WHITEPAPER

The Internet of Things and Getting Security Right

sqs.com

Authors: Stephen Morrow
Principal Security Consultant

Colin Bull
Manufacturing Vertical Consultant

SQS Group Limited UK

Published: September 2016

Transforming the World Through Quality

STEPHEN MORROW

Principal Security Consultant

stephen.morrow@sqs.com

Stephen is a specialist in secure application design, development and testing, and has full lifecycle security and development experience in a variety of major Information Technology projects across the financial, private and public sectors. He is responsible for leading SQS' security testing practice and defining SQS security testing methodologies. Having over 12 years' dedicated security experience delivering a wide range of application security services to a variety of sectors in line with CESG CHECK, OWASP and ISO27001 standards, Stephen is a recognised expert in his field.

COLIN BULL

Manufacturing Vertical Consultant

colin.bull@sqs.com

Colin is a product and manufacturing specialist. He has over 26 years of design, engineering and manufacturing experience, with over 16 years in the development and successful deployment of Product Lifecycle and Manufacturing Execution applications, within Automotive, Aerospace and Defence and consumer appliances. He joined SQS three years ago to lead the UK consultancy in the manufacturing vertical. He has a passion for quality delivery of PLM enterprise applications, MES and integration into ERP and CRM systems. Colin is part of the global consultancy team leading the iIoT and Smart Factory services and innovations.

Contents

Management summary

The mass adoption of the Internet of Things (IoT) is a multibillion-dollar opportunity for product companies and the manufacturing supply chain. An estimated 30bn devices, or "Things", will be connected to the internet by 2020, with a value estimated to be $1.7bn [1]. This is being enabled by the reducing cost and Mohr's cycle of processing power of sensors and chips. Also playing a pivotal role are the emergence of internet gateways such as 4-5G, Low Power WAN, Near Field Communication, Bluetooth and Zigbee protocols. However, this also means there will be significant increases in the number of nodes, networks and systems that create a large attack surface and attract the attention of hackers and other actors with malicious intent. In order to prevent attacks from these individuals, the security posture of these IoT devices needs significant improvement.

Not long ago, cybersecurity-related concerns tended to revolve around the very real threats of data and identity and intellectual property theft. In this space, the bad guys range from script kiddies, experts with malicious intent, hacker groups and hacktivists through to organised crime and in some cases nation states. The archetypal victims typically were consumer-facing retailers and financial institutions that, in some high-profile cases, saw hackers siphon off millions of customer records and account numbers.

While those cases were scary enough, they didn't tend to target enterprises that were dependent on the reliable operation of very expensive physical assets – such as manufacturers. That is changing, however, as bad guys begin to threaten human safety by targeting physical assets and potentially shut down or take control of the physical infrastructure upon which we all increasingly depend.

This means that there needs to be a step change in how security is perceived and avoidance isn't the answer; risk management is.

This white paper discusses the security and risk management solutions necessary to avoid being hacked, prevent data loss and improve the security of the IoT ecosystems.

Keywords

IOT CONNECTED DEVICES SECURITY PRIVACY

THREATS RISKS SOLUTIONS

Introduction

The upcoming age of the Internet of Things (IoT) is going to blur the line between our online and physical lives. This also means that what we see today as internet security attacks will not only affect our online lives but could also directly attack our physical lives as well. The impact of security flaws could lead to the compromising of privacy and cause physical harm; the stakes could not be higher.

If we're going to recognise the benefits of the IoT, we need to get security and privacy right, but, let's be honest, we're still struggling with getting security right in what can be considered less complex systems. We know this because we hear all too frequently in the media of new security breaches that result in a wide variety of negative impacts on both organisations and individuals.

According to a survey conducted by SANS in 2015, many organisations still see security products as the solution to their problems. However, while products are part of the solution, and even necessary in some cases, it does not get to the heart of where the vulnerabilities and weaknesses originate. In fact, application security / secure development is only ranked joint 14th in priorities. Promotion up the rankings of application security and secure coding is necessary, especially with the complex nature of the IoT ecosystem. The IoT ecosystem means that at some stage everything is going to end up connected and thus more complicated, as it introduces a myriad of new requirements, technologies and innovations that further squeeze security budgets.

So what are we to do? First we need to understand what it is we are trying to secure...

Market analysis

Innovation is software led and by 2020 up to 30 bn devices are predicted to be connected to the internet. However, two main concerns in the industry are: realising value from connected devices and security and privacy.

Spending on cybersecurity is increasing. According to a September 2015 forecast from Gartner, worldwide spending on information security will have reached $ 75.4 billion in 2015, an increase of 4.7% over 2014, yet the number of incidents is also increasing. So we have to ask, why is this? Quite simply, security is often neglected in the SDLC.

As more things are becoming connected, with the threat from not just cyber-attack but also physical attack vectors, complexity is increasing. However, the security budget is often spent in ways that do not address the fundamental problems.

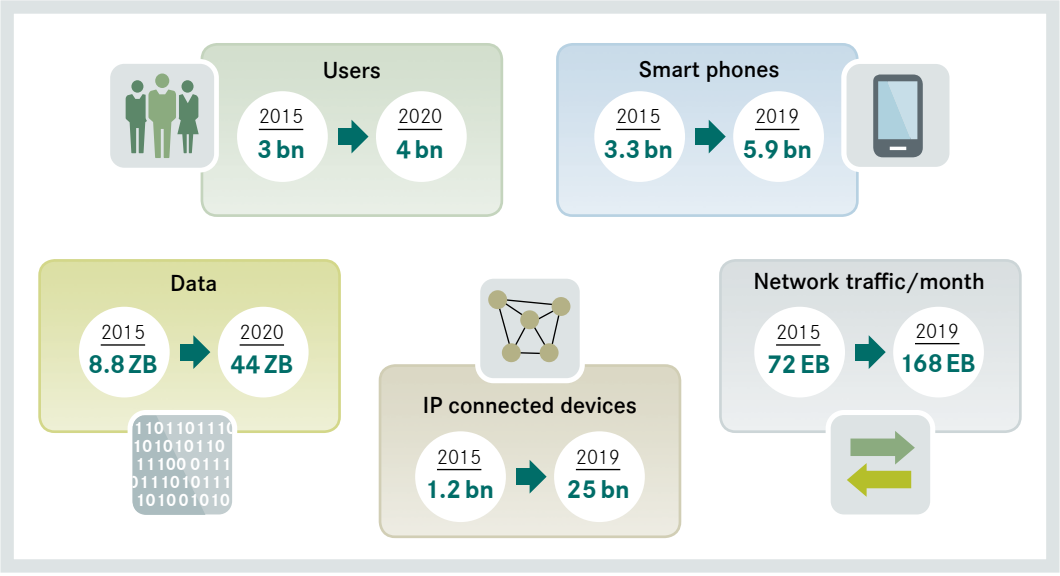

Figure 1: Exponential growth and adoption

The Cyber Security market will experience exponential growth from $106.3 bn to $170 bn by 2020, as the expected numbers of connected devices and users soar.

The IoT security market is expected to grow from $6.89 billion in 2015 to $28.90 billion by 2020, at a compound annual growth rate (CAGR) of 33.2% from 2015 to 2020 [2].

It really is a complicated ecosystem

The Internet of Things is not a new concept. In fact, the IT industry has been discussing the idea for decades. But what is it? Put very simply, the IoT is connecting devices over the Internet and letting them talk to us, each other and other systems. Why would you do this? There are many reasons, but at a high level the benefits of the IoT include:

- Tracking behaviour for real-time marketing;
- Enhanced situational awareness;
- Sensor-driven decision analytics;
- Process optimisation;
- Optimised resource consumption; and
- Instantaneous control and response in complex autonomous systems.

Real world applications are vast and cover many sectors of our society, but some examples include:

- Home automation such as lighting and heating, televisions and even security systems;
- Energy monitoring such as smart metering;
- Retail systems such as NFC point-of-sale terminals and intelligent shopping that can track customers and monitor shopping habits;
- Environmental monitoring such as air pollution, rain, snow, earthquake detection systems;
- Health monitoring such as wearables, wireless surgical implants;
- Connected cars such as e-call and car sharing.

The technology that makes this all possible is vast and includes [3]:

- **Communication:** RFID, EnOcean, NFC, Bluetooth, WiFi, Weightless, GSM, 3G, 4G LTE, ANT, Dash7, Ethernet, GPRS, PLC / Powerline, QR Codes, EPC, WiMax, X-10, 802.15.4, Z-Wave, Zigbee
- **Backbone:** IPv4, IPv6, UDP, TCP, 6LoWPAN, etc.
- **Hardware:** PanStamps, Arduino (RF, Tiny, Uno, etc.), XinoRF, Ciseco Open Control Gateway, Pinoccio, Raspberry Pi, mbed, Wi-Go Module, UDOO, Waspmote, etc.
- **Protocols:** CoAP, RESTful HTTP, MQTT, XMPP, etc.
- **Software:** APIs, Supply Chain
- **Data Brokers / Cloud Platforms**
- **Machine Learning**

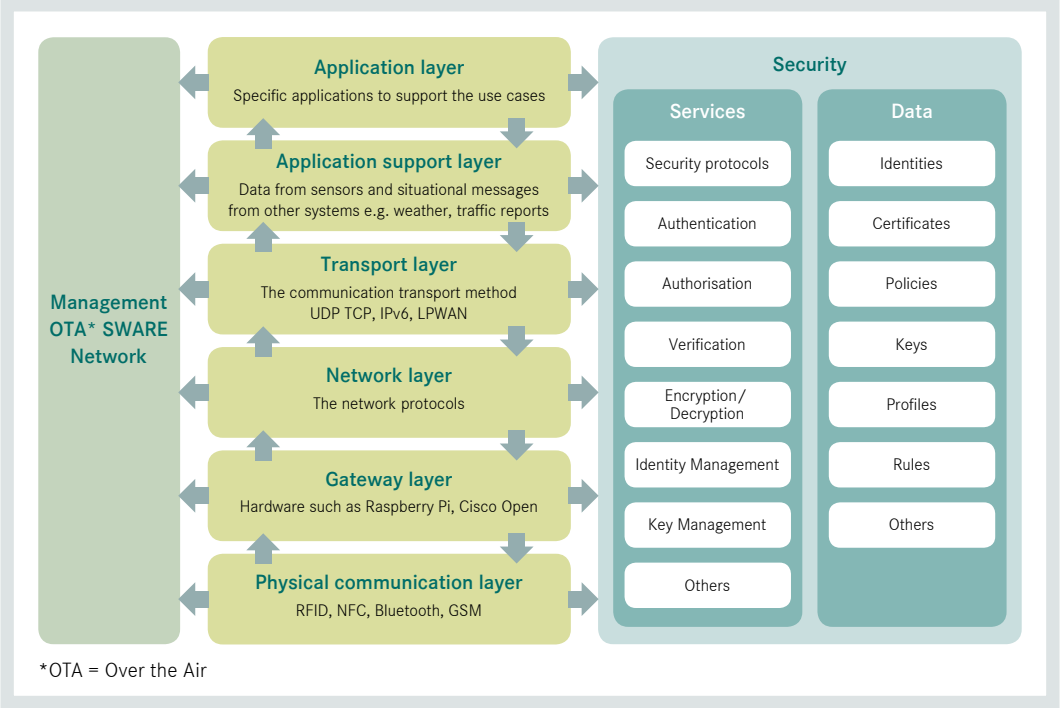

Figure 2: Security and privacy within the IoT ecosystem

The Internet of Things is a multi-layered proposition in which security and privacy within each layer (see Figure 2) has to be considered and managed. Communication security and the privacy of data must be assured on and across each of the layers. The complexity is increased by the fact that each layer has varying degrees of processing power and memory capacity, also compounded by the fact that end devices are moving sometimes at speed across states and country borders, or located in insecure and remote locations, so physical security as well as cyber security has to be considered.

Understanding the threats

From its very early days, the ubiquitous nature of the internet has resulted in it evolving and becoming an integral part of how we live and conduct business today. There have always been risks – there still are – and this is because the technology that makes up the internet has flaws and there is value to be gained by having or gaining access to the information that flows through it. In the typical security breaches that we read about every day, such as Home Depot, TalkTalk and Sony, the business impact we are usually talking about is legal exposure and direct, indirect and/or productivity losses. For example:

- Theft, Money, Digital Assets
- Negative Brand Impact
- Recovery Expenses
- Compliance failures

In these cases, nobody gets physically hurt. On IoT devices any security threat can intersect with public safety and human life. As can be seen from Table 1, the number of devices, physical locations and the processing power introduce a level of risk greater than we have seen during the “internet era”.

Unfortunately, security and safety have typically been considered as two separate areas, yet there are already examples of hacks that demonstrate security vulnerabilities that affect safety in the physical world and this is why improvement is an absolute necessity. See for example [4].

Internet Connected Baby Monitors – In August 2013 Mark Gilbert was in his house with his wife downstairs whilst their two-year-old child was asleep. They had become reliant on the video enabled baby monitors to keep an eye on their children whilst doing their chores or relaxing in front of the TV. They heard voices coming from the child’s bedroom, even calling out her name and uttering expletives. When Mark entered the room, the camera moved to face them, the voice was coming from the baby monitor shouting expletives and threats. Mark quickly switched off the device. Security researchers found that attackers could determine the IP address and simply browse the URL http://{ipaddress}/proc/kcore and download the entire memory off the device. The attacker can then simply open the kcore file to obtain the user-name and passwords and with these credentials an attacker can take control of the device.

Issue	Smart connected product security	Internet security	Implications for smart connected products
Potential risk	Loss of life	Loss of information	Security breaches can affect physical assets, leading to asset loss, or worse, loss of life
Number of End Points	Tens of billions	Half a billion	Higher number of devices to infect and launch attacks
Entry Points	Product software, network, edge and cloud	Applications, network, datacentre, user devices	Complex systems and more types of attack entry points
Physical Access	Disrupted and exposed	Centralised, physically protected	Embedded devices cannot count on physical security measures.
Processing Power	Weak or limited processing power	Powerful processers	Many embedded devices are low power, low ram and cannot support runtime security solutions.

Table 1: Comparison of internet era and connected device security issues

Electronic Lock Picking – Whenever you enter a hotel today, it is likely you will be presented with a card to operate your room door lock. As discovered by Cody Brocious, the Onity lock has a particular security issue in that the programming port is easily accessible to any microcontroller, for example a cheap Ardunio. Using this device to access the locks memory to get the site code and issuing an open command unlocks the door. Hotel chains have reported burglaries from rooms using this method.

Another example affects a Z-Wave enabled door lock. Researchers found that the Z-Wave had a vulnerability surrounding the original key exchange between a lock and the controller. They found that even after pairing they could transmit a key exchange packet that caused the lock to accept a newly shared key, allowing the attacker to bypass the controller and then send open 'open the door' commands.

The truth is that nearly every day there are reports of significant security breaches and this seems to indicate that the industry is willing to live with the associated risks to our data. This is of course after risk management processes have been used to reduce risks to an acceptable level. The same approach cannot be taken for systems that have a human safety or a physical factor, as the risks are far too high. Reliable and rigorously verified security controls that enforce confidentiality, integrity and availability across the IoT landscape are required. In many cases, we need to consider it a safety issue. In this context analysts are indicating that security issues are a significant inhibitor to the widespread deployment of many new IoT services. At the same time, the provision of wide area connectivity to an ever-widening variety of IoT services and devices will only increase the whole ecosystem's exposure to fraud, attack and misuse.

The bottom line is that there's no such thing as 'bug-free' systems, but the impact of a typical security breach can be annoying, and potentially expensive, but not life threatening. There is already much evidence to show that attackers are showing an ever greater interest in this area. If the multi-billion dollar opportunity is to be realised, then those involved in making it happen need to solve the security and privacy issues.

Risks in the supply chain

Product manufacturers are reliant on the components and software delivered by their suppliers. The supply chain of software is an added complication that introduces security risks that are seen only infrequently in traditional systems development. For example, the rate of change of IoT devices and operating systems is leading development teams to rely more frequently on externally sourced software libraries. While the use of external libraries is not new, the degree to which they are being used in IoT development is.

Similarly, the risk that weaknesses in build and configuration management can create vulnerabilities is common to all kinds of software development. For example, when deployed on a device, organisations creating that software are essentially 'giving' their software to potential attackers who can then review and analyse the code. If poor security decisions have been made in the application code, attackers have a greater opportunity to find and exploit those vulnerabilities than with traditional server based software.

IoT software development is also a specialised area and the use of outsourced software development is common. When outsourcing, development teams need to ensure that a thorough risk assessment is conducted for any software introduced into the IoT ecosystem. In short, risk mitigation needs to be embedded into the development process and the developer mind-set. Given the security and privacy risks, it is simply not good enough to treat it as an add-on activity to be conducted separately.

The expertise and resources required to mitigate these risks vary, but it is important to recognise that not all the requirements for better security are onerous: a basic check to verify the integrity of software libraries downloaded from the Internet involves checking that the 'checksum' of the downloaded file corresponds to the publicly documented code. This is a quick and easy check, but how many developers can say that all libraries they use had the checksum verified before being incorporated into production code?

But that is just at one level. When we talk about the supply chain for IoT we are referring to a much wider range of organisations, people, activities, information and resources. For example, we have to consider all of the potential vulnerabilities and weaknesses that could exist in or be introduced by the solutions provided by the following operators:

- IoT Service Providers – enterprises or organisations who are looking to develop new and innovative smart, connected products and services.
- IoT Device Manufacturers – who provide IoT devices for IoT service providers, in order to enable IoT services.
- IoT Developers – who build IoT services on behalf of IoT service providers.
- Network Operators – who provide communication services for IoT service providers.

To meet the needs of security within the IoT there are also some processes and technical challenges that still need to be solved, such as:

- Quality and reliability – Software where smart devices will be considered safety related must go through code analysis to meet ISO26262 for automotive
- Traceability – markets such as defence and aerospace require traceability of components
- Unable to meet requirements for standards such as ISO9001 SAE9120
- Malware – what is in embedded code on the devices? What is the provenance of the code?
- Processing power and latency requirements – The processing power of the product and embedded device could be limited so will not be able to encrypt or decrypt messages or have the ability to hold keys to establish trust.

Strategies for mitigating the risks

Each of the main operators above has its own specific threats with which to be concerned. However, the following strategies will mitigate the risks that these threats pose.

Risk assessments and threat modelling

While the concept of a risk assessment has been around for many decades, many businesses are more familiar with applying the concept to general business risk than to information security. However, an information security risk assessment process is also imperative for the secure operation and longevity of the technological side of a business. Obviously, in Internet of Things technology, where the engineering team is a critical component for the success of the business, the risk assessment process should be the first step the organisation takes in establishing security practices.

While every organisation should create a granular perspective of technological risk, there are high level questions that function as starting points for the risk assessment process:

- What assets (digital or physical) need to be protected?
- What groups of people (tangible or intangible) are potential threat actors?
- What is a threat to the organisation?
- What is a vulnerability?
- What would the result be if a protected asset were compromised?
- What is the probability of the asset being compromised?
- What would the result be when put in context with different groups of attackers?
- What is the value of the asset to the organisation and its partners?

- What is the safety impact of the asset being compromised?
- What can be done to remediate or mitigate the potential for vulnerability?
- How can new or evolving gaps in security be monitored?
- What risks cannot be resolved? What do they mean to the organisation?
- What budget should be applied for incident response, monitoring and risk remediation?

These starting points will help the engineering and information technology teams work more effectively with the organisation. The goal is to ensure that the technical side of the business understands and agrees on the identified risk, is aware of the negative impact that could occur if an attack were to take place and is able to propose adequate countermeasures or remediation that would remove or reduce the risk. This would then be presented to the executive side of the business, which would make a decision on the effort and budget required to implement remediation. Forcing the teams to work together will help create a more realistic perspective of not only the risk to the business but also the value of assets.

Secure by design – embed security into the entire development lifecycle

Translating the outputs of a risk assessment into technical security controls and countermeasures is where gaps in security typically first start to manifest themselves. It is therefore recommended that a structured approach is used during the design phase to optimise infrastructure, communications, application and device security.

Threat modelling is a method used to systematically identify and rate the threats that are most likely to affect a system. By identifying and rating threats based on a solid understanding of the architecture and implementation of your application, you can address threats with appropriate countermeasures in a logical order, starting with the threats that present the greatest risk. Threat modelling has a structured approach that is far more cost efficient and effective than applying security features in a haphazard manner without knowing precisely what threats each feature is supposed to address. With a random, “shotgun” approach to security, how do you know when your application is “secure enough”, and how do you know the areas where your application is still vulnerable? In short, until you know your threats, you cannot secure your system.

Taking this further, the best approach to risk mitigation is to embed security into the product and software development lifecycle. This means including security in the governance, construction, verification and deployment of the systems, product development and operation.

The software development industry is taking a lead in establishing methodologies, standards and processes for ensuring security in system development and industry-led and vendor-neutral initiatives are available that help assess current secure development practices and what, if any, changes need to be made. For example, the Open Software Assurance Maturity Model (OpenSAMM) provides a framework that helps to tailor risk-mitigation activities and is used by organisations to prioritise components of its secure application development programme.

Verifying the security of IoT solutions

Independent Verification and Validation is an accepted approach for complex product design and manufacture. Even if you don't use an external organisation to perform Independent Verification & Validation (IV&V), you allow that department to act autonomously, reporting outside of the project structure, to isolate them from the pressures of delivery and ensure an objective approach and impartial results. The testing organisation is trained and skilled in what they do and in the majority of cases they have a mind-set and a passion for testing products. To do this well they have to define strategies and establish test plans, procedures, environments and standards. This approach is taken so that the products can be certified for consumption by the customers through the relevant regulatory bodies. The more mature the testing organisation is, the easier it is to demonstrate compliance against standards and facilitate certification for variants and upgrades.

Interestingly, when product companies ask their customers, security is generally not a front running consideration and therefore could be perceived as having no value to them. So how can an organisation cover the cost of increased security with a backdrop of what may be considered to have no real value to the end user? The truth is, and experience has shown, that if quality and risk management is built into the entire development processes, then quality comes for free but needs to be balanced [5].

There are a number of threats and risks that need to be identified across the complex ecosystem of the Internet of Things. As can be seen in Figure 3, there are four discrete areas where you need to consider where your vulnerabilities lie.

Leveraging SQS as an independent security testing provider to cost-effectively offload security testing requirements and demonstrate compliance where you do not have the skills, capacity or tooling required to appropriately manage the security risks associated with your software and hardware investments makes sense.

	Threat / Motivation	Service	Result
Software	**Architecture and design flaws, source and byte code level flaws (intentional/unintentional):** • Vulnerabilities – OWASP Top 10, SANS CWE, etc. • Web, cloud, mobile and desktop application vulnerabilities • Weak design / insecure code / poor configuration	• Threat modeling • Architecture & design review • Static application security testing • Dynamic application security testing • Secure SDL consultancy • Mobile application security testing • Cloud application security testing • SharePoint security testing	• Security flaws identified and recommendations for improvement • Early vulnerability detection • Reduced re-work costs • Improved security and time to market • Reduced risk
Hardware	**Hardware design flaws and vulnerabilities:** • Physical access vulnerabilities • Flash and malware installation • Configuration of the physical asset • Condition monitoring	• Secure design consultancy • Cyber physical FMEA • Physical attack design reviews • Cyber physical security testing	• Physical flaws identified • Early vulnerability detection • Reduced risk • Reduced design rework • Improved security and time to market
Infrastructure	**Flaws at the network and infrastructure level:** • Publicly available exploits • Unpatched systems and insecurely configured networks • Viruses and malware • Inadequate security controls and defensive measures	• Penetration testing • Vulnerability assessment • Configuration review • Architecture analysis	• Security flaws identified and recommendations for improvement • Compliance with standards • Improved security • Reduced risk
Organisation	**Gaps in the implementation of, or compliance to, legal or regulatory standards:** • Trigger due to Governance Risk and Compliance (GRC) • e.g. COBIT, ISO27001, BSI, PCI DSS, BDSG	• Assessment • Audit preparation • Gap analysis • Process initiation • Process improvement	• Recommendations for improvement • Information security management systems • Business continuity plans • Compliance

Figure 3: Overview of SQS security services and the needs they address

Conclusion and outlook

The Internet of Things is driving innovation at a pace and it has the potential to deliver better business performance and alternative revenue streams and business models. It will transform the way the consumer interacts with the organisation.

Security for these devices is within not just the device itself but also the software running on the device and any communication channels it uses. As such, security needs to be considered across the entire software development and product development lifecycles. There are many layers to delivering the value of the IoT and each layer presents a challenge on how the data and security are handled.

End devices will need to have physical security considered, especially as they may be situated in remote and insecure locations where hackers might be able to gain physical access to the hardware. Whether the device can be accessed across a network or physically, if it is not secure then it is a target and if successfully attacked, the consequences would be serious.

In the pursuit between getting innovative ideas to the market faster than your competition and profiting from its rewards versus setting up the proper processes to manage risk across the entire product lifecycle, the winners will be the organisations that manage to do both well.

References

[1] Worldwide Internet of Things forecast 2015-220 IDC#256397 taken from infographic http://www.idc.com/infographics/IoT

[2] M2M Magazine Article 2016 taken from http://www.machinetomachinemagazine.com/2016/01/04/internet-of-things-security-market-by-2020

[3] GSMA IoT Security Guidelines http://postscapes.com/internet-of-things-technologies#protocols

[4] Nitesh Dhanjani. Abusing the Internet of Things, 2015

[5] Martin Wieczorek, Dik Vos, Heinz Bons. Systems and Software Quality - The next step for industrialisation, Springer 2014

SQS Software Quality Systems AG
Phone: +49 2203 9154-0
Fax: +49 2203 9154-55
info@sqs.com | www.sqs.com