Cyber Cert Labs

How does the UK PSTI compare with EU CRA?

Updated for 2025

October 2025

How does the PSTI compare with the CRA?

1.0 Introduction

Year on year cyber-attacks are on the rise and digital products with low security are prime targets for attack. A high-profile example from this year is Badbox 2.0, a large scale malware operation that has infected more than 1 million android TV devices.[1,2] The Badbox 2.0 malware is installed during the manufacturing process in many cases due to low supply chain security. The infected devices become part of a botnet which is used to launch thousands of attacks and further infect other devices. The UK government and the European Union have outlined that cybersecurity for digital products is an area where increased regulation is needed. The UK Product Security and Telecommunications Act (PSTI) and the EU Cyber Resilience Act (CRA) aim to address low security standards for digital products and ensure users better understand the security features of devices they own.

2.0 An overview of PSTI

On 29th April 2024 the PSTI came into force, the goal of this legislation is to implement baseline security standards for consumer smart devices. The act applies to manufacturers, importers and distributors of relevant consumer smart device products. Manufacturers of consumer products must ensure their products meet the minimum security standards to set out in the act.

The security requirements are set out in Schedule 1 of the regulation.[3] These actions must be implemented for products that are in scope to address basic security and eliminate potential security vulnerabilities. The basic cybersecurity standards outlined by the law include:

1. Manufacturers must not supply devices with default passwords enabled.
2. Manufacturers must provide a point of contact that security issues can be reported to.
3. The manufacturer must state the minimum length of time the device will receive security updates for.

The law applies to any 'consumer smart device' that connects either to the internet, or to a home network (for example by Wi-Fi). This may include:

- smart speakers, smart TVs and streaming devices
- smart doorbells, baby monitors and security cameras
- cellular tablets, smartphones and games consoles
- wearable fitness trackers (including smart watches)
- smart domestic appliances (such as light bulbs, plugs, thermostats, fridges and washing machines)

The regulation is based on a self-declaration, a digital or physical a statement of compliance accompanying the product. There is a presumption of conformity for products that already align to the ETSI 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements.[4] There is no third-party assessment required in terms of testing for

compliance.
The Office for Product Safety and Standards (OPSS) is responsible for enforcing the PSTI Act. OPSS is part of the Department for Business and Trade and already enforces the UK's existing product safety regulations. The OPSS can use different mechanisms such as Compliance Notices, Stop Notices or Recall Notices to enforce the PSTI Act. Failure to comply with an enforcement notice is an offence liable on summary conviction to a fine.

3.0 An overview of CRA

The Cyber Resilience Act (CRA) entered into force 10th December 2024 which marked the start of a 36 month transition period.[5] From 11th September 2026 manufacturers must comply with the vulnerability reporting obligations as outlined in the CRA and from 11th December 2027 the CRA will apply in full for manufacturers of products with digital elements.

The CRA provides a baseline cybersecurity standard for products with digital elements within the European Union. The CRA aims to address two main problems identified in products with digital elements:

1. Products with digital elements are being manufactured with low levels of cybersecurity. This is resulting in widespread vulnerabilities and a lack of security patching to address these vulnerabilities.
2. Users of products with digital elements have an insufficient understanding of the product security. As well as a lack of information that would allow them to make informed decisions on choosing products with appropriate cybersecurity features and using them in a secure manner.

The CRA applies broadly to all software and/or hardware products that have a connection with other devices and/or networks that will be made available on the EU market. The products are separated into different categories based on the security risk they pose. The majority (90%) of products will fall into the default category which is the lowest risk category. Products that fall into this category can complete a self-assessment to demonstrate conformity with the CRA. Products in the higher risk important and critical category will need to undergo more stringent assessment to demonstrate conformity.

Annex I of the CRA outlines basic security requirements and vulnerability reporting requirements the manufacturer must implement in their product to conform with the CRA. These requirements include:

1. Ensuring the product with digital element is designed, developed and produced with an appropriate level of cybersecurity based on the risks.
2. Carry out a cybersecurity risk assessment.
3. Implement security by design and by default.
4. Ensure the product is made available on the market without known exploitable vulnerabilities.
5. Ensure freely accessible security updates for the lifespan of the product.

6. Protect the access, confidentiality and integrity of stored, transmitted or otherwise processed data.
7. Limit data processing to what is adequate and relevant.
8. Reporting obligations to CSIRT and ENISA when a cybersecurity incident occurs.
9. Documentation requirements for users and for market surveillance authorities.
10. Provide a coordinated vulnerability disclosure policy.

4.0 Mapping between the PSTI and the CRA

Topic	PSTI	CRA
Reach	UK Only Manufacturers in scope are mainly outside the UK so impact is minimal in terms of UK businesses.	EU – 27 member states Manufacturers in scope are widespread due to the wide scope of the CRA in EU member states and third countries.
Enforcement	Office for Product Safety and Standards	Market Surveillance Authorities will be appointed.
Non-Compliance Penalties	The Act specifies the maximum penalty that may be imposed in relation to non-compliance. a) £10 million, or b) 4% of qualifying worldwide revenue for most recent accounting period The Act specifies the maximum penalty that may be imposed in relation to non-compliance that continues beyond the penalty deadline – the daily penalty element – as £20,000 per day. Under certain circumstances Stop Notices and Recall notices can be served.	Failure to comply with CRA essential requirements, vulnerability or incident reporting could incur penalties of: Administrative fines up to €15 Million or 2.5% of global turnover whichever is higher. Failure to comply with other obligations could incur penalties of: Administrative fines up to €10 Million or 2% of global turnover whichever is higher. Supplying misleading information to enforcement bodies or national CSIRT teams could incur penalties of: Administrative fines up to €5 Million or 1% of global turnover whichever is higher. Under certain circumstances EU

		authorities can require the recall or withdrawal of non-compliant products.
Products in Scope	Limited to **Consumer connectable products i**.e. IoT, smart products	Products with digital elements with a connection to other devices or networks. This includes hardware, hardware with software, remote processing, standalone software, IoT, operational technology and other devices for consumers and business purposes. Websites, Cloud solutions and SaaS that do not support remote processing are not in scope. Open-source software that is developed outside of commercial activity is not in scope. Some products that already are covered by regulations such as medical devices, automotive are not covered by the CRA.
Assessment Type	**Self-declaration** through a statement of compliance	Depending on the criticality of the product category. It is estimated that 90% of products will fall into the non-critical default category which will require self-assessment, important products Class 1 and Class 2 will require third party assessment and use harmonised standards approach and critical product will require a formal conformity assessment under common criteria (EUCC).
Mapping to other standards	**ETSI 303 645** Consumer IoT baseline of requirements and **ISO/IEC 29147** vulnerability disclosure standard	Given the wide reach of the products in scope approximately **41 harmonised standards** have been identified by ENISA as having overlap with some or most of the security requirements in the CRA.
Security Requirements Coverage	Limited to the top 3 principles in the Code of Practice for Consumer IoT Security.	Comprehensive with security requirements based on 1. Security by design

	1. No default passwords 2. Vulnerability disclosure 3. Software updates.	2. Risk assessment. 3. Vulnerability management 4. Vulnerability Disclosure 5. Security patching
Reporting Obligations	Manufacturers to supply **one point of contact for reporting security issues**. An acknowledgement receipt and status updates until resolution must be sent to the reporter.	Manufacturers must **report within 24 hours to their Nation CSIRT**, if a actively exploited vulnerability is found. This is followed by a **more detailed report within 72 hours**. A detailed vulnerability description and mitigation **report is requirement within 14 days**.
Documentation Requirements	The manufacturer, importer and distributor must ultimately ensure that the **Statement of Compliance (SoC) accompanies the product** and meets the necessary legal requirements in the PSTI Act 2022 and PSTI Regulations 2023.	To affix the **CE mark** you must follow the **detailed documentation requirements** in the Cyber Resilience Act in ANNEX II and ANNEX V in addition to producing the EU declaration of conformity in ANNEX IV.

5.0 Conclusion

In comparison with the CRA, the PSTI is less robust and far reaching. This may be a deliberate phased approach for the UK to improve product security in stages. The requirements in the Cyber Resilience Act are comprehensive and in depth and will affect thousands of businesses in the EU and beyond. However, the PSTI will affect mostly non-UK IoT device manufacturers selling their products in the UK. This much smaller scope will have a benefit for supply chains and consumers, but it is not the big bang that the CRA promises to be. We should expect more phases to come to cover more products including software and more comprehensive security requirements. This may be done in line with the CRA so that UK manufacturers can align to both the CRA and PSTI simultaneously. There may be a possibility to agree on Mutual Recognition Agreement (MRA) with the UK if the PSTI and CRA closely align in the future.

6.0 References

1. HUMAN Security. (2025). BADBOX 2.0 - HUMAN Security. [online] Available at: https://www.humansecurity.com/company/satori-threat-intelligence/badbox-2-0/.
2. National Cyber Security Centre. (2025) Android BadBox 2.0 Malware. [online] Available at: https://www.ncsc.gov.ie/pdfs/AndroidBadbox2-0.pdf.
3. Legislation.gov.uk. (2023). The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023. [online] Available at: https://www.legislation.gov.uk/uksi/2023/1007/schedules/made.

4. Standard, E. (n.d.). CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements. [online] Available at: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.
5. Europa.eu. (2024). Regulation - 2024/2847 - EN - EUR-Lex. [online] Available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.