IoT SECURITY REGULATION REPORT

WHY IT'S TIME TO REGULATE TO ACCELERATE

Infineon

IoT security regulation is needed to underpin market acceleration

As volumes of IoT deployments scale-up, the question of security has never been more important, writes George Malim, the managing editor of IoT Now. We've looked on in horror at the well-known breaches such as the Jeep hack by Wired magazine and the Las Vegas Casino aquarium water pump cyberattack but these have been in relatively confined, experimental environments and are not at the hyperscale of IoT. The scale in itself is a security issue and that is compounded because IoT is truly global and therefore is enacted under different regulations in different nations.

In addition, IoT relies on different technologies both in the devices and in the networks used to connect them. Some connectivity is fundamentally more secure than others, such as private 5G in comparison to home Wi-Fi, and therefore regulating IoT security is complex and multi-layered. Hunger to get to market first and fast has also weakened prioritisation of security as organisations battle to become market leaders of new sectors

To date, securing IoT has relied on well-established IT, web and network security but there is an increasing need for IoT-specific solutions and a growing awareness that regulation is required. IT security that works well for protecting servers or PCs in offices only goes some of the way to securing remotely deployed sensors, surveillance cameras or the multitude of endpoints and sensitive data that traverse IoT networks. Systems need to take security more seriously to increase customer confidence in IoT and avoid a wave of breaches that hamper the early phases of the massive IoT market.

"There are several key technologies revolving around authentication security that currently transform the IoT device value chain,"

Dimitrios Pavlakis

IoT-specific security regulation is required to establish a framework for IoT security and to clarify what levels of security are needed. This could, ultimately, lead to a certification process in which IoT devices and services could be certified secure. Some are keen to see levels of security defined that reflect the security requirements of different IoT applications, with certification matched to the business value and security risk profile of the deployment.

A sensor that alerts if a bin is empty has a different security priority to a streetlighting system interacting with an autonomous vehicle. Each also will face security constraints in terms of the cost of securing it. The notion of appropriate security that matches and optimises security to the device and its business case needs further exploration and definition to both protect systems adequately and foster user and operator confidence that products are secure.

This is well-understood and reflected by predictions of increased spending on IoT security from analyst firms. In **Figure 1,** IoT Analytics projects a CAGR of 44% in spending on IoT security in the period 2017-2022. Technavio has also been monitoring the IoT security market and predicts it is poised to grow by US$80.94bn during 2020-2024, progressing at a CAGR of almost 37% during the forecast period.

Internet of Things connections are expected to exceed 23 billion across all major IoT markets by 2026, according to new figures from ABI Research. The analyst firm's 'Device Authentication in IoT Technology' report reveals almost all those connections will be faced with incessant and constantly evolving cyber-threats, forcing implementers and IoT vendors to embrace new types of security to protect managed fleets and connected assets. Secure device authentication is among the top-tier investment priorities for key IoT markets, the firm reports. It expects that hardware-focused IoT authentication services will reach US$8.4 billion in revenues by 2026.

"There are several key technologies revolving around authentication security that currently transform the IoT device value chain," said Dimitrios Pavlakis, an industry analyst at ABI Research. "Chief elements among them revolve around IoT identity issuance, provisioning, authentication, encryption key lifecycle management, access management and attestation. These are the prime focus of IoT vendors who capitalise on the emerging threat horizon to better position their services and explore new IoT monetisation models."

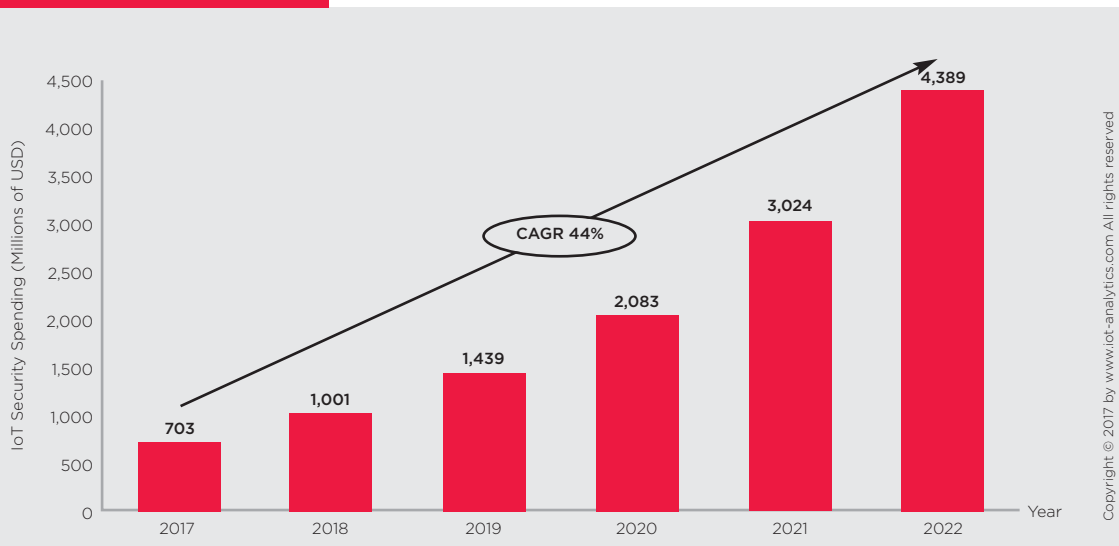

Figure 1:
IoT security is being invested in

Governments in both the UK and United States have been working to enhance consumer protections included in IoT devices

The regulations

Since the first government-mandated IoT-specific security regulation was made with the introduction of security certification criteria for smart meter gateways to support Germany's roll-out of smart meters, other jurisdictions have worked to create IoT security regulation. The German Federal Office for Security in Information Technology (BSI) set out common criteria for securing smart meters as part of the country's Smart Meters Operation Act (MsbG), which came into force in September 2016.

The Act stipulated that once three certified smart meter gateways are available, national roll-out could begin. Certification guarantees that the smart meter gateway meets the strict technical and security criteria defined by the BSI, making them suitable for installation in intelligent metering systems first outlined in the legal framework for smart metering laid down by the Bundesministerium für Wirtschaft und Energie (BMWi).

Germany has not been alone. Governments in both the UK and United States have been working to enhance consumer protections included in IoT devices. In the US, for example, California became the first state to pass an Internet of Things (IoT) security law, which went into effect in January 2020. The state of Oregon is following closely. The legislation, the California Senate Bill 327 (SB-327), requires "reasonable security feature or features that are appropriate to the nature and function of the device." SB-327, which was first proposed in 2018 and became law in January 2020, has received criticism from the security community, which has complained that, while the bill is a good first step, it does not go far enough in regulating IoT security.

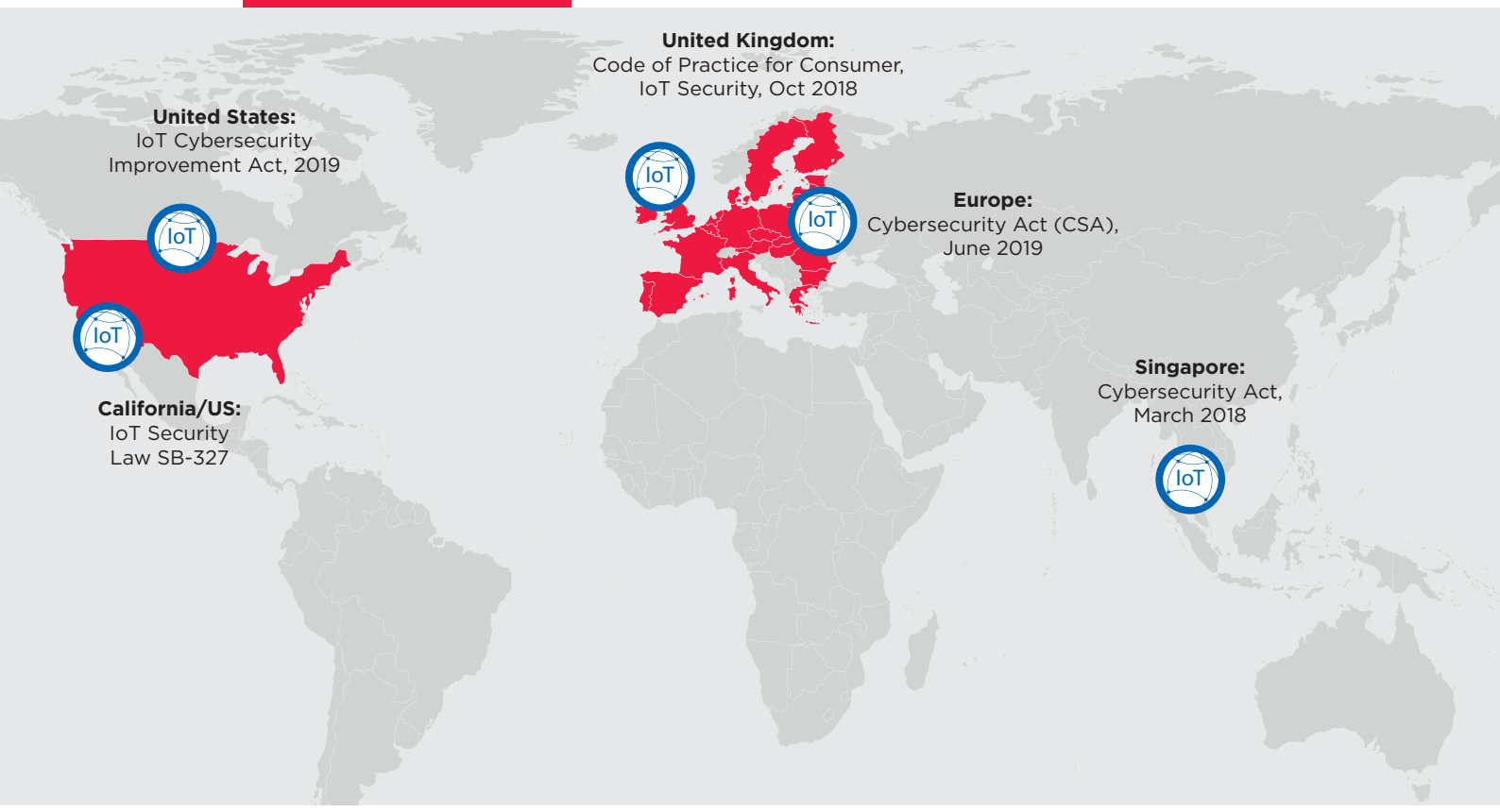

Figure 2:
Pioneering IoT security regulations

Source: Infineon Technologies, 2020

The UK's draft law, announced in late-January 2020, comprises three main requirements for IoT manufacturers

In the UK, the government has also introduced a new draft law that will require certain cybersecurity features to be built into IoT products and clearly labelled on the packaging. Both of these IoT security laws could become templates for other nations.

The UK's draft law, announced in late-January 2020, comprises three main requirements for IoT manufacturers. All consumer IoT device passwords must be unique and not possible to reset to universal factory settings. IoT device manufacturers must provide a public point of contact so that anyone can report a flaw to be "acted on in a timely manner". Finally, manufacturers must also explicitly state the minimum length of time for which devices will receive security updates at the point of sale.

The UK has been early to address the IoT security challenge and previously introduced its Secure by Design Code of Practice for consumer IoT security, which was launched in 2018. However, this was a guidance rather than legislation and had no penalties for manufacturers who did not comply.

Several other attempts at IoT security regulation do exist globally. In the European Union, ENISA (European Union Agency for Network and Information Security) has published its Baseline Security Recommendations for IoT with a particular focus on critical national infrastructure. Other industry initiatives include the IoT Security Foundation's Code of Practice, which provides a basis for testing and certification of IoT security.

Source: UK Department for Digital, Culture, Media and Sport

Figure 3:
Elements of the UK's optional code of practice

These initiatives are far from the end of the IoT security regulation journey and, in the EU in particular, these practices are not mandatory. Regulators need to work out how effective standards and practices can be enforced pragmatically. The task for IoT device manufacturers is to ensure that products are secure by design and by default.

The Singapore Cybersecurity Act is among the most stringent regulation to be applied to IoT

The Singapore Cybersecurity Act is among the most stringent regulation to be applied to IoT and looks to level up digital security and digital resiliency measures across industry sectors that provide essential services in Singapore. KPMG says the Act provides a framework to Critical Information Infrastructure (CII) owners on their obligations to proactively protect their data and networks from cyberattacks. The defined CII sectors in the Act are energy, water, banking and finance, healthcare, transport (land, maritime, and aviation), info-communications, media, security and emergency services, and government.

Organisations in the CII sectors are required to take the following measures:

- Prevent, manage and respond to cyber security threats and incidents;
- Protect Critical Information Infrastructures (CII)
- Share CII information with the Cyber Security Agency of Singapore (CSA) in the event of a cyberattack.

Source: Infineon Technologies

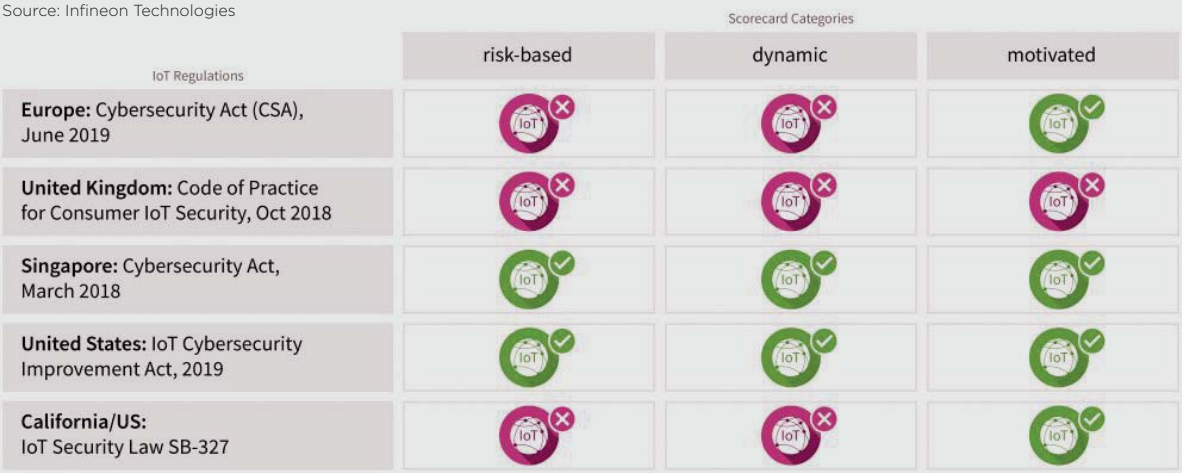

Figure 4:
How current regulations compare

From design to default

The well-intentioned UK Secure by Design Code of Practice provides an effective framework for securing IoT but its lack of enforcement weakens it to being mere guidance. It's therefore clear that enforceable legislation like the Singapore Cybersecurity Act are required and these will play an important role of moving security to become a default in IoT as it is in the IT world.

Along this path, IoT security must become visible and simple to understand for consumers and customer organisations. There will be many different shades of IoT security, as discussed earlier, and an easy means to demonstrate the security credentials of a device or solution is through an independent certification programme. It could be as simple as a traffic light system, or a platinum to bronze spectrum of security levels.

Some have put forward the concept of an IoT security equivalent to the Energy Star certification for energy efficiency of appliances, electronics, HVAC systems and others. Energy Star is a US government programme, but IoT is global and unlikely to be able to wait for government action. Instead, the IoT industry could develop its own security certification system. This would make it easy for customers to immediately understand the security capabilities of an IoT device and purchase accordingly.

The labelling initiative, led by the Finnish Transport and Communications Agency, Traficom, began development late last year

An additional function of this would be that lower security devices may no longer be saleable and therefore the sticker system could provide a generalised uplift to security across all of IoT as users vote with their feet and only buy secure systems.

Finland is leading the charge here and has launched a cybersecurity labelling system to inform consumers of IoT products that meet digital safety standards. The labelling initiative, led by the Finnish Transport and Communications Agency, Traficom, began development late last year. It will see a stamp placed on every smart device that adheres to Finland's cybersecurity safety guidelines.

A website is also available for vendors to become certified with the security badge, and for consumers to make informed purchases. The implementation of the initiative has been led by the National Cyber Security Centre Finland (NCSC-FI) and telecoms operator DNA along with smart device manufacturers Cozify and Polar Electro. The aim is to have stickers on all consumer IoT devices that detail their security status. Such a scheme would be readily extendable to industrial IoT and the business-to-business market.

Source: IoT Analytics Research 2000

Figure 5:
IoT security best practices post COVID-19

IoT security in the time of COVID

As COVID-19 has led to an increase in cyberattacks and to changes in hackers' strategies, companies are taking precautions and revisiting their IoT security setup. In **Figure 5**, IoT Analytics provides its top five security best practices for COVID-19.

The growth in remote working, which is seeing a wide array of devices connecting to corporate networks, is compounded by the rise of IoT devices at home and at work. Most security teams have zero visibility into these and, as consumer IoT devices increasingly share the same – often home Wi-Fi – network as corporate devices, consumer IoT devices effectively expand the organisation's attack surface.

Conclusion

Many IoT devices continue to be released with serious security vulnerabilities which leaves them open to attack. Without a enforced standards governing the security of IoT devices, device manufacturers have been allowed to prioritise time-to-market above security. The lack of regulation has allowed systemic issues such as insecure administrator interfaces, poor authentication schemes and firmware vulnerabilities to persist across brands and types of devices.

Once a smart device is hacked, the opportunities for hackers to attack enterprise assets or steal employee credentials greatly increases. Until meaningful legislation is passed, enterprises are, in effect, having to do the job of their IoT device and solution providers. It's their reputations that are on the line so they are taking responsibility for protecting their assets from the risks of sharing a network with IoT devices.

This presents a substantial opportunity for IoT vendors that can provide secure solutions. If they can communicate simply and effectively via a certification that their device meets specific, well-understood criteria the burden of security can shift, at least in part, from the enterprise to the vendor, making procurement decisions easier and ultimately removing insecure systems from the market.

As IoT matures, device makers have a responsibility to their customers to ensure their devices are secure. This will also benefit them because customers will prefer to buy secure solutions and if fewer breaches occur, IoT will avoid the bad reputation of being an insecure market. On the upside this will stimulate further growth, foster trust and result in more and more organisations and people engaging in IoT at scale. Ignoring optional codes of practice, seeking out the loopholes and continuing to sell insecure devices may look like a way to save development costs and bring cheaper devices to market but in reality, it's a way to hamper the development of IoT in its entirety by weakening the reputation of companies, causing mistrust of IoT and enabling the cyber criminals.

The new regulations and the direction of travel towards legislation and certification that are outlined in this report show the IoT industry is engaging with the security issues it faces. In future we will see certification schemes such as the Finnish initiative go global and it will be another step towards IoT security completed when devices are sold based on their certified security status. There is, however, a need for speed here. IoT can't wait for lengthy standards development processes. The industry should take its own lead and find its own way.

Market dynamics do not work for security in IoT - yet

As volumes of IoT deployments scale-up, the question of security has never been more important. To date, much IoT security has relied on well-established IT, web and network security approaches but there is an increasing need for IoT-specific solutions and a growing awareness that regulation is required. Thomas Rosteck, the division president for Connected Secure Systems at Infineon Technologies, tells George Malim that, ultimately, the market will drive implementation of secure IoT devices but first, security experts must enable greater understanding of IoT security and support development and enforcement of clear regulation

George Malim: To what extent are existing IT and networking security inappropriate for IoT?

Thomas Rosteck: I think IoT is in a similar situation to the PC market in the early 2000s when, with the increasing connectivity triggered by the internet becoming mainstream, threats started to proliferate. Over time, that has led to a situation where it's now difficult to buy a PC without having basic security tools already implemented. That certainly took a while to happen so it's a comparable situation but there are big differences between PCs and IoT.

However the structure in PC and IoT is different. The PC industry overall involves a relatively small number of PC and server manufacturers and very few operating system providers so these could easily come together and agree, as an industry, what approach to take. This is why security in the PC industry is now an obvious and visible feature. If you look at IoT, I would say that we are in the stage where the awareness of security is rising, yet implementation is more challenging. IoT has many more companies involved and many don't necessarily know what threats they must be prepared for and what security they need to counteract them.

In other words, we're in a situation where there's an increasingly bad feeling in people's stomachs but not everyone is reacting to it. ▶

Thomas Rosteck
Division Head Connected Secure Systems
Infineon Technologies

However, there will be no IoT without security in the long run. Security is a fundamental feature of connecting devices in order to communicate in privacy, to share sensitive data among companies, or to set up new digital business models. Yet, as the number of attacks is still relatively limited, users don't necessarily see the risks and device manufacturers do not see the need to act with foresight.

GM: Is specific IoT security regulation needed and what will drive it?

TR: As security is not a marketed feature today, usual market dynamics don´t work. Regulation can help initiate market dynamics to respond to the very realistic threat of increasing cyberattacks. Government initiatives and standards bodies have started thinking about how to define a common set of standards that facilitate security implementation for device manufacturers, make security features comparable and give orientation to consumers.

Because one fundamental problem is that end users have difficulty in understanding what the security level of a device is – or even if any security is there at all. If you go into an electronics store and want to understand the security level of a device it's hard to get an accurate answer. Security is either not mentioned or it's simply described as secure or there is a highly technical explanation that is hard to follow.

As long as security is not a marketed feature it's difficult for consumers to make a consistent decision. If this was clarified, people would only buy secure products and therefore there would only be secure products available. To make market mechanisms of supply and demand work, security features must become far more visible and more widely understood.

And another important aspect is, that a certain security level is not necessarily the same today as it will be tomorrow. Today, if a car parts maker designs a braking system, the physics of braking will be the same today as they will be in ten years but the 'physics' of security will be completely different in ten years as the abilities of attackers will have improved by then. This represents an additional challenge to device manufacturers and calls for regulatory support by standardisation bodies and security agencies.

GM: What would you like to see emerge in terms of IoT security certification and regulation?

TS: I would like to see a form of device certification that reflects the evolving character of security and visualises the product's security level through labelling such as the energy consumption labelling that you see on fridges. If the device has the label, users would see that it fulfils certain requirements and includes a minimum set of features. I think this is a good, clear way to make security transparent to users.

But labels like this will only work if they're mandatory. That triggers everyone to use them. Voluntary codes such as the Security by Design initiative in the UK and similar German regulations remain optional and I don't think that is very helpful because voluntary codes will not be as effective as we need them to be. Don't forget, we will have tons of IoT devices and if they're all insecure we will have a large problem that will hold back IoT.

GM: What IoT security solutions does Infineon see being widely adopted?

TR: From our perspective, there are common reactions to common threats. Everyone knows that grounding your software in hardware that is not easy to manipulate makes sense. For example, a chip-based trusted platform module (TPM) goes on the circuit board of a device and cannot be easily attacked and manipulated from the outside. Starting with a security hardware base and building on that provides apps with a trust anchor. This also helps to address the five key security threats such as confidentiality, authentication, integrity of the product, integrity of the data and availability of the connection and the data.

GM: IoT companies aren't security experts - who can help and abstract the complexity away?

TR: Cybersecurity is a very complex topic and IoT companies usually don't have a lot of knowledge in this area nor do they have the resources to build up security skills. What we recommend is a basic security concept in their devices from when they design them – this is security by design which is a very valid and important term.

The good news is that IoT device manufacturers can take a short cut by referring to the knowledge and experience of the security industry. We've developed an understanding of what the threats in the future will look like and we're investing heavily in developing concepts and architectures that can protect against such attacks. Connected devices are out there for a while and cars, gateways or smart locks need to be secure for the next three, ten,, 15 years and more. The amount of research we do is obviously greater than what an IoT company can do so that's an important part of our capability.

Therefore our strategy is to package what we know into products that are easy to integrate. This helps to eliminate quite a number of common mistakes in the deployment and to always keep security features up-to-date.

Finally, we are very actively involved in defining and developing industry standards and certification schemes that are transparent and open to everyone. There's a risk that if everyone develops security solutions themselves, there will be a lot of implementation problems. Particularly for IoT we need globally harmonised standards for all kind of products from smoke alarms to car factory plants.

Ultimately, the market demand will drive cybersecurity, but we have to act now, by increasing consumer awareness of risks and threats, by defining cybersecurity standards that are transparent and internationally accepted and by providing manufacturers with security products that are straightforward to implement. ■

www.infineon.com/security