FMBusinessDaily

With the PSTI Act 2022 coming into force in April 2024, DHF is urging its members to ‘be prepared!’

2 years ago

The Product Security and Telecommunications Infrastructure Act 2022, which received Royal Assent on 6th December 2022, will come into force on 29th April 2024. British companies have had a period of a year to implement the necessary changes put forth in the legislation. Tamworth-based Trade Association, DHF, is keen to assert its full support for the changes and is encouraging its members to ‘take action’ ahead of the deadline.

The Act applies to all consumer IoT products, including but not limited to connected safety-relevant products such as door locks, connected home automation and alarm systems, Internet of Things base stations and hubs to which multiple devices connect, smart home assistants, smartphones, smoke detectors, connected cameras, connected fridges, washers, freezers, and coffee machines.

“The Product Security and Telecommunications Infrastructure Act 2022 requires manufacturers, importers, and distributors to ensure that minimum security requirements are met in relation to consumer connectable products,” explains DHF’s General Manager & Secretary, Michael Skelding. “It also provides a rigorous regulatory framework that can adapt and remain effective in the face of rapid technological advancement.”

Many IoT products continue to be produced with a default password either commonly used or easily obtainable online which can leave consumers open to cyber criminals. The PSTI legislation covers three main security features: Consumer IoT devices will not be allowed to have universal default passwords making it easier for consumers to configure their devices securely to prevent them being hacked;

Consumer IoT devices will have to have a vulnerability disclosure policy so manufacturers must have a plan for dealing with weaknesses in software meaning it is more likely that such weaknesses will be addressed properly; in addition, Consumer IoT devices will need to disclose how long they will receive software updates meaning that software updates are created and released to maintain the security of the device throughout its lifespan.

“As per the regulatory framework within the law, the government can take action against companies that are not compliant by the deadline date of 29th April 2024,” continues Michael. “Such action could include enforcement notices, compliance notices, stop notices, recall notices, and monetary penalties, for example, the greater of £10 million or 4% of the company’s qualifying worldwide revenue.

“Secured by Design’s (SBD) Secure Connected Device accreditation scheme, developed in consultation with the Department for Science, Innovation and Technology (DSIT), enables companies to get their products appropriately assessed against all 13 provisions of the EN 303 645 standard, a requirement that goes beyond the Government’s legislation, so companies can not only demonstrate their compliance with the legislation, but help protect themselves, their products and customers.”

The SBD Secure Connected Device IoT Assessment identifies the level of risk associated with an IoT device and its ecosystem, providing recommendations on the appropriate certification routes with one of the SBD approved certification bodies. Once third-party testing and independent certification for a product has been achieved, the company can apply to become SBD members, with the product receiving the SBD’s Secure Connected Device accreditation, a unique and recognisable accreditation that will highlight products as having achieved the relevant IoT standards and certification.

According to a recent survey conducted by Smart Home Week, 57% of British homes now contain a smart device, and while 34% of us believe smart lock technology is convenient and efficient, the survey also discovered that 63% of consumers are concerned about the security risks.

Home Office statistics show, 72% of burglaries occur when intruders enter through front doors. Smart locks offer enhanced security measures, for example, fingerprint readers or voice assistant integration, and there is also an added layer of control provided by these devices which enable homeowners to monitor their property remotely.

“We continue to stress to our members the importance of ensuring that all IoT products have the right level of security in place to protect consumers against cyber-crime,” concludes Michael. “Compliance with the Product Security and Telecommunications Infrastructure Act 2022 will demonstrate a company’s willingness to embrace state-of-the-art technology whilst prioritising the safety of its customers.”