Succeed with IoT
Report Series

Locking in Value with IoT Security:
Building trust, protecting profits

beecham research

Shaping the IoT future

Report sponsored by...

In association with...

Contents

CLICK THE IMAGE TO GO STRAIGHT TO THAT SECTION

Introduction

What is the business case for IoT security?
Is it possible to explain this in non-technical terms?

These are the two main questions we have had in mind in preparing this report. All too often, discussions about IoT security become quite technical quite quickly and the business case for investing in it is not explored as fully as it should be. Consequently, IoT security tends to be seen by budget holders as a cost that should be minimised as much as possible. It tends not to be seen as the value-adding enabler that it really is.

Why look at this now?

After many years of being described as 'emerging', IoT is now mainstream. Around 2 billion IoT devices are now connected annually, growing to more than double that rate by 2030. With some 12 to 14 billion IoT devices in the market today, that is set to grow to 25 to 30 billion devices by the end of the decade. These are not only consumer devices. Many are part of critical infrastructure with still more becoming central to business operations. This number of devices represents a massive opportunity for adversaries.

But that is just the tip of the iceberg. With millions of interconnected devices in use, a single security flaw can multiply across vast networks, turning an isolated vulnerability into a widespread threat. This risk is not hypothetical. As an example, just a few years ago, hackers seized control of half a million video cameras, using them in a massive, coordinated assault to crash major online services like Netflix and Yahoo. Each of these cameras shared a firmware weakness, allowing attackers to orchestrate a relentless Distributed Denial-of-Service (DDoS) attack. This is the dark side of IoT at scale – a potential army of everyday devices poised to disrupt industries without warning.

As the base of IoT devices grows quickly over the next few years, the issue of vulnerability detection and monitoring becomes very important. At the same time, governments are watching, regulating, and mandating. Penalties are high to encourage action is taken. As IoT becomes an increasingly central part of operations, businesses must now take all of this into account and pay more attention to the opportunities that a high level of IoT security offers for the bottom line.

What's in this report?

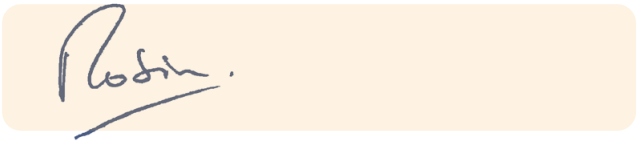
Section 2 takes a look at the IoT security landscape, examining in particular how threats have evolved over time to become much more IoT-specific. It used to be the case that IoT solutions were not particular targets for attack. That has radically changed and this section explains what has been happening in the market.

Section 3 then adds our own primary research findings. Beecham Research regularly interviews market players to find out in more detail the key challenges and opportunities in the market. We also regularly conduct surveys to gain a breadth of view. For this report we conducted both activities and the findings are exclusively reported here.

Section 4 then looks at the responses to challenges identified in Sections 2 and 3. It includes technical insights from our sponsors on how they are addressing these challenges. It also examines best practices that businesses can adopt to strengthen their resilience against IoT cyberattacks. Regulatory and certification insights are also offered, along with recommendations to help protect against future threats.

Section 5 provides more details about our sponsors and how to contact them.

We hope you find this useful.



Robin Duke-Woolley, Founder and CEO. Beecham Research
www.beechamresearch.com

IoT Security Landscape

This section introduces the IoT security landscape by examining how IoT-related threats have evolved over time. Major security incidents are shown in a timeline, then described in more detail. This is followed by an analysis of the 2024 attack numbers and the global IoT Security market. Factors that influence the landscape are also identified.

IoT-Related Security Incidents

The rapid proliferation of IoT has transformed industries by streamlining operations and enhancing connectivity. However, the surge in adoption has also created an expanding attack surface, making cybersecurity incidents more frequent, more damaging, and more indiscriminate than ever before. Adversaries now target a wide range of sectors, from healthcare and manufacturing to smart cities and critical national infrastructure, using IoT vulnerabilities to breach connected systems.

The motivations behind these attacks are also shifting. Although financial gain remains a key driver, a growing number of attacks appear designed to cause disruption, chaos, and reputational damage. Ransomware targeting smart hospitals, cyberattacks crippling supply chains, and state-sponsored intrusions into industrial IoT systems highlight how the stakes are rising. Businesses are no longer just at risk of financial loss—they also face operational paralysis, widespread supply chain disruption, and threats to human safety. In some cases, IoT devices may be weaponised to create further damage.

To understand how we arrived at this crisis point, it is instructive to examine the history of IoT breaches. From early attacks exploiting weak authentication to more recent sophisticated botnet assaults, past incidents reveal a range of IoT vulnerabilities that have yet to be fully addressed. This historical context shapes the current IoT security market, driving demand for stronger defences, better regulation, and more proactive risk management. As threats continue to evolve, businesses must learn from the past to safeguard the future. The question is no longer if an attack will occur, but when.

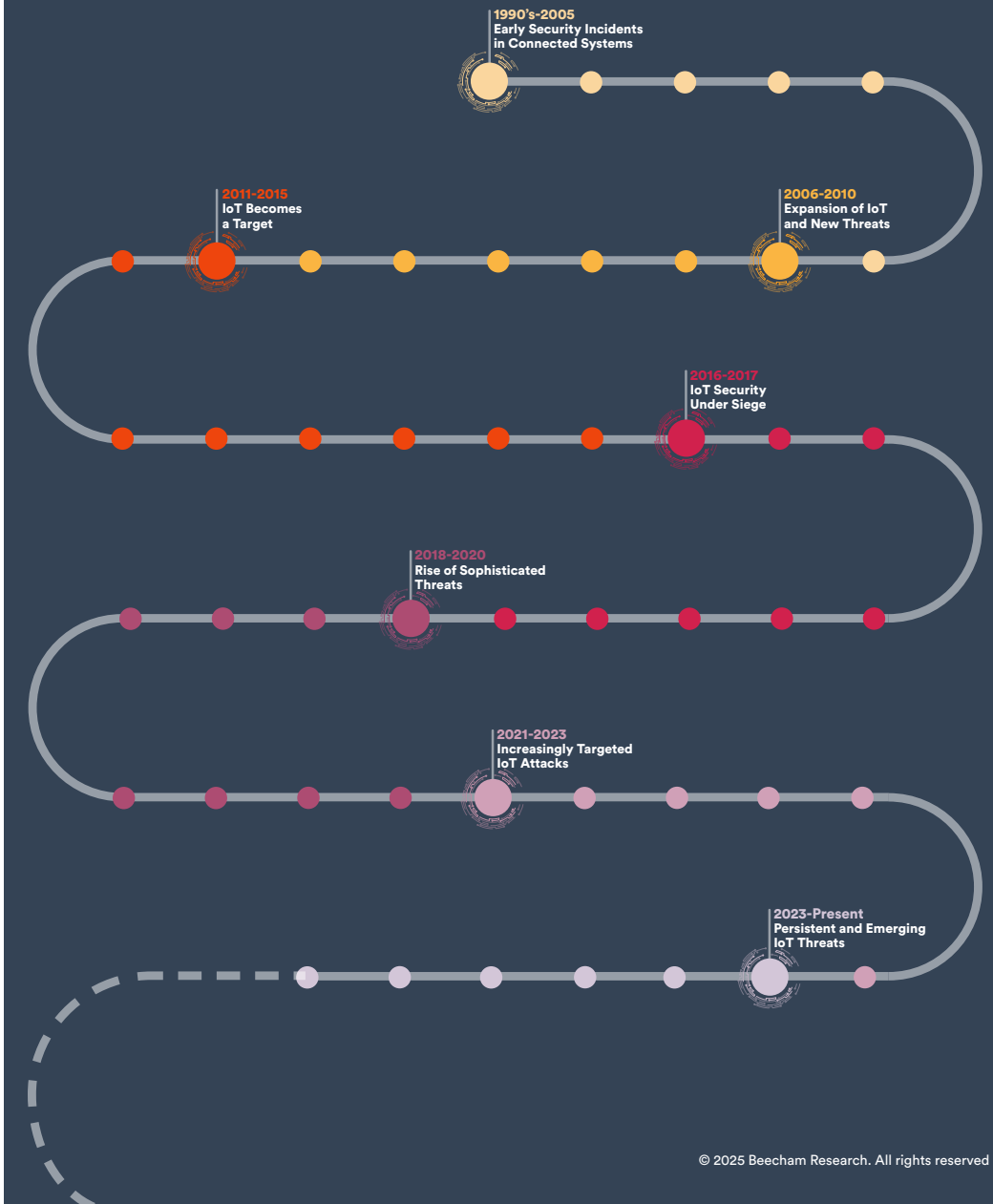
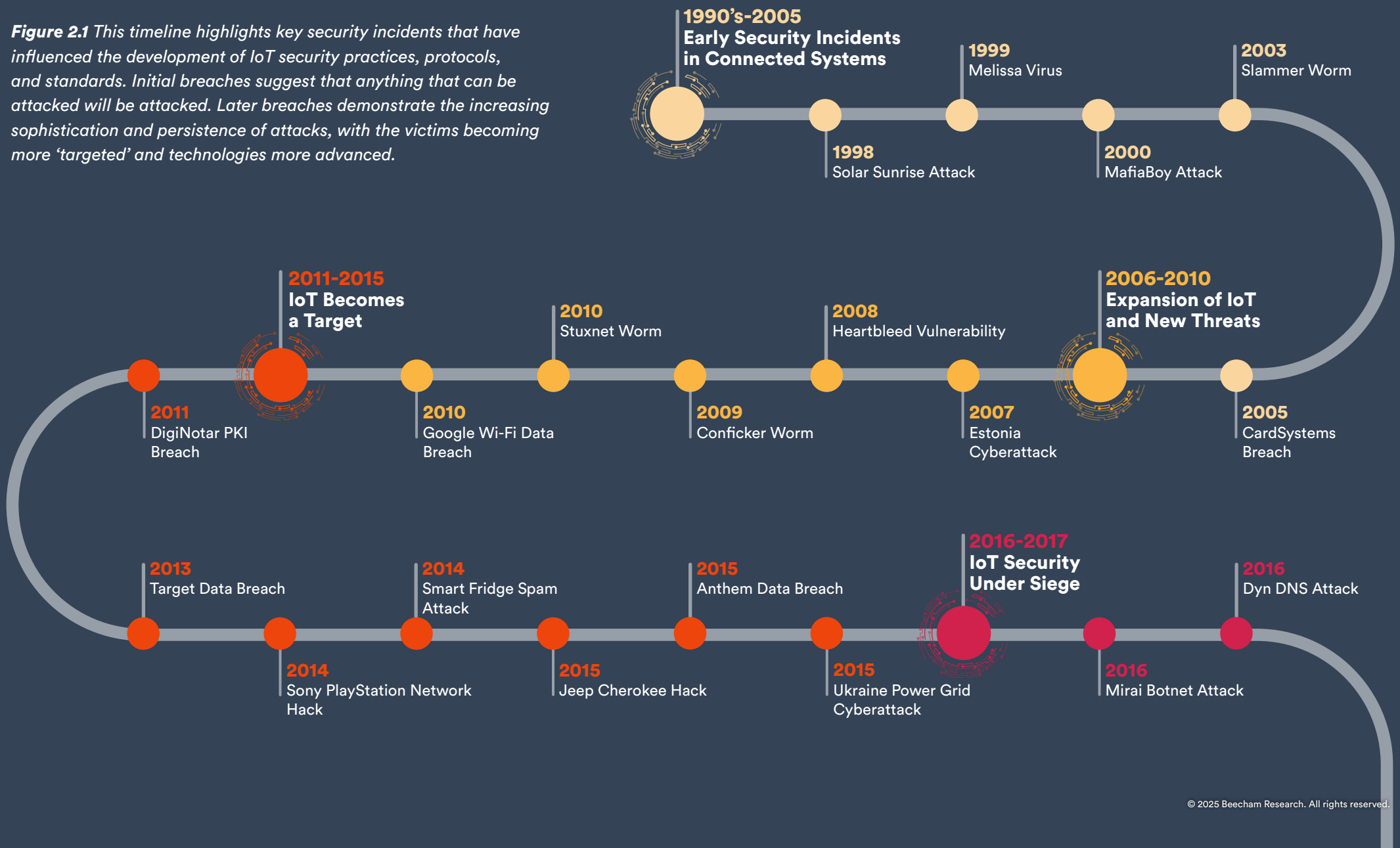
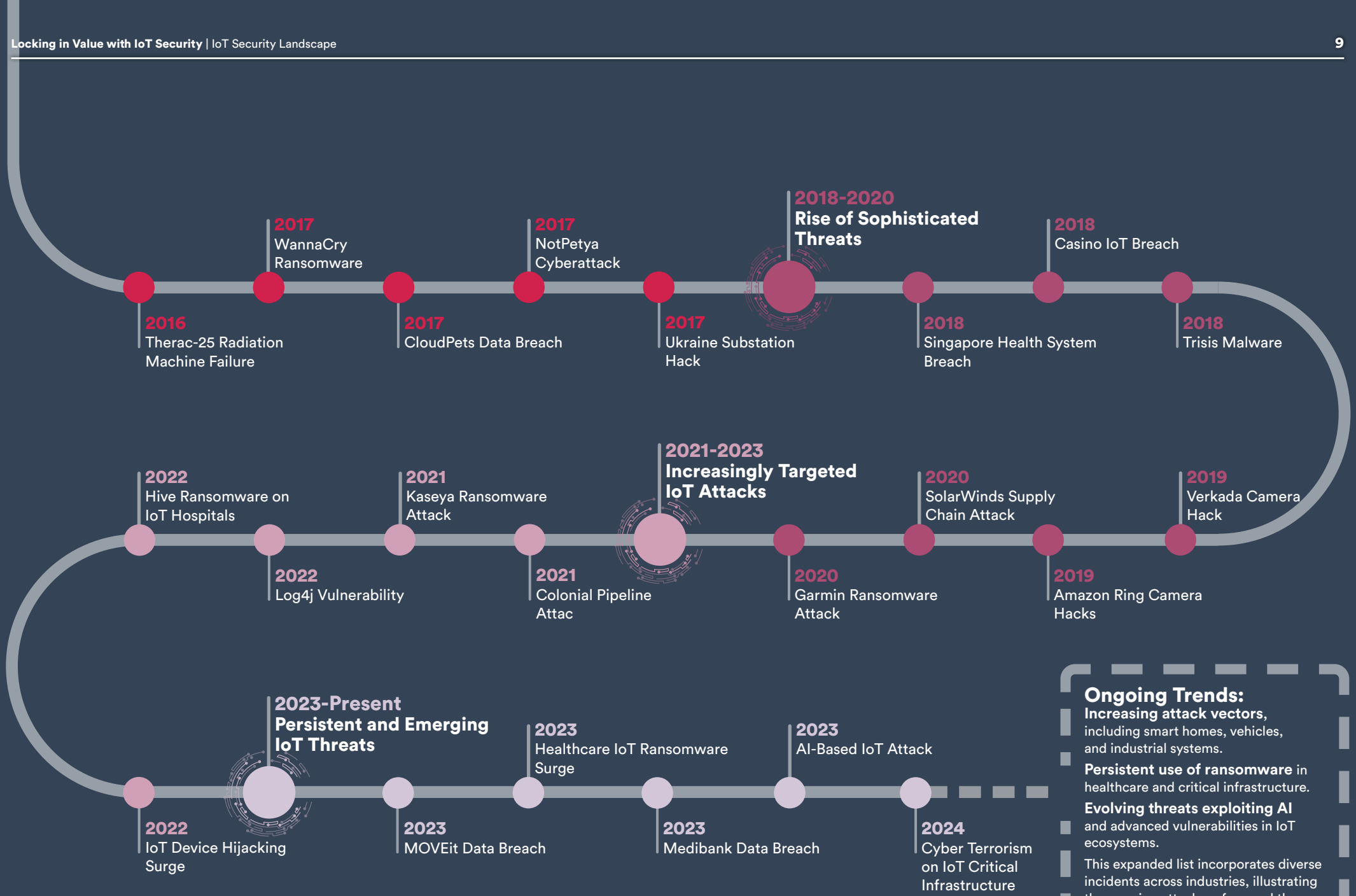


Figure 2.1 *This timeline highlights key security incidents that have influenced the development of IoT security practices, protocols, and standards. Initial breaches suggest that anything that can be attacked will be attacked. Later breaches demonstrate the increasing sophistication and persistence of attacks, with the victims becoming more 'targeted' and technologies more advanced.*





Ongoing Trends:

Increasing attack vectors, including smart homes, vehicles, and industrial systems.

Persistent use of ransomware in healthcare and critical infrastructure.

Evolving threats exploiting AI and advanced vulnerabilities in IoT ecosystems.

This expanded list incorporates diverse incidents across industries, illustrating the growing attack surface and the sophistication of threats targeting IoT systems.

Here is a more detailed breakdown of the incidents focusing on technical vulnerabilities, what was compromised, how the issue was fixed, and any relevant impacts on IoT security development. This expanded detail showcases the technical evolution of threats and resolutions and their relevance to the development of IoT security standards and practices.

1990's-2005 Early Security Incidents in Connected Systems

The era of early connected systems exposed fundamental vulnerabilities, laying the groundwork for future IoT security challenges as connected devices began to emerge.

During this period, the concept of connected devices began to take shape, laying the groundwork for the Internet of Things (IoT). Early implementations, such as the 1998 internet-connected Coca-Cola vending machine at Carnegie Mellon University, showcased the potential of connected systems. However, these pioneering devices often lacked robust security measures, exposing fundamental vulnerabilities. This era highlighted the nascent challenges in securing connected systems, which would become more pronounced as IoT technologies evolved.

1998 Solar Sunrise Attack
Target: US military systems.
Summary: Demonstrated vulnerabilities in connected systems.
Technical Details: Exploited weak passwords and unpatched vulnerabilities in Solaris systems.
What Was Compromised: US military networks.
Resolution: Strengthened access controls and implemented mandatory security updates.
Impact: Highlighted the importance of password policies and regular patch management.

1999 Melissa Virus
Target: Early networked systems and email platforms.
Summary: A precursor to malware targeting connected devices.
Technical Details: Macro-based malware spread via email attachments.
What Was Compromised: Early networked systems and email servers.
Resolution: Organisations implemented email filtering and disabled macro execution by default.
Impact: Laid the foundation for endpoint protection practices still relevant for IoT devices.

2000 MafiaBoy Attack
Target: Websites like Yahoo! and eBay.
Summary: DDoS attacks showing risks in networked systems.
Technical Details: DDoS attacks leveraged compromised network resources.
What Was Compromised: Popular websites like Yahoo! and CNN.
Resolution: Improved DDoS mitigation measures and introduced traffic monitoring.
Impact: Demonstrated scalability risks, relevant for IoT-based botnets.

2003 Slammer Worm
Target: SQL servers.
Summary: Fast-spreading worm disrupted ATMs and emergency systems.
Technical Details: Exploited a buffer overflow in Microsoft SQL Server.
What Was Compromised: ATMs, emergency services, and networked SQL systems.
Resolution: Emergency patches were deployed.
Impact: Raised awareness about software vulnerabilities and the need for secure software updates.

2005: CardSystems Breach
Target: IoT-enabled payment systems.
Summary: Compromised credit card data through vulnerabilities.
Technical Details: Exploited weak network segmentation and insecure storage of cardholder data.
What Was Compromised: 40 million credit card numbers.
Resolution: PCI-DSS standards were updated to enforce stronger data protection.
Impact: Influenced security requirements for IoT-enabled payment devices.

2006-2010: Expansion of IoT and New Threats

The rapid expansion of IoT adoption introduced new risks, with cyber-physical systems like industrial control systems becoming targets of sophisticated attacks

A high-profile incident which illustrates this new vulnerability is the Stuxnet worm discovered in 2010, which specifically targeted Siemens ICS used in Iran's nuclear facilities. This sophisticated attack exploited multiple zero-day vulnerabilities, marking one of the first instances where malware caused physical damage, thereby highlighting the vulnerabilities in critical infrastructure.

2007 Estonia Cyberattack
Target: IoT-connected critical infrastructure.
Summary: State-sponsored attack disrupted government services.
Technical Details: DDoS attacks overwhelmed critical infrastructure systems.
What Was Compromised: Banking, media, and government services.
Resolution: Enhanced network redundancy and DDoS defence mechanisms.
Impact: Set a precedent for securing IoT systems in critical infrastructure.

2008: Heartbleed Vulnerability
Target: Systems using OpenSSL.
Summary: Widespread exploitation of encryption flaws.
Technical Details: Buffer over-read flaw in OpenSSL allowed data leakage from memory.
What Was Compromised: Encryption keys, passwords, and sensitive data.
Resolution: OpenSSL was patched; organisations updated software globally.
Impact: Highlighted the risks of open-source dependencies in IoT ecosystems.

2009: Conficker Worm
Target: IoT-enabled Windows devices.
Summary: Highlighted risks in OT systems using outdated protocols.
Technical Details: Exploited unpatched Windows vulnerabilities to propagate.
What Was Compromised: Windows-based IoT and OT devices.
Resolution: Deployment of patches and improved network segmentation.
Impact: Emphasised timely patching for IoT devices.

2010: Stuxnet Worm
Target: Iranian nuclear centrifuges.
Summary: First cyberweapon targeting IoT-connected OT.
Technical Details: Targeted Siemens PLCs via USB drives and zero-day vulnerabilities.
What Was Compromised: Iranian nuclear centrifuges.
Resolution: Siemens issued patches; affected systems were isolated.
Impact: Marked a shift to securing operational technology (OT) and IoT.

2010: Google Wi-Fi Data Breach
Target: IoT-enabled Google Street View cars.
Summary: Captured private data from unencrypted Wi-Fi networks.
Technical Details: Google Street View cars collected unencrypted Wi-Fi data.
What Was Compromised: User data from open Wi-Fi networks.
Resolution: Google stopped data collection and improved data handling practices.
Impact: Highlighted privacy issues in IoT data collection.

2011-2015: IoT Becomes a Target

As IoT devices became more prevalent, attackers began exploiting their vulnerabilities, with high-profile demonstrations revealing the risks to consumer and industrial IoT alike.

A high-profile demonstration in 2015 involved security researchers remotely hacking a Jeep Cherokee, controlling its steering and brakes via its internet-connected entertainment system. This incident underscored the potential risks associated with connected vehicles and the broader implications for consumer safety.

2011: DigiNotar PKI Breach
Target: IoT devices reliant on PKI for authentication.
Summary: Compromised digital certificates affecting trust in IoT.
Technical Details: Compromise of a certificate authority issuing fraudulent certificates.
What Was Compromised: Authentication mechanisms for websites and devices.
Resolution: Revocation of fraudulent certificates and stricter PKI monitoring.
Impact: Advanced PKI implementation for IoT authentication.

2013: Target Data Breach
Target: IoT-enabled HVAC systems.
Summary: Entry point for attackers to steal credit card data.
Technical Details: Entry via compromised IoT-enabled HVAC systems.
What Was Compromised: 40 million credit card numbers.
Resolution: Enhanced network segmentation and third-party vendor security.
Impact: Raised awareness of third-party risks in IoT supply chains.

2014: Sony PlayStation Network Hack
Target: IoT-enabled gaming devices.
Summary: Highlighted vulnerabilities in entertainment IoT.
Technical Details: DDoS attack exploited weak authentication.
What Was Compromised: Gaming systems and customer data.
Resolution: Improved authentication and network defence.
Impact: Highlighted risks in consumer IoT devices.

2014: Smart Fridge Spam Attack
Target: IoT-enabled smart appliances.
Summary: Botnet used a fridge to send spam emails.
Technical Details: Exploited weak default credentials in smart appliances.
What Was Compromised: Fridges became part of spam botnets.
Resolution: Manufacturers started enforcing stronger default credentials.
Impact: Highlighted risks of consumer IoT with default security flaws.

2015: Jeep Cherokee Hack
Target: Connected vehicles.
Summary: Researchers remotely controlled the car, showcasing risks.
Technical Details: Exploited insecure software updates in automotive systems.
What Was Compromised: Remote control of vehicle functions.
Resolution: Over-the-air updates patched vulnerabilities.
Impact: Led to adoption of secure boot and firmware updates in IoT.

2015: Anthem Data Breach
Target: Healthcare IoT devices.
Summary: Attackers exploited medical IoT systems to steal records.
Technical Details: Exploited vulnerabilities in IoT-enabled medical systems.
What Was Compromised: 80 million patient records.
Resolution: Encryption of sensitive data and endpoint security improvements.
Impact: Increased regulatory focus on healthcare IoT security.

2015: Ukraine Power Grid Cyberattack
Target: IoT-connected OT systems.
Summary: Nation-state actors disrupted electricity distribution.
Technical Details: Malware disrupted IoT-connected SCADA systems.
What Was Compromised: Electricity distribution.
Resolution: Manual controls restored; systems hardened against cyber threats.
Impact: Pushed the development of IoT-specific OT security standards.

2016-2017: IoT Security Under Siege

The proliferation of unsecured IoT devices led to massive, disruptive botnet attacks, highlighting the critical need for better security practices in connected ecosystems.

The Mirai botnet, for instance, emerged in 2016, infecting numerous IoT devices (like IP cameras and routers) by exploiting default credentials. Mirai orchestrated large-scale Distributed Denial of Service (DDoS) attacks, temporarily disrupting major websites and services. This highlighted the critical need for better security practices in connected ecosystems. A 310% increase in attacks on IoT devices during 2016 is well-documented.

2016: Mirai Botnet Attack
Target: IoT cameras, routers.
Summary: Launched massive DDoS attacks using IoT devices.
Technical Details: Exploited default credentials in IoT devices to create a botnet.
What Was Compromised: Cameras and routers used for DDoS attacks.
Resolution: Manufacturers started enforcing secure default configurations.
Impact: Led to regulatory mandates for default credential policies.

2016: Dyn DNS Attack
Target: IoT devices and DNS infrastructure.
Summary: Disrupted major websites via compromised IoT devices.
Technical Details: IoT devices were hijacked via the Mirai botnet to attack DNS servers.
What Was Compromised: Internet infrastructure affecting websites like Twitter.
Resolution: Strengthened DNS security and IoT device configurations.
Impact: Reinforced global awareness of IoT device risks.

2016: Therac-25 Radiation Machine Failure
Target: IoT-connected medical equipment.
Summary: Flawed software led to overdoses, underscoring IoT risks.
Technical Details: Flawed software logic caused unsafe radiation doses.
What Was Compromised: Medical IoT device functionality.
Resolution: Recalled affected devices and improved software QA processes.
Impact: Highlighted life-critical IoT system risks.

2017: WannaCry Ransomware
Target: Healthcare IoT systems.
Summary: Exploited outdated software, affecting medical devices.
Technical Details: Exploited EternalBlue, a Windows SMB protocol vulnerability.
What Was Compromised: IoT-connected medical devices in hospitals.
Resolution: Microsoft issued emergency patches, and systems were updated globally.
Impact: Highlighted the need for prompt patching and endpoint security in healthcare IoT.

2017: CloudPets Data Breach
Target: IoT-enabled children's toys.
Summary: Exposed voice recordings and customer data.
Technical Details: MongoDB database with no password exposed sensitive data.
What Was Compromised: Children's voice recordings and user account details.
Resolution: Database security configurations were updated.
Impact: Brought attention to securing IoT data storage in the cloud.

2017: NotPetya Cyberattack
Target: IoT-enabled OT in supply chains.
Summary: Malware disrupted global shipping operations.
Technical Details: Ransomware spread through supply chain vulnerabilities.
What Was Compromised: IoT-enabled OT in logistics and shipping.
Resolution: Affected companies improved network segmentation and updated software.
Impact: Highlighted supply chain risks for IoT ecosystems.

2017: Ukraine Substation Hack
Target: IoT-connected electrical grids.
Summary: Cyberattack caused blackouts, highlighting OT vulnerabilities.
Technical Details: Malware attacked IoT-connected SCADA systems controlling power grids.
What Was Compromised: Regional electricity distribution.
Resolution: Manual operations restored control; SCADA systems hardened.
Impact: Reinforced the criticality of IoT security in energy infrastructure.

2018-2020: Rise of Sophisticated Threats

Cyberattacks on IoT systems grew more targeted and sophisticated, with adversaries focusing on critical infrastructure and exploiting industrial IoT vulnerabilities to cause real-world harm.

The Triton malware, discovered in 2017, targeted industrial safety systems, aiming to disable them and cause physical harm. This marked a significant escalation in the exploitation of industrial IoT vulnerabilities, demonstrating the potential for real-world damage from cyberattacks.

2018: Singapore Health System Breach
Target: IoT-connected healthcare devices.
Summary: Attackers accessed patient records via vulnerable devices.
Technical Details: Phishing attack gained access to IoT-connected medical records.
What Was Compromised: Personal health records of 1.5 million patients.
Resolution: Network monitoring and phishing prevention were improved.
Impact: Strengthened focus on healthcare IoT cybersecurity frameworks.

2018: Casino IoT Breach
Target: IoT-enabled fish tank thermometer.
Summary: Entry point for hackers to steal high-roller data.
Technical Details: Compromised a smart fish tank thermometer to infiltrate the network.
What Was Compromised: High-roller database from the casino network.
Resolution: Introduced stronger segmentation for IoT devices.
Impact: Highlighted unconventional entry points for cyberattacks.

2018: Trisis Malware
Target: IoT-connected safety systems in industrial plants.
Summary: Attackers sought to disable safety mechanisms.
Technical Details: Targeted Schneider Electric safety instrumented systems in OT.
What Was Compromised: Industrial safety systems.
Resolution: Security patches were deployed; devices were isolated.
Impact: Marked a critical escalation in OT-targeted malware affecting IoT.

2019: Verkada Camera Hack
Target: IoT surveillance cameras.
Summary: Hackers accessed live feeds from thousands of cameras.
Technical Details: Misconfigured credentials exposed live feeds from IoT cameras.
What Was Compromised: Surveillance camera feeds in hospitals, prisons, and schools.
Resolution: Credentials were reset, and access control was strengthened.
Impact: Raised concerns about privacy and security in IoT-enabled surveillance.

2019: Amazon Ring Camera Hacks
Target: Consumer IoT devices.
Summary: Attackers gained unauthorised access to cameras.
Technical Details: Weak password policies allowed unauthorised access.
What Was Compromised: Consumer IoT cameras in homes.
Resolution: Two-factor authentication was implemented for Ring accounts.
Impact: Pushed adoption of MFA for consumer IoT devices.

2020: SolarWinds Supply Chain Attack
Target: IT and IoT systems.
Summary: Exploited vulnerabilities in updates, affecting thousands.
Technical Details: Malware injected into SolarWinds updates affected connected systems.
What Was Compromised: Thousands of IT and IoT systems in government and enterprises.
Resolution: SolarWinds software was patched; monitoring was increased.
Impact: Highlighted risks in software supply chains for IoT.

2020: Garmin Ransomware Attack
Target: IoT fitness devices.
Summary: Service outage due to ransomware attack.
Technical Details: Ransomware encrypted Garmin's IoT-connected servers and applications.
What Was Compromised: IoT-enabled fitness devices and services.
Resolution: Paid ransom (reportedly) and restored encrypted data.
Impact: Stressed the need for backup and ransomware protection in IoT.

2021-2023: Increasing Volume of IoT Attacks

With adversaries exploiting insecure remote access and targeting essential services, the volume and variety of IoT attacks surged, underscoring the urgency of protecting critical IoT systems.

In 2021, the Colonial Pipeline (a major US fuel pipeline operator) suffered a ransomware attack that led to fuel supply disruptions. While not directly an IoT attack, it underscored the vulnerabilities in critical infrastructure and the cascading effects such breaches can cause, emphasising the urgency of securing IoT systems integral to such operations.

2021: Colonial Pipeline Attack
Target: IoT-connected OT systems in energy infrastructure.
Summary: Ransomware disrupted fuel supply.
Technical Details: Compromised IoT-enabled OT systems controlling fuel supply.
What Was Compromised: Pipeline operations causing regional fuel shortages.
Resolution: Ransom paid, systems restored; segmented OT and IT networks.
Impact: Brought IoT cybersecurity in critical infrastructure to the forefront.

2021: Kaseya Ransomware Attack
Target: IoT-enabled supply chains.
Summary: Exploited vulnerabilities in remote management tools.
Technical Details: Exploited vulnerabilities in IT management software affecting IoT.
What Was Compromised: IoT and IT systems in supply chains.
Resolution: Emergency patches were deployed; compromised systems isolated.
Impact: Highlighted the cascading effects of IoT-targeted ransomware.

2022: Log4j Vulnerability
Target: IoT and IT systems globally.
Summary: Exposed millions of devices to potential exploitation.
Technical Details: Exploited flaws in Log4j, allowing remote code execution.
What Was Compromised: IoT and IT systems using the library.
Resolution: Software vendors issued patches; systems were updated globally.
Impact: Exposed widespread risks of third-party dependencies in IoT.

2022: Hive Ransomware on IoT Hospitals
Target: Healthcare IoT systems.
Summary: Caused delays in critical medical operations.
Technical Details: Ransomware encrypted IoT-enabled medical devices.
What Was Compromised: Hospital operations and patient care.
Resolution: Data recovery and hardened endpoint defences.
Impact: Emphasised the need for comprehensive IoT incident response in healthcare.

2022: IoT Device Hijacking Surge
Target: Consumer IoT devices.
Summary: Botnets created from smart devices for DDoS attacks.
Technical Details: Exploited weak default credentials in consumer IoT devices.
What Was Compromised: Devices were recruited into botnets for DDoS attacks.
Resolution: Encouraged stronger default security measures.
Impact: Highlighted the ongoing risks of insecure IoT device configurations.

2023-Present: Advanced Persistent Threats

State-sponsored and organised cybercriminal groups have adopted highly advanced methods, leveraging supply chain vulnerabilities and targeting IoT systems for strategic and financial gain.

Advanced Persistent Threats (APTs) is a recognised term in cybersecurity. It refers to sophisticated, prolonged cyberattacks carried out by well-organised, highly skilled, and often state-sponsored adversaries. These attacks are designed to infiltrate a specific target, remain undetected, and exfiltrate valuable data or disrupt critical systems.

When adversaries target critical services, the stakes are immeasurably higher. Hospitals relying on connected medical devices cannot cease operations without endangering lives, whilst attacks on power grids or water treatment plants can cripple entire regions. Connected cars, if compromised, could cause physical harm or fatal accidents.

This highlights the growing ethical and operational challenge organisations face: mitigating risk while ensuring continuity of service. Relying on IoT and OT technologies creates a double-edged sword of increased efficiency but heightened vulnerability, exacerbated by the impossibility of simply "turning off" systems critical to human safety.

2023: MOVEit Data Breach
Target: IoT-enabled file transfer systems.
Summary: Exploited vulnerabilities, affecting financial institutions.
Technical Details: Vulnerabilities in IoT-connected file transfer systems exploited.
What Was Compromised: Financial data in transit.
Resolution: Patched vulnerabilities and improved file transfer security protocols.
Impact: Reinforced the importance of securing IoT-connected enterprise services.

2023: Healthcare IoT Ransomware Surge
Target: IoT medical devices.
Summary: Operational disruptions and ransom demands.
Technical Details: Ransomware targeted medical IoT systems through phishing and network exploits.
What Was Compromised: Patient data and device availability.
Resolution: Improved monitoring and incident response.
Impact: Highlighted the growing prevalence of ransomware in healthcare IoT.

2023: Medibank Data Breach
Target: IoT-connected healthcare systems.
Summary: Exposed patient data via vulnerable devices.
Technical Details: IoT-connected health devices were compromised via network weaknesses.
What Was Compromised: Patient records and private data.
Resolution: Network security was improved; affected accounts monitored.
Impact: Stressed the need for robust IoT security in health ecosystems.

2023: AI-Based IoT Attack
Target: Smart home systems.
Summary: AI-generated phishing attacks targeted IoT credentials.
Technical Details: AI-generated phishing emails targeted IoT credentials.
What Was Compromised: Smart home devices and networks.
Resolution: User education and stronger authentication policies.
Impact: Demonstrated evolving AI-driven threats to IoT.

2024: Cyber Terrorism on IoT Critical Infrastructure
Target: Energy and water systems.
Summary: Exposed vulnerabilities in IoT-enabled utilities.
Technical Details: Exploited vulnerabilities in IoT-enabled OT systems for sabotage.
What Was Compromised: National energy and water systems.
Resolution: Enhanced monitoring and adoption of zero-trust architectures.
Impact: Reinforced urgency to secure IoT in national critical infrastructure.

2024 Attack Trends: The Numbers

In the APT era, the number of IoT-based attacks continue to rise year-on-year. Recent studies show that:

- In the first five months of 2024, security attacks on IoT devices surged by 107% compared with the same period in the previous year. (SonicWall)
- More than one in five organisations claim to have had a serious or business-disrupting IoT security incident within the last year. (Viakoo)
- On average, 54% of organisations suffer from attempted cyberattacks on IoT devices every week. (Check Point Research)
- There has been an increase of over 400% in IoT malware attacks year-on-year. (Zscaler)
- Almost all organisations (97%) have seen an increase in cyber threats since the start of the Russia-Ukraine war. (Accenture)

As well as the number of attacks rising, the costs of falling victim to a successful attack is getting higher, with the average cost of a successful device attack being more than USD330,000 (PSA Certified). What's more, is that successful IoT attacks are increasingly proving to be more damaging than other types of malicious cyber activity: in fact, 34% of enterprises that suffered a breach via IoT devices faced higher cumulative breach costs than those who suffered a non-IoT related cyber-attack (Forrester).

It is important to note that it is not just the end devices that are at risk. For instance, in smart factories, although the monitoring & control layer and the physical resources are the primary focus areas, attackers are looking for vulnerabilities across all layers of the connected solution – see **Figure 2.3**.

Figure 2.2 *The impacts of falling victim to an IoT attack*

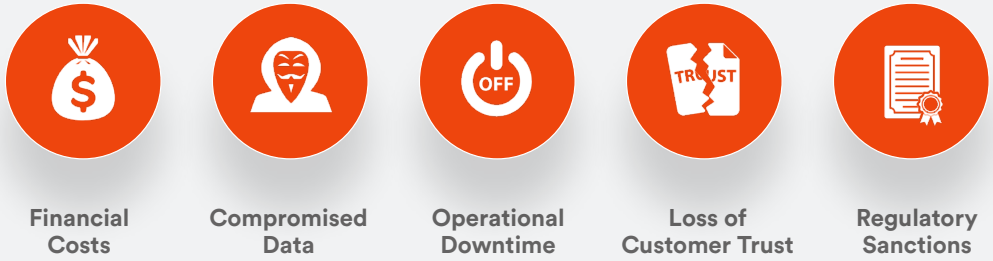
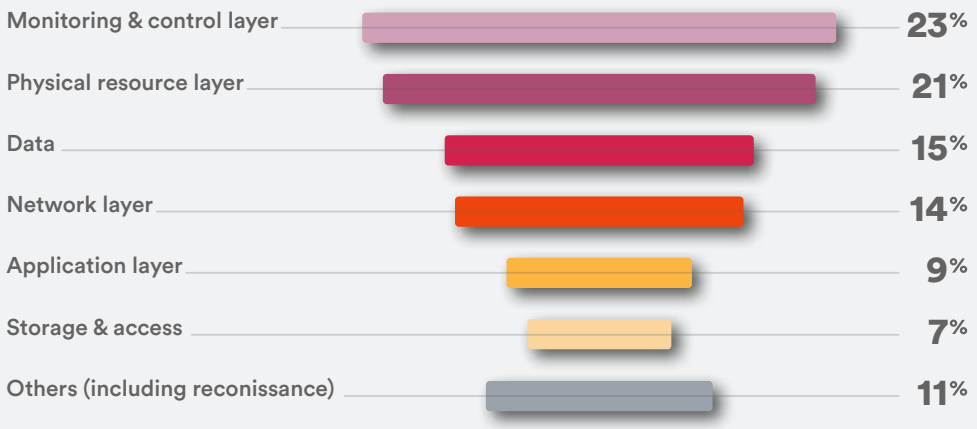


Figure 2.3 *All layers of the smart factory connected solution are being targeted by adversaries. (Source: Sectrio)*



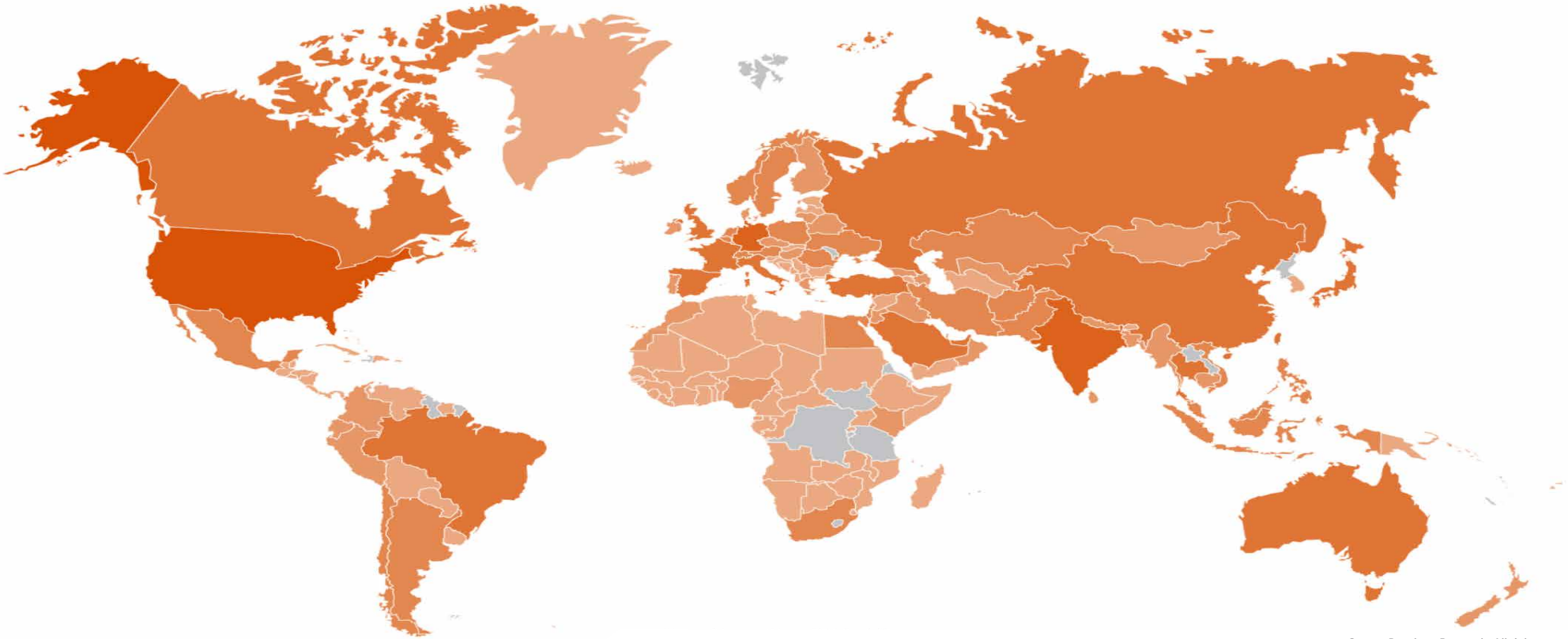
Wherever IoT exists, so do the threats that target it

Manufacturing is widely believed to be the most targeted sector for IoT and OT attacks, due to its reliance on these technologies. In terms of IoT malware attacks, over half of attacks can be attributed to this sector (Zscaler). However, this is more to do with the volume of IoT devices in operation within this sector – a recent report by Sectrio showed that only 1% of malware attacks were designed to be industry or system specific.

There has also been a strong increase in number of attacks in energy/utilities and healthcare, though no sector is immune.

Similarly, threats are occurring globally. In 2024, 176 countries were targeted – 13 more than in the previous year. In general, the richest, most populous, and most technologically advanced countries are seeing the greatest number of threats, simply because these countries have the highest volume of IoT devices and solutions.

Figure 2.4 *Heat map of countries most targeted by cyber adversaries.*
Source: Forescout Research Vedere Labs



IoT Security: The Global Market

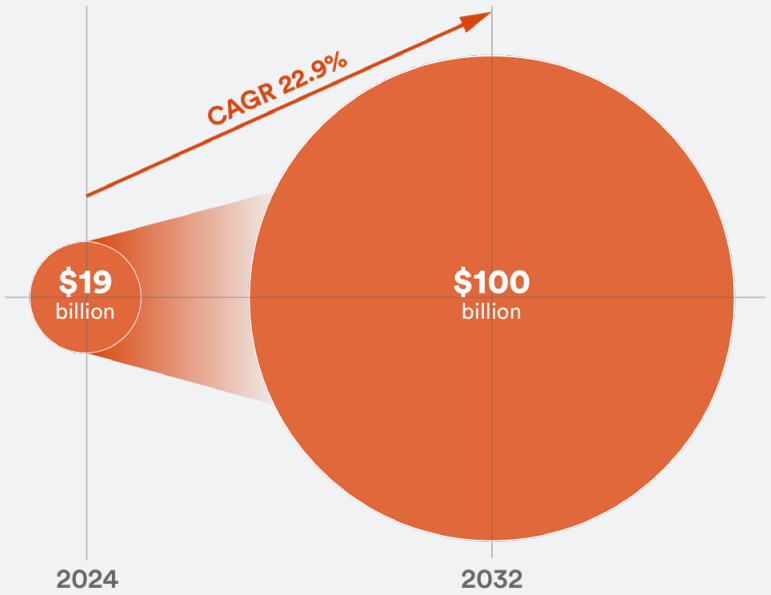
The global IoT Security market was valued at USD19.3 billion in 2024 and is projected to expand at a CAGR of 22.9% across the 2025-2032 forecast period. This growth is driven by the escalating threat landscape and the increasing need for robust security solutions to safeguard IoT ecosystems. Additionally, tightening regulatory requirements are compelling organisations to adopt more stringent security measures. As a result, the market is expected to reach USD100.9 billion by 2032

By comparison, the overall IoT market revenue is anticipated to grow at a CAGR of 14.6%. This shows there is increasing willingness to invest in IoT security.

In fact, according to a 2023 Keyfactor report, budgets for IoT device security are anticipated to see a 45% increase in the next five years. At the same time, over half of the budget is at risk of being diverted to pay the costs of IoT cyber breaches. For instance, it is becoming an increasingly common solution in ransomware incidents for companies to simply pay the ransom demanded.

> ***"Companies must balance the cost of providing solutions with the cost of failing to provide solutions."***

Figure 2.5 *Expected global IoT security market revenue values and growth rate 2024-2032*



Evolving technologies pose both opportunities and threats

Rapid advancements in Artificial Intelligence (AI) are leading to these technologies being embraced across the board by businesses, governments, and organisations worldwide. In fact, the IBM Global AI Adoption Index 2023, claims that 40% of organisations are actively exploring the use of AI in their business operations – with this bringing both risk and reward.

AI and ML are also increasingly being integrated as part of IoT security solutions to enhance threat detection and response capabilities. In fact, although Darktrace reports 74% are seeing AI-powered cyber threats significantly impact their organisations, 96% believe AI is essential within security to counter the AI-powered threats.

There is also an increasing shift towards edge computing thanks to the growing need to process data closer to the source. In some ways, this benefits security as sensitive data can be stored and processed on-site. Additionally, the adoption of blockchain and distributed ledgers offers a decentralised secure method for managing IoT data, preventing unauthorised access and data tampering.

However, edge computing also introduces new security challenges. For instance, low-power IoT devices may not have the capacity to handle advanced security software and may receive a significant proportion of attention from cyber attackers – see **Figure 2.7**.

As this trend accelerates, businesses must not only invest in protecting the edge device but also safeguard the data they generate and transmit.

Figure 2.6 *Results from surveyed respondents in Flexential's 2024 State of AI Infrastructure Report*

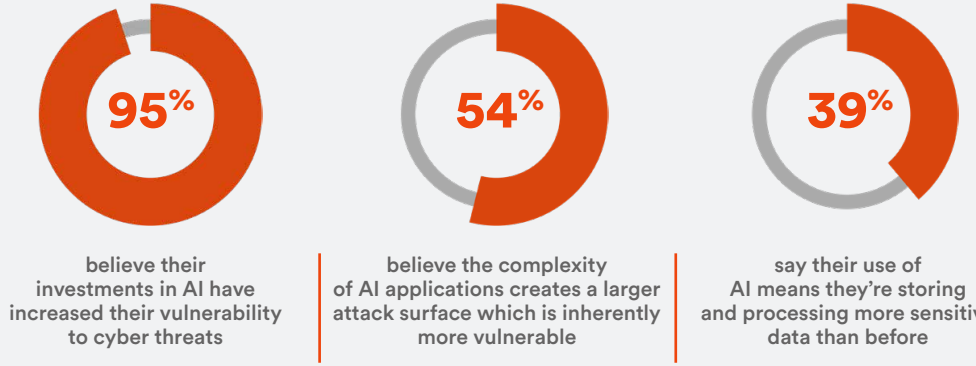
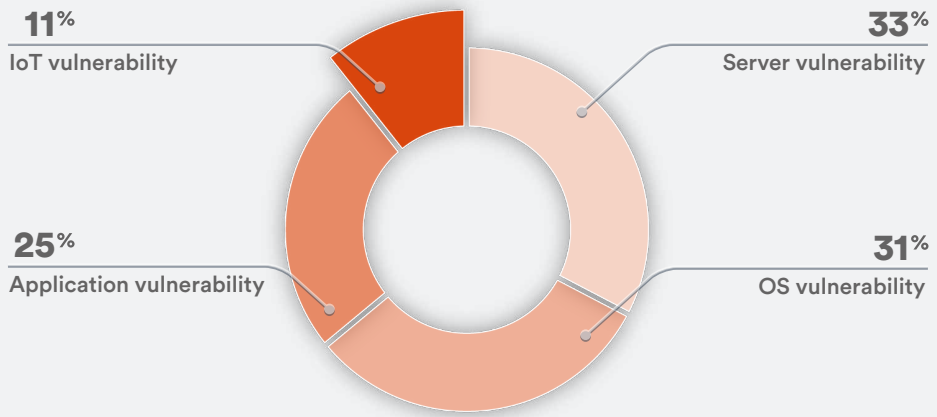


Figure 2.7 *Vulnerability exploits blocked for 110 million unique devices targeted. Source: Symantec*



Legislation to drive further security investments

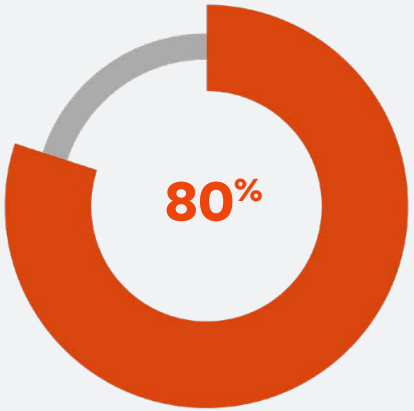
Governments worldwide are implementing stringent regulations to ensure the security of IoT infrastructures, further propelling market demand. Businesses must comply with these regulations, or risk hefty sanctions.

For instance, firms in the UK that fail to adhere to the Product Security and Telecommunications (PSTI) regulations can face fines of up to GDP10 million or 4% of their global turnover – whichever is higher. Similarly, non-compliance with the European Union's Cyber Resilience Act (CRA) could lead to fines of up to EUR15 million or 2.5% of a company's global turnover.

In general, regulatory regions are broken down by country. Therefore, for enterprises operating across multiple countries, compliance with all regional regulations is required; non-compliant companies may find themselves banned.

On the other hand, businesses that continually demonstrate regulatory compliance may have easier access to partnerships and government contracts, as many organisations now prioritise working with vendors that meet high-security standards.

Figure 2.8 *Compliance is now a top priority for 4 in 5 decision makers. Source: PSA Certified.*



the number of technology decision makers who say that compliance with security regulations is a top priority for them in 2024

Security increasingly seen to protect profits

Although the cost of IoT security has historically been a barrier to entry, perceptions are now changing. Once only deployed if a 'free add-on', it is now seen as a vitally important solution feature. For example, in a 2024 Kaleidoscope Intelligence survey, 'extensive security features' was most commonly (60%) ranked as being one of the top 5 factors in an IoT connectivity partner's product.

Furthermore, there is growing consensus that investing in security and ensuring compliance is less expensive than the alternative, with 80% of business leaders stating that building security into their products is a key driver of their bottom line (PSA Certified).

This is supported by a recent Gartner study that found that the average ROI for enterprises implementing IoT security was more than 30%. On the other hand, those who didn't invest in IoT security saw an average negative return of minus 5.6% (Palo Alto Networks).

Ultimately, businesses must now ask if they can afford not to invest in security.

US $5.47 million
average cost to be compliant

US $14.82 million
average cost incurred due to cyber non-compliance*

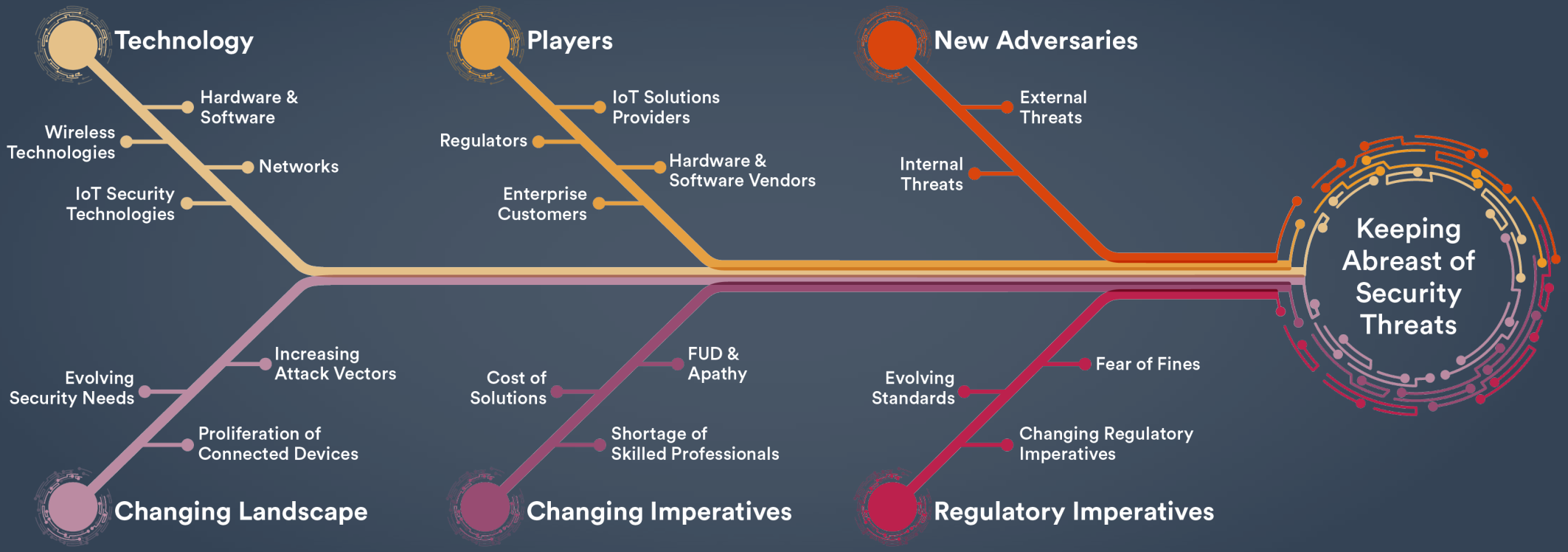
*Includes costs due to business disruption, declines in productivity, fees, penalties, and other legal and non-legal settlement costs.

Results of a benchmark study by Ponemon Institute and Globalscape, 2017

> ***In most cases, addressing the security of a product at the design stage is proven to be lower cost, and requiring less effort than trying to "put security" into or around a product after it has been created (which may not even be possible).***
>
> IoTSF IoT Security Assurance Framework

Multidimensional Factors for Keeping Abreast of Security Threats

The Fishbone Diagram, also known as the Ishikawa diagram, is an analytical tool designed to categorise the factors contributing to a specific outcome or situation - in this case, keeping abreast of security threats.
Each 'bone' represents a factor, each of which can be divided into smaller bones or "influencers" within that category. Beecham Research has identified six factors that must be considered to measure and counteract security threats effectively. Important to note are the factors relating to new legislation, as this will inform the direction of change in the IoT security landscape over the coming years. Technological developments and player initiatives will also play a strong role in helping organisations combat new threats – from both internal and external adversaries.



Technology

- **Hardware and Software**
- **Networks**
- **Wireless Technologies**
- **IoT Security Technologies**

Security solutions are wide ranging and designed to protect devices and data. End-to-end solutions include a variety of measures including device authentication, encrypted communication (using protocols such as TLS and AES), root of trust, secure boot, secure updates, network segmentation, and cloud integration.

Players involved in building solutions

- **IoT Solutions Providers**
- **Hardware and Software Vendors**
- **Regulators**
- **Enterprise Customers**

Large and small companies are involved in building solutions, with affordability being a key differentiating factor. Providers of managed security services are serving a growing market.

New adversaries

- **External Threats**
- **Internal Threats**

The cybersecurity market continues to evolve in response to new, unprecedented threats and adversaries. These threats are not always well-defined, forcing enterprises to continually adapt and develop countermeasures.

Threats can originate from external sources, such as state-sponsored groups and criminal organisations. They can also arise internally, often through disgruntled employees with access to sensitive systems. Hackers (and their motivations) are described by some interviewees in Section 3.

Changing landscape

- **Proliferation of Connected Devices**
- **Evolving Security Needs**
- **Increasing Attack Vectors**

The growing network of connected devices plays an increasingly important role in smart homes, vehicles, and industrial systems. As such, cyberattacks are on the rise, with adversaries utilising AI to exploit vulnerabilities in these ecosystems. In general, threats are evolving in both scale and sophistication, ranging from malware, data breaches, theft, and device hijacking to more targeted attacks – including cyberterrorism. Ransomware attacks in healthcare and critical infrastructure are also increasing.

The risk profiles of many IoT systems are elevated compared with those of enterprise IT, given the IoT's control over physical operations.

The security landscape in IoT covers hardware (such as secure chips), network security, data encryption, and cloud services. Threat types are sector dependent with, for example, cyberattacks in healthcare being different to those within the financial sector.

Changing imperatives

- **Shortage of Skilled Professionals**
- **Cost of Solutions**
- **FUD and Apathy**

Companies often find it hard to measure the return on investment for security, particularly because many IoT devices do not directly generate revenue but instead provide data or other services. This can lead to scepticism about the value of security investments.

Customer awareness of cyber threats is very sector dependent. As such, IoT security is frequently overlooked during the initial design phase, leaving the entire ecosystem vulnerable.

Regulatory imperatives

- **Changing Regulatory Imperatives**
- **Evolving Standards**
- **Fear of Fines**

Regulatory imperatives vary by industry and sector and are subject to continuous change. Sector-specific regulations must be complied with to avoid significant fines.

Industry-specific regulations (such as those in IT) also continue to evolve to address emerging risks. For instance, in 2024, the European Union formally adopted the Cyber Solidarity Act and enacted the Cyber Resilience Act (CRA), both of which are designed to bolster its cybersecurity defences and coordination mechanisms. By creating standardised certification processes, the EU aims to foster trust and increase service quality.

Companies may also seek advice and best practices from independent cybersecurity organisations. For instance, the NIST Cybersecurity Framework recommends structuring a security strategy around five key functions: identify, protect, detect, respond, and recover.

Market Research Findings

Based on exclusive research for this report, including interviews with senior industry experts and recent survey results, this section explores the key trends, perceptions, and challenges shaping the IoT Security market.

IoT Security in the Connected World

As part of the research for this report, Beecham Research conducted a user survey. The main aim of the survey was to study IoT security and its implementation.

About Survey Respondents

Figure 3.1 shows regions where respondent business units are based. Considering the regional splits, this breaks down to 31% in Americas, 46% in EMEA and 23% APAC.

In **Figure 3.2** the majority of respondents' business units (51%) have less than 100 staff. 28% have between 100 and 1000 staff. Lastly, a significant 21% of respondents' business units had over a 1000 staff, representing the larger companies that took this survey.

Figure 3.3 shows the breakdown of the primary roles of businesses. Most respondents fall into the category of IoT Suppliers/Solution Providers (36%), with a significant portion also being Product Makers (17%) and Service Providers (16%). This suggests that the survey insights primarily reflect the perspectives of those building and deploying IoT solutions rather than end users. 'Other types' includes mainly advisors, such as Consultants.

.

Figure 3.1 *In which region is your business unit based?*

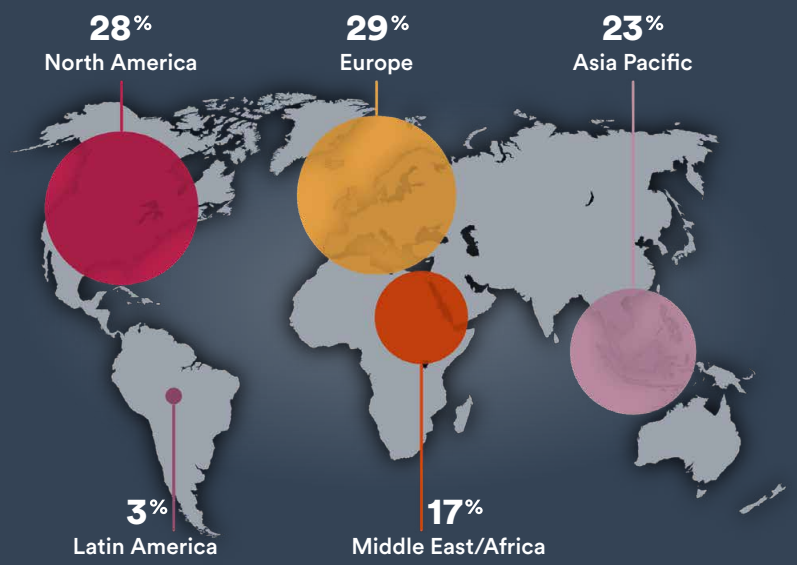
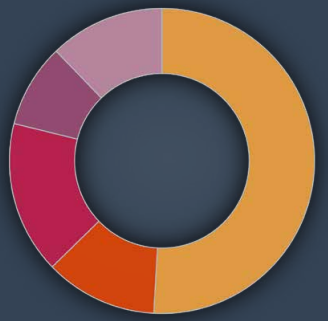
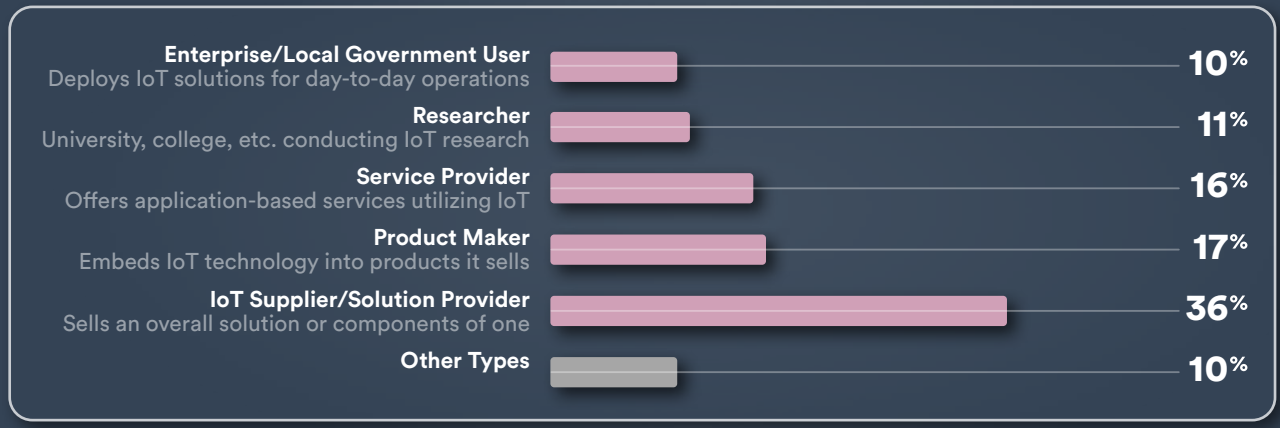


Figure 3.2 *How many staff are employed by your business unit?*



Under 100	51%
100 – 250	12%
250 – 1,000	16%
1,000 – 5,000	9%
Over 5,000	12%

Figure 3.3 *What is the primary role of your business unit in relation to IoT?*



Enterprise/Local Government User Deploys IoT solutions for day-to-day operations	10%
Researcher University, college, etc. conducting IoT research	11%
Service Provider Offers application-based services utilizing IoT	16%
Product Maker Embeds IoT technology into products it sells	17%
IoT Supplier/Solution Provider Sells an overall solution or components of one	36%
Other Types	10%

To understand the dynamics of security, respondents were asked which key sector is important for their business unit. Results from **Figure 3.4** were used to cross-tabulate other responses and observe any significant trends. Telecommunications (30%) stands out as the dominant sector of interest, likely due to the central role of connectivity in IoT ecosystems. Other critical industries such as Energy & Utilities (10%), Transportation/Logistics (8%), and Healthcare (7%) are also well represented.

Importance of IoT Security

In **Figure 3.5** the majority 95% deem IoT Security to be important or 'extremely important'. Cross-tabulation revealed that the telecommunications, energy & utilities, healthcare, and smart city sectors had the most significant amount of interest. This is expected since cybersecurity is integral to the success of businesses operating in these sectors. The remaining 5% of respondents were from retail, mining, and agriculture. This aligns with expectations, as IoT security is not as paramount in these sectors.

Figure 3.4 *Which key sector is particularly important for your business unit (please select one)?*

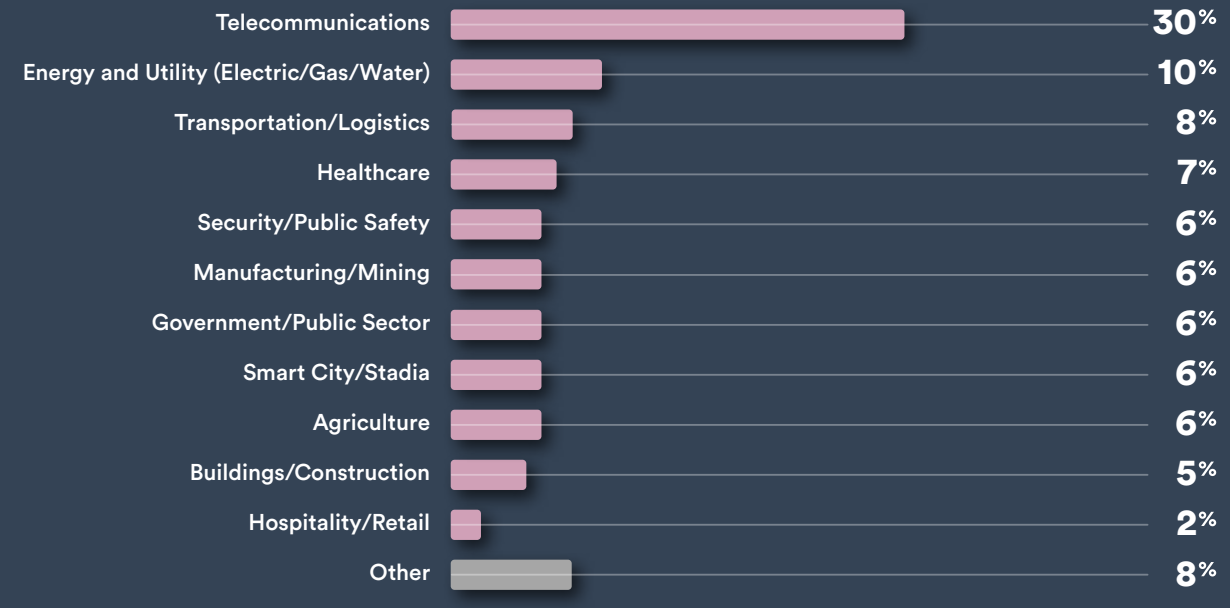


Figure 3.5 *How important is IoT Security in your overall cybersecurity strategy for this sector?*

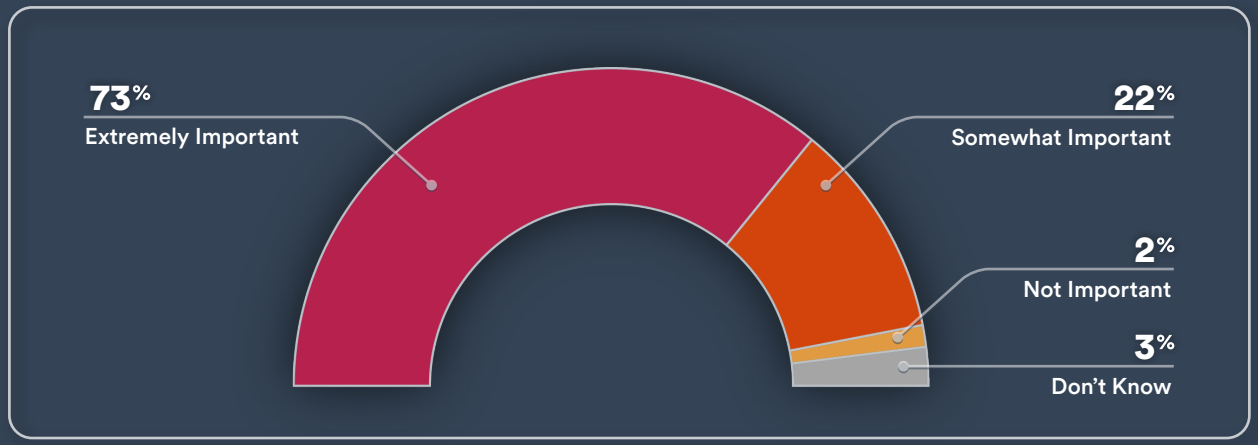


Figure 3.6 shows that critical infrastructure supports business operations for 99% of the respondents, with 45% citing it as essential. Cross tabulation across sectors revealed that telecommunications, energy & utilities, and healthcare are the sectors in which critical infrastructure is most prominently used to support business functions.

Security Measures

To understand current security measures, respondents were asked about the practices they have already implemented, as shown in **Figure 3.7**. The most frequently deployed security measures are device encryption & secure boot (56%), network segmentation for IoT devices (55%), and endpoint security solutions (52%). Zero trust architecture was the least popular, established by only a third (33%) of respondents. Only 8% did not know what security measures their business has implemented.

Figure 3.6 *How important is critical infrastructure to the operations of your business in this sector?*

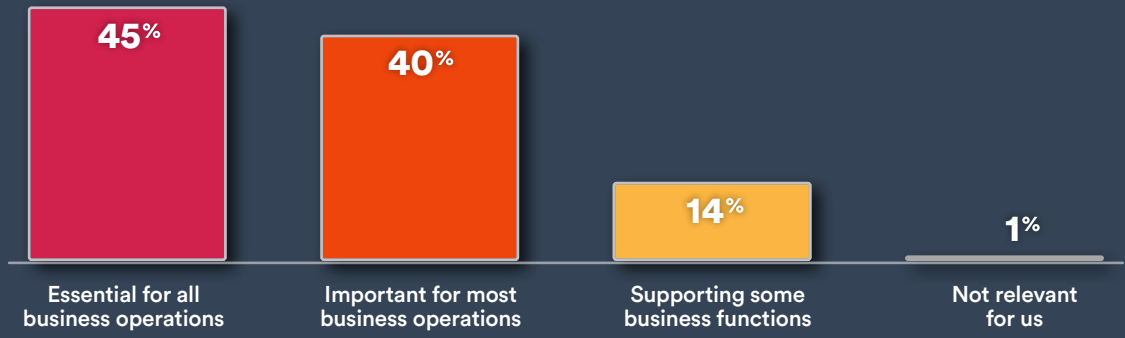


Figure 3.7 *What security measures has your organisation already implemented? (Select all that apply)*

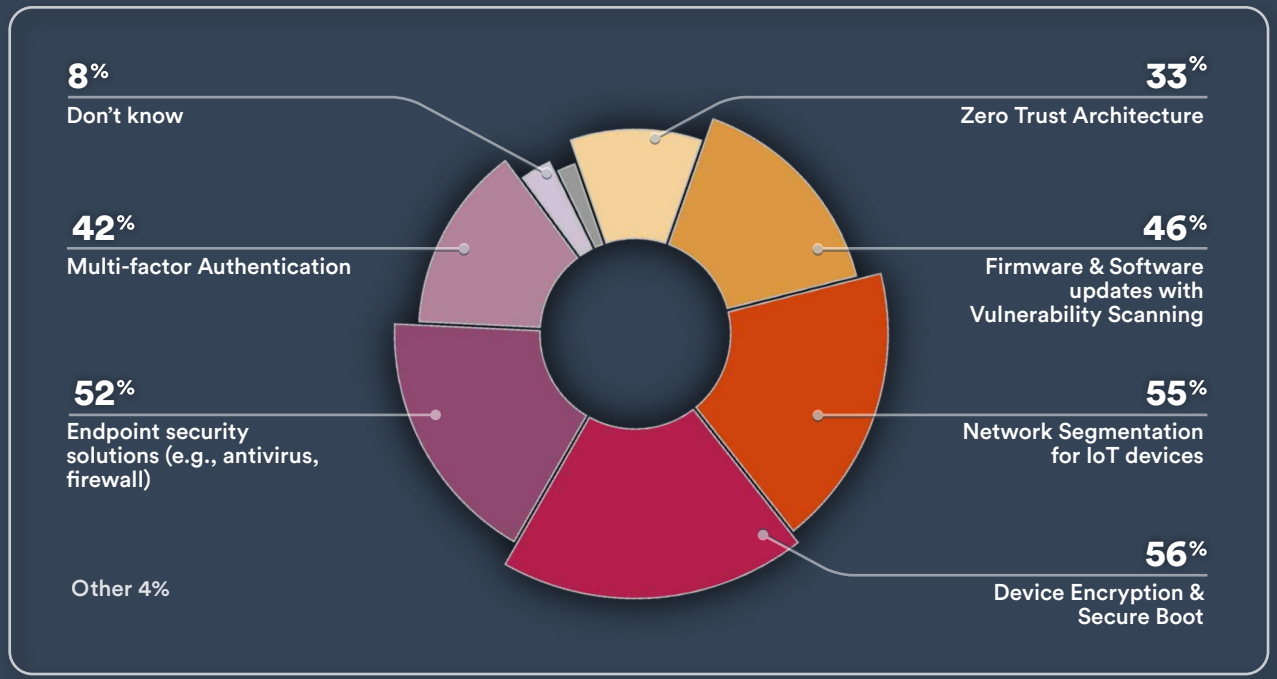


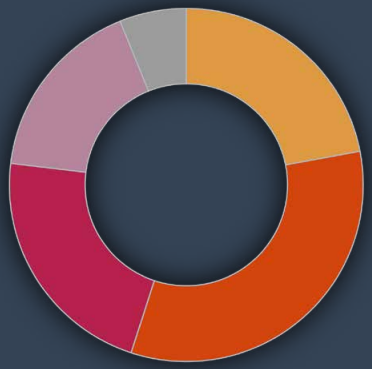
Figure 3.8 shows the status of organisations' IoT Security Frameworks. In total, 77% recognise the importance of an IoT Security Framework and either have a comprehensive framework in place or are updating or developing one. The remaining 23% either 'don't know' or are still evaluating the need for a framework, potentially due to the mindset of 'it won't happen to us'. This leaves them vulnerable to risks that could have severe consequences.

In **Figure 3.9** , it is shown that less than three in five (59%) respondents perceive IoT security to be a necessity from initial design. One in ten (10%) deem it unnecessary or are unsure about its importance. This could be due to cost or time-to-market concerns.

Security as a Service (SaaS)

Figure 3.10 shows that 45% of respondents are interested in SaaS solutions, with 19% already using them. However, this means that more than half of respondents are not interested or, more commonly (31%), 'don't know.' This suggests that security is not being prioritised, and options like SaaS have yet to be explored. This question was used to filter respondents who could answer specific SaaS-related questions, as shown in Figures 3.11 and 3.12.

***Figure 3.8** What is your IoT Security Framework status?*

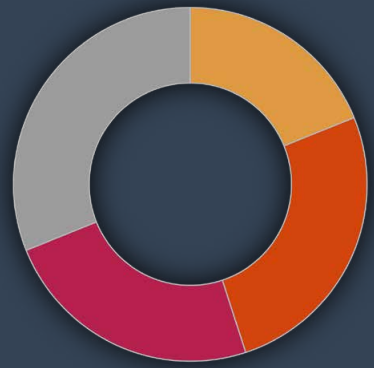


A comprehensive framework is in place	22%
Currently updating/expanding it	32%
In development or planning stages	23%
Evaluating the need for one	17%
Don't know	6%

***Figure 3.9** To what extent is "Security by Design" integrated into your IoT Security solution*

It's a necessity from initial design	59%
Incorporated by service layer/connectivity provider	31%
Not necessary/Not sure	10%

***Figure 3.10** Is your organisation interested in using Security as a Service (SaaS) within your operations?*



We are currently using SaaS security solutions	19%
We plan to implement SaaS security solutions	26%
No, we do not have any plans to use SaaS for security	24%
Don't know	31%

Figure 3.11 illustrates that respondents most commonly obtain SaaS services from connectivity service providers (57%). However, the possibility of sourcing these services from IoT solution/platform providers (35%), cloud providers (35%), and security specialists (31%) suggests a shift towards more tailored and industry-specific security services, likely driven by growing cybersecurity concerns and regulatory pressures. Cellular module vendors was the least popular choice for SaaS services across 'current' and 'possible supply' and the most popular answer for 'no supply/don't know'. This indicates that cellular module vendors are not seen as primary security providers, likely because they are viewed as hardware-focused, with security managed at the network or platform level. It also suggests most organisations prefer security solutions that integrate across their entire IoT ecosystem.

According to **Figure 3.12**, Web & Network Security was reported to be the most essential SaaS service, used by nearly all (96%) of respondents. Identity and Access Management (87%) and Email security (74%) were the next most frequently used SaaS services. This suggests that organisations recognise the importance of securing both communication channels and system access to protect their businesses.

Figure 3.11 *From which types of companies do you currently obtain or plan to obtain SaaS services? (Select all that apply)*

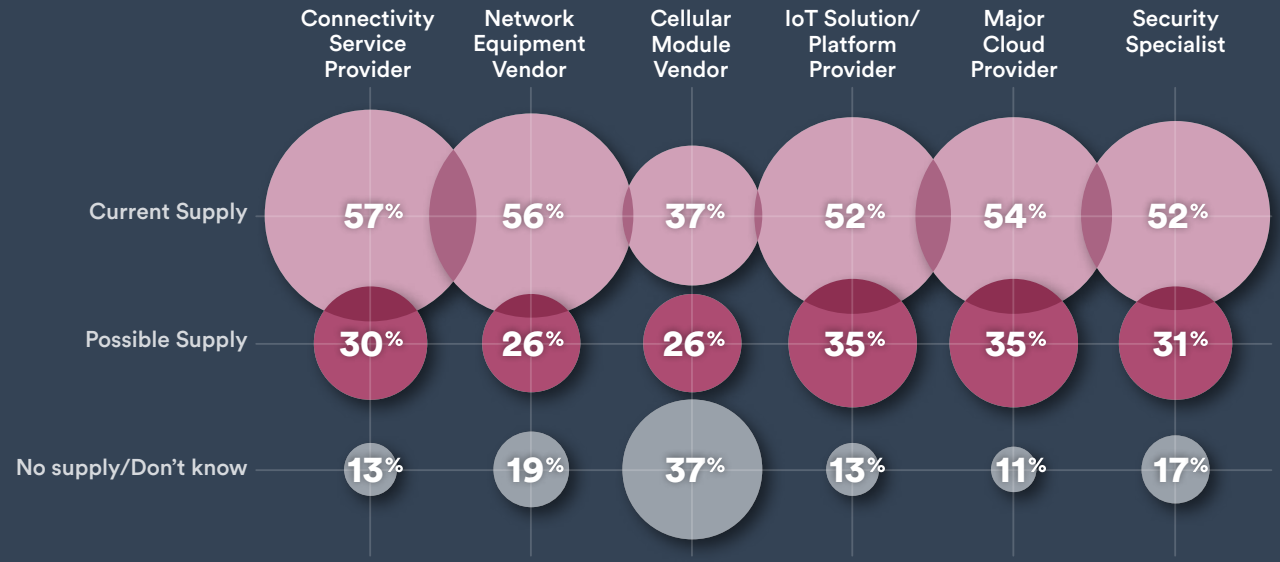
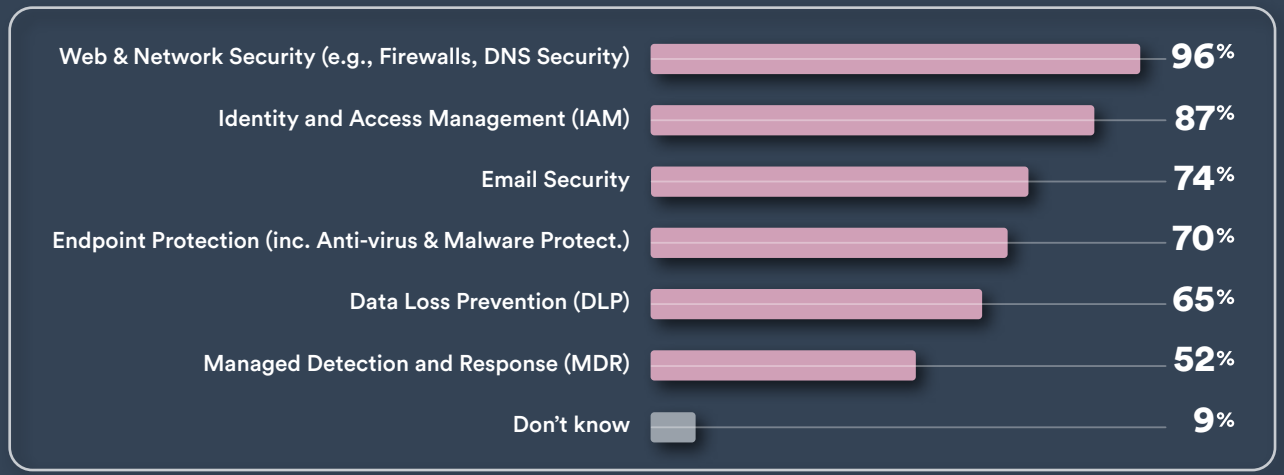


Figure 3.12 *Which of the following SaaS services does your organisation use? (Select all that apply)*



Risks and Implementation

Figure 3.13 highlights several challenges in implementing IoT security, with at least 65% of respondents identifying each issue as 'very challenging' or 'challenging'. The most challenging issue, cited by 82%, was keeping up to date with the latest security threats – technology advancements are known to create new opportunities for threat actors. Lack of standards and fragmented security across suppliers (81%) ranked as the next most significant challenge. This aligns with industry struggles in which interoperability hinders security adoption. In contrast, the ability to scale was seen as less challenging, with respondents not typically linking security and scaling issues. Solutions addressing the most challenging issues are likely to be in high demand in the coming years.

Figure 3.14 shows the prevalence of significant IoT-related security incidents in businesses, with only 18% certain their businesses have experienced one. This suggests a general lack of expectation for incidents - IoT devices are often seen as low-cost and not obvious targets for sophisticated attacks. This could lead to low levels of preparedness, and cause problems if IoT devices are targeted more in the future.

Figure 3.13 *How challenging do you consider the following issues to be in implementing IoT Security?*

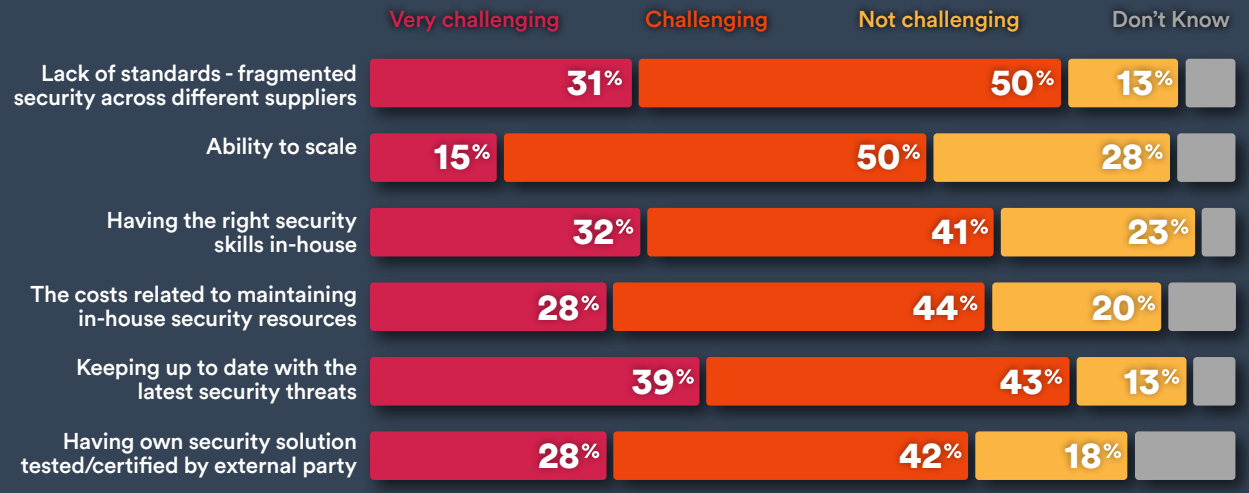


Figure 3.14 *Has your business unit experienced any significant IoT-related security incidents recently?*

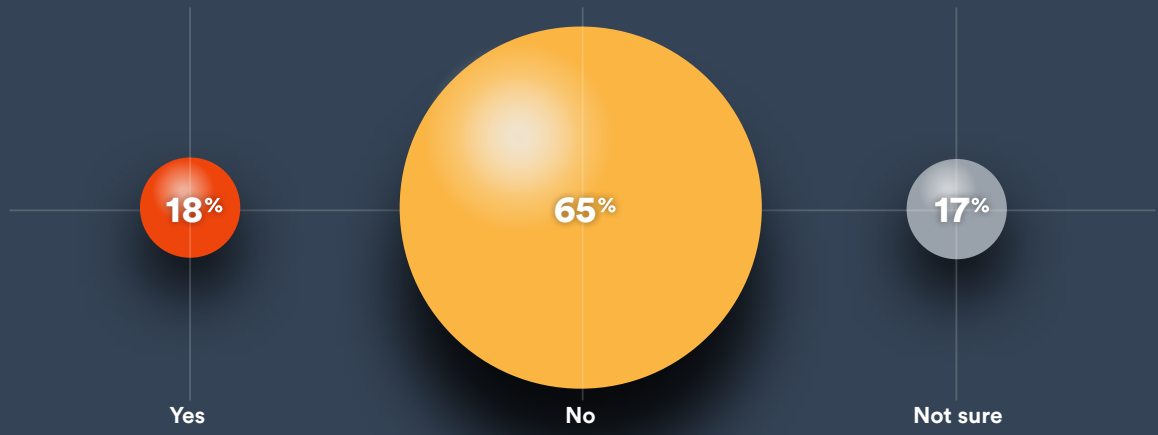


Figure 3.15 shows the most common methods for assessing IoT-related risks in business operations. The top three are risk audits, vulnerability scanning tools, and penetration testing. However, a quarter (25%) of respondents have no formal processes in place, possibly relying on broader IoT security measures or assuming third-party providers handle assessments.

Figure 3.16 shows specific risks relevant to respondents' industries, with unauthorised access (71%) and data breaches (68%) ranking as the top concerns. Cross-tabulation revealed that within telecommunications, privacy risks related to data collection and monitoring, DDOS attacks, and data breaches, leaks, or theft are prominent risks. This aligns with expectations given the industry's focus on sensitive data and network infrastructure. Another high-risk sector is energy & utilities where the most concerning risks are supply chain vulnerabilities, privacy risks related to data collection and monitoring, and DDOS attacks.

Figure 3.15 *How do you assess the risks related to IoT in your operations? (Select all that apply)*

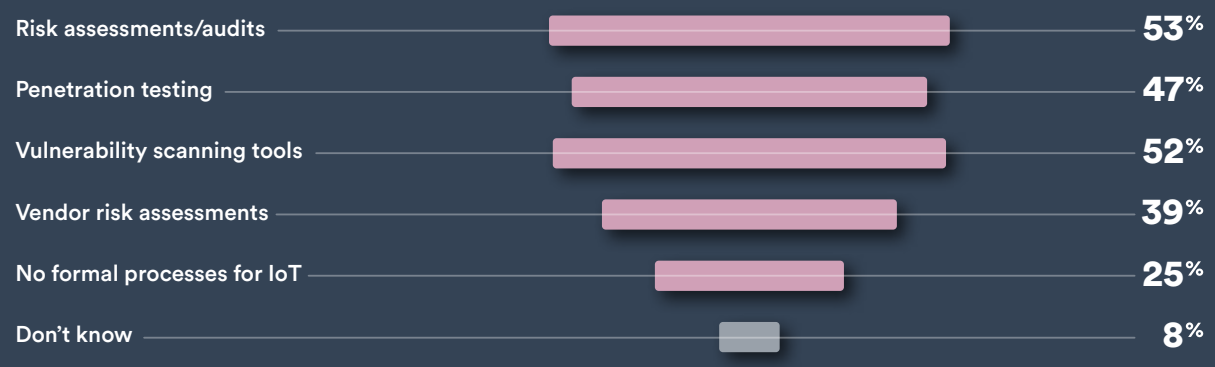
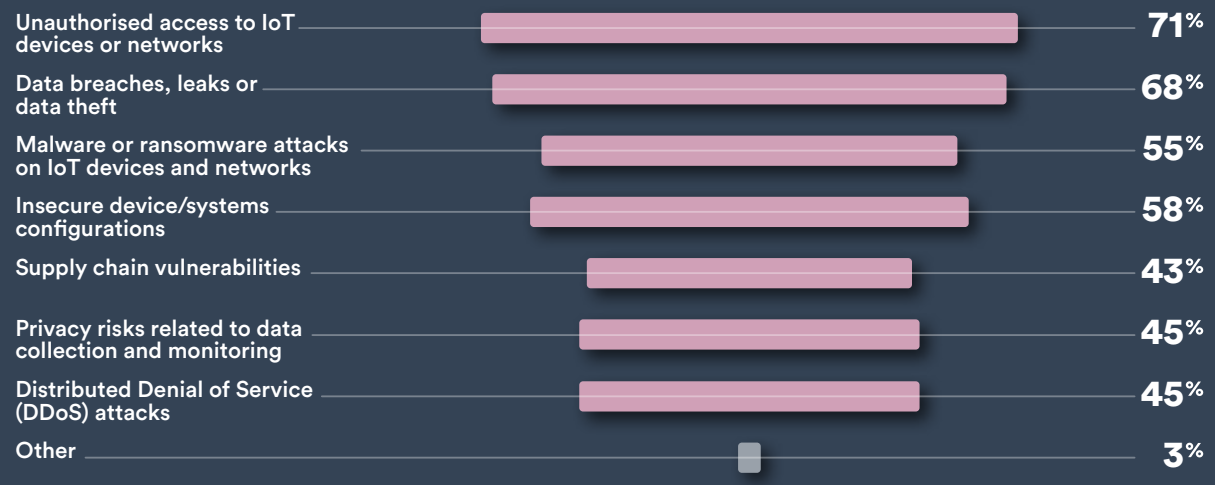


Figure 3.16 *What specific IoT Security risks do you believe are most relevant to your industry? (Select all that apply)*



Costs of Security

Figure 3.17 shows that nearly half (45%) of respondents believe the cost of security is justified and proportional to the risks, indicating a willingness to invest in such solutions. Cross-tabulation reveals that most telecommunications respondents and IoT suppliers/solution providers share this view, with these groups likely understanding the financial and operational impact of breaches. However, 18% view security costs as high relative to the risks, likely reflecting concerns from high-level decision-makers who must justify spending and prioritise other business needs.

Figure 3.18 shows that a combined 75% of respondents perceive an IoT security breach as having a 'critical' or 'very significant' financial impact on their organisation. This emphasises the importance of IoT security in protecting business profts. The 5% of respondents that perceive the financial impact to be minor operate in industries where breaches are less likely to result in significant financial loss such as Buildings/Construction (confirmed through cross-tabulation).

Figure 3.17 *Which of the following statements best reflects your view on the cost of security relative to the risks?*

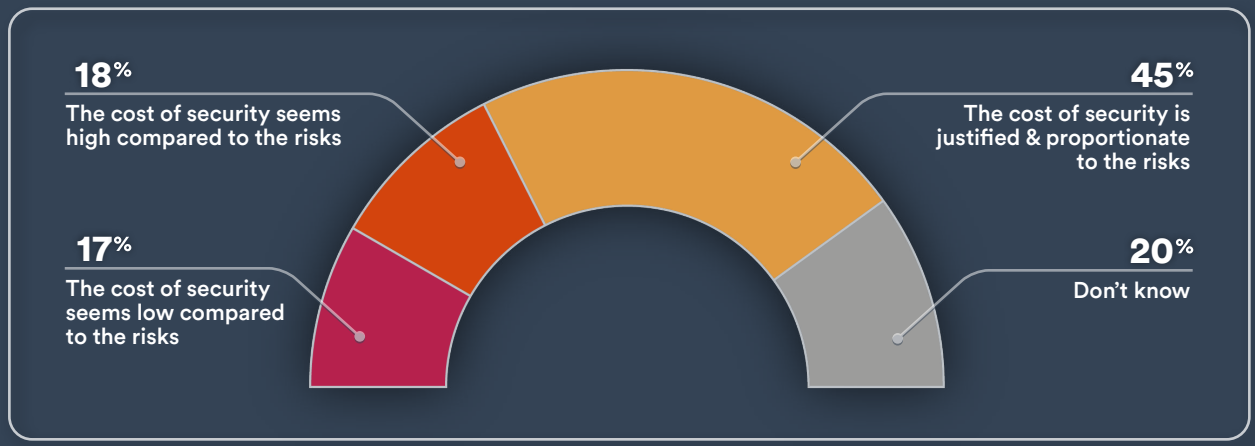
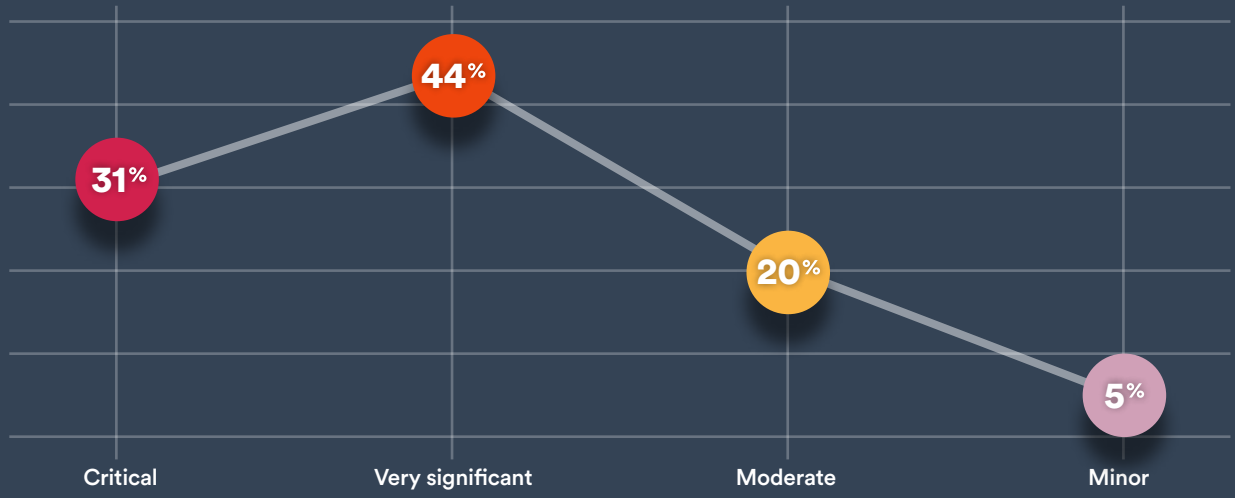


Figure 3.18 *How significant do you perceive the financial impact of an IoT Security breach for your organisation?*



Future Prospects for IoT Security

as shown in **Figure 3.19** only 29% of respondents have plans to improve their IoT security in the near future, leaving the majority (71%) unsure or without IoT security improvement plans for the near future. This signals a lack of urgency around IoT security, either due to uncertainty about the risks, insufficient resources, or a belief that their current security measures are adequate.

Of those planning to improve their IoT security, **Figure 3.20** shows that the most are looking to invest in more advanced IoT monitoring tools (63%) or implement security systems lifecycle assessments (55%). The interest in outsourcing to third parties (25%) and hiring specialised IoT security experts (29%) indicates that many companies are considering external solutions to bridge internal knowledge gaps.

Figure 3.19 *Does your organisation have plans to improve IoT Security within the near future?*

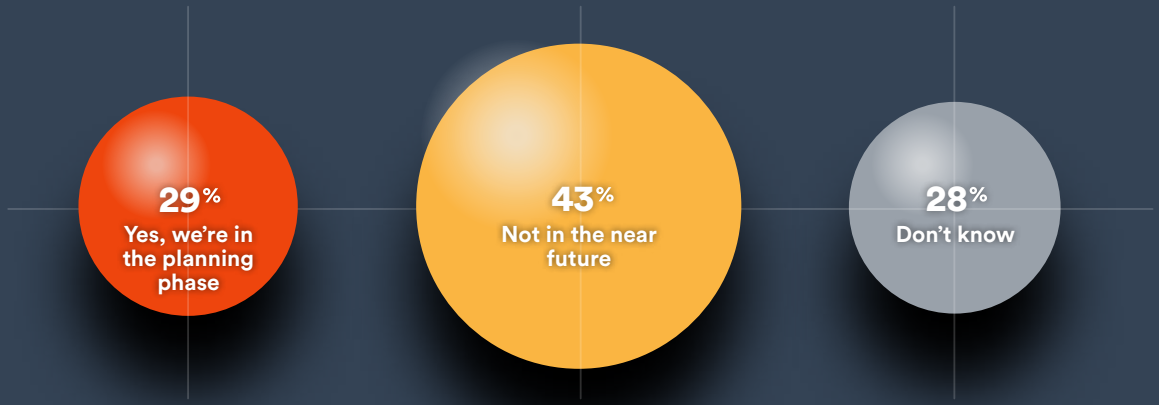
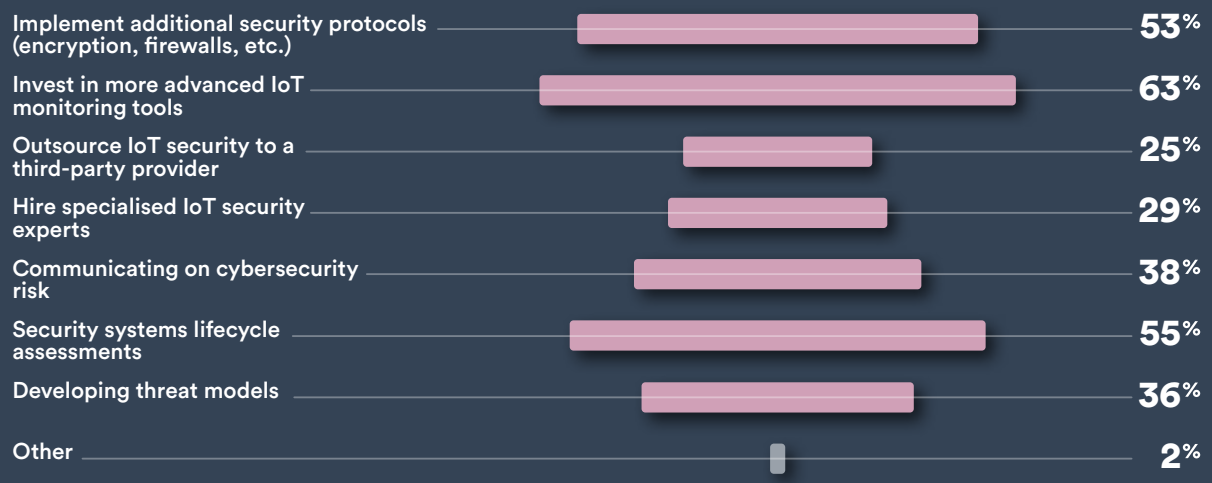


Figure 3.20 *How do you plan to improve IoT Security in the near future? (Select all that apply)*



Survey Analysis Summary

The survey highlights the growing recognition of IoT security as a crucial component of cybersecurity strategies, with 95% of respondents considering it important. However, despite this awareness, implementation gaps remain. While many businesses have adopted basic security measures such as device encryption and network segmentation, 23% lack an IoT security framework altogether.

Security by Design is gaining traction, with 90% of respondents integrating it either at initial design or at the connectivity layer. Interest in Security as a Service (SaaS) is mixed – 45% are considering or already using it, but a significant portion are uninterested, perhaps unaware of its benefits.

Challenges such as evolving threats, a fragmented security landscape, and skill shortages persist, with 82% of respondents struggling to keep up with emerging threats. While 65% of businesses have not experienced a major IoT security incident, this may contribute to complacency, as many still lack formal risk assessment processes.

Despite recognising the financial impact of security breaches, only 29% of respondents have concrete plans to enhance their IoT security. Investments in monitoring tools and security lifecycle assessments are the preferred approaches for those looking to improve.

Overall, while progress is being made, the survey underscores the need for stronger security frameworks, greater industry collaboration, and proactive risk management to protect IoT ecosystems from the emerging threat landscape.

Industry Expert Interviews

As part of this report, Beecham Research conducted one-to-one interviews with ten independent IoT Security experts. Ranging from CEOs and Managing Directors to Executives and Consultants, all interviewees are senior industry figures in organisations that have direct experience in implementing IoT Security solutions.

While our independent survey captures the broader market perspective, these interviews provide a deeper, more specialised view of IoT security, and an assessment of how well businesses are adapting to the realities of the landscape.

The in-depth discussions are particularly valuable in identifying customers' overall security awareness, the key factors influencing their solution purchasing decisions, and how effectively businesses balance their investments against the primary threats. Key quotes from the interviews are highlighted, shedding light on real-world market dynamics and revealing critical considerations for developing a robust IoT security strategy.

Interviewees are all senior executives from:

- *Global Software Licensing Security Executive*
- *Senior Executive, Global Cybersecurity Company*
- *Software Security Consultant*
- *Principal Product Manager - IoT Security Assessment*
- *Senior Professional Services Consultant & Product Trainer*
- *Managing Director, Not for Profit Organisation for IoT Security*
- *CEO, Security Specialist*
- *Senior Executive, Information Management Solutions*
- *Chief Operating Officer, Cybersecurity Solutions Provider*
- *Senior Business Development Manager, PKI as a Service IoT*

Question 1.

How do you see the current market demand for IoT security solutions? Are you noticing a growing interest among your customers, or is there some reluctance in adopting these solutions?

The interviewees attest to a clear growing demand for IoT security solutions due to the increasing complexity and evolution of IoT devices, and the realisation of the risks IoT devices pose. Moreover, new regulations generate more demand, as for example, the US Cyber Trust Mark or industry specific regulations such as the FDA medical device security.

Set against this, demand is still low due to cost factors and the complexity of solutions. Companies may not be fully aware of the risks and dangers; they may also end up dealing with a mix of solutions to achieve the security they need. The reluctance, if any, is from those who don't understand the true costs of security and the risks that come with it, especially in today's day and age where threats are everywhere.

> ***Initial hype around IoT has settled, and now the focus is on practical implementation.***
>
> Global Software Licensing Security Executive

> ***Companies are increasingly compelled by regulations to implement security measures, especially with the risk of fines. Non-compliance can prevent products from being sold in regulated markets, making security a business necessity.***
>
> Senior executive, Global Cybersecurity Company

Question 2. In your experience, do your customers fully understand the security issues surrounding IoT?

Customer awareness of security risks varies significantly. While some industries (like aerospace and medical) are highly aware and compliant with security standards, others may take shortcuts due to a lack of understanding or resources.

In sectors like medical devices, companies are required to follow specific security standards from regulators (FDA in the US) ensuring security is integrated from the start. For smart metering, on the other hand, compliance may vary by region and customer requirements.

The level of understanding of security issues also varies across the world: it is higher in Asian countries, for example, compared with the Middle East. Smaller companies who are resource limited are looking to buy assurances as opposed to security. The integration of IT and OT introduces significant security risks, especially when connected to the Internet. Technology oriented companies have more awareness in comparison to traditional companies.

Some interviewees identified some conflict between the enterprise security team that doesn't want to add more devices, and the business leaders that want productivity through technology. In general, C-Suite executives are interested in business resilience and risk, but don't necessarily understand the nuances of security.

> ***Not fully. Many know IoT has risks, but they often underestimate the potential impact or don't fully grasp the technical details.***
>
> Software Security Consultant

> ***Customers often believe that's the specialists' job to know. However they generally do know there are some issues, but they might not know the depths of these issues.***
>
> Principal Product Manager - IoT Security Assessment

> ***In Industrial IoT (smart metering, medical devices), security is usually a priority from the start. In contrast, consumer IoT products often overlook security during design, only addressing it later, which can lead to vulnerabilities.***
>
> Senior Executive Global Cybersecurity Company

> ***Vulnerabilities in OT can result in severe consequences, including potential harm to individuals or environment damage, making OT security more critical than IT security, which is typically only about data or financial losses.***
>
> Global Software Licensing Security Executive

Question 3.

How do your customers typically respond to the various ‘threat stories’ circulating in the market? Do you find that these stories influence their decision-making processes when it comes to investing in security?

Companies typically react after a major breach, either tightening security or seeking out IoT-specific solutions which include security. Their budgets may open up when these incidents occur to other similar companies to theirs. On the other hand, other companies think it might not happen to them: if it’s in the news all the time, they become desensitised to the severity of it.

There are so many threats now that it is impossible to handle them all.

Cyber terrorism is a threat especially in IT critical infrastructure. Considering all the sensors in industrial installations, they are the perfect vector for cyberattacks and cyber terrorism.

Some replies alluded to other influences on a business, like shareholders and directors, saying that there are other threats to the survival of the business other than cyberattacks.

> ***Yes, absolutely. Selling fear, uncertainty, and doubt. They’re always something on the news and this does influence people.***
>
>  Senior Professional Services Consultant & Product Trainer

> ***Projecting fear is not the way to go. I think fear works to a degree, but you can’t keep peddling fear. I do think those sorts of stories are useful to help companies pay attention, but I don’t think those sorts of stories are what should motivate people.***
>
>  Managing Director, Not for Profit Organisation for IoT Security

> ***Customers sometimes see the issues but they don’t really contact their providers for security about them until it’s too late. So bringing awareness is equally as important.***
>
>  Principal Product Manager - IoT Security Assessment

Question 4.

What criteria do your customers consider when purchasing IoT security solutions? Are they focused on minimal compliance, sector-specific needs, or tailored solutions?

Customers often focus on compliance, but many are now looking for tailored solutions that address specific industry needs and real-time threats. Security solutions must be tailored to the specific operational environment.

Criteria for purchasing are very different for small and large companies. Small and medium sized companies do not go deep into the device security assessment and they mistakenly assume the risk is taken by the manufacturers, and it is the responsibility of the manufacturers to address that. Small companies also tend to look to buy in that expertise and try to gain some assurance; they are focused on immediate business needs and may overlook advanced security requirements.

By contrast, large companies are already preparing for future technologies like quantum computing. Largest companies typically have more resources and better IT-OT integration, while smaller companies may struggle to implement or afford effective security solutions.

The issue that also comes with security is the maintenance cost; the more sophisticated that security is, the more maintenance it is likely to need. In the meantime, the threat landscape keeps on evolving.

From a business risk perspective, companies invest in how valuable or costly they think the risk to be for the operation of their business. Companies that are more risk averse will look to outsource the risk or rely on insurance or assurance.

> ***Small companies, they just want to tick the box. Larger companies have a bigger spend so their budget allows for better investments in security. The criteria vary for customers.***
>
> Senior Professional Services Consultant & Product Trainer

> ***A vendor needs to develop its products and solutions for the most restrictive policies and governance in the world and the major markets; then by default, it is able to generally meet the requirements of all the others. It's a difficult game for vendors to play because all these regulations are constantly changing all over the world.***
>
> CEO, Security specialist

Question 5. Do your customers generally expect that all necessary security features are included in the solutions you provide? Do you offer end-to-end security solutions. If so, how do you ensure it? If not, which specific aspects of security do you cover?

The security landscape in IoT is wide ranging and covers hardware (e.g. secure chips), data encryption, and cloud services. Some providers may focus on securing hardware and digital identities, while others might focus on IT infrastructure monitoring or recovery.

Typical replies as to what is offered include: end-to-end security (covering device authentication, encrypted communication, secure updates, and cloud integration), encryption (TLS and AES), secure boot, root of trust, and network segmentation to protect devices and data.

Some measures are endpoint-based to keep secure from breaches; these include network scanning and authentication. There are also solutions based on e-mail and website appliances, scanning e-mail and web traffic in and out, and pen-testing.

The use of VPNs for secure connections, key management systems and centralised password management as essential tools for securing IoT environments; centralised key and password management systems are vital to ensure that each device has unique passwords and private keys, preventing widespread breaches from a single compromised device. Managing these centrally is far easier and more secure than having the same credentials on multiple devices.

Also offered are multiple solutions focused on certificate life cycle management and public key infrastructure (PKI). However, the extent to which end-to-end security is provided depends on the customer's use case. A solution may comprise integrations with other systems, such as Over-The-Air (OTA) updates or key management.

> ***Large enterprises tend to invest in comprehensive, custom solutions, while SMEs usually opt for more affordable, compliance-driven options.***
>
> Software Security Consultant

> ***We use identity and access management security to give role based access for different individuals and that might be within an organisation.... We allow role based access using sort of high end identity and access management security to give people access to that IoT data.***
>
> Senior Executive, Information Management Solutions

> ***We try to foresee the threats and with our solutions, we provide system updates so firmware of devices and all the software is updated. These devices are deployed safely in our ecosystem or with Cloud platform, gateways, so there is end-to-end security. We also have full encryption for data that is obtained at the device and at the gateways, and so it's encrypted until till it reaches the Cloud.***
>
> Chief Operating Officer, Cybersecurity Solutions Provider

Question 6.

What do you see as the primary security threats facing IoT today? Which specific threats are your solutions designed to guard against?

The security landscape in IoT covers hardware (e.g., secure chips), data encryption, and cloud services. Some companies secure hardware and digital identities, while others might focus on IT infrastructure monitoring or recovery.

Threats are sector dependent. According to one view, most start with phishing; probably 80-90% start with phishing and then move away from that. Overall the sheer scale and volume of end points become access points for attacks.

Identity and access management are vulnerable access points, for users and devices and sensors, which are often placed in a non-secured environment, leaving gateways vulnerable too. Sensor's software is not upgraded as frequently as they should be.

> ***The biggest threats include device tampering, data breaches, DDoS attacks, and weak authentication.***
>
> Software Security Consultant

> ***Working on old firmware or old software, they can be easily manipulated because they are not up to date based on current security requirements, so they are may often than not have a lot of vulnerabilities.***
>
> Chief Operating Officer, Cybersecurity Solutions Provider

Question 7.

In your experience, is it possible to categorise IoT security threats? If so, how do you typically categorise these threats, and what criteria do you use?

The main threats identified are:

- Ransomware attacks: Hackers seek to extort money by holding critical systems hostage.
- Data theft: Sensitive data can be stolen and exploited.
- Bad actors: Some hackers breach systems simply to test their limits or for malicious purposes.
- Harmful attacks: In rare cases, hackers intend to cause physical harm, such as tampering with critical infrastructure or devices in healthcare.

The primary difference between OT and IT security risks is that OT security breaches can result in physical injury or environmental harm.

Internal threats, such as disgruntled employees, can be more dangerous than external hackers, especially when insider knowledge is exploited.

> ***IoT threats fall into categories like physical attacks, network vulnerabilities, software flaws, and data privacy risks and the scale of them can vary from case to case.***
>
> Software Security Consultant

> ***Most hacking today is financially driven, with ransomware being a common method. However, some attacks are government-sponsored or aimed at testing vulnerabilities for future potential use.***
>
> Global Software Licensing Security Executive

> ***We are focusing primarily on external threats, as our company addresses securing IoT devices used by clients. Internal threats as more relevant to OT (Operational Technology) systems within an organisation's infrastructure, which are often handled by ensuring true zero-trust identities on devices.***
>
> Senior Business Development Manager, PKI as a Service IoT

Question 8.

From your perspective, what are adversaries, such as hackers, seeking to achieve or gain out of breaching security?

Motives for breaching security vary – financial gain, data theft, industrial espionage, political motivation or simply to disrupt operations. Very often it is money driven, selling customer data, ransom demand, manipulating elections results, to name a few.

Cyber hacking is a business all to its own and represents a significant piece of the whole GDP in a business. Problems may be state-sponsored or non-government aligned criminal operations.

> ***These sort of breaches did start out with stealing money but the motives have grown a lot since then and various players are at risk across various industries.***
>
> Senior Professional Services Consultant & Product Trainer

> ***Motives include data theft, data leaks, and even data manipulation. Data manipulation is actually very dangerous: When we have AI in our systems and this data is manipulated, AI will use that manipulated data which can affect outputs like downtime and uptime costs in businesses, and could end up affecting profitability. ..And that's only one scenario.***
>
> Chief Operating Officer, Cybersecurity Solutions Provider

Question 9.

How do you think companies balance the cost of security with the required security needs? Can you provide examples of strategies that have been successful in navigating this balance?

Companies must decide how much to invest in security based on their business models. In some cases, security is critical to ensuring revenue (e.g., in IoT business models where usage is tracked for billing), while in others, it might be seen as less urgent.

Often, for reasons like time to market, security is postponed until later stages, making it more difficult and costly to implement.

Smaller companies are limited by budget and spend only how much they have to spend; larger companies also have budgetary constraints but they do not need as strong a justification as small companies. This decision making process is how these companies try to balance cost with needs.

Needs are closely related to compliance. Some companies believe that even if standards are not yet obligatory by law, it is best to follow them.

Companies often find it hard to measure the ROI (return on investment) for security investments, particularly because many IoT devices do not directly contribute to profit but provide data or other services. Since some view security as an overhead, they may be tempted to take shortcuts. However, the risks of not investing in security, such as breaches, fines, and reputational damage, are high. Larger organisations and mission-critical applications typically invest more in security than consumer-grade device makers.

> ***The balance depends on the risk profile. For most, it's about matching security investment with potential risk exposure and regulatory requirements, which varies for different companies in different verticals.***
>
> Software Security Consultant

> ***Compliance has to be followed and so the cost has to be covered. But balancing this cost depends entirely on budget and this budget is different across businesses, sizes, type of data handled, what sort of records and information are involved.***
>
> Senior Professional Services Consultant & Product Trainer

> ***They don't balance it very well. And that's one of the reasons why so many IoT projects don't scale.***
>
> Senior Executive Information Management Solutions

> ***One of the biggest challenges is convincing companies to implement security early in the development process.***
>
> Senior Executive Global Cybersecurity Company

Question 10.

What are your views on managed security services, such as Security as a Service (SaaS)? Do you see it as a key approach moving forward? How can organisations assess what additional security measures are necessary beyond what these services offer?

Managed Security services is growing; for small companies with fewer resources, it may provide a way forward, outsourcing assurance.

Companies may not want to be fully responsible for the whole process of organising cybersecurity, being focused on selling and developing their products. Lack of awareness about cybersecurity is an opportunity in the industry for these managed security services to grow. For these and other reasons there is a good justification for a service model, both in terms of cost and time.

Some companies take a hybrid approach where some of the security elements are handled in-house and the rest are through a third-party.

> ***SaaS is gaining traction, especially for SMEs, but it should be complemented with strong internal controls, monitoring, and threat detection tools.***
>
> Software Security Consultant

> ***Organisations first need to identify what they need security for. They need to try and identify the risks of those assets, or even outsource that process. However it needs to be done, so all areas can be covered and secured.***
>
> Principal Product Manager - IoT Security Assessment

> ***There is value in managed security services, particularly for key and password management. However IoT devices, especially simpler ones like sensors, are not yet well suited to the more complex security standards seen in IT.***
>
> Global Software Licensing Security Executive

> ***It's a challenge because of the mindset of wanting to own and pay once for security solutions, and I don't think that's the nature of connected technology, especially with maintenance involved.***
>
> Managing Director Not for Profit Organisation for IoT Security

> ***Those who are currently working on manufacturing or industrial operational technology, they often lack the know how about cybersecurity which is a big problem; lack of awareness about cybersecurity is an opportunity in the industry for these managed security services to grow.***
>
> Senior Executive Global Cybersecurity Company

Mitigating and Managing IoT Security Threats

This section examines security best practices that businesses can adopt to strengthen their resilience against IoT cyberattacks. Regulatory and certification insights are also offered, along with recommendations to help protect against future threats.

The Evolution of IoT Security Solutions

(This introduction draws on a discussion with Syed Zaeem Hosain 'Z', Founder of Aeris Communications)

Before the term "Internet of Things" (IoT) was coined, the industry was focused on machine-to-machine (M2M) communication rather than security. The primary concern at the time was ensuring connectivity, with little emphasis on potential vulnerabilities.

An early example of the realisation of this risk came in the late 1990s when Z was asked by a senior telecom executive about how to disable a compromised device remotely. This led to the development of a patented system that allowed Aeris to shut down M2M devices in the event of unauthorised use. While this was a pioneering idea at the time, remote shutdown remains a critical mitigation strategy in IoT security today.

In the early 2000s, as the number of connected devices grew, the need for security became evident. The rapid expansion of cellular IoT – without proper safeguards – created an environment where security breaches became inevitable.

Remote device shutdown was an early solution to prevent stolen or compromised devices from causing damage – but this alone is not enough to meet evolving security needs, especially as attackers shift their focus from corporate networks to physical infrastructure. The healthcare industry is a prime target, as IoT ransomware can cripple hospitals and medical services. Many modern CPAP machines, glucose monitors, and other medical devices are IoT-connected, making them potential targets for cybercriminals seeking financial gain.

Beyond healthcare, critical infrastructure like power grids, water treatment plants, and transportation systems are also vulnerable. For instance, a 2014 cyberattack on Ukraine's power grid demonstrated how an attacker could remotely disable a city's electricity by infiltrating IoT systems. Similarly, concerns about IoT-based attacks on aviation are growing, particularly scenarios where hackers compromise aircraft control systems or interfere with automated landing technologies.

Key Security Challenges in the Modern Landscape

With millions of interconnected devices in use, a single security flaw can multiply across networks, turning an isolated vulnerability into a widespread threat. This risk is not hypothetical. For example, just a few years ago, hackers seized control of more than half a million video cameras, using them in a massive, coordinated assault to crash major online services like Netflix and Yahoo. Each of these cameras shared the same firmware weakness, allowing attackers to orchestrate a relentless Distributed Denial-of-Service (DDoS) attack. This is the dark side of IoT at scale – a potential army of everyday devices poised to disrupt industries without warning.

Similarly, a recurring issue in the IoT landscape is unprotected network access – it is common for IoT devices to have public IP addresses, making them accessible to hackers. This is particularly dangerous in the case of applications that have high impact and affect a lot of people. For instance, in 2017, the Triton malware targeted Schneider Electric's Triconex Safety Instrumented Systems. Given these safety systems are used to prevent industrial disasters, the attack had the potential to cause catastrophic physical damage, such as explosions, equipment failures, or even loss of life. This represents the changing nature of IoT attacks – no longer launched just for financial gain, but to cripple essential services, disrupt whole regions, and potentially put lives at risk.

Fraud and unauthorised data usage also present significant security risks, both in isolated cases and across multiple businesses. For instance, in one case, truck drivers in Mexico were found to be removing IoT SIM cards and selling data access. In another, a cellular module supplier was discovered to be secretly transmitting diagnostic data from IoT devices to their own servers, unbeknownst to the customers. More recently, the 2023 MOVEit Transfer attack exploited a zero-day vulnerability in the file transfer software, leading to data breaches across multiple organisations. Data breaches can lead to significant financial and operational costs, as well as significant regulatory sanctions for affected businesses.

With infrastructure, networks, and operations increasingly connected, businesses, users, manufacturers, and providers must work together to protect against cyber adversaries. In other words, in the future everyone must learn to use the Internet in a way that minimises the threat to anyone else – just like driving on the road. You have to drive safely to avoid accidents. In the past, this shared responsibility has not been recognised. In the future, it becomes increasingly essential.

The Business Case for IoT Security

As the base of IoT devices continues to grow quickly over the next few years, the issue of vulnerability detection and monitoring becomes crucial. Businesses are facing threats that have moved from general Internet to increasingly specific IoT attacks. Furthermore, the issue is not just a direct attack on one device – it is the potential for taking over a large number of devices to target a completely unrelated service.

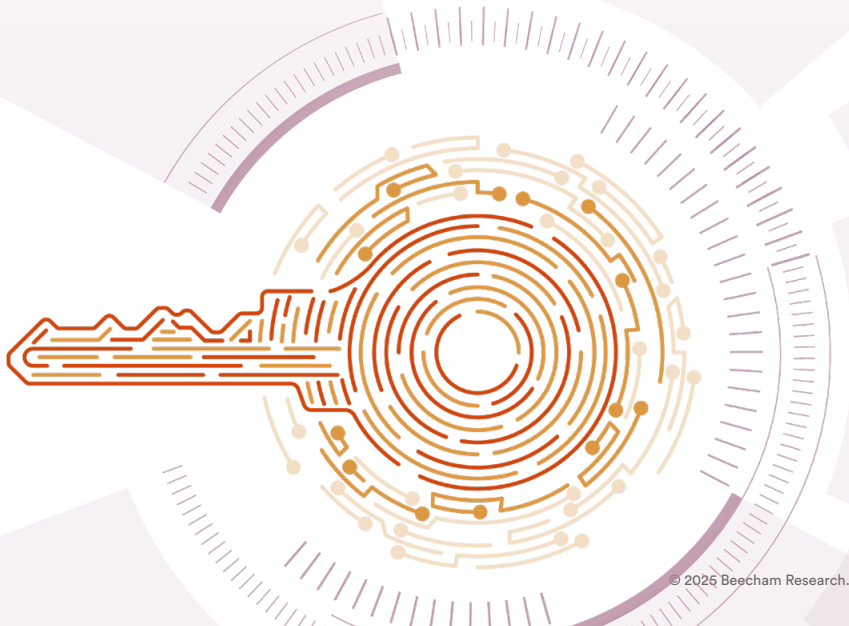
At the same time, governments are watching, regulating, and mandating, with the European Union's CRA marking an important step forward in IoT security legislation. Penalties are high to encourage action, with the costs for compliance now lower than the financial consequences of non-compliance.

Security used to be considered a straight cost, to be minimised as much as possible. Today, it must be viewed as an enabler: if business cannot be conducted securely, then the level of that business will almost certainly be negatively impacted.

The following sections examine how security can be built into IoT solutions – first, through a framework to help understand, prevent, and respond to attack threats. Next, through understanding the architecture of the IoT stack, the vulnerabilities of each element, and the importance of implementing security as an end-to-end solution. Security by Design is introduced as a proactive approach to cybersecurity, with its key principles and benefits outlined.

This is followed by an examination of IoT security regulations – how they evolved, why they matter, and where they differ between regions. Certification options are shown, with accreditation crucial to building trust with clients, partners, and regulators.

Technical insights from our report sponsors are featured throughout, demonstrating solutions to some of the most challenging issues within the IoT security landscape.



IoT M2M Council

The IMC (IoT M2M Council) provides a structured approach to addressing security challenges across the IoT ecosystem.

It divides security into three key layers:

1. Device security - securing IoT endpoints through hardware-based protections, secure firmware, and authentication mechanisms.

2. Network security – protecting data in transit using encryption protocols, authentication measures, and intrusion detection.

3. Cloud/service security - safeguarding back-end infrastructure by enforcing access controls, encrypting stored data, and implementing continuous monitoring.

This framework offers a holistic approach to security, ensuring that vulnerabilities are addressed at every level of IoT deployment. Its scalable and flexible structure allows businesses to implement security measures according to their specific needs while ensuring compliance with industry regulations. Additionally, by mitigating risks and reducing attack surfaces, it enhances overall market confidence in IoT technology.

Beyond security, this approach plays a crucial role in standardising IoT security practices, offering a common reference point for manufacturers, developers, and service providers. This standardisation not only strengthens security but also encourages innovation by providing a safer environment for deploying new technologies.

Joint Task Force on IoT Security

The IoT M2M Council and the Global Certification Forum have formed a Joint Task Force to evaluate the development of a certification program for the security of IoT deployments. The objective of the group is to determine if such a certification program is viable, and if so, what its scope and timeline might be.

The Joint Task Force is just getting started and there will be a regular series of online and in-person meetings – the first of which was held on 6 February.

Thus far, the following principles have been agreed:

- To add real value, the program will cover not just devices, but also the network and cloud/app platform layers of the IoT stack.
- The program will make use of relevant, existing standards that are available in the public domain wherever appropriate.
- The program will be more practical and prescriptive than many currently available standards.

Some of the leading technology and service providers to the IoT sector - including Aeris, Anritsu, AWS, Cisco Systems, DEKRA, Digi International, Element Material Technologies, Eurofins, filancore, Finite State, Giesecke + Devrient, Globalstar, Keyfactor, Keysight, MultiTech, Qualcomm, Quectel, Rohde & Schwarz, Samsung Eletronics, SGS, Somos, Tartabit, Tata Communications, Telefonica, Telit Cinterion, Thales, TUV, Verizon, and Vodafone - have already agreed to participate in the Joint Task Force.

Application to participate in the Joint Task Force is open through the IMC website.

Establishing Security Protocols

As IoT networks expand, securing devices and data requires a structured and proactive approach. The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides five key pillars: Identify, Protect, Detect, Respond, and Recover.

This is a basic framework that has been widely adopted internationally and built upon by other security-focused organisations. Taking initiatives from these principles, organisations can build resilient cybersecurity defences.

Figure 4.1 *NIST Cybersecurity Framework*

Identify

Asset Management, Business Environment, Governance, Risk Assesment, Risk Management Strategy

The first step in securing IoT ecosystems is understanding risk. Organisations can catalogue assets, assess vulnerabilities, and map system interactions to identify potential gaps in security. With this visibility, mitigating risk becomes more transparent. This phase also includes regulatory alignment, ensuring policies comply with legal frameworks like the EU Cyber Resilience Act (CRA) and the UK Product Security and Telecommunications Infrastructure (PSTI) Act. A well-defined risk management strategy helps prioritise security efforts and resource allocation.

Protect

Awareness Control, Awareness & Training, Data Security, Info Protection & Procedures, Maintainance

Once the risks are identified, protection measures can be implemented to prevent unauthorised access and data breaches. Embedding Security by Design principles in IoT development reduces vulnerability prior to deployment. Protective strategies include strong authentication protocols, end-to-end encryption, and access control. Regular software and firmware updates over the air help to secure newly discovered vulnerabilities. Additionally, staff training and increasing security awareness contribute greatly to reducing human error and enhancing security resilience.

Detect

Protective Technology, Anomalies & Events, Continuous Security Monitoring, Detection Process

Cybersecurity threats constantly evolve, making early detection critical. To react to this condition, continuous monitoring is used to identify anomalies and unauthorised access attempts in real time. Detection mechanisms include intrusion detection systems (IDS), anomaly detection, and automated tools. These technologies provide security teams with actionable insights, allowing them to respond to threats before they escalate.

Respond

Response Planning, Communications Analysis, Mitigation, Improvements

When a security breach occurs, swift action is vital to contain the risk and minimise damage. Organisations should have a predefined incident response plan, ensuring security teams can isolate compromised systems, assess the threat, and mitigate risk effectively. Effective incident communication ensures affected users, regulatory bodies, and stakeholders are informed. A rapid, structured response helps limit operational disruption, preserving business continuity and reputation.

Recover

Recovery Planning, Improvements, Communications

After a cybersecurity incident, the focus shifts to restoring systems and preventing future breaches. This involves forensic analysis to determine root causes and updating security measures based on lessons learned. A business continuity plan ensures operations resume quickly with minimal impact. Strengthening IoT security practise through continuous improvement and monitoring ensures greater resilience against future threats.

Build Secure, Buy Secure, Be Secure

The IoT Security Foundation (IoTSF) is a global not-for-profit membership organisation established to combat the challenges of an increasingly connected world.

Dedicated to driving security excellence, the IoTSF:

1. Develops and publishes security guidelines and frameworks, intended to help organisations design, implement, and maintain secure IoT solutions.

2. Educates stakeholders through workshops, webinars, programmes, and conferences.

3. Promotes collaboration between manufacturers, developers, researchers, and security experts, and fosters partnerships between industry, governments, and academic institutions.

4. Advocates to policymakers for stronger security measures in IoT legislation.

Together, these activities offer an international response to the complex challenges posed by cybersecurity and are integral in raising the bar on digital safety and security.

IoT Security Assurance Framework

One of IoTSF's most notable publications is its IoT Security Assurance Framework (Release 3.0). Formerly known as the IoT Security Compliance Framework, it is intended to help companies make high-quality, informed security choices by guiding them through a comprehensive requirement checklist and evidence gathering process.

The evidence gathered during the process can be used to declare conformance with best practice to customers and other stakeholders.

Further best practice publications are available on the IoTSF website. Each publication includes contributions from security practitioners, researchers, industrially experienced staff, and IoTSF's membership and partners.

Members of the IoTSF also have access to an Assurance Questionnaire – a companion audit and assessment tool to the Framework.

***Figure 4.2**. Key compliance requirements of the IoT Security Assurance Framework*

Key Requirement	Action Required
Management Governance	There must be a named executive responsible for product security, and privacy of customer information.
Engineered for security	The hardware and software must be designed with attention to security threats.
Fit for purpose cryptography	These functions should be from the best practice industry standards.
Secure network framework and applications	Precautions have been taken to secure Apps, web interfaces, and server software.
Secure production processes and supply chain	Making sure the security of the product is not compromised in the manufacturing process or in the end customer delivery and installation.
Safe and secure for the customer	The product is safe and secure "out of the box" and in its day-to-day use. The configuration and control should guide the person managing the device into maintaining security and provide for software updates, vulnerability disclosure policy, and life cycle management.

The Importance of End-to-End Security

The Architecture of IoT Platforms

For any IoT solution involving connected devices, there are three key elements that must be managed:

1. Devices
The hardware at the edge of the network forms the 'things' of IoT and, equipped with sensors, they gather data which will be transferred over a network. The platform must be able to manage individual devices in the network, provision them for use, and update them securely over-the-air.

2. The Connection
Communication technologies transmit data from the device to a server where it can be processed. Some areas that need managing are connectivity options, coverage, network protocol support, and billing/usage.

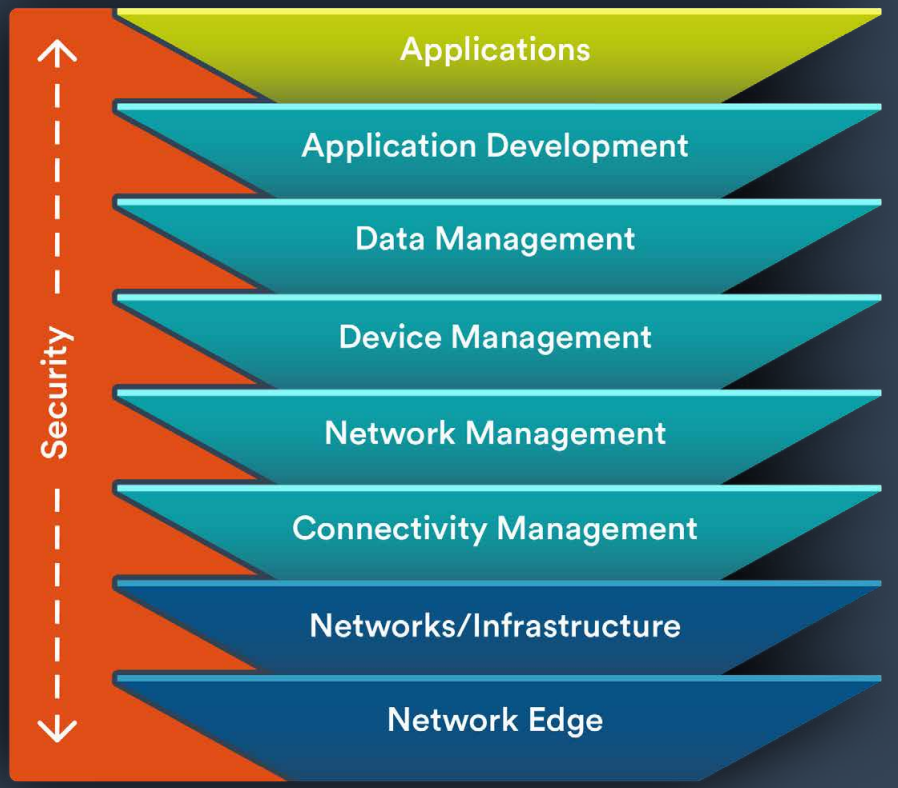
3. Data
Once generated, IoT data needs to be stored and processed – sometimes in real time – to create results. Workflow handling, visualisation, orchestration, and data analytics all form part of Data Management.

Additionally, an application needs to be developed or provided to make specific use of the data created.

In combination, these elements form a stack that sits above the sensors and network infrastructure, and beneath the application development and application – see **Figure 4.3**.

Since Device Management requires the connectivity to be in place before it can function for remote devices, it sits above Connectivity Management.

Figure 4.3 *Implementing security across the entirety of the IoT stack is vital to safeguard against cyberattacks*



A Holistic Approach to IoT Security

Different components of the IoT solution have unique vulnerabilities, and all must be secured to reduce the risk of a successful attack. In fact, the larger and more complex a solution, the more challenges it must overcome both to operate effectively and remain secure.

IoT solutions are frequently attacked at the various interfaces. For instance, between devices and gateways, gateways and the cloud, and the cloud to the application. In addition, the devices and gateways are vulnerable, with many lacking the power to run sophisticated security software. Meanwhile, services in the cloud can become compromised, if strong authorisation or encryption protocols are not implemented.

Given the varied attack surfaces within an IoT solution, high levels of security can only be realised if security mechanisms are an integral component of the overall architecture. In contrast, a fragmented approach often leads to gaps that attackers can exploit. This holistic approach is known as end-to-end security.

Security has moved on from being a specialist, technical subject and has become a significant concern for C-level management as well as system designers and solution providers. This means that this broader audience needs a better understanding of the basic security requirements, which include authorisation, availability, confidentiality, identification, integrity, non-repudiation, root of trust, and secured updates.

Unless security concerns are comprehensively addressed and trust enabled, then IoT's full potential will not be realised.

Vodafone's IoT Security Solutions

Vodafone's vision is a secure connected future for our customers and society.

Vodafone has 900 cyber experts worldwide and we certify our technology function and 11 markets to ISO27001 standards.

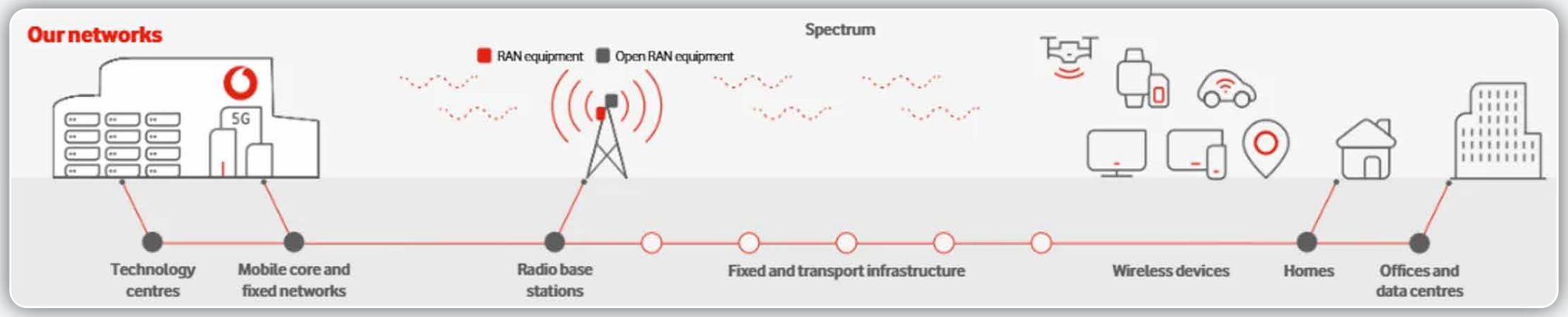
Vodafone Business IoT's security measures reflect a meticulous approach to addressing the diverse challenges of IoT ecosystems. These solutions focus on securing IoT deployments (device, connectivity and data/cloud) and integrate advanced technologies and methodologies, ensuring scalability, resilience, and regulatory compliance.

IoT Services

Vodafone's IoT solution has been built with privacy and security in mind.

- Vodafone operates a private core network for its IoT business customers, this is separate to the consumer mobile core network.
- We deploy 3GPP radio standards providing radio level encryption.
- Provide private APNs enabling a closed user group for devices.
- And offer encrypted and private backhaul solutions.
- We also carry customers' application layer security, enabling full end to end encryption.

End to end, what this means is that Vodafone's Internet of things (IoT) business offering isn't really the 'internet of things'. It can be considered as an 'intranet of things', dedicated to essential and critical business services.



Vodafone Business IoT's Managed Connectivity Platform
The IoT Platform, developed by Vodafone, is designed with security as a fundamental feature, incorporating safeguards at every level. This platform simplifies IoT adoption by unifying critical components:

SIM Management: Vodafone provides full management capabilities of the SIM estate using it's IoT Platform. The SIM state is always in a customer controlled operating state. Changes to the SIM state can be performed using the platform or API, to which users must be identified and authorised, using multi factor authentication. The use of Business Rules within the Platform also allows the customer to set notifications based on preferred SIM behaviour.

Connectivity: Integrates Vodafone's global IoT network footprint for seamless and reliable operations. This service is crucial for securely connecting many devices while maintaining data integrity.

Security: Deployed perimeter security controls include but are not limited to; Secure Data Centre's, Web Application Firewalls, Distributed Denial of Service protections and Intrusion Detection and Prevention products.

Operations: All security incidents or suspected incidents are reported to the Vodafone Security Operations Centre (SoC). Where a security incident occurs, we have a consistent incident management framework to manage our response and recovery. The focus of our incident responders is always fast risk mitigation and customer security.

Future
5G: As we deploy 5G core networks alongside our 5G radio networks, often described as 5G Standalone, we have updated our security standards to implement the latest 5G features in our core networks. We also test security in our radio networks using independent third-party testing companies.

AI: We take the responsible use of AI seriously and seek to balance the opportunities and risks associated with AI, and more recently generative AI ('Gen AI'). Teams from across the business are collaborating under the guidance of a global AI governance board which agrees policy, mitigates risks.

Quantum: We are preparing for a time when quantum computing is available at scale. We have developed a risk-based approach to mitigate the risks of existing cryptography, which could be more easily broken by a quantum computer. We are identifying potential quantum vulnerabilities, defining supplier requirements and developing the ability to update our cryptography when new threats emerge. Vodafone also co-chairs the telecommunications industry-wide task force on this issue.

Industry: We actively engage with stakeholders across industry, with regulators, standard-setting bodies and government.

Vodafone exemplifies how a company's strategic direction directly informs its technical solutions. Their proactive stance on IoT security reflects a balance between innovation and robust security measures. The company's recognition in the industry and its advanced technical initiatives ensure it remains a trusted partner for organisations seeking secure IoT solutions.

Security by Design

Security by Design is a proactive approach to cybersecurity that ensures security is embedded into systems, applications, and devices from the outset, rather than being added retroactively.

This methodology integrates security measures into the architecture, code, and operational processes of solutions, reducing vulnerabilities and mitigating risks before they become significant. It is particularly critical for IoT, where connected devices often operate in complex environments and are vulnerable to cyber threats.

Key Principles of Security by Design in IoT

Secure Authentication & Identity Management

Every IoT device should have unique, cryptographically secure credentials to prevent unauthorised access.

Data Encryption & Integrity

Sensitive data should be encrypted both at rest and in transit to prevent interception and tampering.

Least Privilege & Zero Trust Architecture

IoT devices should have the minimum level of access necessary to function, and connections should be continuously verified.

Regular Software Updates & Patch Management

Secure Over-The-Air (OTA) updates should be integrated into IoT devices to allow for timely security patches.

Threat Monitoring & Anomaly Detection

Built-in security monitoring should detect abnormal behaviour, such as unexpected traffic patterns, indicating potential compromises.

Why is Security by Design Essential for IoT?

IoT ecosystems present unique security challenges, including resource-constrained devices, long lifecycle management, and difficulty in patching vulnerabilities post-deployment. Many IoT devices lack built-in security mechanisms, making them prime targets for cyberattacks such as botnets, data interception, and unauthorised remote control. Security by Design mitigates these risks by ensuring that security is not an afterthought but an integral part of IoT development.

A proactive security approach means addressing risks before they become threats. For example, default passwords are a well-known weakness exploited in IoT attacks—Security by Design dictates that devices should enforce strong authentication mechanisms from the outset. Similarly, secure boot processes ensure that only trusted firmware is executed when a device powers on, preventing malicious modifications.

Aeris IoT Watchtower™

Aeris IoT Watchtower™ is the industry's first agentless cellular IoT security solution, designed to seamlessly integrate with both existing and new installations. It provides deep visibility and valuable insights that enhance operational efficiency, enforce regulatory compliance, and mitigate security risks to critical infrastructure and customer data.

Organisations can achieve regulatory compliance through monthly auditable risk assessment reports, continuously improve their compliance posture with ongoing monitoring, and implement self-service incident mitigation and response. It also enables enterprises and mobile operators to scale their IoT deployments securely, mitigating cybersecurity threats in an increasingly connected world.

How it works

Built on Aeris' IoT services platform, and the Aeris IoT Accelerator Platform™, a carrier-grade core network managing over 84 million IoT devices across 29 mobile operator partners worldwide, Aeris IoT Watchtower ensures seamless global connectivity with enterprise-grade security.

Aeris IoT Watchtower offers comprehensive protection for cellular IoT devices, traffic, and data. It identifies suspicious, malicious, and anomalous traffic, prevents the exploitation of known device vulnerabilities, blocks harmful traffic without disrupting device operations, and minimises the attack surface by enforcing device access only to an explicitly approved list of destinations.

Why Aeris IoT Watchtower?

Unlike traditional IoT security solutions that require complex systems integration, Aeris IoT Watchtower provides a fully managed security layer directly within the Aeris platform. As an Over-the-Top (OTT) solution, it delivers:

Security-First Approach

- AI-powered threat intelligence to detect and block malicious traffic.
- Zero-trust policies that minimise attack surfaces - without requiring device modifications.
- Real-time device behaviour monitoring to prevent vulnerability exploitation.

Regulatory Compliance at Scale

- Automated security enforcement for faster incident response.
- Auditable risk assessments to ensure compliance with global regulations, including NIS2 in Europe.

Streamlined IoT Operations

- Per-device traffic monitoring to minimise downtime.
- Real-time inventory visibility for simplified device management.
- Agentless, zero-touch deployment, reducing complexity and costs.

Aeris IoT Watchtower has already been deployed by leading enterprises across the US in fleet management, logistics, and medical devices, as well as through strategic partnerships in Europe. Aeris is also entering into new partnerships with OEMs and device manufacturers who wish to deliver more secure IoT solutions, bundling devices, connectivity, and security into one solution.

> ***"IoT is a powerful driver of a smart, sustainable future, but security risks and operational complexity have slowed its adoption. With Aeris IoT Watchtower, enterprises and mobile operators can expand their IoT programs with confidence, ensuring seamless global deployments while protecting their networks against emerging threats."***
>
> Aziz Benmalek, CEO, Aeris

Who Defines Security by Design?

Security by Design is defined and guided by governments, international standards organisations, industry bodies, and cybersecurity experts.

Key contributors include:

- National Institute of Standards and Technology (NIST) – Provides IoT security guidelines through frameworks such as SP 800-183 and SP 800-193.
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) – Develops global security standards, including ISO/IEC 27001 for information security and ISO/IEC 62443 for industrial cybersecurity.
- European Union Agency for Cybersecurity (ENISA) – Offers IoT security frameworks and mandates "Privacy by Design and by Default" under GDPR.
- UK National Cyber Security Centre (NCSC) – Provides best practices for IoT security, including device security certification schemes.
- Cybersecurity & Infrastructure Security Agency (CISA) (US) – Publishes secure software development frameworks and national cybersecurity directives.
- Industry-Specific Standards – Organisations such as the ioXt Alliance, GSMA, and leading tech companies (e.g., Microsoft, Google) contribute to secure-by-design guidelines.

Benefits of Security by Design in IoT

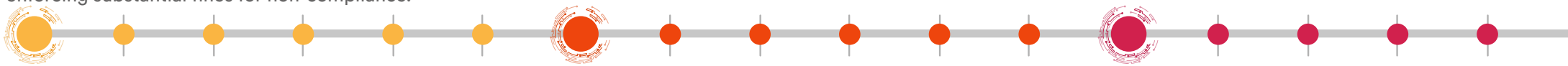
Implementing Security by Design in IoT results in stronger resilience against cyberattacks, lower long-term security costs, and better compliance with global security regulations. Furthermore, organisations that integrate security from the outset improve consumer trust, differentiate their products in the market, and reduce risks associated with vulnerabilities that are difficult to fix post-deployment.

Summary

As IoT adoption continues to grow, Security by Design is no longer optional - it is essential. By embedding security into every layer of the IoT ecosystem, from device firmware to cloud services, organisations can create a safer, more secure, and more reliable digital future. Aligning with established cybersecurity frameworks and best practices ensures compliance, mitigates risks, and fosters long-term resilience in the face of evolving cyber threats.

Regulatory Evolution: A Timeline of Cybersecurity Legislation

The EU and UK have led the global effort to regulate cybersecurity, responding to breaches and emerging threats with mandatory security frameworks. Their approach has influenced international markets, raising the security requirement for IoT and enforcing substantial fines for non-compliance.



Early 2010s: Network and Information Systems (NIS) Directive. The EU introduced the NIS Directive to establish basic cybersecurity standards for critical infrastructure operators including energy, transport, and healthcare sectors. It marked the first EU-wide cybersecurity law, responding to increasing cyberattacks on essential services.

2016: General Data Protection Regulation (GDPR). This landmark data protection law, driven by concerns over massive data breaches and privacy violations, introduced strict data protection rules, including significant fines for non-compliance (up to 4% of global annual turnover). GDPR set a new global standard for data protection.

2019: EU Cybersecurity Act. This act established the first EU-wide cybersecurity certification framework, ensuring that digital products and services meet minimum security requirements. Responding to the growing risks in IoT security by mandating third-party certification for critical infrastructure and high-risk technologies.

2021: NIS2 Directive Expansion. A response to high-profile ransomware attacks (such as Colonial Pipeline), NIS2 extended cybersecurity obligations to more sectors, including cloud computing, digital services, healthcare, manufacturing and supply chains. It introduced stricter incident reporting rules and penalties for non-compliance, reinforcing cybersecurity as a legal duty.

2022: Product Security and Telecommunications Infrastructure (PSTI) Act (UK). The UK's first consumer IoT security law, banning default passwords and enforcing mandatory vulnerability reporting and security updates.

2022: Cyber Resilience Act (CRA). The EU introduced the Cyber Resilience Act (CRA), a major IoT security regulation. It ensures that manufacturers follow Secure by Design principles, implement vulnerability management, and provide long-term security updates. Failure to comply can result in fines of up to €15 million or 2.5% of global annual turnover. This act raises the minimum IoT security requirement up to a security best practice, making the EU the leader in mandatory cybersecurity for connected devices.

2023: Digital Operational Resilience Act (DORA) (EU). Focuses on cybersecurity in financial services, ensuring banks, insurance companies, and payment processors meet strict resilience and incident reporting requirements.

2023: SEC Cybersecurity Disclosure Rules (US). Requires public companies to disclose cyber incidents and their cyber risk management strategies, increasing transparency.

2025: UK Cyber Security and Resilience Bill. The UK plans to introduce this bill to enhance national cybersecurity protections. While not as expansive as the EU CRA, it focuses on securing critical infrastructure and improving incident response capabilities.

IoT Security Solutions Overview

Digi International employs a comprehensive and multi-layered approach to IoT security, integrating advanced technologies and best practices to safeguard devices, networks, and data, while enabling customers to monitor their devices and respond to evolving threats through remote monitoring and over-the-air security update capabilities.

True Security: Integrated Capabilities and Proactive Management

Security today is not a "set it and forget it" task. Connected systems must not only integrate security measures but also provide the remote monitoring tools to detect intrusions and the remote management capabilities to thwart attacks and update firmware with the latest detection and mitigation tools.

Digi solutions integrate the Digi TrustFence® security framework, using multi-layered security measures, including:

- Secure Boot: Ensures that only authenticated firmware is executed during device startup, preventing unauthorised code execution.
- Protected Hardware and Network Ports: Mitigates the risk of unauthorised physical or network-based intrusions.
- Network Authentication: Provides data authentication and device identity management, ensuring devices are not shipped with default credentials.
- Secure Connections: Utilises the latest encryption protocols for data in motion and over-the-air (OTA) transmissions, maintaining data integrity across networks.

Additionally, Digi provides critical remote monitoring and management solutions for ongoing monitoring and control of deployed devices. These include:

Digi Remote Manager®: A cloud-based platform that provides remote device and network management, including security updates, configuration management, and real-time diagnostics. Digi Remote Manager allows for centralised oversight of IoT deployments, enabling rapid response to network issues and facilitating large-scale firmware updates to address security vulnerabilities.

Digi ConnectCore® Cloud Services: These are cloud and edge tools for rapid device deployment, and easy asset management of deployed devices built with Digi ConnectCore system-on-modules (SOMs).

Digi ConnectCore® Security Services: These are services and tools that enable customers to maintain the security of their devices built with Digi ConnectCore SOMs throughout the entire lifecycle of the product. These services enable the monitoring and analysis of security risks and vulnerabilities for a custom software bill of material (SBOM) and binary image running on Digi ConnectCore SOMs.

The combination of integrated device security measures and remote monitoring and management tools enables OEMs and organisations to launch IoT projects with confidence and keep their device security up to date over their entire lifecycle.

Why These Regulations Matter for IoT Security

One of the key drivers of cybersecurity investment is regulatory enforcement. Significant financial penalties for non-compliance effectively prevent insecure devices from entering the marketplace.

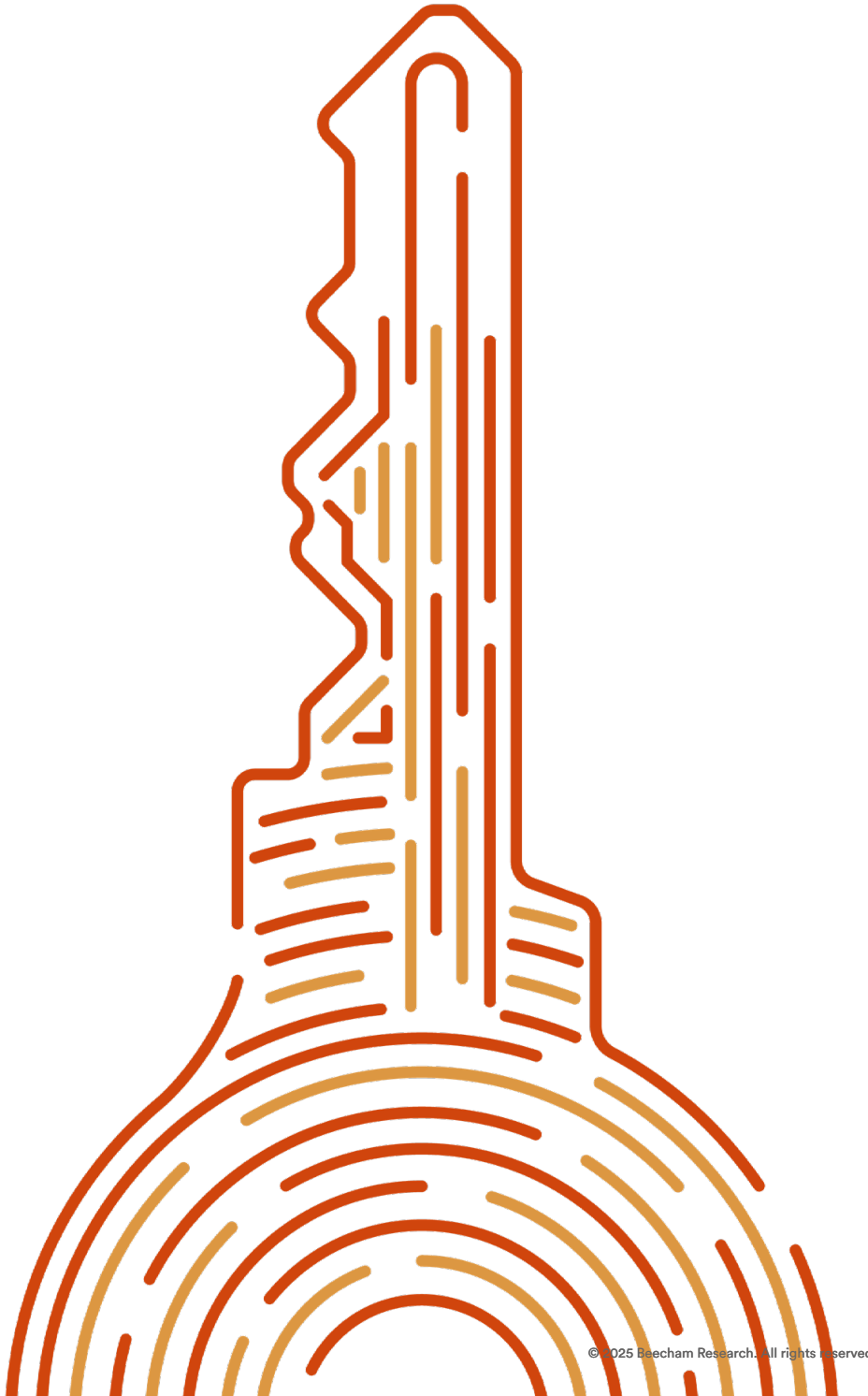
The EU's GDPR, NIS2, and CRA have set a new global benchmark. The US relies largely on voluntary compliance while the EU mandates strict enforcement with substantial financial penalties. As a result, companies operating in global IoT markets must meet EU security standards or risk exclusion. The UK, while outside the EU, continues to align cybersecurity laws with EU frameworks to maintain trade and security compatibility. These regulations justify and encourage investment in security to achieve compliance and maintain market access.

Diverging Approaches: US vs EU in Cybersecurity Standards

The US and EU take fundamentally different approaches to cybersecurity regulation. The US prioritises rapid innovation and first-to-market strategies, often relying on proprietary standards set by industry leaders rather than centralised government mandates. A good example of this is the US building sector, where companies develop their own safety and quality standards, which later coalesce into industry-wide practices.

Conversely, the EU takes a more structured approach, preferring to define standards before allowing products to enter the market. This pre-regulation model ensures that security is built into products from the outset, aligning with the Security by Design philosophy seen in GDPR, NIS2, and the Cyber Resilience Act.

While the US model fosters rapid innovation, it also means that security gaps may only be addressed after incidents occur. The EU model, while slower to market, ensures that security and compliance are embedded into the regulatory framework from the beginning.



Certification

Security certification is the process of assessing and verifying an organisation's or product's compliance with established security standards. This can apply to hardware, software, or processes.

Achieving security certification enhances trust – confirming to clients, partners, and regulators that security controls are in place. It also demonstrates a commitment to cybersecurity best practices. With IoT security increasingly becoming a priority across the value chain, certification can provide a competitive advantage in the marketplace.

The IoT landscape features numerous certification organisations, each addressing different aspects of security and compliance. Below are several examples. Further work is ongoing within the IMC/JTF to develop a certification programme for the security of IoT deployments.

IoT Device Security

PSA Certified
Ensures IoT devices (hardware and software) comply with security requirements. Promotes the adoption of best security practices, ensuring proactive threat management.

TÜV SÜD & TÜV Rheinland IoT Security Certification
Globally recognised bodies with IoT security certifications based on accepted cybersecurity frameworks. Covers penetration testing, firmware analysis, and device security assessments.

ioXt Alliance Certification
An industry-driven certification covering smart home devices, industrial IoT, and mobile applications. Assessment based on eight key principles, including secure device identity, verified software updates, and secure interfaces.

CTIA IoT Cybersecurity Certification
Provides industry-wide security benchmarks for IoT devices operating on wireless networks. Ensures compliance with best practices for device identity, authentication, and Over-The-Air (OTA) updates.

IoT System Security

IEC 62443 Certification
An internationally recognised set of standards for securing industrial automation and control systems (IACS). Covers secure product development, network segmentation, and incident response.

EISO/IEC 27001
An internationally recognised standard for information security management systems (ISMS). Provides a structured framework to manage sensitive company information securely.

Consumer IoT Devices

US Cyber Trust Mark
A government-backed voluntary labelling programme that encourages secure sourcing of IoT components. Helps consumers identify IoT devices that meet FCC cybersecurity requirements.

ETSI EN 303 645
A security standard for consumer IoT devices referenced by UK, EU, and international IoT security regulations. Covers no default passwords, vulnerability reporting, and secure data management.

IoT Practitioner Expertise

Certified IoT Security Practitioner (CIoTSP)
Globally recognised certification that validates the expertise of professionals responsible for securing IoT environments. Covers network security, data encryption, and access control for IoT systems.

ISACA IoT Fundamentals Certificate
A well-respected certification that provides professionals with the necessary knowledge to assess and manage risks associated with IoT technology. Focuses on governance, security controls, and external threats.

Balancing Innovation and Security Compliance

For companies operating in multiple regions, a hybrid approach is essential. Businesses must navigate the fast-paced innovation environment of the US while ensuring compliance with the EU's stricter security regulations. The global trend is shifting towards mandatory security requirements, meaning that businesses must future-proof their cybersecurity strategies to remain competitive in both markets.

Regulatory efforts raise the minimum cybersecurity standard worldwide, compelling manufacturers to adopt Security by Design principles. Countries such as Japan and Australia have mirrored EU regulations, while US federal agencies now enforce stricter security under Executive Order 14028 and the US SEC disclosure rules increase corporate responsibility for cybersecurity governance.

As cyber threats evolve, regulatory compliance is no longer just about avoiding fines, it's a competitive necessity in a market where security expectations are rising.

Key Takeaways for the IoT Industry

- Mandatory security standards are becoming the norm, with regulatory fines increasing compliance pressure.
- EU cybersecurity laws have global influence, requiring international companies to adopt strong Security by Design practices.
- Regulations now cover supply chains, cloud services, financial institutions, and consumer IoT, demanding continuous security monitoring and updates.

FINITE STATE

Finite State Platform

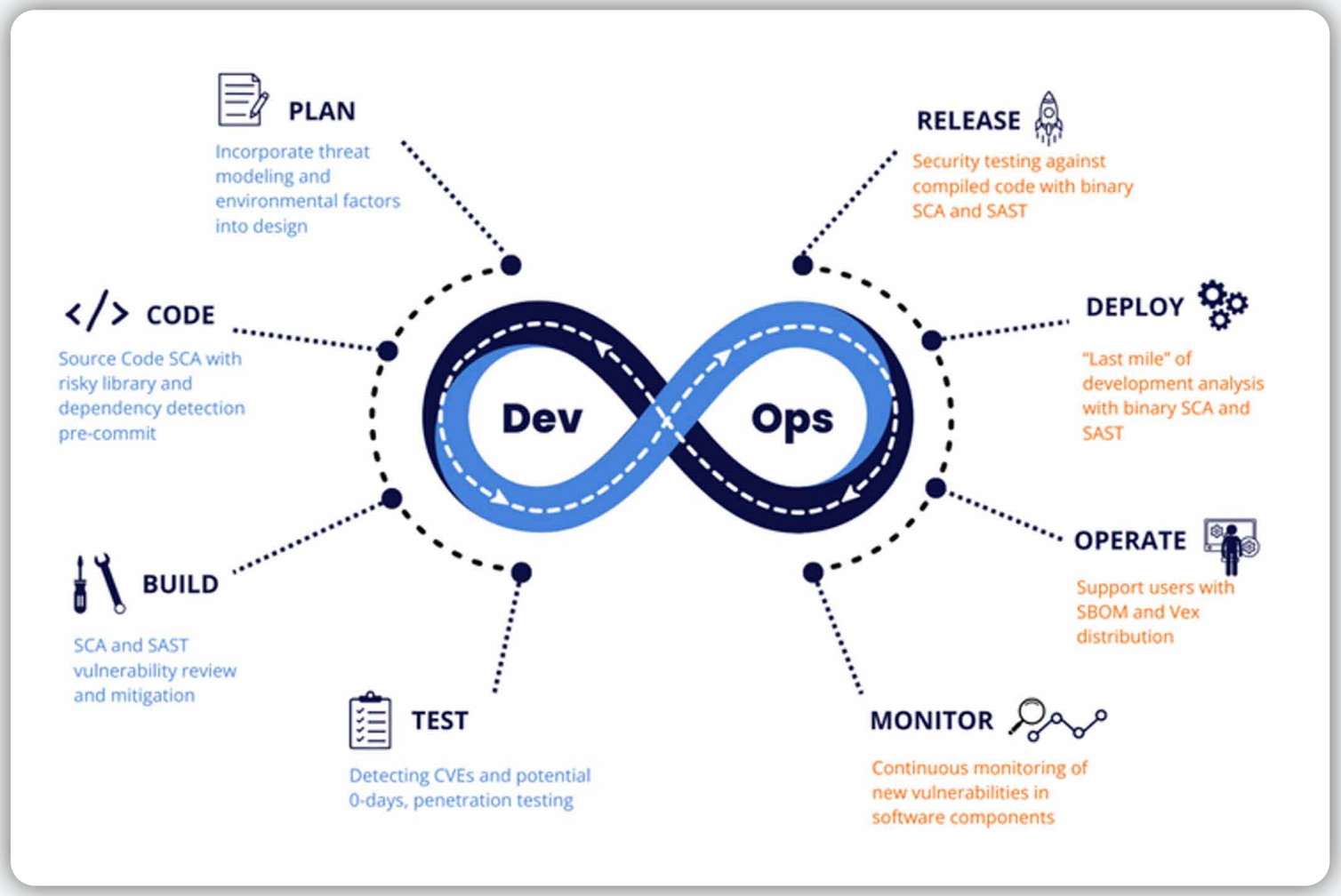
The Finite State Platform is an end-to-end solution for device and supply chain security, offering:

Advanced Firmware Analysis: The platform performs integrated binary and source code analysis to uncover vulnerabilities, hardcoded credentials, and misconfigurations in firmware and software.

Automated SBOM Generation: It creates accurate SBOMs to provide transparency into device software components, enabling effective vulnerability management.

Real-Time Vulnerability Monitoring: The platform continuously tracks vulnerabilities across supply chains, enriching data with insights from over 200 threat sources to ensure up-to-date risk assessments.

Remediation Guidance: The platform offers detailed mitigation strategies that integrate seamlessly with existing DevSecOps tools to facilitate faster resolution.



FINITE STATE

EU Cyber Resilience Act (CRA) Compliance

Finite State helps manufacturers comply with the EU CRA by providing:

- Secure by Design Guidance: Supports device makers in integrating security features into the development process, ensuring compliance with CRA's requirements.
- Lifecycle Security Management: Assists in maintaining device security through regular updates and vulnerability monitoring.
- Regulatory Documentation: Provides tools to generate and maintain technical documentation, including SBOMs, as mandated by the CRA.

Software Supply Chain Security

Finite State addresses software supply chain risks through:

- Third-Party Component Analysis: Examines all third-party and open-source components used in devices for potential vulnerabilities that could impact security.
- Industrial Supply Chain Insights: Offers solutions to secure operational technology (OT) devices and ICS systems, protecting critical infrastructure from cyberattacks.
- Emerging Technology Readiness: Evaluates the security implications of adopting new technologies in industrial supply chains, ensuring resilience against future threats.

Real-World Applications and Insights

Finite State actively shapes the IoT security conversation through:

- Thought Leadership: CEO Matt Wyckhouse regularly discusses global IoT security challenges, including regulatory trends and the future of secure device design, at leading industry events like CES 2025 and is a part of the IMC-GCF Joint Task Force on IoT Security.
- Industrial Cybersecurity Advocacy: The company emphasises the importance of securing industrial supply chains while integrating emerging technologies, ensuring comprehensive protection for operational technology environments.

Summary

Finite State continues to lead the IoT and software supply chain security sector, providing organisations with the tools and expertise needed to navigate complex regulatory requirements and secure their connected devices.

Through its advanced platform capabilities, strong focus on compliance, and commitment to Secure by Design principles, Finite State enables organisations to build and maintain secure device ecosystems in an increasingly interconnected world.

Looking Forward

(This section draws on a discussion with Matt Wyckhouse, CEO of Finite State)

As IoT continues to expand, so too will the complexity and scale of security threats. In the coming years, some of the most significant risks are likely to stem from increasingly sophisticated AI-related cyberattacks. AI poisoning – where attackers manipulate training data to create biased or flawed AI models – poses a particularly significant risk, particularly when the AI is integrated into critical infrastructure.

Additionally, the use of Large Language Models (LLMs) in enterprise operations will significantly expand the attack surface. When embedded into IoT devices, LLMs can introduce unintended API behaviours and unpredictable decision-making, making manual security processes redundant. This necessitates the adoption of AI-driven security measures, as an arms race between AI-powered attackers and AI-powered defenders becomes increasingly likely.

To enhance transparency in AI-driven IoT systems, organisations are encouraged to introduce AI Bills of Materials (AI BOMs). Similar to Software Bills of Materials (SBOMs), AI BOMs aim to improve visibility into AI models used in IoT devices, helping businesses assess potential biases and risks while strengthening overall security and compliance efforts.

Another growing concern is supply chain infiltration, whereby attackers compromise upstream providers to introduce vulnerabilities into widely deployed IoT systems. A key example is the SolarWinds attack, in which hackers inserted malicious code into a trusted software update. This update was deployed across thousands of organisations, including US government agencies and major corporations, allowing the malware to spread undetected. The hackers maintained undetected access for around 14 months before being detected and, although the purpose of the hack remains unknown, there were huge opportunities for data theft and espionage.

Similar tactics could be used against IoT manufacturers in the coming years, with adversaries embedding security flaws at the firmware level. Addressing these risks is particularly challenging, as IoT security incidents often require navigating through multiple supply chain layers to identify the true source of a vulnerability. This process is frequently delayed by companies at each stage deflecting responsibility. Increased transparency and collaboration are therefore essential to addressing this challenge.

Key Recommendations for Long-Term Security

For companies aiming to improve their IoT system resilience, the following activities are recommended:

Follow Security Best Practices: This involves building in Security by Design, avoiding hard coded credentials, and ensuring automated security testing is part of development workflows.

Deploy run-time security: Unlike traditional IT environments, IoT lacks real-time security monitoring tools, and the disparity is growing, increasing the risk of undetected threats. Investment in runtime security solutions is needed to provide better visibility and incident response.

Invest early in SBOMs and vulnerability management: Understanding third-party software components plays a major role in mitigating security and licensing risks. Compliance efforts should start early in product design cycles, as retrofitting can be more complicated and costly.

Implement automated and AI-driven vulnerability analysis: These models can scan vast amounts of data, automating vulnerability triage and reducing false-positives, to determine threats. With attacks evolving in sophistication, defence strategies must as well.

Recognise that security is a cultural shift: Achieving security maturity takes time, and it should be viewed as a continuous process rather than a one-time task. This requires an organisational buy-in, both in terms of implementing security into products and training teams to prioritise security along with functionality.

Interview with Matt Wyckhouse

CEO of Finite State, on IoT Security & Compliance

With global regulations like the EU Cyber Resilience Act (CRA) shaping the IoT security landscape, how is Finite State positioning itself to help manufacturers stay ahead of compliance requirements while maintaining innovation?

The CRA has significantly raised cybersecurity standards for IoT manufacturers, making security best practices the regulatory baseline requirement. Companies must now meet stricter security demands, which includes SBOMs, supply chain transparency, security testing, and vulnerability management. Non-compliance carries severe consequences, with penalties of up to €15 million or 2.5% of global turnover - whichever is higher - and restrictions on selling products in the EU.

Finite State helps manufacturers comply with these requirements by automating SBOM generation, continuously monitoring for threats, and managing vulnerabilities to prevent exploitable weaknesses in IoT devices. Our tools seamlessly integrate into development workflows, making security implementation accessible without overhauling existing processes. This also ensures security throughout the product lifecycle. Furthermore, we offer a specialised focus on embedded and IoT devices, unlike many security solutions that primarily target cloud applications. This includes comprehensive security validation services across automotive, industrial control systems, and healthcare products - from development through to deployment.

While large companies like Google and Apple already have established security best practices, many smaller manufacturers urgently need to introduce or elevate theirs to meet the new regulatory demands – and our platform can help them do this.

Given the increasing complexity of supply chains in IoT and operational technology, what are the biggest challenges Finite State sees in securing third-party components, and how does your platform address these risks?

The fragmented nature of IoT supply chains presents unique security challenges. Unlike traditional software environments, where patches can be applied independently, IoT devices rely on firmware and software from multiple third-party suppliers, including chipset manufacturers. If a vulnerability is found, multiple suppliers – often several layers deep – must be involved in fixing it. This can lead to delays and slow response times.

Another issue is regulatory expectations versus real-world supply chain constraints. The CRA mandates that vulnerabilities must be reported within 72 hours and remediated swiftly. However, multi-tiered supply chains complicate compliance. Security patches can have unintended functionality consequences (such as altering power consumption), affecting device performance and negatively impacting operations.

Finite State tackles these challenges by automating third-party software security assessments, continuously monitoring emerging threats, and delivering actionable remediation guidance integrated with existing development workflows. Greater transparency and collaboration between suppliers is crucial for improving security across the IoT ecosystem.

FINITE STATE

As IoT devices become more integrated into critical industries like healthcare and energy, what do you see as the key technological advancements needed to ensure long-term security in these environments?

The use of AI-driven solutions will be essential for enhancing the accuracy and speed of threat detection. Traditional security tools generate extensive vulnerability lists, which require time-consuming manual triage. In contrast, AI can rapidly assess large amounts of data, prioritise real threats, and reduce the frequency of false positives. Additionally, AI-driven reachability analysis helps determine whether a vulnerability is truly exploitable within a system. This massively eases the burden on security teams, allowing them to focus on addressing real threats.

Another key area for development is runtime security. Although real-time monitoring is well-established within traditional IT environments, IoT solutions often lack continuous security oversight, leaving them vulnerable to undetected threats. As edge computing becomes mainstream, IoT devices will increasingly handle sensitive data and control physical infrastructure, further amplifying security risks. Implementing runtime security enhances resilience by providing continuous, real-time visibility and protection. An automated incident response also helps maintain system integrity by isolating the threat and minimising potential damage. This enables critical operations to continue running with minimal disruption.

Finite State champions the 'Secure by Design' philosophy. Why is it important for companies to integrate security early in the development process, and what challenges do they face in doing so?

Many companies make the mistake of treating security as an afterthought, adding it late in development rather than embedding it from the start. Integrating security early helps prevent vulnerabilities and ensures compliance with regulations like the CRA. It also helps companies avoid common issues like hardcoded credentials and insecure coding practices. Adopting SBOMs is also important to vulnerability management, as understanding third-party software dependencies will help companies mitigate risks.

However, security is not just a technical challenge – it requires a cultural shift. Manufacturers must prioritise security alongside product functionality, ensuring that security testing is built into development workflows from the start. This takes time, particularly for companies that have not previously prioritised cybersecurity. Nevertheless, the urgency of CRA compliance regulations provides a strong motivator for companies to make these investments sooner rather than later.

Conclusion

IoT security remains an ongoing challenge, with expanding attack surfaces and growing regulatory scrutiny. Companies must shift from a reactive to a proactive security model, investing in continuous monitoring, AI-driven automation, and network segmentation. Solutions providing real-time threat detection and mitigation can help businesses secure their IoT infrastructure before they face financial and operational disruptions.

Although AI presents a significant threat, the future of IoT security lies in AI and automation. As attack complexity increases, machine learning tools will play a crucial role in identifying and stopping cyber threats before they cause damage. Businesses that fail to implement strong IoT security measures today risk facing catastrophic consequences tomorrow.

Sponsors' IoT Offerings:

This section presents profiles of our sponsors and highlights how they are addressing the challenges of IoT Security. For more details, please contact them directly.

aeris®

WEBSITE

For more than three decades, Aeris® has been a trusted cellular IoT leader enabling the biggest IoT programs and opportunities across Automotive, Utilities and Energy, Fleet Management and Logistics, Medical Devices, and Manufacturing.

Our IoT technology expertise serves a global ecosystem of 7,000 enterprise customers, 30 mobile network operator partners, and more than 80 million IoT devices across the world. Aeris powers today's connected smart world with innovative technologies and borderless connectivity that simplify management, enhance security, optimise performance, and drive growth.

To learn how Aeris IoT Accelerator Platform™, Aeris IoT Watchtower™ and Aeris Mobility Suite™ can secure and supercharge your critical IoT programs, visit aeris.com and follow us on LinkedIn.

Driving Global IoT Expansion for Mobile Operators

Aeris is enabling international IoT expansion through partnerships with major mobile operators worldwide. As the largest orchestrator of eSIMs for IoT, Aeris' platform extends global reach for its carrier partners while ensuring seamless, secure connectivity for enterprise customers.

As global IoT adoption accelerates, Aeris and its expanding network of mobile carrier partners are at the forefront of delivering secure, scalable, and seamless IoT connectivity.

Connecting Partners Worldwide

The world is more connected than ever. But connectivity alone isn't enough. Businesses need security, intelligence, and seamless integration to truly thrive. This is where Aeris comes in. Aeris provides the IoT software platform that simplifies

aeris

WEBSITE

global IoT deployments – securely, intelligently, and seamlessly – empowering our partners to deliver greater value to their customers.

Aeris is also entering into new partnerships with OEMs and device manufacturers who wish to deliver more secure IoT solutions, bundling devices, connectivity and security into one solution.

Powering the Future of Secure, Scalable IoT

Through recent acquisitions, Aeris continues to transform and grow, driven by innovations in:

- AI-powered IoT security.
- Advanced analytics.
- eSIM-based global network portability.
- Expanded 5G Standalone (5GSA) coverage.

Where the future is: Aeris IoT Acuity™

Aeris IoT Acuity is a bundled solution that combines Aeris' IoT connectivity services with Aeris IoT Watchtower's security capabilities. It offers enterprises an integrated approach to secure IoT deployments and block suspicious activity before it escalates.

Capable of monitoring and reacting to threats in real-time, it delivers the highest level of protection for IoT devices. With "flip the switch" activation, adoption is easy and agentless.

Acuity deliverables

- **Real-time asset inventory** of devices using the cellular network.
- **Real-time security insight** into device state and behaviour.
- **Continuous monitoring** for indicators of compromise, with associated alerts and alarms.
- **Monthly Security Assessment Report.**

Key Business Benefits

- **Compliance** with regulations through auditable reports.
- **Risk identification** through real-time awareness of possible malicious behaviour.
- **Faster time to resolution** of issues with real-time deep forensics.
- **Cost control** through awareness of traffic spikes and data flows to specific IP endpoints.

Now, more than ever, companies must shift from a reactive to a proactive security model to mitigate and manage threats.

Why ISO 27001 Matters to Aeris

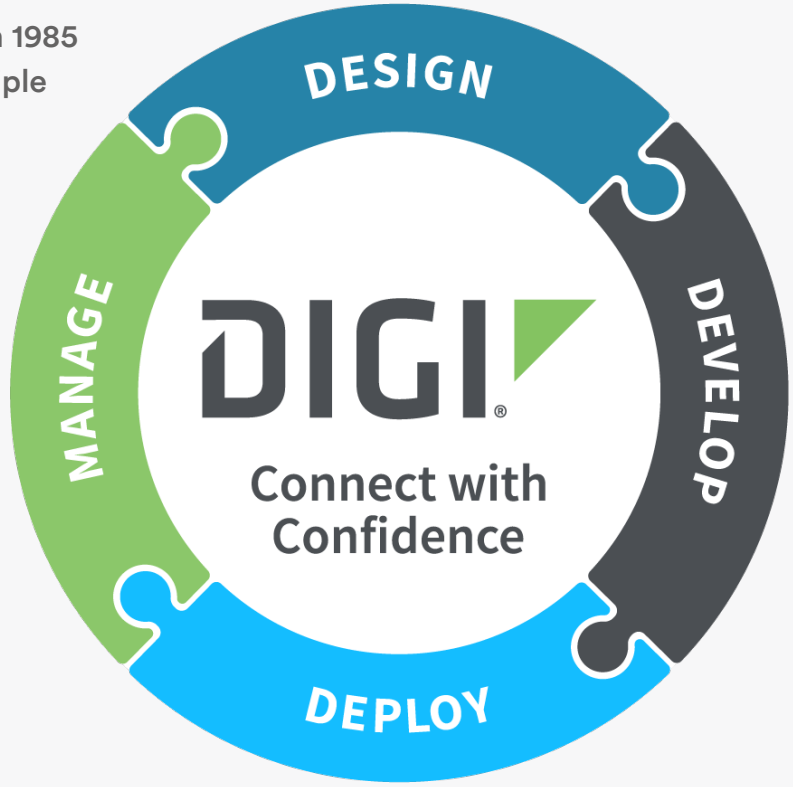
ISO 27001 certification demonstrates that Aeris prioritises data security for cellular IoT at every level. By adhering to this rigorous standard, we can help ensure:

- **Proactive Risk Management**: Identifying and addressing vulnerabilities before they escalate.
- **Regulatory Compliance**: Meeting and exceeding industry-specific legal requirements.
- **Customer Confidence**: Providing peace of mind that sensitive information is handled securely.
- **Operational Excellence**: Seamlessly integrating security into daily processes.

At Aeris, data security is more than compliance - it's a cornerstone of our business. By partnering with an ISO 27001-certified company, you can trust in secure, reliable solutions designed for today's connected world.

WEBSITE

Digi International, a global leader in IoT connectivity and solutions, was founded in 1985 and is headquartered in Hopkins, Minnesota, USA. With a presence spanning multiple industries, Digi has established itself as a global leader in secure IoT solutions.



Digi's portfolio includes a comprehensive suite of embedded systems for OEMs, as well as cellular connectivity and infrastructure management solutions for organisations needing secure, reliable high-performance networking. These complete solutions integrate remote monitoring and management to enhance the reliability, scalability, and security of IoT deployments.

Additionally, Digi offers wireless design services for OEMs seeking engineering, certification, enhanced embedded security and go-to-market support, as well as professional services to help organisations and municipalities plan, configure, and deploy secure device networks.

Digi's solutions are trusted across multiple sectors including healthcare, industrial automation, energy, transportation, emergency response, and smart cities, and these solutions are designed to work securely and reliably in the most demanding mission-critical applications — including in harsh environments.

Digi's Commitment to Security

Digi's approach to security is designed to ensure that organisations integrating or deploying Digi's solutions can ensure their devices are secure over their entire lifecycle. A robust framework of advanced technology, as well as remote monitoring and control, enables organisations to safeguard devices, networks, and data and keep remote devices up-to-date as security threats evolve.

Security by Design with Digi TrustFence

Digi solutions are built with security as a foundational principle. The Digi TrustFence® Security by Design approach means devices have integrated safeguards to help protect against unauthorised access, data breaches, and other vulnerabilities, providing customers with a strong foundation for securing their IoT systems.

Key features of Digi TrustFence include:

Secure Boot Processes: Digi devices are equipped with secure boot technology, ensuring that only authenticated and trusted firmware is loaded during startup. This prevents malicious software or unauthorised code from being executed on the device.

Data Encryption: Digi employs robust encryption protocols to protect data, ensuring the confidentiality and integrity of sensitive information. By leveraging advanced encryption standards, Digi safeguards data from interception and tampering.

Authentication Mechanisms: Digi products feature strong authentication protocols, such as digital certificates and two-factor authentication, to verify the identity of users and devices accessing the network or system.

WEBSITE

Secure Remote Management with Digi Remote Manager
Digi Remote Manager® (Digi RM) is a cornerstone of Digi International's cybersecurity strategy, offering a cloud-based platform for monitoring, managing, and securing IoT devices and networks. Digi RM provides organisations with centralised visibility and control over their connected assets, ensuring that they can rapidly and proactively identify and address potential security risks.

Key security features of Digi Remote Manager® include:

- Secure Device Provisioning: Devices connected through Digi RM are securely onboarded, reducing the risk of unauthorised access during deployment.
- Over-the-Air (OTA) Updates: Digi RM enables remote firmware updates, to ensure devices can be kept up to date with the latest security patches and software enhancements.
- Event Logging and Auditing: Digi RM provides detailed logging and auditing capabilities, allowing organisations to track device activity and detect suspicious behaviour. This visibility supports compliance with regulatory requirements and strengthens incident response.
- Real-Time Alerts: Digi RM continuously monitors device health and performance, generating real-time alerts for potential security issues, such as unauthorised access attempts or abnormal behaviour.

Additional Value-Added Services
OEMs today are facing new regulations requiring ongoing security management of the devices they bring to market. To support these requirements, Digi offers a full suite of developer tools as well as security services and cloud management services designed to ensure they can integrate ongoing remote management into their device designs.

Proactive Threat Mitigation
Digi International takes a proactive approach to cybersecurity by continuously enhancing its security measures. These measures include:

- Regular Security Assessments: Digi conducts rigorous testing, including penetration testing and vulnerability assessments, to identify and address potential security weaknesses in its products.
- Compliance with Industry Standards: Digi's products and services support compliance with leading industry standards and regulations, such as GDPR, PCI DSS, and ISO 27001 to ensure customers can confidently deploy Digi solutions in regulated environments.
- Collaborating with Technology Providers: Digi collaborates with cybersecurity organisations and technology developers to leverage best practices and emerging capabilities in IoT device security.

Digi's Security Office

Cybersecurity is constantly evolving, with new threats emerging regularly. To address these challenges, Digi actively monitors trends in IoT cybersecurity, while also adopting cutting-edge technologies such as AI-driven threat detection. Digi also interacts with security researchers and regularly communicates new vulnerabilities that may impact customers, as well as threat mitigations, via the company's security site.

Conclusion

Digi International's approach to cybersecurity and device security is to provide highly robust, reliable, and secure IoT solutions. Through security-focused design, advanced management tools, proactive threat mitigation, and customer education, Digi empowers organisations to confidently deploy connected systems while protecting their assets, data, and networks.

FINITE STATE

WEBSITE

Founded in 2017 and headquartered in Columbus, Ohio, Finite State is a leading cybersecurity company specialising in securing connected devices and their supply chains. The company provides cutting-edge solutions for securing Internet of Things (IoT) devices, industrial control systems (ICS), and embedded systems across their entire lifecycle. Through advanced firmware analysis, comprehensive Software Bill of Materials (SBOM) management, and regulatory compliance expertise, Finite State empowers organisations to secure their products against emerging threats.

Finite State serves a diverse client base including IoT manufacturers, industrial enterprises, and global organisations navigating complex regulatory requirements such as the European Union's Cyber Resilience Act (CRA). Their solutions deliver end-to-end security capabilities that address software supply chain risks, enhance product security, and ensure compliance with evolving global standards.

Strategic Approach to IoT Security

Finite State combines cutting-edge technology and deep industry expertise to address the most pressing security challenges in the IoT ecosystem through three key elements:

Comprehensive Platform Capabilities: The platform's automated vulnerability detection system identifies potential security risks early in the development cycle, significantly reducing the risk of exploitation. Its advanced SBOM management provides unprecedented visibility into software components, enabling organisations to maintain a detailed inventory of their device components. The platform's lifecycle security management ensures continuous protection from initial design through post-deployment operations.

Secure by Design Principles: Finite State enables manufacturers to integrate security measures throughout the development lifecycle, ensuring alignment with international regulatory requirements like the EU CRA. This proactive approach prevents security breaches rather than merely responding to them, reducing both costs and disruption. By addressing security during development, organisations can avoid the significant challenges of post-deployment remediation while ensuring compliance with regulatory requirements and avoiding penalties and market access restrictions.

Focus on Software Supply Chain Security: The platform provides deep visibility into device firmware and third-party components, ensuring the integrity and security of industrial supply chains. This comprehensive approach enables organisations to identify and mitigate risks across their entire device ecosystem.

WEBSITE

Vodafone is a leading European and African telecoms company - providing mobile and fixed services to over 330 million customers in 15 countries and partners with mobile networks in 47 more. In Africa, its financial technology businesses serve almost 83 million customers across seven countries – managing more transactions than any other provider.

Beyond traditional telecommunication services, Vodafone is a global leader in IoT and has one of the world's largest managed IoT service platforms. Leveraging its extensive network infrastructure and innovative technologies, Vodafone's IoT business (Vodafone Business IoT) has developed a reputation for delivering scalable and secure IoT solutions and is a trusted partner for organisations seeking secure IoT solutions. Its offerings cater to a diverse range of industries, including healthcare, automotive, energy, and critical national infrastructure..

Strategic Approach to IoT Security

Vodafone adopts a proactive, multi-faceted approach to IoT security that aligns with its mission to promote trust and innovation. Key elements of this approach include:

- Comprehensive Security Frameworks: Vodafone integrates end-to-end encryption, robust authentication protocols, and network segmentation into its IoT solutions to protect data and devices from breaches.
- Regulatory Advocacy: Through white papers and partnerships, Vodafone actively shapes IoT security regulations, ensuring alignment with global standards and fostering cross-sector collaboration.
- Customer-Centric Solutions: Vodafone tailors its security offerings to meet the unique needs of specific industries, ensuring that businesses can leverage IoT technologies with confidence.

We follow a security and privacy design process for all components, the platform, the SIMs, connectivity and branded devices. Vodafone Business IoT's cloud-based connectivity platform has been designed purely for IoT, is a proved scalable solution for business who want to operate globally and has an easy-to-use interface with comprehensive features that enable IoT devices to be managed easily. The platform simplifies IoT device management by giving businesses visibility and control over their IoT SIMs and enables businesses to manage and monitor their connected assets through a single portal. Furthermore, it feeds businesses insights and analytics – helping businesses to reduce operational complexity, automate processes and reduce operating costs.

Trust in our network and critical-industry expertise

For more than 30 years, we've been the service provider for businesses across critical industries like healthcare, government, emergency services, automotive and utilities have turned to. They trust us to deliver, not just their fixed and mobile communications, but to also host their applications in our cloud and run their IoT business.

For the 10th year in a row, Vodafone has been recognised as a Leader in the 2024 Gartner® Magic QuadrantTM for Managed IoT Connectivity Services, showcasing its ability to execute its vision and innovate within the IoT security landscape.

Beecham Research is a leading technology market research, analysis and consulting firm established in 1991. We have specialised in the development of the rapidly-growing Connected Devices market, often referred to as M2M and IoT, worldwide since 2001. We are internationally recognised as thought leaders in this market and have deep knowledge of the market dynamics at every level in the value chain.

Our clients include component and hardware vendors, major network/connectivity suppliers, system integrators, application developers, distributors and enterprise users in both B2B and B2C markets. We are experts in M2M/IoT services and platforms and also in IoT solution security, where we have extensive technical knowledge.

Shaping the IoT future