bsi.

...making excellence a habit.™

The Internet of Things:

grasping opportunity, managing risk

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.

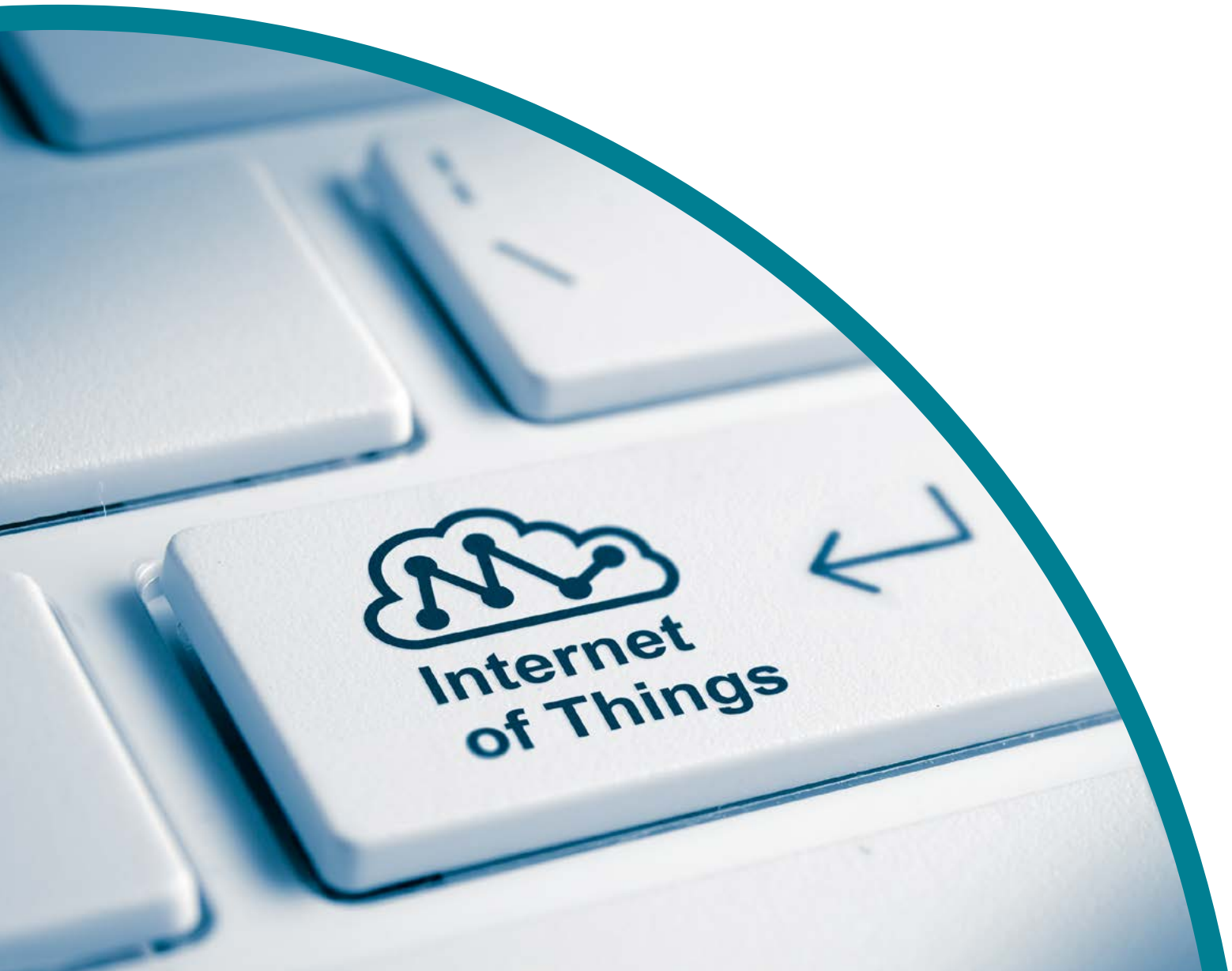
[A] Source: McKinsey, 2015
[B] Source: PwC, 2015
[C] Source: Gartner, 2017
[D] Source: Gartner, 2017
[E] Source: DCMS – Secure by Design Report, March 2018
[F] Gartner IoT report announcement, 25 April 2016

The Internet of Things: grasping opportunity, managing risk

Contents

Executive summary

- The Internet of Things (IoT) refers to devices and systems that not only communicate with each other, but learn and act with minimum human intervention
- The IoT heralds transformational changes, bringing new user experiences for consumers and operational efficiencies for businesses, with its impact felt right across society
- But alongside great opportunities, the IoT also brings significant risks, with increasing consumer and business concerns regarding the performance and security of IoT-enabled devices and systems
- In particular, security threats are increasing rapidly, causing significant harm and hampering mass IoT adoption
- The issue of security is causing a lack of consumer trust in the IoT and undermining business confidence that investment in connected products will yield a healthy and reliable return
- Manufacturers of IoT devices should be concerned to address IoT security risks to reassure themselves, their customers, their investors and other stakeholders
- There are practical measures they can take to improve security and embrace the IoT in a way that will build consumer trust and business confidence
- BSI services and the BSI Kitemark will ensure – and demonstrate – that IoT products and systems will deliver securely. Now is the time to embrace them



Introduction: with opportunity comes risk

The Internet of Things heralds transformational changes for organizations, consumers and society as a whole. But alongside potentially great rewards, it also brings significant risks – which manufacturers of connected products should be concerned to address.

Whether you manufacture consumer electronics or products for a business-to-business market, the IoT has major security implications for your business.

Security risks apply even to devices and systems that do not directly have a safety or security function, and which you may never have regarded as a likely target for cyber criminals. In the burgeoning world of the IoT, all connected products, from TVs and computers to smart meters and even washing machines, are vulnerable to external threats.

But solutions are at hand – and now is the time to embrace them.

What is the Internet of Things?

The IoT is all about internet-enabled machine-to-machine communications. But it means more than just connected devices. It is the free exchange of data and discussion/interaction between machines, encompassing machine learning, artificial intelligence, data analytics and machine-to-machine decision-making.

The Groupe Spéciale Mobile Association, (GSMA), which represents mobile network operators worldwide, offers the following definition:

"The Internet of Things describes the coordination of multiple machines, devices and appliances connected to the internet through multiple networks. These devices include everyday objects such as tablets and consumer electronics, and other machines such as vehicles, monitors and sensors equipped with communication capabilities that allow them to send and receive data."

What physically is the IoT?

Devices and controllers, connected to the internet interacting with cloud storage, analytics and applications, over a range of networks.

A hybrid network could be a mixture of standalone IoT devices capable of performing long range communications, with a star network and some mesh network elements.

The hybrid network gains in resilience, increasing the number of nodes that can perform the communication tasks independently.

The IoT opportunity

The IoT presents a huge opportunity to transform our lives for the better, with the potential to make an impact right across society.

Take the simple task of controlling your household lighting and heating. Rather than doing this manually, or using your 'phone to do it remotely, the IoT allows the devices in your home to 'learn' your habits and preferences, while simultaneously monitoring temperature and daylight, checking on the weather forecast, analyzing gas and electricity prices, and then providing you with your ideal environment at the most cost-effective price. It is an entirely automated process, revolving around real-time communication of accurate intelligence based on analysis of big data – and it all takes place without you having to think about it.

The same model applies for businesses, moving far beyond environmental control and energy management to encompass a host of other areas, such as access and security, fire detection and alarm, water and waste services, enterprise integration, factory production systems – and much more.

The hallmark of the IoT is that it takes the fallible human out of the process wherever possible, creating improved outcomes at lower cost – and this is where its disruptive benefit lies.

The IoT offers the prospect of 'doing things better and doing new things'. It promises both improved operational performance for businesses and also enhanced user experience for consumers. On the one hand, the IoT heralds the digital transformation of customer/user experience; on the other, it enables a business to respond and adapt to changing consumer demand, scaling up or down quickly and efficiently. And this creates a 'virtuous circle', with a more efficient and effective organization further satisfying customers.

New and improved customer experiences brought about by successful adoption of the IoT can help boost existing business, create new revenue streams, and generate increased profits.

In short, the digital transformation brought about by the IoT offers a major boost to organizational performance.

Digital transformation is underway

Change is already well underway across manufacturing industry, consumer products and retail, bringing significant economic and social benefits.

A study by consultants PwC found that even by 2015 65% of CEOs saw the IoT as strategically important in digital transformation. More recently, research group Gartner estimated that there were already 8.4 billion Internet-connected devices in use, generating revenues of $2 trillion, and that by 2020 there would be 20 billion devices worldwide.

Experts agree that the pace of change is accelerating, with the number of connected – or 'smart' – devices increasing to an average of 15 per household by 2020. Management consultancy McKinsey predicts the value of the IoT will reach $11 trillion a year by 2025.

Secure by Design, a recent UK Government report from the Department for Digital, Culture, Media and Sport, (DCMS), which leads on cyber-security, anticipates further benefits for consumers and companies alike. "The networks and data that flow from connected devices will support an extraordinary range of applications and economic opportunities," it says, citing new and better products and services, companies using data to better anticipate and meet people's needs, companies providing useful, tailored information to inform consumer decision-making, and new features to save people time and money, for example on home energy and security.

Along with smart consumer products and services, the report notes that the IoT is also being put to effective use across a range of industries, such as automating industrial manufacturing processes in areas as diverse as the agriculture and automotive sectors. And it is being utilized in the public sector, for example, in health, social care, urban infrastructure and services, and transport.

Becoming IoT ready

A 2017 study from research group IDC, Prepare for Billions – The IoT 2020 IT Infrastructure Readiness Indicator, shows how organizations can move to a higher state of IoT readiness by describing high readiness firms, or 'IoT All-Stars', in three areas.

Three key areas:	
Attitude toward IoT	IoT All-Stars see IoT as an opportunity to transform their businesses. They are ambitious with their IoT initiatives and tend to be frustrated by technology limitations that slow them down or hold them back.
Moving from data-centric to action-centric IoT	IoT All-Stars are likely to employ 'action-centric' IoT devices. These devices are active change agents that not only carry out all the functions of data-centric IoT, but can also respond to or act based on specific circumstances. Such firms make use of the advanced technologies and business processes that facilitate and automate these activities in real time or near real time.
Readiness in technology adoption	IoT All-Stars employ diverse types of IT infrastructure technology that directly influence or are influenced by the IoT strategy. They have a propensity to leverage advanced network technologies, invest in advanced IT infrastructure provisioning and management frameworks, and develop custom next-generation applications in aid of their IoT strategies. Such firms (to the extent they are allowed by industry regulations) make informed use of on- and off-premises cloud types and tiers for efficient data capture, analysis, and insight. The IDC report concludes that companies seeking to advance their IoT IT infrastructure readiness should assess the design of their IT infrastructure. Whether they could take a clean-slate approach to building a modern IT infrastructure or upgrade existing infrastructure, "the goal of IT infrastructure should be agility, flexibility, and scalability to support strategic IoT-centric business outcomes such as timely insight from diverse and disparate data sources". It adds, "IT infrastructure upgrades that enable a shift to higher levels of IoT readiness ought to be treated as strategic activities as opposed to a chore to be taken on reactively."

Obstacles to adoption

With so much momentum behind it, it would be easy to regard the rapid roll-out of the IoT as an inevitable, universal force for good, with few drawbacks. In fact, significant obstacles are hindering the mass adoption of the IoT.

It is important for companies not to get carried away with the amazing technology and how it can transform society. First and foremost, digital technology is an enabler – so manufacturers must not lose focus on the key purpose of their product or system. Take the example of a smart lock: an early one tested by BSI may have been extremely 'smart', with a great app, but it took our experts less than 30 seconds to break in. It failed in its primary function!

Similarly, adding a smart temperature sensor to, say, a container does not guarantee that the temperature of the contents will be thoroughly and accurately measured and monitored. The data provided will be useless unless it can be trusted – and this demands that due attention is given to the measurement process, including issues such as tolerances, calibration and sampling rate.

A significant drag on IoT adoption is the challenge of interoperability: will an IoT product work with other devices, controllers and applications? Will the data be in the right format to interact with other systems?

Many IoT suppliers have indicated that companies' existing or 'legacy' systems are the biggest problem. Most IoT systems have to interact with some part of an organization's existing infrastructure and this is where the problems really begin. Will it keep working? How long will the platform be supported? What third-party plug-ins are used, which the supplier has no control over?

And then there is cost. This is largely driven by return on investment (ROI), and unless manufacturers and end-users have confidence that IoT-enabled products will perform reliably for their projected lifespan, the risk to returns will be too great to justify the investment required.

But one obstacle to the successful uptake of the IoT dwarfs all others – security risks.

IoT security: you are at risk!

Adoption of the IoT continues to explode, but it could be even more transformative but for widespread concerns regarding the security of IoT-enabled products and systems.

IoT security will affect you!

Until now, the all too common response to cyber risk from consumers and businesses has been blind trust in the maxim, "It won't happen to us". While many have got away with this head-in-the-sand approach in the past, they will not do so in future. With IoT-enabled devices encompassing a myriad of everyday products, such as lightbulbs and power sockets, IoT security risks threaten everyone; manufacturers, businesses, retailers and consumers.

In March 2018, Interpol, the international crime policing organization, warned bluntly, "All devices which can connect to the Internet are potentially at risk of a cyber attack." The following August, the FBI, the US law enforcement agency, highlighted that cyber criminals are using IoT devices for malicious activities that could spike consumers' internet service bills and threaten the reliability of their internet connections.

Recent research from Infoblox, a US network security specialist, shows it is not just consumers who are vulnerable. Enterprises of all sizes could be putting themselves at risk of cyber attack because of so-called 'shadow' IoT connecting to their networks.

Many companies have thousands of devices connecting to their networks each day – with around a third of those surveyed having more than 5,000 devices detected, including fitness trackers, smart kitchen appliances, TVs, digital assistants and game consoles. Such devices are easy to recognize on the network, with online services that can be used for that purpose, so even the cybercriminals described as 'low level' can gain access to them.

Gary Cox, Technology Director, Western Europe at Infoblox, says: "Due to the poor security levels of many consumer IoT devices, there is a very real threat posed by those operating under the radar of organizations' traditional security policies. These devices present a weak entry point for cyber criminals into the network, and a serious security risk to the company."

The UK Government's Secure by Design report 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."

Common IoT threats

- ### Hacking and data theft
  Cyber crimes include the now familiar crime of system hacking and theft of personal and company data. Serious breaches have become commonplace, forcing organizations to reconsider how they handle valuable data to ensure it remains secure. The recent implementation of the General Data Protection Regulation (GDPR) has increased the challenge by expanding the definition of personal data to encompass many IoT applications.
  More alarming still is the risk of hacking that makes domestic appliances such as cookers and boilers unsafe, and even nation-state level attacks on power stations or transport networks. Smart cities, for example, employ 200,000 traffic sensors globally, which are potentially vulnerable to such attacks.
- ### Denial of service
  Distributed Denial of Service (DDoS) attacks involve hijacking insecure devices and using them to attack servers. They were highlighted in May 2017 by the WannaCry 'ransomware' cyber attack, which targeted computers running Microsoft Windows by encrypting data and embedding demands for ransom payments in the Bitcoin cryptocurrency. Still in circulation, the equally infamous Mirai botnet targets IoT devices, including cameras, routers and DVD recorders, and was used in 2016 to carry out one of the largest DDoS attacks against internet services in history, even disabling much of the US Internet, including Amazon, Twitter, PayPal and Spotify. Cyber security firm F-Secure, which operates an international network of decoy 'honeypot' servers to track the latest cyber threats, says that variations of Mirai remain the most prevalent malware.
- ### Destruction of service
  Now, an arguably even greater threat lies not in mere denial of service, but in destruction of service (DeOS). In its latest cyber security report, networking giant Cisco warns of a coming wave of computer viruses capable of eliminating organizations' back-ups and safety nets, destroying businesses in one fell swoop.
  The report says the DeOS breed of virus benefits from the growth of the IoT, which increases 'attack surfaces'. It points to the increasing number, size and complexity of attacks and the relative vulnerability of unwieldy systems with a proliferation of devices, operating systems, connectors/connectivity, versions and protocols.

The increasing threat

IoT hacks inflict huge financial costs on businesses and end-users, and they are on the increase.

While the overall cost of an IoT system hack varies depending on the number of affected devices and the length of time an issue persists, recent research from University of California Berkeley found that DDoS attacks involving IoT devices can cost hundreds of thousands of dollars.

A study of 400 small businesses in the US that use connected devices found 48% had already experienced at least one IoT breach. Additionally, the research showed that among companies with annual turnover of less than $5m, the costs of IoT hacks made up 13.4% of revenue. For larger organizations, costs ran to tens of millions of dollars.

During the first half of 2018, malware designed specifically for IoT devices grew threefold over the same period in 2017, with over 120,000 modifications of malware, according to research from IT security specialist Kaspersky Lab.

The study reveals that the growth of malware families for smart devices is snowballing and "part of a dangerous trend that could leave consumer devices vulnerable to illegal activity including cryptocurrency mining, DDoS attacks, or being used in large scale attacks by becoming part of a botnet".

The company has set up its own honeypots to lure cybercriminals and analyze their activities online. Of the wide range of compromised devices used by the cybercriminals to attack the honeypots, routers were used most often, the source of 60% of attacks. The remaining attacks were carried out by a variety of devices including DVRs and printers. Surprisingly, 33 attacks were even carried out by connected washing machines.

David Emm, Principal Security Researcher at Kaspersky Lab, says: "For those who think that IoT devices don't seem powerful enough to attract the attention of cyber criminals, and that they won't become targets for malicious activities, this research should serve as a wake-up call."

Fragile consumer trust

Although few consumers have a detailed understanding of IoT security threats, major incidents and constant media coverage has made the vast majority aware of, and concerned about, them. A survey carried out for the Smart Home Forum 2018 shows that consumers' biggest fear about living in a smart home is hacking (felt by 62%). Only 22% trust smart home technology, and around half are even unsure if it is a positive development. Most do not know where to turn for advice – and when they do seek help, 35% rely on friends and family, who are unlikely to be experts.

Another consumer study by F-Secure has uncovered an 'early adopter paradox', where even those most eager to purchase new connected devices tend to delay or avoid new IoT purchases because of privacy or security concerns.

Based on nearly 20,000 consumer interviews in the US and Europe over the last five years, the study finds that homes are getting 'smarter', with nearly one in four US homes use a digital assistant such as Amazon Alexa or Google Home, a category of products that did not exist in 2015. And early adopters love the IoT, with 9 out of 10 saying that they are excited about the technology. But two-thirds of them have delayed making new purchases of smart home devices because of privacy concerns.

Tom Gaffney, F-Secure's Operator Consultant says, "Consumers are moving to connected devices both by choice, to enhance their lives, and also by necessity, given that it's almost impossible to find a TV that isn't considered 'smart' today. But, these numbers might be even higher if consumers, especially the consumers most open to considering new technology had more confidence in the IoT."

Gaffney adds, "Early adopters' worries about protecting their personal data are valid, considering the current issues challenging devices that stay online all the time yet aren't normally secured in the way the most PCs and many smartphones are."

Building business confidence

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

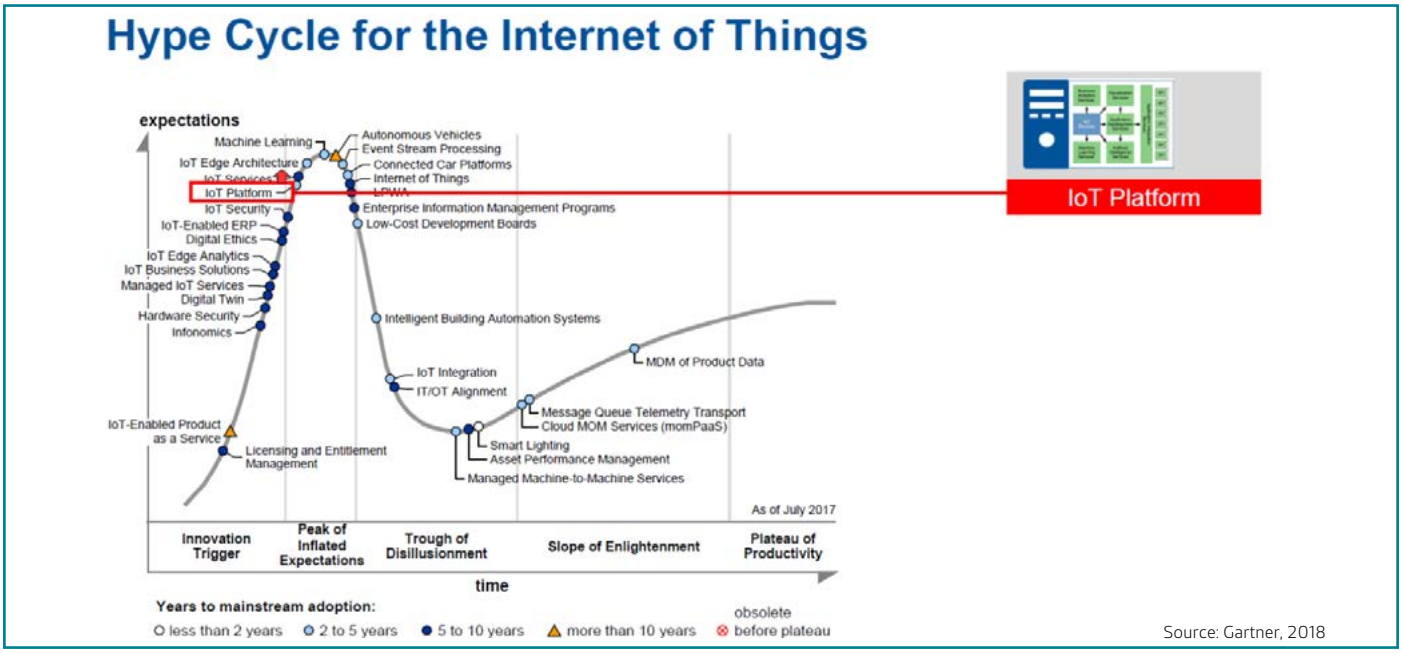
According to Kaspersky's Emm: "At this point, even if vendors improve the security of devices currently on the market, it will be a while before old, vulnerable devices have been phased out of our homes. In addition, IoT malware families are rapidly being customized and developed and, while previously exploited breaches have not been fixed, criminals are constantly discovering new ones."

If implemented correctly, the IoT can deliver securely, but how do manufacturers build consumer trust and business confidence in the face of such threats? Immediate measures to reduce the security risk include:

- Always changing pre-installed passwords, replacing them with complicated passwords that include both capital and lower case letters, numbers and symbols
- Installing updates for firmware as soon as possible. Once a vulnerability is found, it can be fixed through patches within updates
- Rebooting a device as soon as it begins acting strangely, which might help remove existing malware, although it will not reduce the risk of getting another infection

While the IoT clearly has the potential to undermine organizational resilience, it is also part of the solution, acting as a huge enabler in the key areas of information resilience, operational resilience and supply chain resilience.

Infoblox's Cox observes, "Networks need to be a frontline defence – gaining full visibility into all connected devices, whether on premise or while roaming, as well as using intelligent DNS solutions to detect anomalous and potentially malicious communications to and from the network, can help security teams detect and stop cyber criminals in their tracks."



Source: Gartner, 2018

The IoT and resilience

The IoT clearly has the potential to undermine organizational resilience through security breaches or poor interoperability. However, if implemented correctly, it is also a critical part of the solution, acting as a huge enabler in the key areas of information resilience, operational resilience and supply chain resilience. The ability to monitor and control a huge number of factors almost instantly anywhere in the world, and to spot trends through analysis of the data collected, can help build agility and efficiency, and develop differentiated solutions.

In short, the IoT is both the 'bad guy' and the 'good guy'. And BSI can help you build a resilient organization to capture the opportunities the IoT presents, while minimizing your risk.

Assurance solutions from BSI

Experts agree that the IoT threat to consumers has been allowed to increase because of inadequate security policies, regulations and end-user education.

But welcome change is now in the air. In the US, the state of California recently passed a law effectively banning weak and default passwords in devices, perhaps a step towards global regulation. In the UK, the Government and industry have launched a collaborative approach to protect consumers while continuing to support and foster innovation, but has indicated that it may regulate the IoT industry if voluntary regulation fails.

In October 2018, the DCMS published practical guidance to ensure that consumer IoT products are designed with security in mind, and to help users make their devices more secure. The code – which contains 13 guidelines for securing IoT devices – was developed in conjunction with the National Cyber Security Centre (NCSC), and endorsed by the IoT Security Foundation, of which BSI is a member.

How BSI can help

BSI is the only organization currently set up to independently verify or certify compliance with the Code. Organizations need the assurance of robust information security standards that provide ongoing, lifetime resilience. 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.

BSI Kitemark certification

BSI has a world-class cyber security capability, recognized by CREST global accreditation, combined with decades of experience in product assurance and testing. Through a collaborative approach based on extensive dialogue with stakeholders, and incorporating the Government's Code, BSI has developed a solution, IoT Kitemark certification.

The BSI Kitemark helps consumers to 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 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.

Verification

Security should be an essential part of the design process for all consumer IoT products. BSI works with its clients to verify their compliance with good IoT security design practice. Through BSI's verification service, organizations can demonstrate to their customers that products are secure for their intended use.

Testing

BSI's highly skilled team, operating in its state-of-the art IoT laboratory, provides fast, effective testing for a huge range of IoT products. BSI works with makers of IoT devices who put the safety and security of their customers at the heart of their business. 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.

It's time to act...

There are safe ways to adopt the IoT that will build consumer trust, business confidence and organizational resilience. BSI can help you implement them. Now is the time to act.

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 opportunity and risk, visit **bsigroup.com**