bsi.

...making excellence a habit.™

The Internet of Things:

get serious about security

A whitepaper

IoT: the numbers

$11 trillion

per year value from the Internet of Things (IoT) by 2025[A]

65% of CEOs

see the IoT as strategically important in digital transformation[B]

8.4 billion

connected devices in 2017[C]

$2 trillion

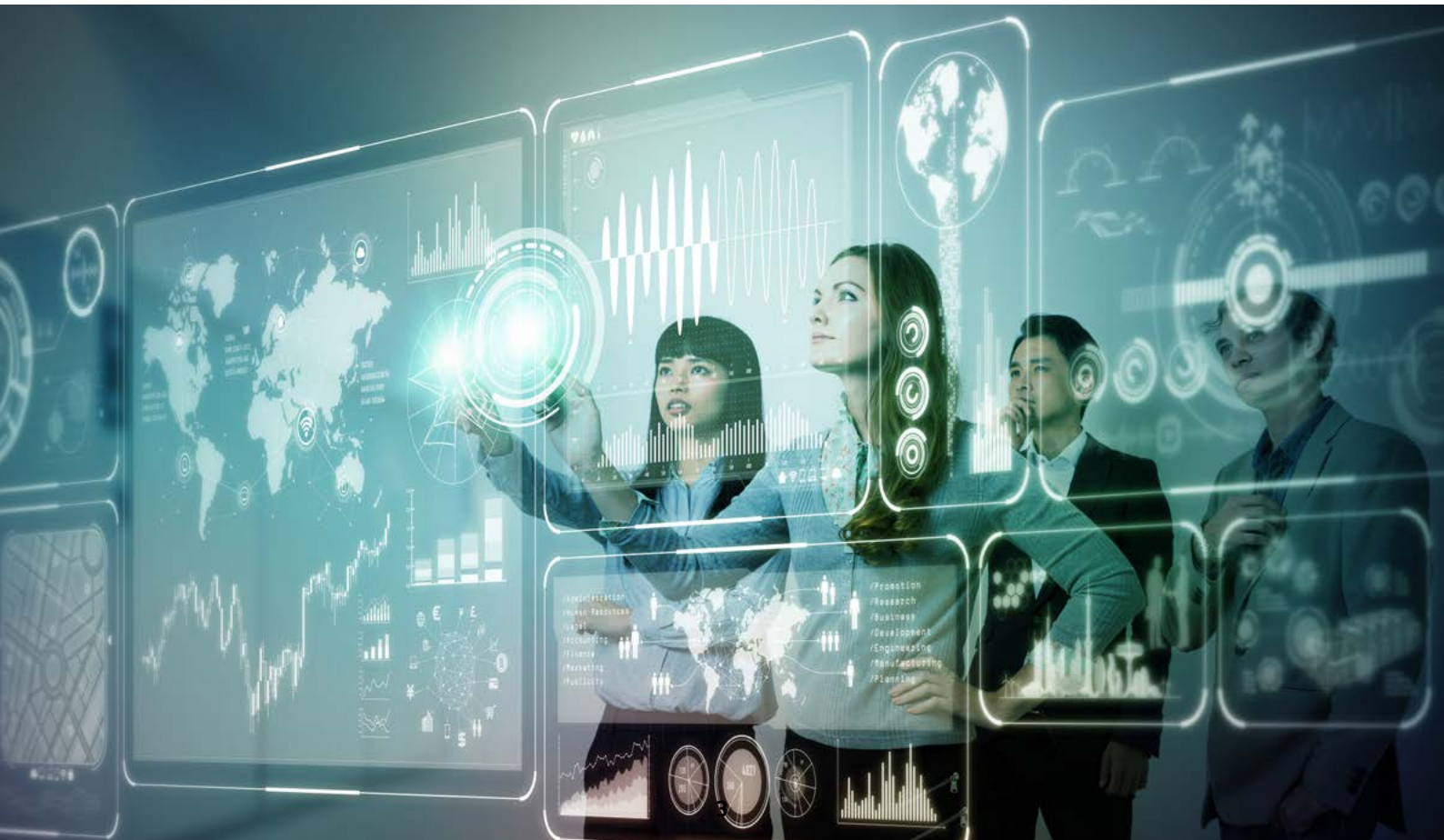
revenues in 2017[D]

It is estimated that every household in the UK owns at least 10 internet connected devices, with this number expected to increase to 15 by 2020[E]. By the same time it is estimated that over a quarter of identified attacks will involve IoT devices[F], as recent high-profile breaches have demonstrated.

[A] Source: McKinsey, 2015
[B] Source: PwC, 2015
[C] Source: Gartner, 2017
[D] Source: Gartner, 2017
[E] Source: DCMS – Secure by Design Report, March 2018
[F] Gartner IoT report announcement, 25 April 2016

The Internet of Things: get serious about security

Contents



Executive summary

- The Internet of Things (IoT) has brought benefits, but also risks – particularly security risks
- The security threat to IoT is real, dangerous and increasing
- As a supplier of a connected product or system, you have a commercial imperative and a duty of care to your customers to ensure that it is secure
- Security goes beyond password protection and encryption
- A range of basic issues must be addressed – highlighted by expert research and a new international technical specification released by the European Telecommunications Standards Institute (ETSI)
- The challenges include compliance with the General Data Protection Regulation (GDPR) – and the code of practice addresses key GDPR issues
- Failure by manufacturers to address security challenges will increase consumer mistrust and reduce business confidence in them and their products
- Such failure will have serious negative repercussions, from legal action being taken and fines being levied against them, to falling sales and profits, together with damaged reputation and reduced business investment
- There is an alternative. Meeting security challenges by embracing IoT best practice, can help to build a robust commercial proposition and a resilient organization. With independent verification, you can stand out from the competition, gaining the trust and confidence of consumers and business and maximizing sales and profit
- The ETSI technical specification forms the heart of BSI's IoT assurance scheme, which includes a new IoT BSI Kitemark
- Now is the time to act – and BSI can help

Introduction: a wake-up call

The IoT has brought benefits and continues to grow exponentially, but it could be even more transformative but for widespread concerns regarding the security of IoT-enabled products and systems.

Security risks apply whether you supply consumer electronics or products for a business-to-business market. All IoT devices and systems are vulnerable to external threats, including those that do not directly have a safety or security function, and which you may never have regarded as a likely target for cyber criminals – such as connected washing machines.

The UK Government's 2018 report, Secure by Design, warns of the potential for widespread disruption and serious harm: "Cyber criminals could exploit vulnerabilities in IoT devices and associated services to access, damage and destroy data and hardware or cause physical, or other types of harm. Where these vulnerabilities can be exploited at scale, impact could be felt by multiple victims across geographic boundaries."

Lack of consumer trust potentially undermines manufacturers' confidence in making a healthy return on investment in IoT products and systems.

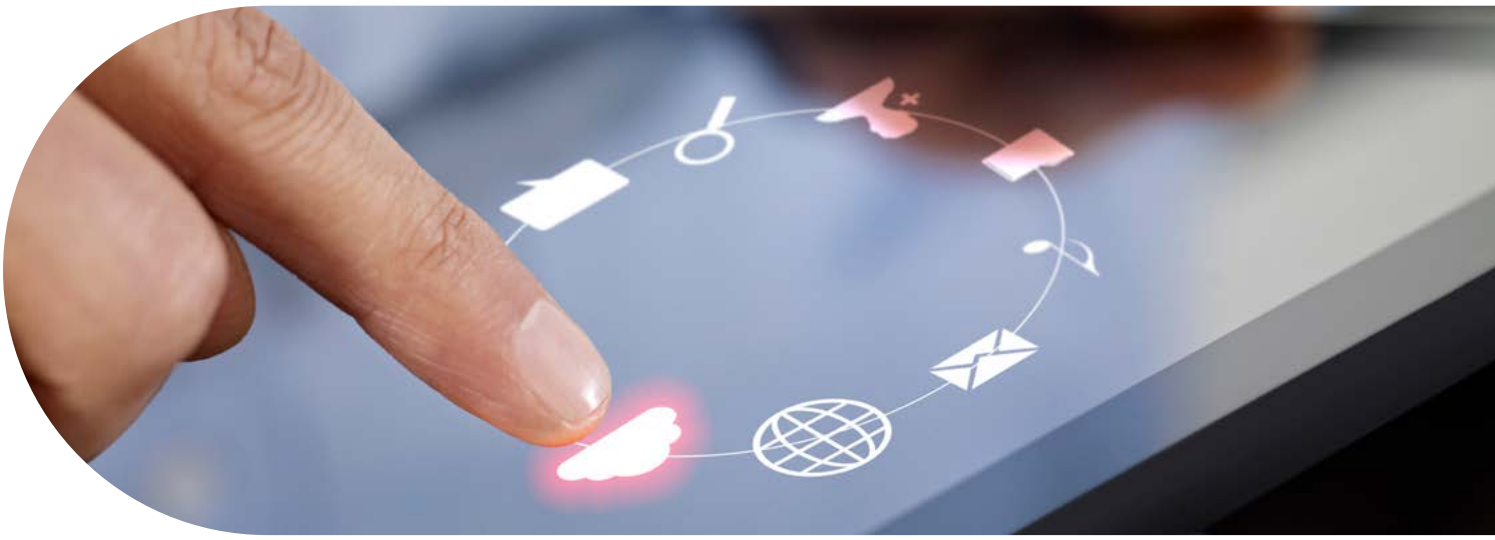
The costs and risks may be perceived to be too high to justify investment in areas such as IoT skills and new product development.

As a manufacturer of an IoT product you may well assume that you have ticked the box marked 'security' if your product has a secure third-party IoT system embedded in it. Or you may be comforted in the knowledge that it features a secure password and encryption, or password and blockchain security. But in a world now rife with sophisticated cyber crime, you may be dangerously mistaken.

The demands on service providers will only increase as the average household moves toward the use of many connected devices at the same time. Currently, many smart manufacturers are not paying enough attention to the security of their products. It is vital that this change – and that security is implemented at the design stage, rather than considered as an afterthought.

There is always an onus on the provider of a connected product or system to 'own' the security of that system. As well as commercial drivers, they have a duty of care to customers to ensure that it is secure, rather than relying on a third-party supplier or an inadequate technology.

Addressing key security issues



It now takes more than password protection and encryption to ensure security, as shown by research from the Open Web Application Security Project (OWASP), whose members include security experts from around the world.

OWSAP has created a top ten of things to avoid when building, deploying, or managing IoT systems. This list contains the highest priority issues for manufacturers, enterprises, and consumers which is designed to help them to address security concerns.

In the UK, the Government and industry launched a collaborative approach to protect consumers while continuing to support and foster IoT innovation. In October 2018, the Department of Culture, Media and Sport (DCMS), which leads on cyber-security, published practical guidance, in the form of an IoT industry code of practice, to ensure that consumer IoT products are designed with security in mind, and to help users make their devices more secure. The code was developed in conjunction with the National Cyber Security Centre (NCSC), and endorsed by the IoT Security Foundation, of which BSI is a member.

In early 2019, ETSI (European Telecommunications Standards Institute), released the first globally applicable technical specification for consumer IoT security, ETSI TS 103 645. This builds on the UK government's Code of Practice and has been designed to work for European and wider global needs.

OWASP has recently released an updated list of the top 10 most critical security vulnerabilities of IoT applications:

1. **Weak, guessable or hard-coded passwords**
2. **Insecure network services**
3. **Insecure ecosystem interfaces**
4. **Lack of secure update mechanism**
5. **Use of insecure or outdated components**
6. **Insufficient privacy protection**
7. **Insecure data transfer and storage**
8. **Lack of device management**
9. **Insecure default settings**
10. **Lack of physical hardening**

The industry technical specification

The ETSI technical specification is made up of 13 guidelines for securing IoT devices, together with explanatory guidance summarised below:

1. No default passwords

All IoT device passwords shall be unique and not resettable to any universal factory default value.
Primarily applies to: device manufacturers.
Guidance issued with the Code observes, "Many IoT devices are being sold with universal default usernames and passwords (such as 'admin, admin'), which consumers are expected to change. This has been the source of many security issues in IoT and the practice needs to be eliminated. Best practice on passwords and other authentication methods should be followed."
This advice is supported by research from IT security company Kaspersky Lab, which found the most popular method of spreading IoT malware is still 'brute-forcing' passwords, where hackers repetitively try various password combinations before eventually gaining access to a device. It was used in 93% of attacks.

2. Implement a vulnerability disclosure policy

All companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.
Primarily applies to: device manufacturers, IoT service providers and mobile application developers.
The guidance expands: "Knowing about a security vulnerability allows companies to respond. Companies should also continually monitor for, identify and rectify security vulnerabilities within their own products and services as part of the product security lifecycle. Vulnerabilities should be reported directly to the affected stakeholders in the first instance. If that is not possible vulnerabilities may be reported to national authorities at: security@ncsc.gov.uk. Companies are also encouraged to share information with competent industry bodies."

3. Keep software updated

Software components in internet-connected devices should be securely updateable. Updates shall be timely and should not impact on the functioning of the device. An end-of-life policy shall be published for end-point devices that explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.
Primarily applies to: device manufacturers, IoT service providers and mobile application developers.
The guidance explains: "The provenance of security patches should also be assured and they should be delivered over a secure channel. The basic functions of a device should continue to operate during an update wherever possible, for example a watch should continue to tell the time, a home thermostat should still operate and a lock should continue to unlock and lock. This may seem primarily a design consideration, but can become a critical safety issue for some types of devices and systems if not considered or managed correctly.
Software updates should be provided after the sale of a device and pushed to devices for a period appropriate to the device. This period of software update support shall be made clear to a consumer when purchasing the product. The retailer and/or manufacturers should inform the consumer that an update is required. For constrained devices with no possibility of a software update, the conditions for and period of replacement support should be clear."

4. Securely store credentials and security-sensitive data

Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable.
Primarily applies to: device manufacturers, IoT service providers and mobile application developers.
The guidance explains: "Reverse engineering of devices and applications can easily discover credentials such as hard-coded usernames and passwords in software. Simple obfuscation methods also used to obscure or encrypt this hard-coded information can be trivially broken. Security-sensitive data that should be stored securely includes, for example, cryptographic keys, device identifiers and initialisation vectors. Secure, trusted storage mechanisms should be used such as those provided by a Trusted Execution Environment and associated trusted, secure storage."

The industry technical specification (continued)

5. Communicate securely

Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All keys should be managed securely.

Primarily applies to: device manufacturers, IoT service providers and mobile application developers.

"The use of open, peer-reviewed internet standards is strongly encouraged," it adds.

6. Minimize exposed attack surfaces

All devices and services should operate on the "principle of least privilege"; unused ports should be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.

Primarily applies to: device manufacturers and IoT service providers.

"The principle of least privilege is a foundation stone of good security engineering, applicable to IoT as much as in any other field of application," comments the guidance.

7. Ensure software integrity

Software on IoT devices should be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/ administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.

Primarily applies to: device manufacturers.

The Guidance expands: "The ability to remotely recover from these situations should rely on a known good state, such as locally storing a known good version to enable safe recovery and updating of the device. This will avoid denial of service and costly recalls or maintenance visits, whilst managing the risk of potential takeover of the device by an attacker subverting update or other network communications mechanisms."

8. Ensure that personal data is protected

Where devices and/or services process personal data, they shall do so in accordance with applicable data protection law, such as the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Device manufacturers and IoT service providers shall provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this must be validly and lawfully obtained, with those consumers being given the opportunity to withdraw it at any time.

The industry technical specification (continued)

Primarily applies to: device manufacturers, IoT service providers, mobile application developers and retailers.
The guidance expands: "This guideline ensures that:

- IoT manufacturers, service providers and application developers adhere to data protection obligations when developing and delivering products and services
- Personal data is processed in accordance with data protection law
- Users are assisted in assuring that the data processing operations of their products are consistent and that they are functioning as specified
- Users are provided with means to preserve their privacy by configuring device and service functionality appropriately"

9. Make systems resilient to outages

Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect.
Primarily applies to: device manufacturers and IoT service providers.
The guidance states, "IoT systems and devices are relied upon by consumers for increasingly important use cases that may be safety-relevant or life-impacting. Keeping services running locally if there is a loss of network is one of the measures that can be taken to increase resilience. Other measures may include building redundancy into services as well as mitigations against DDoS attacks. The level of resilience necessary should be proportionate and determined by usage but consideration should be given to others that may rely on the system, service or device as there may be a wider impact than expected."

10. Monitor system telemetry data

If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies.
Primarily applies to: IoT service providers.
If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies.

11. Make it easy for consumers to delete personal data

Devices and services should be configured such that personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data.
Primarily applies to: device manufacturers, IoT service providers and mobile application developers.
Devices and services should be configured such that personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data.

12. Make installation and maintenance of devices easy

Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device.
Primarily applies to: device manufacturers, IoT service providers and mobile application developers.
The Guidance explains, "Security issues caused by consumer confusion or misconfiguration can be reduced and sometimes eliminated by properly addressing complexity and poor design in user interfaces. Clear guidance to users on how to configure devices securely can also reduce their exposure to threats."

13. Validate input data

Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.
Primarily applies to: device manufacturers, IoT service providers and mobile application developers.
The code guidance comments, "Systems can be subverted by incorrectly formatted data or code transferred across different types of interface. Automated tools are often employed by attackers in order to exploit potential gaps and weaknesses that emerge as a result of not validating data. Examples include, but are not limited to, data that is:

- Not of the expected type, for example executable code rather than user inputted text
- Out of range, for example a temperature value which is beyond the limits of a sensor"

The ETSI technical specification and the GDPR

The recent implementation of the General Data Protection Regulation (GDPR) – which is binding on all manufacturers and service providers offering their products or services in the EU – has increased the security challenge for IoT suppliers by expanding the definition of personal data to encompass many connected applications.

The ETSI technical specification links directly to the GDPR, exploring what organizations are doing with their data, and what they should do, to ensure it remains secure.

A product on its own cannot offer GDPR compliance – it needs the whole organizational process to be assessed to confirm that – but the code addresses certain GDPR issues. Specifically, implementing principles 8 and 11 will meet key elements of the GDPR, while general security, and the need to look at the whole organization, will enable full compliance.

Building resilience with BSI

BSI has a world-class cyber security capability, recognized by CREST global accreditation, combined with decades of experience in product testing and assurance.

Operating in its state-of-the art IoT laboratory, BSI's highly skilled team, also provides fast, effective testing for a huge range of IoT products. By providing valuable feedback on the security of product design early in the process, BSI can help accelerate and de-risk time-to-market in a highly competitive and time-critical industry.

BSI works with clients to verify their compliance with good IoT security design practice. Through BSI's verification scheme, they can demonstrate to their customers that products are secure for their intended use.

Now, through a collaborative approach based on extensive dialogue with stakeholders, and underpinned by the OWASP research and the ETSI technical specification, BSI has developed an IoT assurance solution, the IoT Kitemark.

The BSI IoT Kitemark helps consumers confidently identify connected products that they can trust to be safe, secure and fit for purpose. These devices will have been rigorously tested to ensure they perform as expected, communicate correctly, and are safe and secure for their intended use. Key strengths of the BSI Kitemark are that it is:

- Appropriate – risk-based and dependent on use/environment
- Flexible – with a tailored 'pick list' of solutions from master scheme
- Adaptable – evolving with technologies, threats and standards
- Comprehensive – covering supply chain, installed systems, and cloud layer/applications

Organizations need the assurance of robust information security standards that provide ongoing, lifetime resilience. BSI is the only organization currently set up to independently verify or certify compliance with the Code. BSI can help embed trust and confidence, supporting you in ensuring your products are safe, secure and will perform as intended for as long as required.

Take action today

As a business looking to exploit the burgeoning IoT opportunity, there are safe ways to do so that will build consumer trust, business confidence and organizational resilience. But it takes more than a secure password and encryption to make a secure IoT system. BSI can help you meet the challenge. Now is the time to get in touch.

About the author

David Mudd is Global Digital and Connected Product Certification Director for BSI. He acts as expert and ambassador on the IoT, supporting the delivery of excellence and expertise across the 193 countries in which BSI operates. He sits on the IoT Security Foundation's working group for testing and certification, and has authored regulatory and technical guidance, written articles for a range of publications and is a successful global, keynote speaker and presenter.

Why BSI?

By Royal Charter

BSI works as a trusted, independent convenor of communities to shape, share, embed and support innovation in IoT and the safe and reliable use of 'smart' applications, data and devices. Through our community of IoT experts and organizations BSI is at the forefront of shaping new opportunities and creating industry-led best practice in IoT. That's why we're best placed to help you embed trust and confidence in your products.

Working with over 86,000 clients across 193 countries, BSI is a truly international business with skills and experience across a number of sectors including automotive, aerospace, built environment, food, and healthcare. Through its expertise in Standards Development and Knowledge Solutions, Assurance and Professional Services, BSI improves business performance to help clients grow sustainably, manage risk and ultimately be more resilient.

Our products and services

Knowledge

The core of our business centres on the knowledge that we create and impart to our clients. In the standards arena we continue to build our reputation as an expert body, bringing together experts from industry to shape standards at local, regional and international levels. In fact, BSI originally created eight of the world's top 10 management system standards.

Assurance

Independent assessment of the conformity of a process or product to a particular standard ensures that our clients perform to a high level of excellence. We train our clients in world-class implementation and auditing techniques to ensure they maximize the benefits of standards.

Compliance

To experience real, long-term benefits, our clients need to ensure ongoing compliance to a regulation, market need or standard so that it becomes an embedded habit. We provide a range of services and differentiated management tools which help facilitate this process.

bsi.

For more information on IoT security, visit **bsigroup.com**