Overcoming IoT Security Challenges

As we move towards a world where almost everything is connected, people must be able to trust the devices and the data they generate. That means IoT technologies have to be designed with security in mind.

Here, we outline the challenges that creates for original equipment manufacturers (OEMs), and in particular, business leaders who are tasked with seizing the opportunities presented by the IoT while managing the practicalities of building a secure device.
Overcoming IoT Security Challenges

More companies are putting connected devices at the heart of their digital transformation strategies but how do we ensure the benefits of the technologies outweigh the risks?

The potential of the Internet of Things (IoT) is often measured by the number of devices that have been or will be connected. With forecasts suggesting there will be over 75 billion IoT connected devices by 2025, the growth is impressive but does not shed light on the impact those devices will have on businesses and society.

That is hard to define because it is a future we are still imagining. For example, we know infrastructure could run more efficiently than ever before; that people’s health may improve with the development of state-of-the-art medical devices, and we will be able to save lives and improve mobility when autonomous vehicles appear on our roads. But is it time to ask ourselves if this is a future we are prepared for? Are the foundations we are building it on secure?
What are the key security challenges for OEMs?

1. Addressing the lack of security expertise
2. Aligning a unified approach to security
3. Right-sizing security to minimize downtime
4. Creating a security-by-design culture
5. Getting regulation ready
6. Future-proofing beyond device shipping
7. Reducing the cost of failure
8. Prioritizing security to build consumer trust
Addressing the lack of security expertise

In recent years, cybersecurity has become a sought-after skill, which means finding the right people with the experience needed to protect devices and data can be a challenge.

Traditionally, many companies focused their attention on developing unique features and services and, therefore, lack the expertise and resources to build-in security from the outset. That includes understanding the threats to their device and implementing good security principles.

The result is unused network ports, improper device attestation, and provisioning, and physical interfaces that are not needed, for example, JTAG access and hardcoded credentials. This increases the attack surface unnecessarily.

Key Takeaway

Having one security expert in your organization isn’t enough. Instill knowledge transfer and equip the wider organization to understand security, giving them the right frameworks and drawing on expertise from across the industry. Make security an integral part of how all developers build the products.
Aligning a unified approach to security

The data that is being gathered by IoT devices enables business leaders to make more informed and timely choices, but they need to know that every device that is generating information has a consistent level of security built-in.

If devices come from different manufacturers, who all work to their own security standards, there will be no consistency in the approach or implementation, and leaders will struggle to understand and trust the devices. Also, inconsistency puts IoT networks at risk, leaving them vulnerable to attack.

Key Takeaway

Device makers should ensure a consistent standard of security is designed-in to the hardware and firmware of all devices. The ecosystem has an important role to play in this. We all need to work together to identify and share industry best practice, so we can overcome current and future security threats and make sure everything is built on a common foundation of security.
Right-sizing security to minimize downtime

Hackers are always looking for new ways to attack IoT devices, which means OEMs’ commitment to security has to be sustained. New vulnerabilities and threats will continue to emerge so device makers cannot address security once, and then forget about it.

However, the ongoing effort requires ongoing investment - more time and resources have to be allocated to security, as capital (CapEx) and operational expenditure (OpEx), which puts a strain on limited budgets.

Key Takeaway

As the costs of security are determined by the number of measures needed to adequately protect a device, and the number of assets in need of protection, manufacturers must be able to identify the right level of security for their product. This will help OEMs avoid under- or over-investing in security. Designing-in security from the outset will also save time and costs associated with patching or retrospectively fixing hardware security issues.

In addition, using certified components will help device makers reduce the total cost of ownership because security has already been built in. The benefits extend to customers as well - trusted frameworks, and drawing on industry best practice, will help OEMs minimize downtime in their operations.
Creating a security-by-design culture

To build security into a device, OEMs should consider how they will, for example, avoid cloning and reverse engineering, and protect their product from software and hardware attacks. That means security should be implemented in the early stages of the product development lifecycle.

To do this, device makers need to adapt their development processes. It may also call for a shift in organizational culture, which can be challenging.

Key Takeaway

OEMs should ensure their product development lifecycle starts with security. Threat modeling and security analysis will help identify and assess the threats to a device, as well as appropriate countermeasures. Engaging security experts from the outset will ensure the right behaviors and approach are embedded within the organization and that security is designed-in to every product.
An increasing number of governments and standards organizations have responded to a rise in the number of attacks on IoT devices in recent years and are trying to protect consumers' data and privacy by introducing new security laws, regulations, and baseline requirements. They vary between countries, regions, and states, which makes it hard for device makers that are shipping their products nationally or globally to know what rules they have to comply with in each location. They also focus on different aspects of security and that creates confusion and fragmentation within the industry.

Key Takeaway

To meet the requirements in the world’s biggest markets, OEMs should base security initiatives on best practice, as demonstrated by industry leaders. In addition, they should look for security frameworks that align with multiple regulations and certify their device so they can provide customers with evidence of implementation.
Future-proofing beyond device shipping

Cyberattacks are inevitable. That means OEMs should carefully plan their response now rather than thinking the matter can be addressed if an incident occurs.

As we connect more devices, the attacks surface will continue to grow, and attempts to access products and data will become increasingly sophisticated. However, more often than not, hackers will take the path of least resistance. That is why security patches are so important.

Key Takeaway

Hardware security is difficult to update, so device makers should ensure security is built into a device from the ground up. Security should also be implemented and work seamlessly across all layers.

It is also vital that security is available and affordable throughout the device lifecycle. While product lifecycle management and patching are complex and expensive, retrofitting is very costly, time-consuming, and complicated.

Disaster management and restoring normality is key.
Reducing the cost of failure

OEMs are risking their brand, investments, and even their existence if they do not take security seriously. And yet, that risk is not easy to qualify or quantify, which means risk modeling and liability assessments can be challenging.

This leads to questions like how we will quantify the risk impact of technology enablement to support business risk judgments and in what ways will the responsibility and liability for failure be defined.

Key Takeaway

OEMs need to take a proactive approach to security, so they are not creating issues due to their inaction. One reason for that is the cost of failure is high. According to insurer Hiscox, the median cost of a cyber event to the nearly 2,000 companies it surveyed for its recent Cyber Readiness Report was $57,000.

The situation is even worse if people’s lives are affected because the impact extends far beyond financial costs.
Prioritizing security to build consumer trust

The IoT has captured consumers’ attention. A study carried out by market research and consulting firm, Parks Associates, found adoption rates for smart home devices rose from just under 10% in 2014 to almost 30% five years later. The number of devices in the average household also increased, along with homeowners’ intention to buy at least one product.

OEMs now have an opportunity to build on that momentum. However, they should have aware - the same Parks Associates research also shows that almost half of the people who don’t own a smart device are not buying one because of their concerns about privacy and security.

Key Takeaway

Consumers are savvier than ever before, and they want to know that devices have been developed with security built-in. That means manufacturers need to re-think their approach to product development. In the past, they may have focused on the features of a device, for example, power efficiency. Now, they have the add on consumers’ technical concerns and provide security functionality out-of-the-box.

They should also seek independent certification to help to demonstrate that security has been designed in correctly. This will help OEMs increase their top and bottom line.
A checklist for OEMs looking to implement security

- Rely on industry-leading security experts
- Follow industry best practice
- Use freely available resources
- Demonstrate your commitment to security
- Comply with new and emerging baseline requirement
To help OEMs overcome the challenges of developing secure devices we have developed PSA Certified, an industry-backed security framework, and independent assurance scheme that makes it quicker and easier to build trust in connected products...

How PSA Certified Can Help

By tapping into the knowledge and experience of world-leading security experts
The PSA Certified framework was developed by seven industry-leading firms. It is reviewed and updated regularly by security experts.

By following industry best practice
The framework and accompanying resources have been built systematically and have been made available by partners within the ecosystem.

By aligning security with market requirements
The program offers mapping to new and emerging security laws, regulations, and baseline requirements.

By enabling OEMs to showcase their commitment to security
A multi-level evaluation process is overseen by independent labs. The certification scheme enables OEMs to demonstrate that they have taken the steps necessary to protect a device.

By reducing the complexity of security
Free and easy-to-access resources include threat models, security goals, a Root of Trust, and APIs. In addition, PSA Certified hardware and software components are independently assessed as having security built-in. They are available to OEMs to help ensure the required level of security has been implemented. Reducing the complexity of security means device makers can minimize their reliance on security experts.
Discover More

Find out how a robust framework and security certification program can help you overcome your barriers.

Read the PSA Certified Program Overview