Is your IoT product security ready for mandatory compliance by April 2024?

Ignitec

We are an award winning product design consultancy, we design connected products and instruments for pioneering technology companies.

Is your IoT product security ready for mandatory compliance by April 2024?

Reading time 14 mins

Key Points

- There are approximately 17 billion IoT (Internet of Things) devices worldwide.
- 73% of IoT device manufacturers do not comply with security rules, and only 1-5 manufacturers in the UK have IoT security protocols embedded into their products.
- The total cost of cybercrime to the UK economy is approximately £27 billion annually.
- The Product Security and Telecommunications Infrastructure (PSTI) Act comes into effect on 29 April 2024 and will require manufacturers of UK consumer connectable products (‘smart’ devices) to comply with mandatory obligations.
- To meet the minimum security requirements, businesses that produce or supply IoT-connected devices must give clear information on the support period their products provide, ensure that no product uses default passwords, and outline clear procedures on how to report security vulnerabilities.
- Companies with IoT products that do not comply with the new law will be subject to government action, including enforcement notices, monetary penalties (up to £20,000 for every day a business fails to meet its obligations), and forfeiture.
- Ignitec’s Cyber Essentials certification highlights our commitment to safeguarding our clients and the products we develop for them from potential threats. Call us for a quote on how we can do the same for you.

Safeguard your products against cyber threats to keep users safe and meet mandatory legal requirements. Call us for a quote!

Get in touch

Ben Mazur

Managing Director

Last updated Apr 9, 2024

I hope you enjoy reading this post.
If you would like us to develop your next product for you, click here

The Internet of Things (IoT) is one of the fastest-growing technologies and has seen exponential growth in recent years. There are approximately 17 billion IoT devices worldwide – from fridges and cars to umbrellas and pet feeders – all connected to the Internet, continuously collecting data and empowering users. But with great power comes great responsibility, especially regarding IoT product security: How is user information and privacy kept safe? Who is responsible for software vulnerabilities that cause data breaches? How are security risks managed? How can products be more cyber-secure and resilient?

The UK's Product Security and Telecommunications Infrastructure Act (PSTIA) comes into effect on 29 April 2024 and aims to resolve these concerns. The new law will require manufacturers of UK consumer connectable products ('smart' devices) to comply with the mandatory obligations set out in the Act and ensure that products meet the relevant minimum security requirements:

1. Precise information on the support period must be provided at the Point of Sale.
2. Each product must have a unique password, i.e. no easily guessable or default passwords.
3. The business's vulnerability disclosure policy (VDP) must outline precise procedures for reporting security vulnerabilities. Download the free Vulnerability Disclosure Toolkit from the National Cyber Security Centre.

Ignitec is Cyber Essentials Certified, highlighting our commitment to treating our client's data and the products we develop with extreme care. If you're developing a smart device and unsure whether your IoT product security meets mandated compliance regulations, call us. Our team of multidisciplinary experts, from software developers to electronics engineers, will help you ensure that your products don't simply meet minimum security standards – they'll exceed them!

Related services

Product design

Software Development

Intrinsically Safe

Why is mandatory security necessary for connected devices?

There's an average of 9 connectable consumer products (e.g. baby monitors, smartphones and TVs) in each UK household. However, the level of security these products have is very poor: Only 1 in 5 manufacturers have cybersecurity protocols embedded into their products, but consumers overwhelmingly assume that these products are safe. In addition, many IoT products are produced with a default password that's either commonly used (e.g. password, or 0000) or easily obtainable online – a vulnerability regularly exploited by hackers.

73% of IoT device manufacturers do not comply with security rules, highlighting a failure to prioritise consumer safety. The total cost of cybercrime to the UK economy is approximately £27 billion

annually. UK data breaches and cyber attacks in recent years with the most wide-reaching impact have included:

- In July 2023, the popular BBC programme Countryfile inadvertently broadcast usernames and passwords for secure IT systems on national TV.
- The Sellafield nuclear site in Cumbria, Western Europe's most hazardous nuclear site, was allegedly hacked by groups with links to China and Russia. The site is currently under investigation and prosecution for security offences.
- In October 2023, Russian hackers claimed responsibility for crashing the Royal Family's website and taking down the Manchester Airport website, while someone unknown staged a cyber attack against Volex, the manufacturer of critical power and transmission products.
- A whopping 188 cybercrimes in 2022 were reported. They included incidents where the data of thousands of British school children were posted online after the schools refused to pay a ransom, the source code for Grand Theft Auto (a popular video game worldwide) was leaked online, and Funky Pigeon (online greeting card company owned by WH Smith) was forced to take some of its online ordering systems offline.

What types of cybercrimes do IoT products need protection from?

Cybercrime and the security it requires fall into different categories, necessitating comprehensive and robust IoT product security protocols. The most common include:

1. Ransomware: A type of malware that encrypts files on a victim's device, rendering the files inaccessible and demanding payment (a ransom) from the victim in exchange for decrypting them. For example, a smart home security system infected with malware could lock the homeowner out of their system, preventing them from accessing security camera feeds or controlling door locks until they pay the ransom.

2. Data breach: This occurs when unauthorised individuals gain access to sensitive or confidential information stored by an organisation, potentially exposing personal or financial data.
For example, a data breach in an IoT-enabled healthcare device, such as a wearable fitness tracker, could result in unauthorised access to users' GPS location, compromising privacy and security.

3. Denial of service (DoS): Disrupts the normal functioning of a system, network, or service by overwhelming it with a flood of illegitimate traffic, rendering it unavailable to legitimate users.
For example, an attack targeting the cloud-based servers that control a smart irrigation system floods the servers with a massive volume of illegitimate traffic, rendering them unable to process legitimate requests from the IoT devices in the field. This could result in crops suffering from inadequate watering, leading to reduced yields or even crop failure and a significant financial impact on farmers.

4. Phishing: A cybercrime tactic in which attackers attempt to trick individuals into divulging sensitive information, such as login credentials or financial details, by impersonating trustworthy entities in electronic communications.
For example, an email phishing campaign targeting users of a popular smart home device may trick recipients into clicking on a malicious link or downloading a fake software update, leading to the compromise of their device credentials or personal information.

5. Hacking: The unauthorised access to computer systems, networks, or devices that exploit vulnerabilities for malicious purposes, such as identity theft, social engineering, stealing data, disrupting operations, or gaining control.
For example, a hacker gaining unauthorised access to a connected car's infotainment system could manipulate the vehicle's controls, such as braking or steering, putting the safety of passengers at risk.

For users of IoT devices with poor or non-existent security protocols, falling victim to any of these crimes could result in more than a loss of privacy: bodily harm and financial loss are real threats that can't be taken lightly. At the same time, the responsibility for IoT product safety lies with the companies developing them to ensure risks are identified, assessed, and managed throughout the product development cycle.

For companies prioritising consumer safety, developing products in-house is one of the best ways to ensure that IoT product security is as robust and comprehensive as possible. At Ignitec, we can monitor and conduct rigorous testing and vulnerability assessments at every stage of product development – ensuring that the IoT device you put on the market is less likely to cause harm to users and your business integrity. Call us for a confidential consultation, and let's get you PSTIA ready!

Tips on improving your IoT product security protocols

Businesses that produce or supply IoT-connected devices (including manufacturers, importers, and distributors in the supply chain) need to ensure they are updated on the new PSTI law (read the factsheet here) and have taken the appropriate steps to ensure compliance with the three central mandates listed above.

These security requirements are based on the UK's Code of Practice for Consumer IoT security, the leading global standard for consumer IoT security ETSI EN 303 645, and on advice from the UK's technical authority for cyber threats, the National Cyber Security Centre.

If you're an IoT product developer, you should put mechanisms in place to ensure that product security keeps pace with external developments – especially the tools that attackers use – which will evolve.

- Perform security-focused testing and verification regularly, informed by the threats to which your product is expected to be exposed.

- Studying user interactions with a product can help you learn if it’s not being used as expected, how this impacts security, and where to implement changes for better security outcomes.
- Good usage monitoring (see product design thinking) can help you actively identify attempts to bypass or subvert security measures.
- Maintaining and regularly reviewing a log of all product defects will help identify security implications and prioritise remediation.
- Developing and following a clear roadmap for security improvements will help ensure the product continues to offer the best possible protection as it is developed over time.
- Product updates that address security issues should be made available promptly to minimise the window of opportunity for an attacker.

Not everything that affects the security of your product is under your control – hardware components may become hard to source, support for software may end, and third-party suppliers may suffer a security incident. Thus, the new IoT product security law also seeks to ensure that other parties in the supply chain play a role in preventing insecure consumer products from being sold to UK consumers and businesses.

- Maintain a register of all components supplied by a third party, including free or open source ones, and routinely check for vulnerabilities that affect them.
- Third-party suppliers should only be allowed to retain the information they need and access the systems that are necessary for them to fulfil their role. Accurate records of third-party information holdings can help you assess the impact if they are compromised.
- Business continuity plans should be updated regularly, and you should ensure you follow the measures defined in them. For example, creating secure offsite and offline backups will help with disaster recovery, but only if they are updated frequently, and the restoration process is tested regularly.
- Plan for toolchain elements becoming obsolete, which may result in loss of functionality or, if cloud-based, complete unexpected withdrawal.

UK penalties for non-compliant IoT products

The regulations outlined in the Product Security and Telecommunications Infrastructure Act are comprehensive, and the accompanying enforcement framework is equally robust. It includes civil and criminal sanctions to communicate the sincerity with which the UK government will approach product security. Companies with IoT products that are not compliant with the new law will be subject to

government action, which can include:

- **Enforcement Notices:** Compliance notices, Stop notices and Recall notices.
- **Monetary Penalties:** the greater of £10 million or 4% of the company's qualifying worldwide revenue, or up to GBP20,000 (USD24,800) for every day that a business fails to meet its obligations.
- **Forfeiture:** of stock in the possession or control of any manufacturer, importer or distributor of the products or an authorised representative.

A final word on security protocols for IoT products

As IoT technology becomes increasingly integrated into critical systems such as healthcare, policing, transportation, energy, and personal environments, the potential consequences of security breaches escalate. Ensuring robust security measures is paramount to protect against cyber threats, safeguard privacy, maintain trust in the technology, and prevent potentially catastrophic consequences of compromised devices on individuals and society.

Call us if the technical or software requirements needed to get your products compliant are challenging. We'll be able to get you up to speed quickly and cost-efficiently – confident that your customers are as protected against cybercrime as possible.

Suggested reading

Building resilient business solutions: Creating cyber-secure products to safeguard against vulnerabilities

Ignitec is now Cyber Essentials certified

Consumer consent, privacy and ethics of wearables

FAQ’s

Why is IoT product security important?

IoT product security is vital to protect against cyber threats that could compromise sensitive data and disrupt essential functions of interconnected devices. Without robust security measures, IoT devices are vulnerable to hacking, putting individuals and critical infrastructure at risk.

How can IoT product security be improved?

Improving IoT product security involves implementing encryption protocols, regular software updates, and strong authentication mechanisms to prevent unauthorised access and safeguard data integrity. Additionally, promoting cybersecurity awareness and collaboration between stakeholders can help address evolving threats effectively.

What are the common vulnerabilities in IoT product security?

Common vulnerabilities in IoT product security include weak authentication mechanisms, insecure network connections, and lack of timely software updates. Addressing these vulnerabilities requires comprehensive security protocols, regular vulnerability assessments, and adherence to industry best practices.

How does legislation impact IoT product security in the UK?

Legislation in the UK aims to enhance IoT product security by establishing minimum security requirements for manufacturers and promoting transparency in IoT device security features. Regulatory frameworks encourage compliance with security standards and accountability for ensuring consumer safety in the rapidly evolving IoT landscape.

What role do software updates play in IoT product security?

Software updates are essential for addressing security vulnerabilities and patching known exploits in IoT devices. Regular updates ensure that devices remain resilient against emerging threats and maintain optimal security posture, reducing the risk of cyberattacks and protecting user data.

Which industries are most affected by IoT product security concerns?

Industries such as healthcare, finance, transportation, and energy are particularly susceptible to IoT product security concerns due to the critical nature of their operations and the vast amounts of sensitive data involved. Ensuring robust security measures in these sectors is essential to mitigate risks and maintain public trust.

Who is responsible for ensuring IoT product security?

Responsibility for ensuring IoT product security lies with manufacturers, developers, regulators, and users alike. Manufacturers must design devices with security in mind, developers must implement secure coding practices, regulators must establish and enforce security standards, and users must follow best practices for device usage and maintenance.

What are the potential consequences of IoT product security breaches?

IoT product security breaches can lead to unauthorised access to sensitive data, disruption of essential services, financial losses, and damage to reputation. Additionally, compromised IoT devices may be exploited for further cyber attacks, posing significant risks to individuals and society as a whole.

How can consumers protect themselves from IoT product security risks?

Consumers can protect themselves from IoT product security risks by ensuring they purchase devices from reputable manufacturers, regularly updating firmware and software, using strong passwords,

and avoiding connecting devices to insecure networks. Additionally, being vigilant for signs of suspicious activity and promptly reporting any security concerns can help mitigate risks.

What are the key components of IoT product security?

Key components of IoT product security include encryption for data protection, authentication mechanisms for access control, secure communication protocols, and regular security updates. Additionally, implementing measures for threat detection, incident response, and user education are essential for comprehensive security posture.

When should IoT product security measures be implemented?

IoT product security measures should be implemented throughout the entire product lifecycle, from design and development to deployment and maintenance. Proactive security measures should be integrated at the earliest stages of product development to ensure robust protection against potential threats.

How can businesses ensure compliance with IoT product security regulations?

Businesses can ensure compliance with IoT product security regulations by staying informed about relevant legislation, conducting risk assessments to identify security gaps, and implementing appropriate security controls and measures. Additionally, regular audits and compliance checks can help businesses maintain adherence to regulatory requirements.

What are the best practices for securing IoT product networks?

Best practices for securing IoT product networks include segmenting networks to isolate IoT devices from critical systems, implementing strong access controls and authentication mechanisms, monitoring network traffic for anomalies, and regularly updating firmware and software to patch vulnerabilities.

Why is encryption important for IoT product security?

Encryption is essential for IoT product security as it ensures that data transmitted between devices and servers remains confidential and cannot be intercepted by unauthorised parties. By encrypting data at rest and in transit, IoT devices can protect sensitive information from being compromised in the event of a security breach.

What role does user awareness play in IoT product security?

User awareness plays a crucial role in IoT product security as informed users are better equipped to recognise and mitigate security risks. Educating users about best practices for device usage, password management, and identifying phishing attempts can help prevent security breaches and protect against cyber threats.

How can IoT product security be integrated into business risk management strategies?

IoT product security can be integrated into business risk management strategies by conducting thorough risk assessments to identify potential security threats and vulnerabilities associated with IoT deployments. Implementing robust security controls, incident response plans, and regular security audits can help mitigate risks and protect business interests.

What are the challenges of implementing IoT product security measures?

Challenges of implementing IoT product security measures include ensuring interoperability across diverse devices and platforms, managing the complexity of interconnected ecosystems, and addressing resource constraints in terms of budget and expertise. Additionally, balancing security requirements with usability and functionality can present challenges for developers and manufacturers.

How can IoT product security contribute to building consumer

trust?

IoT product security can contribute to building consumer trust by demonstrating a commitment to protecting user privacy, securing sensitive data, and maintaining the integrity of devices and services. Transparent communication about security measures, compliance with industry standards, and responsiveness to security incidents can foster trust and confidence in IoT products and brands.

What are the emerging trends in IoT product security?

Emerging trends in IoT product security include the adoption of artificial intelligence and machine learning for threat detection and mitigation, the use of blockchain technology for secure data transactions, and the implementation of device identity management solutions. Additionally, regulations and standards for IoT security are evolving to address new challenges and mitigate emerging threats effectively.

Why IoT in asset tracking is essential for your business growth and development

Last updated Jul 24, 2024 | BUSINESS SERVICES, INSIGHTS, IoT, PRODUCT DESIGN

IoT in asset tracking helps businesses save costs, improve efficiency, and grow flexibly and sustainably.

read more