Fire Protection Association®

RISCAuthority

S35 Internet of Things – Connected Security Devices and Systems

RISK INSIGHT, STRATEGY AND CONTROL AUTHORITY

REDUCING INSURABLE RISK THROUGH RESEARCH, ADVICE AND BEST PRACTICE

Version 1 Published 2023

Cover image: Getty/MF3d

IMPORTANT NOTICE

This document has been developed through RISCAuthority and published by the Fire Protection Association (FPA) and endorsed by the British Automatic Fire Sprinkler Association (BAFSA). RISCAuthority membership comprises a group of UK insurers that actively support a number of expert working groups developing and promulgating best practice for the protection of people, property, business and the environment from loss due to fire and other risks. The technical expertise for this document has been provided by the technical directorate of the FPA, external consultants, and experts from the insurance industry who together form the various RISCAuthority Working Groups. Although produced with insurer input it does not (and is not intended to) represent a pan-insurer perspective. Individual insurance companies will have their own requirements which may be different from or not reflected in the content of this document.

FPA has made extensive efforts to check the accuracy of the information and advice contained in this document and it is believed to be accurate at the time of printing. However, FPA makes no guarantee, representation or warranty (express or implied) as to the accuracy or completeness of any information or advice contained in this document. All advice and recommendations are presented in good faith on the basis of information, knowledge and technology as at the date of publication of this document.

Without prejudice to the generality of the foregoing, FPA makes no guarantee, representation or warranty (express or implied) that this document considers all systems, equipment and procedures or state of the art technologies current at the date of this document.

Use of, or reliance upon, this document, or any part of its content, is voluntary and is at the user's own risk. Anyone considering using or implementing any recommendation or advice within this document should rely on his or her own personal judgement or, as appropriate, seek the advice of a competent professional and rely on that professional's advice. Nothing in this document replaces or excludes (nor is intended to replace or exclude), entirely or in part, mandatory and/or legal requirements howsoever arising (including without prejudice to the generality of the foregoing any such requirements for maintaining health and safety in the workplace).

Except to the extent that it is unlawful to exclude any liability, FPA accepts no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from the publication of this document or any part of it, or any use of, or reliance placed on, the content of this document or any part of it.

Contents

1 Introduction

The Internet of Things (IoT) is bringing many opportunities to positively impact our lives and businesses. With this, however, come the risks associated with connected devices, particularly those around security, privacy, and safety, that can make it difficult for manufacturers and suppliers to build trust in new products and services. To overcome this, suppliers of IoT connected devices and systems must be able to demonstrate security, safety, functionality, interoperability (will it work with other devices), and durability.

Security systems with connections to internal and external networks have increased exposure to malicious attack. To ensure effective security from cyber attack, hacking, and other forms of interference, requires these types of systems to meet suitable certifications and be appropriately designed, installed, commissioned, and maintained. This is a fast-developing subject area and those involved with internet-connected security devices and systems are advised to keep up to date with developments in technology.

2 Scope

This guide is intended to inform insurance risk consultants, underwriters and other insurance professionals and security equipment users, of the main hazards, controls, guidelines, and accreditations that make up the landscape for internet-connected security devices.

In scope:

- **Premises:** domestic and small/medium commercial
- **Equipment:** any internet connected security device such as intruder alarms, video surveillance systems (VSS), smart locks, smart doors, smart key-boxes

This guidance focuses on end point devices such as smart locks, but it should be borne in mind that, for complete protection, other elements such as user and site IT networks/ routers must also be secure.

3 Background to IoT connected security devices and what can go wrong

For internet connected building security devices (equipment in scope listed above), vulnerabilities can be introduced by factors such as deficient design and poor supply chain management, e.g. security updates not implemented on installed systems or system components.

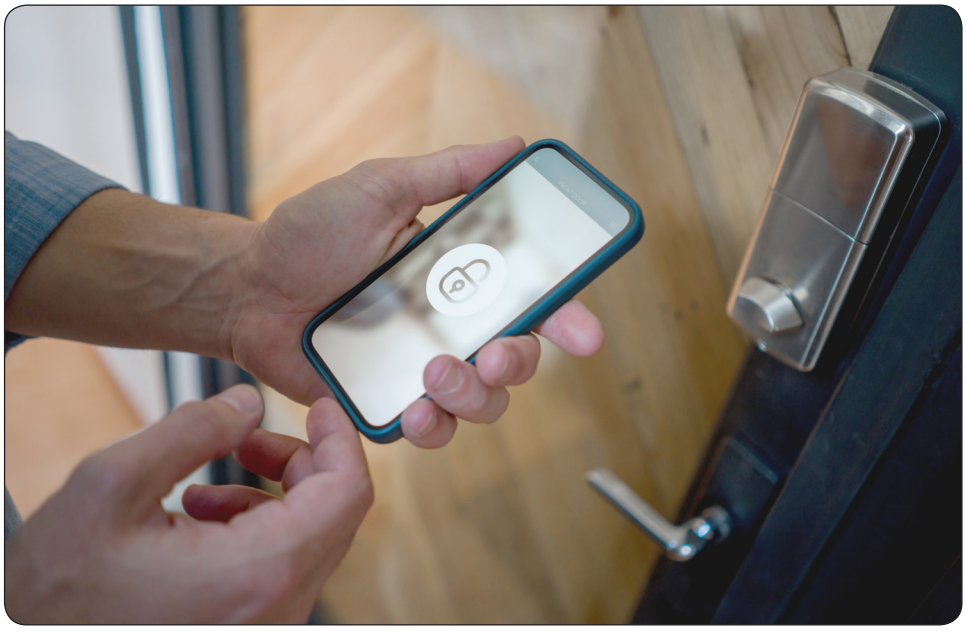
Vulnerabilities are defined by the National Cyber Security Centre as "a weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system".

Good practice is essential to protect security systems/devices against many types of attack. The codes/certifications and recommendations discussed in this short guide are primarily focused on protection of security devices and systems against attacks targeting fundamental design and operational/maintenance weaknesses. However, it should be noted that sophisticated or sustained attacks, including attacks with sustained physical access to devices, may be difficult to mitigate against.

A cyber attack is an attempt by malicious actors (individuals or organisations) to damage, destroy, disrupt, or gain unauthorised access to internet-connected security systems/devices, using unanticipated attack vectors. As with all threats to business and assets, mitigation features should be sufficient to remove or control the risk.

Examples of basic protection requirements from cyber attack include:

- Adequate password security, including unique and sufficiently randomised passwords per device, when pre-installed.
- Device limitations on the number of authentication attempts within a certain time interval, with increasing time intervals between attempts. After a limited number of failed authentication attempts, devices should lock-out.
- Suitable and adequate testing and validation of individual devices and systems.
- Protection of devices from unauthorised software and firmware updates, and disabling of device functionality with excessive data input or corruption of memory.
- Minimising wireless data transfer, network, and physical interfaces that could expose devices and systems to attack.
- Systems to alert to the administrator when abnormal events are detected, for example when a device receives executable code rather than user-inputted text, or erroneous data is input.



4 Codes and certifications

4.1 Relevant codes of practice and white papers

BSIA

https://www.bsia.co.uk/

IoT security codes of practice:

- BSIA Form 343 - *Manufacturers of safety and security systems – cyber security code of practice*
- BSIA Form 342 - *Installation of safety and security systems – cyber security code of practice*

These broadly follow the European Telecommunications Standards Institute (ETSI) cyber security baseline requirements. BSIA Codes of Practice (CoPs) focus on IoT-connected security systems purchased from a professional designer, installer and maintainer, who will leave a system installed securely, distinct from IoT connected security equipment purchased by a user directly from a manufacturer, wholesaler, or retailer (a 'plug and play' scenario), for which system security cannot be fully validated or certified.

The BSIA Cyber Security Product Assurance Group (CySPAG), operate a registration scheme for approved security equipment manufacturers and installers.

HM Government

https://www.gov.uk/government/collections/secure-by-design

Key IoT security guidance:

- *Guiding principles on cyber security*
  Voluntary guiding principles to improve the online security of customers of internet service providers
- *Code of Practice for Consumer IoT Security*
  Practical steps for IoT manufacturers and other industry stakeholders to improve the security of consumer IoT products and associated services
- *Secure by Design: Improving the cyber security of consumer Internet of Things Report*
  Advocating a fundamental shift in approach to moving the burden away from consumers having to secure their internet-connected devices and instead ensure strong cyber security is built into consumer IoT products and associated services by design

https://bills.parliament.uk/bills/3069

- Product Security and Telecommunications Infrastructure Act 2022
  An act to make provision about the security of internet-connectable products and products capable of connecting to such products; to make provision about electronic communications infrastructure; and for connected purposes

(See Principles section below for further details).

ETSI EN 303 645 – Cyber Security for Consumer Internet of Things: Baseline Requirements

Building security into IoT products from their design, to prevent large-scale, prevalent attacks against smart devices, by establishing a security baseline for connected consumer products and providing a basis for IoT certification schemes

4.2 Schemes

BSI IoT Kitemarks; tested and accredited to 3 levels (residential, commercial, enhanced)

Residential	Commercial	Enhanced
For products used in residential environment	For products used in commercial environment	For residential or commercial products for high value and/or high-risk applications and environment
Security testing	Deeper security tests	Advanced security tests
Vulnerability testing	Security testing	Deeper security tests
	Vulnerability testing	Security testing
		Vulnerability testing

The BSI Kitemark is a UK product and service quality trademark, respected throughout the world, owned and operated by the British Standards Institute.

The BSI Kitemark certification scheme has been carefully developed based on the most relevant global and well-known security standards (for example EN 303 645), providing continual assurance and covering product supply chain and life cycle. BSI IoT Kitemark covers the testing and certification activities for hardware and software (web and mobile apps).

Products that BSI can test and certify include:

- Smart locks
- Smart padlocks
- Smoke detectors with IoT connectivity
- Alarms with IoT connectivity
- Smart home appliances
- Heating solutions with IOT connectivity
- Smart lightning solutions.

To obtain the Kitemark, products/services need to:

- Achieve and maintain compliance to ISO 9001 (quality management) and pass the following tests:
  - Functionality – relevant product performance and safety tests
  - Interoperability – testing between devices and the internet
  - Security – testing against best practices and security standards, including scanning for known vulnerabilities and security flaws
- Receive on-going regular monitoring and assessment comprising:
  - Functional/interoperability tests
  - Penetration tests
  - Kitemark audit to review testing results in context of the product, and review what actions have been taken.

https://www.bsigroup.com/en-GB/industries-and-sectors/internet-of-things/IoT-Assurance-Services/

As a minimum, certified locks and apps, within systems meeting the ESTI CoP should be used, but full certification of all home security devices/systems is preferred.

SBD (Secured by Design) – Secure Connected Device Accreditation

https://www.securedbydesign.com

Secured by Design (SBD) is the official police security initiative, owned by the UK Police Service. SBD operates an accreditation scheme on behalf of the UK Police Service for products or services that have met recognised security standards.

SBD have launched a new 'Secure Connected Device' accreditation which will highlight IoT products in the UK that have achieved the appropriate IoT standards/certifications, helping consumers to make better informed choices when buying such devices. The SBD scheme follows government legislation and has been developed in consultation with the Department for Digital, Culture, Media and Sport (DCMS).

The Secure Connected Device accreditation requires for the IoT product to be assessed and certified against all 13 principles presented in ETSI EN 303 645 (listed later in this guide) and other relevant IoT standards. It must be assessed by an SBD approved third-party certifying body, such as IASME or BSI, and annual assessment is required to maintain the accreditation.

If a security product or service has an IoT element to it, it will be required to not only meet traditional physical security standards, but also meet the requirements of the Secure Connected Device Accreditation to gain both the SBD membership and its accreditation.

The SBD IoT Device Assessment identifies the level of risk associated with IoT devices and their ecosystem (i.e. app/cloud/other devices), providing recommendations on the appropriate certification route they need to take. Currently, there are two levels of certification that have been adopted within the Secure Connected Device framework, which are the IASME (Information Assurance Small and Medium Enterprises) IoT Cyber Assurance Level 2 and the BSI IoT Kitemark.

The IASME's IoT Cyber assurance Level 2 is the baseline requirement for IoT products with a lower level of risk, but is still assessed against all 13 provisions of ETSI EN 303 645, which goes beyond the requirements of the new legislation. This certification requires audit by an independent assessor, who conducts an on-site audit of the controls, processes, and procedures covered in the IASME Cyber Assurance standard. A lower standard "Level 1" IASME assessment is based on answers to a questionnaire that are reviewed by a Certification Body.

The BSI IoT Kitemark is a requirement for all IoT products that have been identified as high-level risk within the Secure Connected Device framework.

https://iasme.co.uk/internet-of-things/about-iot-cyber-assurance-level-two/

UL 2900-2-3: Standard for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signalling Systems

https://www.ul.com/

This UL standard forms part of a series of standards covering general software cyber security requirements for network-connectable products. Part 2-3 relates to particular requirements for security and life safety signalling systems and provides a foundational set of cybersecurity performance and evaluation requirements that manufacturers of network connectable products can use to establish a baseline of cyber-protection against known vulnerabilities, weaknesses, and malware.

UL's Cybersecurity Assurance Program (UL CAP) can test and evaluate a product's software for the presence of malware, vulnerabilities, and weaknesses, and certify the product's software architecture and design to the specifications enumerated in the Outline of Investigation.

A three-tiered security approach is applied, with increasing levels of security for each tier. Tests include automated software testing for invalid, unexpected, or random data (fuzz testing), known vulnerability detection, code and binary analysis, risk control analysis, structured penetration testing, and security risk controls assessment.

Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
Recommended as a minimum level of assessment.	An assessment of the security capabilities of a product with knowledge of internal security controls of the product.	This security evaluation standard applies to the evaluation of security and life safety signalling system components.
Includes the foundational cyber security testing requirements for security risk assessment of software in products covered in the Outline of Investigation.	Includes all of L1 assessment and testing requirements and additional supplemental requirements for security risk assessment of software in products.	Includes L1 and L2 assessment and testing requirements and additional supplemental requirements of the vendor process and management.
		An assessment of security capabilities of a product with knowledge of internal security controls of the product and knowledge of the business practices of the vendor to support the lifecycle of the product.

UL 2900-2-3 applies to, but is not limited to, the following products:

- Alarm control units
- Network-based intrusion detection system
- General purpose signalling units
- Digital video equipment and systems
- Mass notification and emergency communication/evacuation equipment and systems
- Control servers
- Alarm automation system software
- Alarm receiving equipment
- Anti-theft equipment
- Automated teller machines
- Fire alarm control systems
- Network connected locking devices
- Physical Security Information Management (PSIM) Systems
- Smoke control systems
- Smoke/gas/CO detection devices
- Audible and visual signalling devices (fire and general signalling)
- Access control equipment and systems
- Smart locks.

TÜV SÜD – ETSI EN 303 645 testing and Attestation of Conformance (AoC) – tested and accredited to 3 levels (basic, substantial, high)

Basic	Substantial	High
Makes cyber attack more difficult and challenging	Provides substantial resistance against cyber attack	Provides high resistance against cyber attack
Product: document review and technical testing, including safety	Product: document review and technical testing, including safety	Product: document review and technical testing, including safety
Company: testing of internal processes	Company: testing of internal processes	Company: testing of internal processes
	Penetration test	TÜV SÜD penetration test (including source code review) and additional tests
	Cloud test	Cloud test
	Inclusion of suppliers/ subcontractors	Inclusion of suppliers/ subcontractors
	All ETSI EN 303 645 mandatory requirements and additional tests	All ETSI EN 303 645 mandatory requirements and additional tests

5 Overall insurer view of good practice

Key factors for insurers to consider when accepting internet-connected security devices and systems:

- BS IoT Kitemarked (or equivalent accreditation) products installed to ETSI or BSIA guidelines.
- IoT security equipment providers should be able to demonstrate:
  - Compliance with the "13 principles" (see below)
  - A suitable vulnerability disclosure policy (i.e. a point of contact for technical response to vulnerability queries)
  - Robust supply chain management and QC for system components
  - System updates (including firmware updates*) for the full (intended) life of products, e.g. 3, 5, or 10 years
  - Ownership/control of software/firmware code
  - Security system components are designed and installed to recognised security system standards, e.g. BS EN 50131 - Alarm systems. Intrusion and hold-up systems
  - Security systems are installed by a UKAS (United Kingdom Accreditation Service) accredited installer.

*Note that Wi-Fi (broad bandwidth) connection may be required for firmware updates as these can require more energy than can be achieved using Bluetooth. Bluetooth (low bandwidth) is suitable for short-proximity lock/unlock functions.

6 The principles

The ETSI EN 303 645 cybersecurity standard outlines 13 cyber security principles for consumer IoT:

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store sensitive security parameters
- Communicate securely
- Minimise exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is secure
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for users to delete personal data
- Make installation and maintenance of devices easy
- Validate input data.

The UK Government introduced new legislation: the Product Security and Telecommunications Infrastructure (PSTI) Act in 2022 to establish mandatory security requirements for internet-connectable smart devices, i.e. IoT devices.

Product security measures of the act cover:

- security against cyber-attacks of consumer connectable products
- security requirements relating to consumer connectable products for manufacturers, importers and distributors
- enforcement with civil and criminal sanctions aimed at preventing insecure products being made available on the UK market.

The first three provisions of the ETSI EN 303 645 standard will be mandated by the UK government, although all principles are important and form part of the various accreditation schemes.

7 Conclusion

Any internet-connected device is inherently vulnerable to cyber attack, and so good security controls are essential to maintain the integrity of the device and the assets it protects. As well as the product itself, there are other areas that need to be considered:

- **The software and operating system:** are these secure and regularly updated in a timely manner?
- **Supply chain:** are all components and elements involved with the production and supply of the device secure (i.e. third-party components, third-party software, the third parties themselves etc)?
- **The connection:** is the connection to the internet secure?
- **The installation:** has the device been installed and configured correctly by an appropriate installer?
- **The user:** will the user be aware of how to ensure their device is secure and updated?
- **Maintenance:** will maintenance, repair, and regular software updates be timely and appropriate and actioned by approved companies?

The BSI Kitemark scheme complies with the well-established ETSI EN 303 645 standard, upon which the BSIA and UK Government Standards are based. It not only applies to the product but, all of the points above, as well as other controls such as having a vulnerability disclosure policy i.e. obliging manufacturers to fix vulnerabilities and inform users of any security issues. Other comparable accreditations, such as TÜV SÜD, UL, and SBD offer similar assurances to insurers.

Fire Protection Association
London Road
Moreton in Marsh
Gloucestershire GL56 0RH
T: +44 (0)1608 812500
E: info@riscauthority.co.uk
W: www.thefpa.co.uk

RISK INSIGHT, STRATEGY AND CONTROL AUTHORITY

REDUCING INSURABLE RISK THROUGH RESEARCH, ADVICE AND BEST PRACTICE