The Internet of Things (IoT) has exploded into the connected world and promises much: from enabling the digital organisation, to making domestic life richer and easier. With those promises come the inevitable risks: the rush to adoption has highlighted serious deficiencies in both the security design of IoT devices and their implementation. Coupled with increasing governmental concerns around the societal, commercial and critical infrastructure impacts of this technology, the emerging world of the IoT has attracted significant attention.

**SECURING THE IOT**

**TAMING THE CONNECTED WORLD**

The Internet of Things (IoT) has many definitions ranging from “systems that involve computation, sensing, communication, and actuation” (NIST) to “the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment” (Gartner). IoT devices are characterised by connectivity, physicality and sensors, and they are often further defined as either consumer IoT or industrial IoT. These terms will be used throughout this paper, but it is acknowledged that this is a fast-changing area of technology with devices that may have multiple uses.

The IoT is often perceived as new and cutting edge, but similar technology has been around since the last century. What has changed is the ubiquity of high-speed, low-cost communication networks, and a reduction in the cost of compute and storage. Combined with a societal fascination with technology, this has resulted in an expanding market opportunity for IoT devices, which may be broadly split into two categories: consumer and industrial IoT.

**ABOUT THIS BRIEFING PAPER**

The IoT can be broken down into consumer-orientated products and industrial-orientated products; however, Member organisations can face risks from both these aspects of the IoT as it enters the workplace by design and also by stealth. It is important that information security functions take a proactive approach to this potentially poorly secured world and ensure that the IoT does not represent a weak spot in organisational defences.

Based on external and Member research (supplemented by a short series of special interest group meetings held in Finland, the Netherlands and the United Kingdom), this ISF briefing paper explores:

- definitions of the IoT
- technical characteristics
- fundamental security issues
- emerging security practice
- legal and regulatory landscapes.

**DEFINING THE INTERNET OF THINGS**

The Internet of Things has many definitions ranging from “systems that involve computation, sensing, communication, and actuation” (NIST) to “the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment” (Gartner). IoT devices are characterised by connectivity, physicality and sensors, and they are often further defined as either consumer IoT or industrial IoT. These terms will be used throughout this paper, but it is acknowledged that this is a fast-changing area of technology with devices that may have multiple uses.

The IoT is often perceived as new and cutting edge, but similar technology has been around since the last century. What has changed is the ubiquity of high-speed, low-cost communication networks, and a reduction in the cost of compute and storage. Combined with a societal fascination with technology, this has resulted in an expanding market opportunity for IoT devices, which may be broadly split into two categories: consumer and industrial IoT.
1 Consumer and industrial IoT

The consumer IoT

The consumer IoT (sometimes known as the “Internet of Toys”) comprises a set of connected devices, whose primary customer is the private individual or domestic market. Typically, the device has a discrete function which is enabled or supplemented by a data-gathering capability through on-board sensors and can also be used to add functionality to common domestic items, such as refrigerators.

The ‘smart’ home, encapsulates many of the characteristics of the consumer IoT, featuring a multitude of connected devices and providing a previously inaccessible source of data about consumer behaviour that has considerable value for organisations.

Whilst the primary target market for IoT devices is individuals and domestic environments, these devices may also be found in commercial office premises – either an employee has brought in the device or it has been installed as an auxiliary function (e.g. a smart coffee machine).

The applicability of consumer IoT devices for both the domestic environment and the commercial workplace is illustrated in Figure 1.

Figure 1: The consumer IoT in a domestic and office environment

ISF Member organisations may be involved in the direct manufacture of consumer IoT devices, the supply of components to manufacturers, the development of related software products or the retailing of consumer IoT devices. Other Members should expect to find these devices within corporate environments.
The industrial IoT
The industrial IoT encompasses connected sensors and actuators associated with kinetic industrial processes, including factory assembly lines, agriculture and motive transport (the term cyber-physical systems is also used). Whilst these sensors and actuators have always been prevalent in the context of operational technology (OT), connectivity and the data processing opportunities offered by cloud technologies mean that deeper insight and near real-time feedback can further optimise industrial processes. As a consequence, industrial IoT is seen as core to the digitisation of industry.

Examples of industrial usage relevant to the IoT are illustrated in Figure 2. These extend from manufacturing environments, transport, utilities and supply chain, through to agriculture.

Figure 2: Possible uses of the industrial IoT

Opportunities associated with the IoT
Consumer IoT products often focus on convenience or adding value to services within a domestic or office environment, focusing on the end user experience and providing a rich data source that can be useful in understanding consumer behaviour. Meanwhile, industrial IoT deployments offer tangible benefits associated with digitisation of processes and improvements in supply chain efficiencies through near real-time monitoring of industrial or business processes. Examples of the use of both consumer IoT and industrial IoT are presented on page 4.
CONSUMER IOT

Smart appliances
Improves usability and customer satisfaction in domestic settings, allowing advancements in product formulation from data captured on consumer behaviour.
Creates an attractive office environment from the use of smart appliances in common areas, such as tea and coffee points, and may be installed by outsourced service providers.

Health tracking
Provides health benefits from the use of fitness trackers to allow individuals to monitor and improve their health.

Smart meters and home heating systems
Enables the consumer to intelligently manage their home power consumption. Provides the capability for utility companies to incentivise power usage in low demand periods, increasing overall efficiency.

Caring for an elderly population
Supports vulnerable people by using IoT devices to proactively monitor elderly populations, enabling them to maintain a more independent lifestyle.

Security systems
Secures domestic and commercial office premises through connected and video-enabled devices, which can be remotely monitored.

INDUSTRIAL IOT

Smart farming
Facilitates crop management at a micro granular level, for example, at a plant versus field level, with increases in yield and a decrease in the use of fertilisers due to highly targeted application.

Real-time fuel management
Optimises fuel consumption through the deployment of IoT devices for transport fleets, such as shipping, so that overall organisational consumption of fuel can be managed with financial and environmental benefits.

Supply chain
Enables the more efficient management of supply chain due to improved visibility, allowing leaner and more efficient processes to be developed.

Transportation
Creates an enabling infrastructure for passenger management by revealing actual usage of facilities and travel patterns.

Governmental planning
Informs town and city planning, such as roads and hospitals, through data captured via smart cities initiatives.

IoT devices have also been used for controlling purposes in abusive domestic relationships.¹ The term 'gaslighting' is sometimes used to refer to this situation – a reference to a 1930’s play about domestic abuse.

2 Technical characteristics of the IoT

The IoT, both consumer and industrial, shares many technical characteristics with information technology (IT). However, there are important differences.

ARCHITECTURE

Consumer IoT devices are often battery powered. Minimising the power consumption of the device is therefore an important consideration that will determine the architecture, including communication protocols used and the viability of security controls such as encryption and patching. Protocols such as Zigbee, Bluetooth LE or LoRaWan are preferred for battery powered devices, whereas devices with a mains supply are more likely to adopt mobile network spectrums (such as 3, 4 or 5G) or Wi-Fi connectivity. The usability of the device is also a key consideration and can be reflected in its architectural and technical characteristics.

Industrial IoT devices tend to have different constraints, reflected in their design. Many are installed in hostile industrial environments, demanding a more sophisticated technology approach. They often are required to interface with, or use, legacy protocols. Isolating these OT environments from other environments can also be important to maximise their availability and to prevent malware leakage from IT environments, which can be more tolerant to outages. In contrast to the consumer IoT, integration of industrial IoT devices into management systems is often a requirement.

With the advent of the IoT comes an associated explosion in the amount of data that is available to organisations. This has led to a renewed interest in architectures that support artificial intelligence, data analytics, augmented reality and edge/fog computing.2

A common solution architecture that can be applied to both the consumer and the industrial IoT is illustrated below:3

<table>
<thead>
<tr>
<th>SENORS AND ACTUATORS</th>
<th>HUBS AND GATEWAYS</th>
<th>EDGE PROCESSING</th>
<th>DATACENTRE/CLOUD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture</td>
<td>Aggregation</td>
<td>Analytics</td>
<td>Consumption</td>
</tr>
<tr>
<td>Sensors capture information and actuators make things move.</td>
<td>In a number of cases, hubs and gateways are used to aggregate information. This functionality may be closely located to the physical device or constitute on-board functionality of the device.</td>
<td>As many devices are constrained in processing ability or power consumption, analysis of data is typically handled at a different level from the device.</td>
<td>The richness of the IoT world is in the datasets that are produced, and analysis of multiple datasets usually requires significant processing capability.</td>
</tr>
</tbody>
</table>

Consumer

Data is captured from on-board sensors such as GPS positioning, heart rate, step counters.

Aggregation is typically provided by an associated application (app) running on a different device, such as a smartphone.

Analysis may require the use of a PC or a virtual service provided by the device manufacturer.

The manufacturer may collate information from multiple sources to provide deeper insight into product usage and capability.

Industrial

Data is captured from sensors or actuators monitoring or running the process.

Aggregation will be performed by the Supervisory Control and Data Acquisition controllers (SCADA) or Distributed Control Systems (DCS) or local hubs.

Analysis is most frequently provided by a function outside of the OT industrial environment, such as local IT services, pertinent to the particular facility.

Often performed at an organisational level to create a data lake (cloud based), where fresh organisational insight can be revealed.

It is acknowledged that, especially for industrial environments, the compatible Purdue model for control hierarchy can also be helpful.4

It is important to note that there is a subtle delineation between Industrial Control Systems (ICS) and industrial IoT. ICS runs the machinery and uses supervisory systems (SCADA/DCS) to both control and monitor the process. Industrial IoT deploys sensors to capture additional data at a high volume and uses that data to provide added value to the process or to feed a data lake where new insight can be gained from analysis of that data. In reality, an industrial sensor or actuator may physically perform both tasks, but they are logically separate.

---

4 T. J. Williams, "Purdue Model for Control Hierarchy", ISBN 1-55617-265-6
TECHNOLOGY STACK
One of the core differentiators of the IoT environment, when compared to IT, is the complicated set of technologies and protocols that persist and must coalesce in order to provide an integrated IoT solution. This is true both of consumer and industrial devices.

For the consumer IoT, the devices tend to be particularly constrained in terms of power consumption (i.e. they are battery powered) and form factor (e.g. they are designed to be worn). The technology selected for the device will reflect those constraints – for example, a wearable device may require a ruggedised chip set and components that can survive exposure to water.

For the industrial IoT, many installations such as factories will have been in existence for decades using technologies or protocols that are deemed legacy items (such as Microsoft XP). Additionally, as many components will be bespoke or proprietary, there is often little commonality in the technology stacks.

The difference between the IoT and IT technology stacks can also be attributed to the inherent design principles of the IoT. Whilst IT is about processing relatively large amounts of data in a processor and power rich environment, IoT is about frequent processing of small amounts of data in a processor and power constrained environment. This difference is reflected in the network protocols used, such as User Datagram Protocol (UDP), which has fewer overheads than Transmission Control Protocol (TCP); application protocols that are optimised for the IoT such as Constrained Application Protocol (CoAP); and the use of specialised wireless technologies such as Long-Range Wireless Area Network (LoRaWAN).

The need to optimise existing protocols and to develop new ones to accommodate the needs of the IoT results in a large number of competing or overlapping technologies and protocols. This can make the task of integrating, securing and supporting the technology stack in an IoT deployment challenging.

FORM FACTORS
IoT devices are effectively connected computers, but their design is usually not that of a traditional PC. Many of the more familiar computer components (such as keyboard or screen) are missing or hidden for aesthetic, cost or practical reasons.

Consumer IoT devices range from the very small or wearable devices (e.g. watches or fitness trackers), where a keyboard would be impractical, to devices where the design and fashionability of the device precludes a screen (such as voice assistants) or the price point may simply be too low to incorporate an input or output capability. In many cases, the consumer IoT device is paired with an app (typically on a smartphone), which will allow some limited interaction with the device.

Industrial IoT devices may operate in extremely hostile environments and may need to be protected from heat or dust. Conversely, they may need to operate in very clean environments (such as clean rooms). In either case, components such as keyboards and screens can be fragile.

In both the consumer and industrial context, the IoT device does not gather data primarily via a traditional input or output component such as a keyboard or screen. Instead its main role is to gather data from embedded sensors and, therefore, input or output components are unnecessary for normal functionality. Even where there is a paired or controlling device, the IoT device form factor generally precludes traditional forms of security management such as input of a password or patching. Coupled with battery life restrictions and reduced functionality, these devices are often simply not capable of providing information that can be helpful in identifying security issues, such as event logging.

Many sophisticated Security or Network Operations Centres (SOC/NOC) will effectively be blind to IoT implementations as IoT may not support standard logging. However, IoT devices can capture potentially valuable information about a security event, and specialist event management software that is optimised for an industrial IoT environment is starting to come to market. The ISF report *Building a Successful SOC: Detect earlier, respond faster* may form a useful reference point.

---

3 Fundamental security issues

There are a number of security issues that are common to both the consumer and the industrial IoT.

🎉 TRUST

IoT devices are often part of a wider implementation that is key to the overall functionality. Few devices exist in isolation, and it is the internet component of the IoT that reflects that dependency. For a home or commercial office to be truly 'smart', multiple devices need to work in cooperation and for a factory to be 'smart', multiple devices need to operate and function as an intelligent whole. Whilst there are some exceptions to this, particularly in the consumer IoT, this reflects an immaturity in the implementation of (rather than a failure of) the final vision of a connected inter-dependent world.

As devices can come from different manufacturers, and there is a considerable complication of standards and protocols, many devices cooperate on the basis of trust. This is because they have no ability to validate incoming data or instructions from other devices, providing an inherent contrast to the growing popularity of 'zero-trust' models. It means that the devices can be vulnerable to forged or manipulated instructions and therefore to attempts to hack the IoT device itself or other directly or indirectly connected systems.

🎉 DESIGN

The IoT technical characteristics described previously preclude a number of security controls – such as encryption, authentication, certificate management, validation and logging – for reasons of practicality (such as battery life), aesthetics (such as form factor) or cost. Without these fundamental security controls in place, the capability of a device to be secured is very limited, and basic security design is often neglected as a consequence.

In the industrial IoT in particular, a design assumption is frequently made that the industrial operation is technically isolated from other systems and security controls are therefore not required. In practice, this design assumption is flawed and exposes the IoT devices, and connected ICS systems in that environment, to both internal and external threats.

🎉 UPDATEABILITY

The IoT incorporates a large number of use cases in both the consumer and the industrial modes, and the design lifetime of these devices will similarly vary according to those use cases. From the fashionable, relatively disposable, low-cost device that is quick to market and quick to be superseded by a new version, to the newly built smart factory that requires considerable investment, the life expectancy of a device can vary from six months to 30 years.

For a device that is expected to be obsolete in six months and whose functionality has a low criticality, the ability to update and patch that device may be perceived to be less important than for the device which supports critical national infrastructure over thirty years. The difficulties in being able to update and patch are common to both consumer and industrial IoT, and reflect lack of input devices, difficulties in access to the device, and the impact of downtime. The associated impacts however, can be dramatically different.

⚠️ VULNERABILITIES

There are countless different types of IoT devices on the market in both the consumer and industrial space, but removing the cover of the device often reveals a discrete number of components and manufacturers, such that the ecosystem is relatively homogeneous. This means that a vulnerability discovered in a single commonly used component can have an amplified effect and result in thousands of models of IoT devices sharing the same vulnerability.

An example of the homogeneity of the IoT device space can be seen in the Mirai botnet which caused significant damage in 2016. The vulnerability that enabled the exploit of IoT devices, including CCTV cameras and recorders, printers and routers, is often attributed to a vulnerability in a common component manufactured by Chinese company Hangzhou XiongMai Technologies, which was widely distributed to a large number of IoT device manufacturers.⁶

---

USABILITY
The target market for IoT is so vast that, for both consumer and industrial deployments, only a very low level of technical expertise can be assumed for the user. In the consumer market, the user is presumed not to be capable of tasks that are familiar in the IT world, such as resetting passwords, installing malware protection or configuring the device. Consequently, devices may simply not offer that capability. A device that is useable out of the box (plug and play) is typically the market requirement.

Similarly, in the industrial environment there will be a low tolerance for additional training for staff and those working in a fast-moving operational environment will not be motivated to spend time correctly setting up a new device. Such low expectations over setup and maintenance for IoT devices means that the security ‘bar’ is set at its lowest, if set at all.

LEGACY
IoT devices typically generate large quantities of small pieces of data from their sensors. To make best use of this data, and to infer information and value from it, it needs to be analysed and stored. This is not the job of the device itself (see the table on page 5) as they simply do not have the capacity to do this. External storage sources, such as cloud services, tend to fulfil this role. However, it is likely that over time manufacturers and smaller supporting cloud services will go out of business or fail to safeguard this data (particularly for devices with shorter lifespans), resulting in the data being lost or abandoned and inaccessible to the user. This will give rise to the ‘Internet of Abandoned Things’, with implications for both consumers and industry as valuable data and devices are rendered useless.7

CONNECTIVITY
By far the most problematic element for the IoT is connectivity between OT networks supporting IoT devices and IT networks supporting office-based IT. A particular weak point in security is where the consumer IoT, the industrial IoT and the OT and IT world combine and overlap as shown in Figure 3. This can be by design or by coincidence but can result in joined networks running significantly different protocols, different states of patching and different vulnerabilities, all creating an environment that is attractive to malware.

Office and IT networks that have consumer IoT devices installed on them (e.g. smart coffee machines or heating, ventilation and air conditioning units) may find that these devices constitute weak points that may be exploited on their network and used in a stepping stone attack.8

Conversely, for industrial environments, the relative lack of security of IoT devices makes them, and the industrial processes that they support, vulnerable to malware and attacks originating from a connected IT network. Whilst it is common practice to separate the networks (referred to as air-gapping), this can give a false sense of security since it is often bridged deliberately (to enable additional functionality) or accidentally (e.g. sharing a printer between two networks).

There is commonality between the security issues mentioned above across consumer and industrial IoT, but they may manifest themselves in different ways, as summarised on page 9.

---

<table>
<thead>
<tr>
<th>CONSUMER IOT</th>
<th>INDUSTRIAL IOT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trust</strong></td>
<td>As instructional messages to actuators are often not authenticated, they can be altered by malicious actors who have gained access to the network resulting in unplanned kinetic movement of equipment and compromise of safety.</td>
</tr>
<tr>
<td><strong>Design</strong></td>
<td>Design parameters often assume that the device operates in a separated and protected environment, so software design may not contain the sort of validation and checking that is normal for externally facing IT systems. This can make the device, and the environment it is part of, susceptible to outages as the result of a denial of service attack.</td>
</tr>
<tr>
<td><strong>Updateability</strong></td>
<td>Many of the devices are intended to have short lifespans, and the manufacturer may neglect to install any update capability, resulting in an exposure to exploits that will compromise the device or render it obsolete.</td>
</tr>
<tr>
<td><strong>Vulnerabilities</strong></td>
<td>Industrial IoT components are often subject to certifications, which may preclude updates being applied (such as healthcare devices). Devices can also often form an integral part of an industrial process. Consequently, downtime for patching (or caused by failed patching) can be very problematic and result in a reluctance to patch and an associated exposure to attack.</td>
</tr>
<tr>
<td><strong>Usability</strong></td>
<td>Commonly sourced components can be exploited due to vulnerabilities or hidden or undocumented functionality (e.g. microphones) to extract personal or sensitive data.</td>
</tr>
<tr>
<td><strong>Legacy</strong></td>
<td>Vulnerabilities of IoT devices can be used to compromise more extensive connected networks, such as an electricity grid, as part of a stepping stone attack.</td>
</tr>
<tr>
<td><strong>Connectivity</strong></td>
<td>The market has a disproportionate number of small start-ups both in manufacture and in associated services such as cloud, exposing risks related to those parties going out of business, leaving the device useless and the data lost.</td>
</tr>
<tr>
<td></td>
<td>Operational costs related to training employees in set-up procedures result in security configuration tasks being neglected, with an associated exposure to exploits.</td>
</tr>
<tr>
<td></td>
<td>Although the industrial market is not dominated by start-ups, the long life expectancy of industrial equipment means that, over that time, manufacturers of industrial IoT devices will go out of business and support for the device will be terminated, leaving it unpatched and vulnerable.</td>
</tr>
</tbody>
</table>

4 Emerging security practice

The explosive adoption of IoT now has real momentum and powerful drivers, such as the digitisation of industry, behind it. There are successful use cases in both the consumer and the industrial realms, but also significant concerns regarding the risks.

Whilst there is insufficient maturity in this topic to talk about good security practice, conversations with Members, industry bodies and other stakeholders, indicate that there is a body of emerging security practice which Members may find helpful to review.

**ASSET DISCOVERY**

Key to managing the risk from both consumer and industrial IoT is to understand the degree to which IoT has gained a foothold into an organisation. As IoT is often not considered to be within the remit of IT, it can be procured without coming to the attention of the IT function (e.g. as an upgrade to an industrial process) or simply brought in by staff (e.g. voice assistants) and installed in the office. Creating and maintaining a basic asset register for IoT will enable a greater understanding of the risk areas but it does necessitate a thorough discovery exercise. Tools that can be helpful in discovering IoT include Shodan, signal discovery tools and specialised security event management tools that look for anomalies or protocols that are characteristic of IoT devices.

As consumer IoT may have entered the commercial workplace through informal means, it can create significant hidden vulnerabilities in environments that have previously been considered to be secure. This makes the task of asset discovery particularly important for office environments.

*Addresses fundamental security issue: Vulnerabilities*

**DIGITAL TWINNING**

Understanding the impact and vulnerabilities of IoT, especially within the industrial environment, can be challenging. The operational and safety-focused orientation of industrial and kinetic processes means that there is little tolerance for patching downtime, and a reluctance to update software for fear of disrupting the industrial process.

One of the solutions that is starting to emerge is digital twinning, where a virtual analogue of the industrial system is created and used as a test bed. Figure 4 shows an example of a digital twin in the automotive industry.

Other techniques that can be useful to address this problem include abstraction, where a simplified interface construct is used to analyse the behaviour of the IoT device.13

*Addresses fundamental security issue: updateability*

**MICRO-SEGMENTATION**

Network segmentation is a familiar concept to IT practitioners and micro-segmentation is essentially a fine-grained approach segmenting even down to the device or data level (the term pico-segmentation is also used).14 For the IoT, this can restrict communications between devices so that, for example, only medical IoT devices are permitted to talk to other medical IoT devices. This can address the issues associated with connectivity between IT and OT networks, and also provide containment in the event of an attack.

*Addresses fundamental security issue: connectivity*
SUPPLIER MANAGEMENT

As the risks associated with IoT have come to the fore, suppliers of IoT devices are being asked the question – is it secure? Often this is treated as a new requirement that demands significant effort to retrofit security into devices. Simply having an ongoing collaborative dialogue with key suppliers and vendors of IoT devices about security, in addition to ensuring that security requirements are built into procurement processes for industrial and office-based devices, will be beneficial in the longer term.

For Members that manufacture or retail IoT devices, it is increasingly important that they have an end-to-end understanding of the security of the components and software used within those devices, from the chipset used, through to software design and the end product. Penetration testing of devices should also be part of the product development lifecycle.

Addresses fundamental security issues: design, trust

CERTIFICATION AND LABELLING

For manufacturers of IoT devices, both in the consumer and industrial areas, there is considerable pressure from governments and regulators to adopt a certification or labelling regime such that the security level of the device is visible, including details of vulnerabilities. For the consumer, this will provide an informed choice and should encourage the adoption of security principles in consumer devices. For industry, particularly where the device is part of a safety-critical operation, this is more familiar territory and existing standards for industrial control systems (such as IEC 62443-3-3:2013) already include similar measures. An international approach to labelling and certification would be preferable, and for Members who supply or retail these devices, there is currently an opportunity to influence the outcome of these discussions.

Addresses fundamental security issues: design, vulnerabilities

COMMUNICATION

In the IoT context, two worlds collide – that of IT and OT. Both have their experts, both have their philosophies. Creating an awareness of the issues that occur when IoT devices become connected, in both the office and the industrial environments, will undoubtedly lead to more aligned and more secure deployments. But this extends further than the functional departments. Plant operators need to understand how an IoT deployment works, and that it can also be subverted and attacked from outside that plant. Similarly, train drivers, ship captains, and pilots need to know when they should not trust the readings on their dials, how to react to a cyber incident and what actions to take. People are part of the IoT and need to be included in any strategy.

Addresses fundamental security issues: trust, usability, legacy

AVAILABLE REFERENCE RESOURCES

Whilst the emerging security practice does not directly tackle all the issues, it does provide a helpful starting point. There is also a useful and growing set of guidance emerging from industry bodies that should be a source of reference for Members, including the documents listed below:

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CSA</td>
<td><a href="https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework">https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework</a></td>
</tr>
</tbody>
</table>
5 Legal and regulatory landscapes

Whilst the IoT has arguably been in development since the last century, the accelerated growth of the IoT is a more recent phenomenon. It has exposed new risks to consumers, industry, and particularly to national infrastructure. Concerns around the lack of security in these areas have spurred regulators and legislators into action.

GOVERNMENTAL CONCERNS REGARDING IOT

A growing understanding at the governmental level of the weaponisation of cyber attacks by nation states has resulted in significant concern about the resilience of critical infrastructure and smart city initiatives. This includes utilities such as electricity and water, transport infrastructures and even military capabilities.

The way in which IoT can undermine existing security models – providing weak spots for attackers to target, and exposing existing, previously isolated, infrastructure to cyber attack – has amplified government attention across the world on the vulnerabilities associated with IoT.

A legal and regulatory regime is a likely outcome of governmental concern, but the resulting country-specific regulation and legislation may prove problematic for IoT device manufacturers seeking a single set of global standards that they can adhere to. It is expected that internationally recognised standards (such as ISO) will emerge in the longer term that will help to resolve potential inconsistencies, but in the interim, multiple and conflicting requirements will be the norm.

The ISF briefing paper Information Security in Smart Cities provides an overview of vulnerabilities associated with smart cities and the Internet of Things.

PRIVACY

Many consumer IoT devices (especially fitness and healthcare devices) are capable of acquiring significant amounts of sensitive personal data from an individual and sending that data to cloud services for processing by organisations, raising a number of concerns related to privacy. The low level of security controls adopted by these devices also makes sensitive personal data (often of vulnerable people, such as children) further exposed to hacker attacks.

The high degree of technical innovation associated with the IoT is expected to lead to new legal challenges in upholding personal privacy. Already, the concept of a personal area network (where multiple, wearable IoT devices build a digital picture of an individual in real time) has been established. The prevalence of sensor technology that can read an individual’s ‘digital aurora’ as they go about daily life has raised considerable concerns around tracking of individuals and the legal implications of that tracking (not just in terms of the use of personal information, such as selling it to third parties, but also the consequence of revealing sensitive military locations and other classified information).

Driven by strong research activity in this area, there has been a substantial media focus on these privacy issues and, coupled with the EU General Data Protection Regulation, this has further spurred regulatory interest in the privacy of IoT devices.

EMERGING GUIDANCE, REGULATION AND LEGISLATION

Guidance on securing the IoT has been forthcoming from a considerable number of bodies including ENISA, NIST and multiple governments, as well as from industry bodies such as the Internet of Things Security Foundation. Many governments are consulting on converting these guidelines into mandatory requirements and considering consumer labelling schemes for security.

Emerging legislation related to the IoT includes:
- Security of Connected Devices Act (California, USA) – enacted legislation which requires unique passwords for IoT devices
- Cyber Security Act (EU) – enacted legislation which sets up a security labelling scheme for IoT devices
- Mandating security requirements for consumer Internet of Things (IoT) products (UK) – proposed legislation on various aspects of IoT security.

One characteristic of IoT devices, particularly when there is a high safety-related component, is that existing safety guidelines and product recall requirements will also be applicable in addition to IoT-specific requirements. Manufacturers of healthcare-related devices and dual-use devices (devices that have multiple use cases) may find that there is a growing burden of regulatory requirements for such devices.

---

**LIABILITIES**

The legal liabilities associated with IoT devices are relatively untested.\(^{17}\) Whilst IoT devices are generally tangible products, the software that controls their behaviour is intangible, and that software enjoys a less rigid legal framework, being largely exempt from product liability laws.

For interconnected consumer devices, such as those in the IoT, the situation is more complex. The parties to a single device may include multiple hardware manufacturers, software designers, retailers and white label (rebranding) companies, all based in different jurisdictions. For industrial devices, the consequence of failure can be far reaching – a kinetic accident may well result in fatalities – and here the law is equally unclear on liability. What is clear is that legal redress tends to follow the money, so the company most likely to be sued is the one with the most money in this complex nexus.

The lack of clarity regarding how the law applies to IoT devices is likely to encourage test cases against IoT providers, and ultimately may lead to a fundamental revision in product liability laws. Until that time, uncertainty around the legal liabilities of IoT devices will remain.

**CYBER INSURANCE**

As the IoT becomes a reality for consumers and a core part of industry digitisation, the dependencies and liabilities give rise to new risks. As a consequence, the insurability of these risks needs to be taken into account. It is already apparent from external research that the impact of the IoT on the insurance market will be significant and wide ranging.

Research commissioned on the IoT notes fundamental changes to underwriting and pricing models driven largely by the accessibility of IoT data on customer behaviour.\(^ {18}\) Coupled with improvements in safety-related IoT devices in high-risk industrial environments, this is expected to move the insurance industry to a data-driven real-time model that has significant implications for capital reserves.

Foreseeable developments include transformative IoT initiatives, such as driver telematics enabling pay-as-you-go insurance models, as well as new insurance liabilities encompassing everything from everyday consumer IoT devices, to national transport structures and utilities.

---


6 Taming the Internet of Things

The Internet of Things has become a reality and is already embedded in industrial and consumer environments. It will further develop and become a critical component of not just modern life, but critical services. Yet, at the moment, it is inherently vulnerable, often neglects fundamental security principles and is a tempting attack target. This needs to change.

There is a growing momentum behind the need for change, but a lot of that momentum is governmental and regulatory-focused which, history tells us, can be problematic. The IoT can be seen as a form of shadow IT, often hidden from view and purchased through a non-IT route. Hence, responsibility for its security is often not assigned or misassigned. There is an opportunity for information security to take control of the security aspects of the IoT, but this is not without challenges: amongst them skills and resources.

Nevertheless, there is a window of opportunity to tame this world, by building security into it. As most information security professionals will know, this represents a cheaper and less disruptive option than the alternative.

WHERE NEXT?
The ISF encourages collaboration on its research and tools. ISF Members are invited to join the Securing Industrial Control Systems community on ISF Live to share experiences and discuss security implications of the IoT.
ABOUT THE ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

WARNING

This document is confidential and is intended for the attention of and use by either organisations that are Members of the Information Security Forum (ISF) or by persons who have purchased it from the ISF direct. If you are not a Member of the ISF or have received this document in error, please destroy it or contact the ISF on info@securityforum.org. Any storage or use of this document by organisations which are not Members of the ISF or who have not validly acquired the report directly from the ISF is not permitted and strictly prohibited. This document has been produced with care and to the best of our ability. However, both the Information Security Forum and the Information Security Forum Limited accept no responsibility for any problems or incidents arising from its use.

CLASSIFICATION

Restricted to ISF Members, ISF Service Providers and non-Members who have acquired the report from the ISF.