UK PSTI EXECUTIVE BRIEF

An IoTSF Regulatory Watch group publication

IoT Security Foundation – Executive Brief

Product Security and Telecommunications Infrastructure Act 2022 (PSTI)			
Official Source	https://www.legislation.gov.uk/ukpga/2022/46/ https://www.legislation.gov.uk/uksi/2023/1007/contents/made		
Geographic Region	United Kingdom	affected industries	cross-industry
Scope	Internet-connectable consumer products and products capable of connecting to such products		
In brief	1. Passwords must be unique and not easily guessable 2. Manufacturers must provide information on how to report security issues 3. Manufacturers must provide information on minimum security update periods 4. Provide statement of compliance		
Consequences	Up to GBP 10m or 4% of global annual revenue		
Baseline Standard	ETSI EN 303 645		

Digital security is a challenge for every organization stretching from traditional information technology systems and GDPR, through to trade secrets, operational capability, brand impact, and the protection of customer experience.

Unfortunately, many organizations remain unaware of major product security legislation due to be enforced from April 2024, and the critical impact this will have on the executive management.

The Product Security & Telecoms Infrastructure (PSTI) Bill passed royal assent in 2022, and was adopted into legal statute on 28th April 2023, with a 12-month grace period. This new bill imposes responsibilities on the manufacturers, importers and vendors regarding the cybersecurity of the connectable products they supply. It provides for sanctions similar to those surrounding GDPR, with the responsible directors, managers, et cetera also being held liable. As such, it is critical that the executive team ensures compliance with this new legislation, **by the deadline of 29th April 2024**.

It should be noted that the PSTI bill will be followed by broader regulations due for introduction in jurisdictions around the globe over the coming years. These include the EU Cyber Resilience Act and US Cyber Security Labelling Program for Smart Devices which will add to the basic requirements introduced in UK PSTI.

The PSTI legislation is critically important to Chief Executives, Chief Operating Officers, Chief Legal Officers, Company Secretaries, and all divisional General Managers where their business lines deliver consumer-oriented connected electronic or mechanical systems. This includes products from coffee machines and connected kettles, through to lightbulbs, heating and ventilation systems, toys, and connected white goods, encompassing any connected product that a general-public consumer may encounter. It is the responsibility of the end product manufacturer/distributor/importer to ensure that their product complies with the legislation.

The legislation prescribes a range of critical penalties, which could pose an existential threat to many organizations. These include a fine of up to £10 Million or 4% of global revenues (whichever is larger), which is comparable with those available under the GDPR. Plus, sanctions may be applied to executives, not just the company. It covers all products sold, made available or used to deliver a service in the UK which are covered by the legislation, where manufactured locally or delivered via a global supply chain **after the 29th of April 2024 deadline.**

Recommendations

- It is strongly recommended that executives treat the PSTI legislation with the same care they took for GDPR and ensure they understand the impact it will have on their businesses and plan accordingly. Ignorance is no defence in this legislation.

- All executive teams are recommended to review PSTI legislation adherence at least once a quarter, to ensure affected business groups are observing the legislation or have a clear remediation program.

- All executive teams should nominate an officer responsible for corporate compliance to the legislation. This may be the Company Secretary, the Chief Legal Officer, or the Chief Operations Officer, however it is recommended that this is a separate delegate to the person responsible for the implementation to enable challenging conversations.

- Where practicable, it is suggested that organizations reach out to a third-party product security company with the appropriate expertise and resources to ensure compliance with the legislation, and their duty of care for end users. Ultimately, however, it is the responsibility of the manufacturer to ensure compliance.

- Organizations are advised to ensure any business lines which are developing connected devices for end consumers have adopted and followed a rigorous cybersecurity framework, such as the free of charge IoT Security Assurance Framework [1] from the IoT Security Foundation. This task-oriented framework ensures that an organization can demonstrate a cyber-aware development process, highlighting any critical shortcomings, and providing reassurance. An accompanying tool is also available exclusively for members which supports compliance procedures.

Legislative Requirements

The IoT Security Foundation, and many global organizations including the European Telecoms Standards Institute (ETSI) and US National Institute of Standards and Technology (NIST), have collaborated to develop 13 provisions for consumer cyber-aware product development. To reduce the initial impact on industry, the UK government has limited legislation to three initial requirements, which are covered within the current (2023-1007) PSTI legislation.

Password Compliance

Legislation requires that every device should have a unique password or user-defined password. This is to ensure that passwords are not easily guessable or accessible by an unauthorised entity. Guidance on best practice can be found in the IoTSF Assurance Framework, NIST 800-63b and other guidance documents.

Remediation & Updates

It is accepted that software will contain bugs, even with the utmost care from developers. At the Personal Computer level we are used to manufacturers issuing regular patches to rectify vulnerabilities via a security update. This however is not often the case for IoT products.

Where flaws provide an opportunity for an attacker to take control of a device, it must be possible to reset the device, regain control, and/or ultimately remediate the software with a patch. If a product is capable of implementing security updates the manufacturer should make them available via a product support service. The legislation requires the manufacturer to state the time period for which security updates will be provided; this period can be extended but never reduced. This time period has to be clearly communicated to consumers.

Businesses will need to manage their legal responsibilities across the life cycle of the product. Corporate considerations include the need to develop, deliver and maintain update infrastructure for the stated period. Regular review of the business impact and readiness to support security updates should be conducted for all relevant products. This may be for some time after initial manufacture ceases, with the potential for software releases years after a traditional product life cycle has completed.

Vulnerability Reporting

Where vulnerabilities in a product are discovered, it is important that an organisation has in place a means to handle them effectively, for example by implementing a PSIRT (Product Security Incident Response Team) process. This is to help mitigate the effects handling a vulnerability imposes on an organisation; the earlier a vulnerability is resolved the cheaper it is to do so.

The legislation requires that manufacturers provide at least one point of contact to whom product vulnerabilities should be reported. This allows security researchers and other 3rd parties to inform them of issues found with a given product. The organisation must then

acknowledge receipt of the report and provide progress updates until the reported issue is resolved.

To aid the process of vulnerability management and remediation it is recommended vendors create a Software Bill of Materials (SBOM) for every product so they can quickly identify any vulnerabilities which may be reported to them or in the public databases. For background on this requirement the IoT Security Foundation has several documents discussing vulnerability disclosure and software bill of materials at [1].

Conclusion

UK PSTI legislation is already active with enforcement from 29 April 2024, with the potential for significant impact on organizations selling into the UK market. Not only are large penalties available, but substantial brand damage is likely to result from failure to comply. Further legislation, following on from this foundation, is imminent in other global jurisdictions. It is critical that you become aware of this threat and take immediate action to protect stakeholders. The act can hold the company and individual officers of the company responsible. We therefore strongly recommend that product security is made the responsibility of a senior executive with the authority to ensure necessary actions are performed.

The IoTSF will continue to monitor developments related to the UK legislation, which in some cases, might provide further clarity on how some of the provisions can be interpreted and implemented.

[1] IoT Security Assurance Framework and other relevant guidance documents are available at https://iotsecurityfoundation.org/best-practice-guidelines/