IoT NOW
ANALYST REPORT

SECURE IoT

How common guidelines will address the vulnerabilities

The authors are **Saverio Romeo**, principal analyst and **Dr. Therese Cory**, senior analyst, at Beecham Research

Secure IoT through common guidelines and context-awareness

Security is critical to the success or failure of the Internet of Things (IoT) vision. Critical flaws at the heart of the internet, such as the Heartbleed bug, have highlighted engineering fallibility. The successful attacks in industrial applications, such as Stuxnet, have highlighted hidden aspects of cyber warfare. In addition, attacks on consumer IoT devices such as smart home devices – connected lighting and connected baby monitors, for example – have emphasised the broad capability of attacks and their immediate impact on consumers' fear.

As the Internet of Things vision becomes the driving paradigm for changes in society and in economic activities, increasingly, the vulnerability present in that change requires attention. Facing that vulnerability through a strategic and multidisciplinary approach for IoT security is not an easy task for the community of cybersecurity experts, IoT experts and policy makers and ethicists.

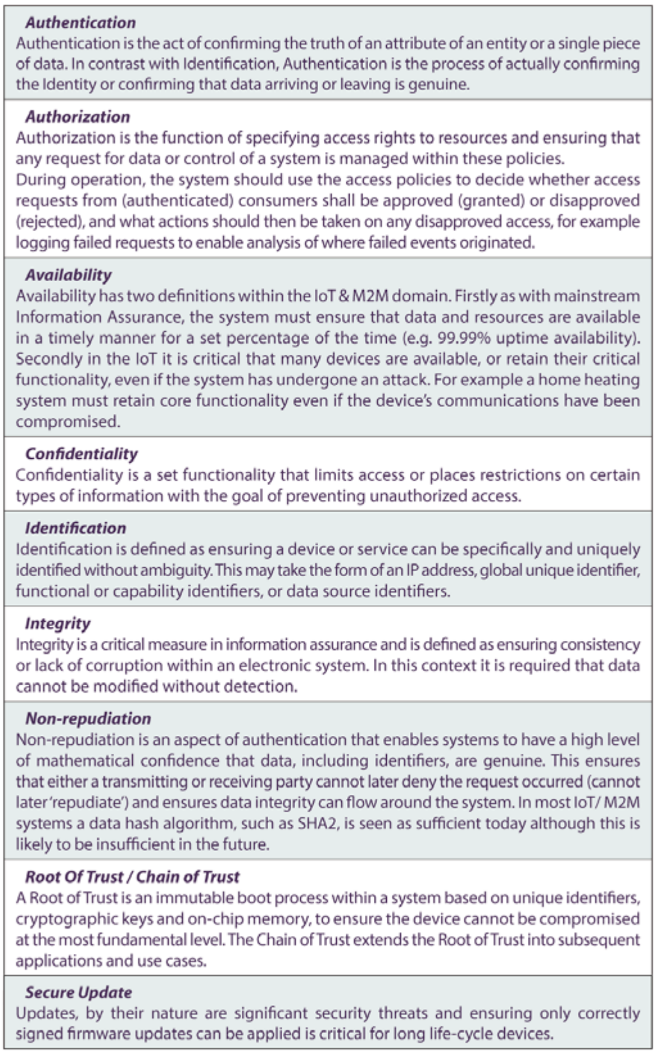
Cybersecurity is an engineering and scientific area of great complexity, but, with an extraordinary impact on governments, consumers and businesses. Therefore, building a bridge between cybersecurity experts and organisations and individuals vulnerable to attacks is necessary. This Insight Report discusses IoT security in the smart home as a consumer IoT context, in the industrial internet as an intensive enterprise IoT context; and in the smart city as a government-led context.

The Insight is structured in five sections. The first section will introduce the main concepts and challenges in providing security for the IoT. The next four sections will discuss approaches to security in smart homes, industrial internet and smart cities. The last section will provide some concluding remarks.

IoT security- concepts and key challenges

Defining security is an ambitious task. The concept of security encompasses nine key elements as shown in **Figure 1.**

Figure 1. Essential pillars in security



Authentication
Authentication is the act of confirming the truth of an attribute of an entity or a single piece of data. In contrast with Identification, Authentication is the process of actually confirming the Identity or confirming that data arriving or leaving is genuine.

Authorization
Authorization is the function of specifying access rights to resources and ensuring that any request for data or control of a system is managed within these policies.
During operation, the system should use the access policies to decide whether access requests from (authenticated) consumers shall be approved (granted) or disapproved (rejected), and what actions should then be taken on any disapproved access, for example logging failed requests to enable analysis of where failed events originated.

Availability
Availability has two definitions within the IoT & M2M domain. Firstly as with mainstream Information Assurance, the system must ensure that data and resources are available in a timely manner for a set percentage of the time (e.g. 99.99% uptime availability). Secondly in the IoT it is critical that many devices are available, or retain their critical functionality, even if the system has undergone an attack. For example a home heating system must retain core functionality even if the device's communications have been compromised.

Confidentiality
Confidentiality is a set functionality that limits access or places restrictions on certain types of information with the goal of preventing unauthorized access.

Identification
Identification is defined as ensuring a device or service can be specifically and uniquely identified without ambiguity. This may take the form of an IP address, global unique identifier, functional or capability identifiers, or data source identifiers.

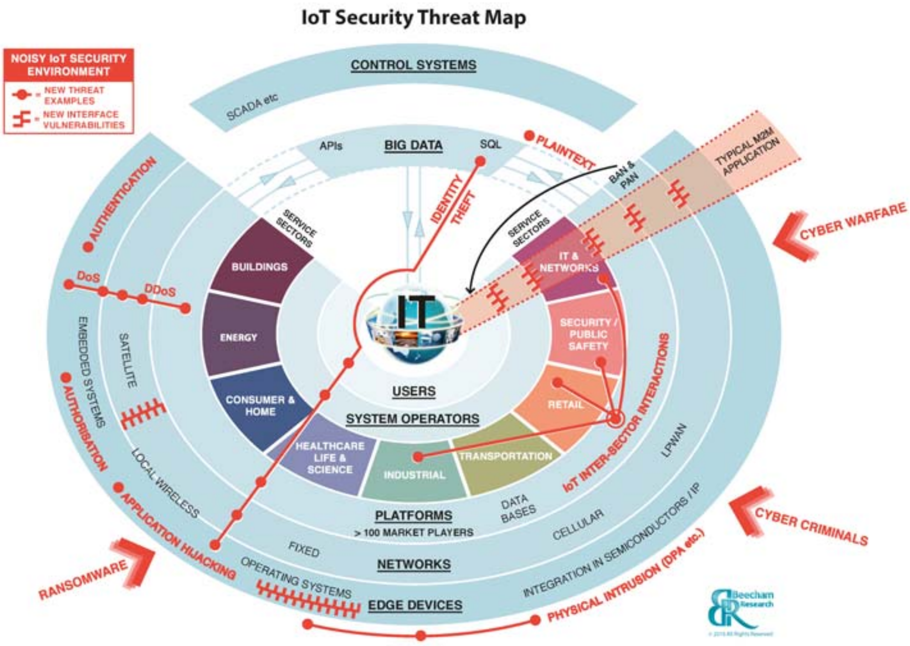
Integrity
Integrity is a critical measure in information assurance and is defined as ensuring consistency or lack of corruption within an electronic system. In this context it is required that data cannot be modified without detection.

Non-repudiation
Non-repudiation is an aspect of authentication that enables systems to have a high level of mathematical confidence that data, including identifiers, are genuine. This ensures that either a transmitting or receiving party cannot later deny the request occurred (cannot later 'repudiate') and ensures data integrity can flow around the system. In most IoT/ M2M systems a data hash algorithm, such as SHA2, is seen as sufficient today although this is likely to be insufficient in the future.

Root Of Trust / Chain of Trust
A Root of Trust is an immutable boot process within a system based on unique identifiers, cryptographic keys and on-chip memory, to ensure the device cannot be compromised at the most fundamental level. The Chain of Trust extends the Root of Trust into subsequent applications and use cases.

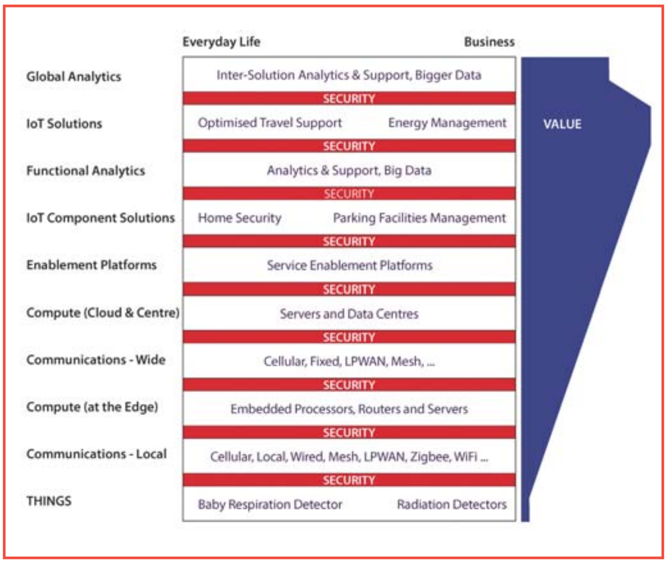
Secure Update
Updates, by their nature are significant security threats and ensuring only correctly signed firmware updates can be applied is critical for long life-cycle devices.

Figure 3. The Beecham Research Threat Map



In the evolving IoT market, security does not just refer to security of information, it expands into the entire complexity of the IoT vision. Before discussing in more detail the challenges in the IoT security, it is also important to highlight that security issues in the IoT strongly relate to privacy and trust issues. Having said that, it is important to stress that installing security capabilities does not necessarily imply the right to privacy and trusted relationships. Privacy and trust go beyond the technological domain into ethics and legislation. Therefore, an IoT security strategy should take into consideration multidisciplinary aspects to be effective.

Although this paper concentrates on the technological aspects of security in the IoT, it is important to deconstruct an IoT solution in its components to see the need for security. **Figure 2** shows the hierarchical level of an IoT solution.



	Everyday Life	Business
Global Analytics	Inter-Solution Analytics & Support, Bigger Data	
	SECURITY	
IoT Solutions	Optimised Travel Support	Energy Management
	SECURITY	
Functional Analytics	Analytics & Support, Big Data	
	SECURITY	
IoT Component Solutions	Home Security	Parking Facilities Management
	SECURITY	
Enablement Platforms	Service Enablement Platforms	
	SECURITY	
Compute (Cloud & Centre)	Servers and Data Centres	
	SECURITY	
Communications - Wide	Cellular, Fixed, LPWAN, Mesh, ...	
	SECURITY	
Compute (at the Edge)	Embedded Processors, Routers and Servers	
	SECURITY	
Communications - Local	Cellular, Local, Wired, Mesh, LPWAN, Zigbee, WiFi ...	
	SECURITY	
THINGS	Baby Respiration Detector	Radiation Detectors

Figure 2. Levels of hierarchy in an IoT solution

All the levels of an IoT solution need to be suitably secured but it is also important to assess the value of the different layers to ensure that costs and benefits are well understood.

More complexity is introduced when we see the Internet of Things vision as the enabler of interconnected smart contexts or spaces. The solution does not engage with the business problem on its own, using one type of device, one type of connectivity, one protocol and one set of data. There are several different devices, using different protocols, different types of connectivity and using different sources of data. The points of attack are therefore multiplied as shown in the Beecham Research Threat Map in **Figure 3**.

The enormous challenge for the IoT strategy and solution designer is using the Threat Map to identify the right approach to protect the smart context in which they operate. The next sections will explore how this happens in three spaces: the home, industrial plant, and the city.

Security for the smart home

Vulnerabilities in the smart home environment

The internet now pervades nearly every aspect of our lives. The many benefits IoT promises to bring include better, faster automation, greater insight and improved user interaction with products. The place most people will feel this impact will be at home, where connected appliances, televisions, lighting and heating systems are already finding space in everyday households.
Virtually any consumer electronic device can be made smart by being fitted with a powerful embedded computer designed to be always on and networked via the internet. This brings many advantages, but it does increase the potential attack surface.

There is therefore a very real concern about security, and ▶

again there are few places that raise greater security concerns than within our homes. But what are the implications for consumers if any of the devices used in the home is hacked? Many home networks are different to enterprise infrastructure and traditional information that security solutions were developed for. This makes securing the smart home a different kind of challenge, one with its own unique vulnerabilities and threats, many of which are still unknown.

A true web of things introduces connections between multiple systems at multiple touch points. Whilst the benefit of the additional connections is adding value, this complicates the security landscape. In addition, the connections between the systems are not always secure. The smart home is the intersection point of many systems including vehicles, energy grids, media streaming and physical security. An exploitable vulnerability within the home could lead to more serious breaches in any of the systems it touches.

Because smart homes are a key point of interaction between people and technology, securing this environment requires social, political and economic input perspectives.

There are two broad types of smart home infrastructure. The first scenario stems from the earlier days of building automation which depicts an environment where there is a single system, sometimes integrated into the building at the time of construction. This is then fed and managed by a single supplier.

However, with the rise of intelligent smart home hubs, another model has emerged where the control hub coordinates all of the devices. This aims to add value through the synergistic properties of bringing the separate services together under one roof. It also addresses the majority of users' dislike of multiple proprietary applications for their numerous products.

What is expected to become more prevalent is the emergence of an environment that lies somewhere between these two scenarios, with the added complexity of devices communicating with one another within the home, without the internet but instead via new connectivity protocols such as Bluetooth, 6LowPAN, ZigBee and Z-wave.

How to introduce security in the smart home

The smart home environment exposes three main vulnerability areas: end user expertise, business models and pervasive and persistent insecurity. What can be done therefore, to create a secure smart home? Beecham Research believes three types of guidelines should be followed in order to address security shortfalls: technology, policy and support services.

Technology

The first step is to ensure that all data must be encrypted, rendering it unreadable to intruders. Dynamic encryption keys should be used wherever possible, alternatively static keys must be well protected. This becomes a challenge particularly within mobile applications used to control the connected products. Data encryption should be the responsibility of all those members of the solutions chain that handle the data, from the OEM collecting the data, the service provider transporting the data and the cloud provider hosting the data. Crucially also, the connections between these parties must be secure, as outlined in the threat map.

Smart home systems therefore must be secure by design. This must extend across products and services, as well as through the entire supply chain. Ensuring a secure design across the entire smart home ecosystem will emphasise the fact that responsibility for security does not lie solely with the home owner.

Policy

Equally important are the processes by which security features are specified, designed, implemented and operated. The best IoT practices rely on security policies to be properly implemented across hardware and software, protecting data at rest and in transit, and therefore must be applied across the entire IoT service – user applications, data centre servers, network gateways and the devices themselves.

Support services

The speed of technological innovation has led to shortened lifecycles of many electrical goods, predominantly because processing power increases have meant that old hardware cannot support newer software. As a result, software support is being abandoned much sooner than previously anticipated. Vendor support for software and operating systems are vitally important, especially for security, where many updates include vulnerability patches.

Future business models

The evolution of the smart home has advanced significantly over the past three years, causing increased attention from different parties, ranging from traditional IT vendors (Microsoft, Cisco), start-ups (Notion, Ecovent) and mobile network operators (AT&T, Verizon Wireless) to home appliance manufacturers (Bosch, Siemens) and even ▶

governments. The market is still in its relative infancy in spite of being under development for many years, and therefore the predominant current business model focuses on shipping physical units.

Much of the opportunity for security revenue lies with OEMs at different levels – from chipset vendors, to vendors' in-house development teams. However, with the emergence of service offerings, there are greater opportunities, and even obligations, for service and cloud providers, mobile network operators and other third parties.

IoT security must be implemented with a layered approach, and this starts with the physical device. The vast majority of this security will be embedded, offering a similar hardware sales revenue model for security companies and chipset vendors.

In summary, it is worth noting that the smart home security market is slightly behind the curve compared with the smart home products and services market. Most security options are focused on the embedded security options, and are not yet addressing security services. This is in part due to the complexity of creating such a system, also it's in part due to the level of risk that a managed security service provider would be taking on, especially in the smart home vertical.

Hence the sector needs to do more to get ahead of the curve and be more proactive, compared with the reactive status it currently holds, waiting to see where the next major threat will be.

Security in the industrial IoT

What is the industrial IoT?

The Industrial IoT (IIoT) covers a long list of industries, ranging from manufacturing, mining, agriculture, chemical plant, petrochemicals, power grids, food and beverage production and allied services.

Manufacturing controls require the continuous measurement of a wide range of variables from a wide range of sources, making this ideal for wireless sensor technology, particularly for devices located in hard to reach places. Devices that form part of Industrial IoT networks are huge in number and growing all the time. Furthermore, reports of data loss and corruption, access intrusion and distributed (DDoS) denials of service have been growing at an alarming rate.

The IIoT has its origins in traditional industrial automation. In the past the focus in manufacturing has been on automating manual work processes. The industry now is characterised by the need for almost-zero error tolerances and ever more rapidly moving research and development cycles. The IIoT takes this further, utilising advances in software and data analytics to allow companies to make faster smarter decisions that optimise processes, and pass on these benefits to customers. This vision, known as the intelligent or smart factory, envisages a new way of organising manufacturing processes in which different parts – from suppliers to logistics to the entire lifecycle of the product or material – become closely and intelligently connected with the corporate boundaries.

Industrial automation is also tied into next generation manufacturing processes with the involvement of the internet. The term Industry 4.0 was first coined by a group of advisors to the German government on how to develop its technology strategy.

A typical factory may operate various production lines that involve a number of critical processes. By bringing intelligence to sensors either locally or through cloud computing, devices can be made to slow down or shut down processes to prevent major accidents.

Vulnerabilities in the industrial IoT environment

The timely transfer of, and taking correct actions based on, the information in a production line system depends on sufficient security protection. This is important in industrial IoT since most operations depend on the transmission and receipt of real-time data. Trustworthiness of data is key in industrial IoT; without sufficient security, there can be no trust.

Every element in the supply chain is at risk; in all cases, security must be designed in from the outset, not as a bolt-on afterthought. IIoT solutions are increasingly incorporating elements of security at different points, such as in the links between secured communication subsystems to ensure coverage of all parts of the supply chain. These may involve hardware, operating systems, embedded security and the application layer and other parts, and are being independently developed by several different supply chain players for a variety of needs.

The IoT is increasingly powering critical devices in industrial systems such as production lines and power grids, not to mention medical devices such as insulin pumps. The damage from failing to protect such systems will rise exponentially. Some of the highest risks from hacking of IIoT systems come from connected devices in widespread use, from computers, smartphones and various other smart devices. ▶

Recent risks have been identified as a consequence of internet technology becoming more complex and sophisticated, for example:

- The transition from IPv4 to IPv6 – the future IPv6 will reportedly support trillions upon trillions of devices, so assuring security will be a proportionately larger challenge

- There will be new protocols in addition to those utilised today, some more secure than others. Implementers will have to select the best-suited protocols for products and IoT enabled services. That said, no one device is 100% secure today

- The ever increasing number of networked devices some of which are remote or inaccessible increases their vulnerability to breaches

- Secure over the air firmware updates to IIoT devices are necessary but risky as they introduce points of vulnerability.

In September 2016, the Industrial Internet Consortium published a report detailing a security framework for the IIoT. The report states that five IIoT characteristics – safety, reliability, resilience, security and privacy will act as the pillars of trustworthiness in IIoT systems. It also defines risk assessments, threats, metrics and performance indicators to help business managers protect their organisations. To ensure end-to-end security, industrial users must assess the level of trustworthiness of the complete system, however achieving this in an industrial setting means dealing with many levels and dimensions of complexity.

How to introduce security in the Industrial IoT

There is no single approach to the implementation of security in all M2M solutions. Hence there are different security approaches being taken by different market sectors to address different threats, trust requirements, vertical markets, communications methods and more in the appropriate ways. There are also different levels of security that need to be implemented, depending on the severity of the security breach, with mission critical systems requiring the highest level of security.

Some of the main factors defining security include:

- **Confidentiality** – Ensure that data and activity is protected against unauthorised access

- **Authentication** – Confirm data arriving or leaving is genuine and identify the source and recipient. At the receiving end, permission must be granted to decrypt and utilise the data. Authentication ensures that only the permitted party is authorised to do so

- **Authorisation** – Ensure that any request is one that should be allowed – this depends on the ability of devices and services to come to reasonable decisions about the authenticity of the people and machines using them

- **A root of trust** – A set of unconditionally trusted functions, typically linked to a computing engine, because it must perform actions. M2M and IoT-connected devices are coming to depend on chips to establish their system's root of trust. Without a trustable base of hardware like a chip to build upon, seemingly perfect protections like secure boot can be compromised

Hence the imperative is to protect data – both at rest and in transit – by making sure that data sent across the cloud is always encrypted, all the way to the end application. Significant effort is therefore required in the identification, authentication and authorisation of all the above components as well as their users.

With the advent and spread of the eSIM, there are many existing SIM based use cases that are going to become more widely used for manufacturing IIoT security. Moreover, more use cases will be enabled by new roots of trust.

Smart city

What is a smart city?

The term smart cities refers to the broad concept of using technology to gather and analyse city data in order to increase efficiencies in city operations and improve quality of life for citizens. Broadly speaking, it brings together city activities ranging from networks of local businesses, local government to education, healthcare, transportation and utilities.

Each activity produces different sources of data that can be integrated, enabling a systemic view of the city. By collecting and cross-analysing large amounts of data from diverse sources, cities aim to understand the linkages between these different activities, and how integrating these systems may be exploited so that the city may understand how it works as a whole.

All cities are unique with their own priorities and preferences – so there is no single blueprint for architecting a smart city solution. How cities work is also changing. In the 21st century, their workings will be based on their digital infrastructure and the data generated from this. The big data that is captured and analysed from the broad range of connected objects will inform how this data is analysed, managed and used for decision making, so as to provide best value for the cities and their citizens. ▶

Vulnerabilities in the smart city environment

Security is defined as preventing illegal access to information with the ability to corrupt data, putting into doubt the integrity of the data itself and compromising its authenticity. It also protects against attacks that cause physical disruptions in the availability of city services. As digital citizens are more and more instrumented, with data available about their location and activities, privacy is eroded. Hence the legal concepts of a citizen's right to privacy are intertwined with the challenge of cyber security of the smart city.

Wireless sensors now control a growing portion of the city infrastructure from traffic lights to water management systems, and smart city applications are becoming ever-larger targets for cyber terrorists. To date, the kinds of devices typically deployed to run critical national infrastructures have relied heavily on the isolation of their networks, to avoid being breached. In parallel, whilst spending on smart city technologies and sensor networks has escalated, in many cases insecure legacy systems are involved, and connectivity to the internet opens the door to hacking. Moreover the more sophisticated the device, the higher the probability that it has vulnerabilities and/or configuration flaws, and smart city component devices will likely be targeted by cybercriminals.

In parallel, back office city infrastructures and functions are also changing with new interconnected systems for monitoring, control and automation.

Security in the networked city is significantly more complex than in existing M2M applications or traditional enterprise networks. The involvement of the cloud and the internet adds an additional dimension of risk compared with traditional embedded networked systems. As embedded devices become increasingly networked, extra measures must be taken to ensure overall security.

What is more, smart city infrastructures develop faster than security tools do. The scenarios of such attacks come from the characteristics of such devices: for one, many such devices are in public places, therefore accessible, and with an internet connection. They may process personal data including financial data. Examples include touch screen payment kiosks, cycle rental kiosks and government office terminals. However as research from the Securing Smart Cities Initiative shows, many such terminals do not have the reliable protection that prevents the user from exiting the kiosk mode and gaining access to the operating system functions.

According to IOActive for example, some 200,000 traffic sensors in cities around the world are vulnerable to a hack; these devices may communicate traffic information wirelessly through texts that fail to authenticate the data they receive, leaving them open. If the sensors in the devices are breached and hackers input fake data, this could potentially lead to widespread traffic jams or crashes.

City networks may also be vulnerable to threats from internal sources, such as infected devices city employees may bring to work. All-in-all, the current attack surface for cities is huge and wide open.

Identifying points of attack

In 2015, the National Institute for Standards and Technology (NIST) in conjunction with the Cyber Security Research Alliance (CSRA) hosted a workshop entitled 'Designed-in Cybersecurity for Smart Cities: A Discussion of Unifying Architectures, Standards, Lessons Learned and R&D Strategies'.

The workshop identified the following risks:

- The web of interconnected sensors and devices that define a smart city provide countless points of entry for an attacker seeking to compromise systems
- Cyberattacks may have physical consequences if smart cities rely on collected data to make automatic adjustments to real-world conditions. For instance, interfering with the traffic data relied on by traffic lights could lead to car accidents
- Smart city operations will involve the collection and storage of large amounts of data from many disparate sources, necessitating the use of cloud services. Smart city architects will need to ensure that data in transit as well as data in storage will be secure
- Smart city architectures will be composed of devices and sensors from different vendors, not to mention the hardware and software. Systems engineers will need to continually update the security settings for a diverse range of devices in order to ensure that a security flaw in one component does not compromise other parts of the system.

How to introduce security into the smart city
In May 2015, a group of security specialists, including experts from Kaspersky Lab and IOActive Labs launched a not-for-profit initiative entitled Securing Smart Cities. They claim that no comprehensive system as yet exists for vetting security and responding to cyberattacks at city level, and aim to remedy this by addressing existing and future cybersecurity problems of smart cities through collaboration between companies, governments, media outlets and other not-for-profit initiatives and individuals across the world.

The group plans to set up basic cybersecurity checklists for smart cities, including properly installed encryption, passwords and systems that can be easily patched for security holes. It also seeks to set up better security ▶

requirements and approval procedures for the vendors of these critical systems. In addition, it wants to run regular tests to look for loopholes, and set up emergency response teams that can compile reports of vulnerabilities, coordinate patches and share that information with other cities.

The organisation offers a smart city technology adoption guide that lays out guidelines for adopting smart city technology. As new points of connection are introduced, the city should have processes to methodically evaluate the security risks and appropriate mitigations for each connected system inside each organisation.

The Smart Cities Council has also published its Smart Cities Readiness Guide. This contains 27 foundational principles. Of those, 17 are universal principles that apply to every department. One of the most important is to have a citywide cybersecurity policy in place.

Security and privacy is defined as an enabler which cuts across all the city responsibilities. For example, where energy intersects instrumentation, there are devices such as smart meters. Where it intersects data management, there are meter data management systems (MDMS). With this type of structure, it is possible to understand why it is helpful to share infrastructure, share policies, share costs and share data between departments.

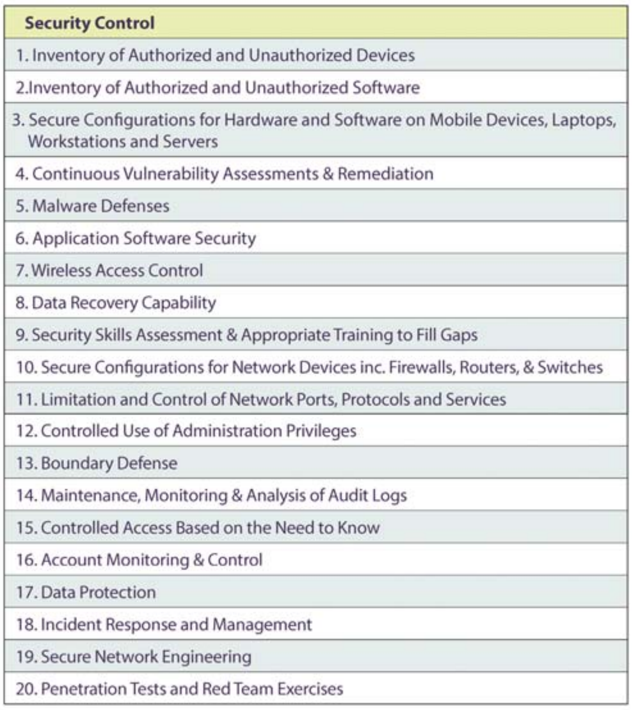
A city becomes truly smart when it takes a holistic, integrated view, when it shares infrastructure rather than duplicating functionality in each department and creates citywide policies: hence the importance of having a citywide cybersecurity policy across all functions.

Providing security through common frameworks and guidelines

This market insight has introduced the main concepts of IoT security and explored how security is approached in three contexts of great relevance for the market place. Even though the approaches are different because of the context in which they are applied, they provide the IoT community with a common message. To enable a safe, secure and robust Internet of Things it is critical that security can be achieved from end-to-end, from the servers and cloud services that are subject to tradition IT security measures all the way to the vast and diverse number of edge devices that will be deployed over the next 10-15 years.

To achieve that robustness, the industry should move along common frameworks and guidelines. The insight has shown how the segments analysed are exploring those. There is also an increasing attention on guidelines at national and super-national levels through initiatives such as the IoT Security Foundation in the UK and the Cybersecurity Strategy for the European Union. Among all those, the 20 Critical Security Controls – shown in **Figure 5** – defined by the Council of Cybersecurity, a non-profit organisation of cybersecurity experts with global scope, have become almost the de-facto set of guidelines for security in the IoT. ▶

Figure 5. 20 critical security controls by the Council of Cybersecurity



Security Control
1. Inventory of Authorized and Unauthorized Devices
2.Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
4. Continuous Vulnerability Assessments & Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Access Control
8. Data Recovery Capability
9. Security Skills Assessment & Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices inc. Firewalls, Routers, & Switches
11. Limitation and Control of Network Ports, Protocols and Services
12. Controlled Use of Administration Privileges
13. Boundary Defense
14. Maintenance, Monitoring & Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring & Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

The 20 critical security controls become particularly relevant in relation to the continuous emergence of edge devices, which are, currently, the component of the IoT vision perceived to be more vulnerable. The challenge is to provide devices with robust architecture, but still easy to use for end users. Therefore, the 20 controls can be the guidelines to evolve existing IoT device architectures – secure element, secure microcontroller, secure microprocessor – and make them safer. This Insight will not explore the matter further, but highlights the importance of achieving robust security at the edge device level because these are the entry points of IoT systems in an ubiquitously connected world.

Finally, it is also important to highlight that thinking about security at application level is also critical, considering that applications are the interface between connected objects and users.

Conclusion

IoT security is not an easy topic to grasp, but it is one of vital importance for the safety of the environments the Internet of Things is shaping and transforming. Achieving that requires common and synergistic efforts of all the stakeholders involved. That's a long list comprising governments, standard and certification bodies, owners and users, system integrators, telecoms operators, OEMs, silicon vendors and IP vendors. Those efforts will translate into shared frameworks guiding the development of the necessary security tools for all the components of an IoT solution in a specific context.

Beecham Research is a leading market research, analysis and consulting firm, specialising in the worldwide M2M/ Internet of Things market. We are internationally recognised as thought leaders in this area, where we have deep knowledge of the market dynamics at every level in the value chain.

We are experts in M2M/IoT services and platforms, and also in IoT solution security, where we have extensive technical knowledge. We explore the impact of the Internet of Things in various sectors and are also the leading analysts in satellite M2M.

Our range of clients includes component and hardware vendors, major network/connectivity suppliers (cellular, fixed, satellite, short/long range), system integrators, application developers, distributors and enterprise adopters in both B2B and B2C markets.

www.beechamresearch.com