities are not patched or when corruption has occurred, and recovering reliably to a known good state even when the platform is compromised. When implemented correctly, a cyber resilient architecture allows for a device to be recovered, even after it has been compromised and hacked. If we compare this to today, recovering a badly compromised device usually involves manual intervention. For example, a new firmware or a new OS must be loaded from an external storage device or a second computer before a device can rejoin network services using passwords or other credentials. But with billions of IoT devices in use right now, it is extremely difficult to manually intervene when one has been compromised. Not only that, but IoT devices of the future will be built from the same imperfect software in use today and manual remediation will become increasingly impractical and unfeasible due to the sheer number of devices.

Creating cyber resilient devices, however, negates this issue, as the device can protect itself, respond to attacks and recover without any human intervention. The role of IoT is growing in importance for enterprises and consumers alike but having a way to securely manage devices and regain control without manual intervention is vital for ensuring security in the long-term.

Guidance for cyber resilient devices

Not every organization has the required knowledge or experience to create this new layer of security. Not-for-profit organizations and groups, such as the Trusted Computing Group's Cyber Resilient Work Group, bring together members of leading technology companies to define, develop, and promote global, industry-wide specifications and standards with guidelines that are simple to follow. This Work Group has recently released a new specification, titled *Cyber Resilient Module and Building Block Requirements*, that helps organizations develop a solid foundation for cyber resilience and reduce the risk of cyberattacks.

By following a set of building blocks, cyber resilient capabilities can be easily implemented into devices at the stage of manufacturing. As devices are made up of numerous firmware layers and components, many of which have potential vulnerabilities, it is possible they may need servicing of the code and configuration of one or more layers.

By following these key steps, cyber resilient devices can be built with a limited range of resources, as often the technologies that support secure and reliable remote device management and recovery have several barriers, such as cost. With the ability to create these devices with limited means, more organizations of all sizes and budgets will be able to build in efficient security measures from the get-go. Enhancing the security of IoT devices cannot fall to one of two individual groups; it requires the ongoing effort and support of the entire ecosystem.

Preventing the damage of attacks

There is also a real risk when it comes to businesses who utilize devices within their day-to-day operations. Not only can attacks cause on average $200,000 worth of damage, but vitally important systems can be taken offline or taken control of, while extremely sensitive commercial information is often stolen and used for industrial espionage. It came to light in 2020 that US aerospace and satellite companies were attacked in 2015, with hackers stealing intellectual property and important commercial data, costing millions of dollars and causing a breach of national security.

No matter the industry, businesses need to ensure that they are proactively preventing the damage of attacks, rather than waiting until it is too late and paying a costly ransom or having to rebuild their business—and public trust. Cyberattacks are inevitable, but businesses must take every action possible to minimize the downtime and long-term damage to their company.

Securing IoT for the future

The use of IoT offers businesses a wide range of benefits, including improved efficiency, enhanced productivity. and reduced costs. With IoT devices generating large volumes of data that can be used to streamline operations and inform strategic business decisions, those not utilizing IoT are at a significant disadvantage compared to others in the same industries. However, if the security of these devices is not a priority, the use of them can do more harm than good by opening the door to cyberattacks and the financial, reputational, and logistical disadvantages these bring. With the latest data breach report by IBM and the Ponemon Institute finding that the cost of a data breach has increased by 10 percent since 2019, there is no better time than now to prioritize the creation of cyber resilient devices for a secure IoT future.