Capgemini Consulting

SOGETI
High Tech

Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT

Capgemini recently launched a new global service line dedicated to cyber security that draws expertise from key disciplines within the Group. As the security of IoT products and systems is a key focus area for Capgemini, Capgemini Consulting and Sogeti High Tech – a subsidiary of the Capgemini Group that is specialized in product engineering – launched a study to understand the implications of cyber security threats for the Internet of Things (IoT). This research paper presents our perspective on how organizations can prepare themselves to address these threats and secure the IoT opportunity.

The Internet of Things Opportunity Hinges on Security

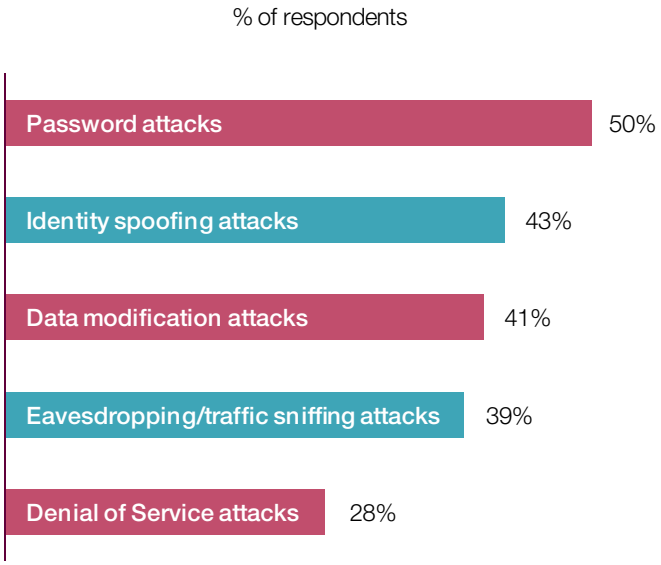
> *While car manufacturers are currently focusing mainly on infotainment-related connectivity, in the coming years we will see many more developments in the field of car-to-car communication and remote diagnostics. But this also means that we will be more and more vulnerable to malicious attacks.*
>
> - A leading car manufacturer

There is little arguing the transformative potential of the Internet of Things (IoT)[1]. However, the IoT business opportunity rests precariously on one critical factor – security. A spate of recent hacks and breaches has revealed glaring vulnerabilities in the IoT. Consider for instance, the breach in US-based retailer Target's payment systems in late 2013. This was the largest data hack in US retail history and resulted in the theft of 40 million credit card numbers[2]. What is extraordinary about this attack is that hackers gained access to Target's network through Internet-enabled heating, ventilation and air-conditioning systems installed in its retail stores[3].

The security risks of the IoT apply equally to the world of connected consumer devices as they do to industrial systems. For instance, security researchers Chris Valasek and Mathew Solnik conducted experiments to show car makers how hackers could potentially gain access to the engine or the steering wheels of a connected car. The researchers also showed how hackers could then wrench the wheels of the car to one side or even turn off the engines without warning[4]. While these experiments required physical access to the vehicle, the possibility of a remote attack is not as far-fetched as it might seem, given the pace at which technology is advancing.

As the IoT continues to grow to an estimated 26 billion devices by 2020[5], Internet-enabled systems will become increasingly attractive targets for cyber attacks[6]. As an executive at a leading car manufacturer told us: "While car manufacturers are currently focusing mainly on infotainment-related connectivity, in the coming years we will see many more developments in the field of car-to-car communication and remote diagnostics. But this also means that we will be more and more vulnerable to malicious attacks.[7]" To understand more about organizations' security concerns, our global survey (see research methodology at the end of this paper) probed which exposures concerned them most (see Figure 1).

Figure 1: Top Security Threats to IoT Products



Source: Capgemini Consulting and Sogeti High Tech, "Security in the Internet of Things Survey", November 2014

N=109

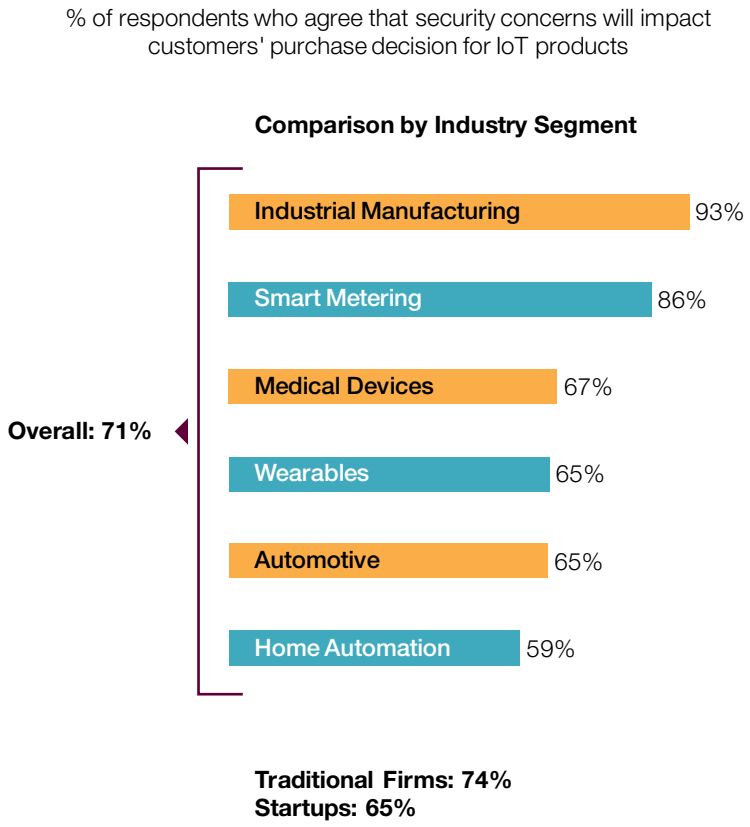
> *71% of respondents in our survey agreed that security concerns will influence customers' purchase decision for IoT products.*

3

"Hackers gained access to Target's payment systems through Internet-enabled heating, ventilation and air-conditioning systems installed in its retail stores."

The growing risk of these attacks could undermine the IoT business opportunity. 71% of respondents in our survey agreed that security concerns will influence customers' purchase decision for IoT products. Industrial manufacturing and smart metering firms acknowledge this to a greater degree than firms in other segments such as automotive and home automation (see Figure 2). This may not be surprising if we consider that industrial manufacturing and smart metering firms were among the earliest to embrace connectivity. The CEO of a leading smart metering firm affirmed this, saying: "The integrity of energy consumption data is extremely important in our industry and has now become a potential business stopper.[8]"

Figure 2: Impact of Security Concerns on Customers' Purchase Decision for IoT Products



Source: Capgemini Consulting and Sogeti High Tech, "Security in the Internet of Things Survey", November 2014
N=109

"Security researchers have conducted experiments to show car makers how hackers could potentially gain access to the engine or the steering wheels of a connected car."

Losses arising from cyber attacks on IoT systems can hit organizations hard. Target faced plummeting sales and saw a 46% drop in profitability as a result of the November 2013 attack. In addition, the company could potentially face a fine of $400 million to $1.1 billion if a government probe finds it guilty of not following industry-specific security standards[9].

Given the massive fallout of cyber attacks, do organizations prioritize security adequately and are they prepared to address the growing risks of connectivity? Is security a core focus for organizations as they develop their IoT products? In the following pages, we examine how organizations approach security issues, assess the challenges they face in securing their IoT products, and present a blueprint to make security the cornerstone of an IoT strategy.

"The integrity of energy consumption data is extremely important in our industry and has now become a potential business stopper."

- A leading smart meter manufacturer

4

Raising the IoT Security and Privacy Game

Ramping Up Security Levels

Despite increasing cyber attacks on IoT devices and ample warning from security experts, most organizations do not provide adequate security and privacy safeguards for their IoT products. Only 33% of executives in our survey believe that the IoT products in their industry are highly resilient to cyber security attacks. Among industry segments, home automation and medical device manufacturers reported the lowest levels of resilience (see Figure 3). This is particularly worrying given the expected uptake of IoT devices in these segments. For instance, the number of patients using connected medical devices is expected to grow from 3 million at the end of 2013 to over 19 million by 2018[10].

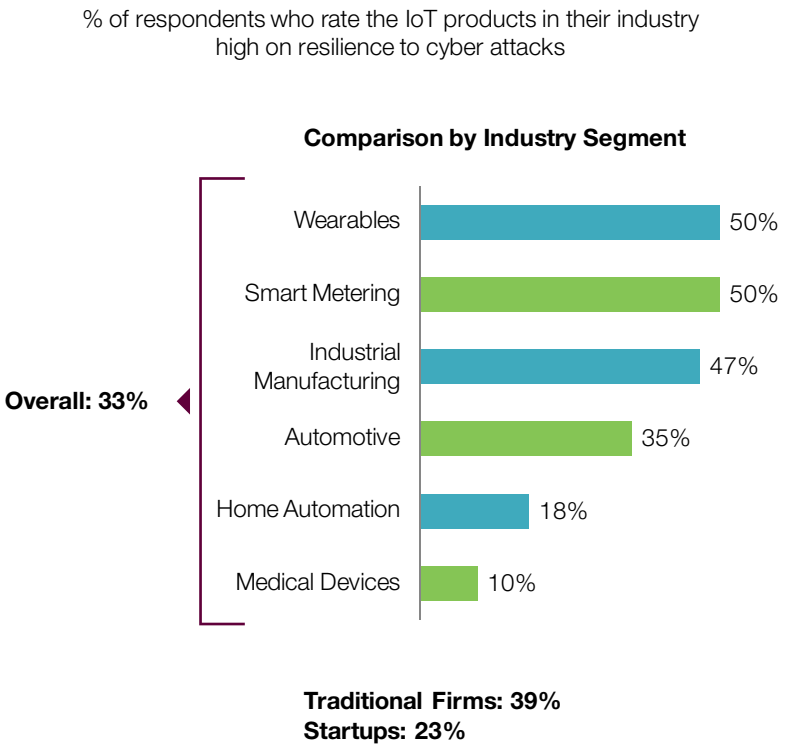
Research shows that existing security features in IoT products are not adequate. An HP study revealed 250 vulnerabilities in ten commonly used IoT devices, including connected TVs, webcams, thermostats, door locks and home alarms. Most products supported very weak authentication features that directly exposed them to security risks. In fact, 8 out of 10 devices failed to require a password stronger than "1234"[11]. Another significant risk factor is the continued use of the default password provided by the manufacturer, which can often be easily cracked by hackers.

> *"Only 33% of executives in our survey believe that the IoT products in their industry are highly resilient to cyber security attacks."*

Vulnerabilities arising from lack of encryption features are also a concern. In 2014, an Israeli security firm uncovered a critical vulnerability in a telematics device developed by Zubie – a US-based connected-car startup. The research team found that Zubie's hardware, which tracks a car's performance to provide drivers with instructions on improving driving efficiency, did not encrypt communications between the device and server. Researchers were able to demonstrate how hackers could exploit this weakness to send malicious updates to the device, steal data on the car's location and performance, and even unlock doors remotely[12].

> *"In 2014, an Israeli security firm showed how hackers could exploit a critical vulnerability in a popular vehicle-telematics device to send malicious updates to the device, steal data on the car's location and performance, and even unlock doors remotely."*

Figure 3: Resilience of IoT Products to Cyber Security Attacks



Source: Capgemini Consulting and Sogeti High Tech, "Security in the Internet of Things Survey", November 2014
Note: Surveyed companies commented on the level of resilience of IoT products in general and not specifically on their own products
N=109

> *47% of organizations do not provide any kind of data privacy information regarding the data generated from their IoT products.*

The poor security features in IoT products have inevitably attracted government attention. The US Federal Trade Commission (FTC) took action against TRENDnet, a manufacturer of Internet-connected home security cameras, for allowing users' login credentials to be transmitted unencrypted over the Internet, which resulted in hundreds of camera feeds being hacked and posted online. Among other things, the FTC barred TRENDnet from misrepresenting the security of its cameras and charged it with providing consumers with free technical support for two years to help consumers update or uninstall their cameras[13].

Privacy Policies Lack Maturity

Data privacy is also emerging as a major concern for consumers, which comes as no surprise. In a recent survey of US consumers, 66% of respondents expressed concerns about data privacy issues stemming from IoT products[14]. However, our benchmarking assessment of organizations' IoT data privacy policies (see research methodology at the end of this paper) reveals significant concerns.

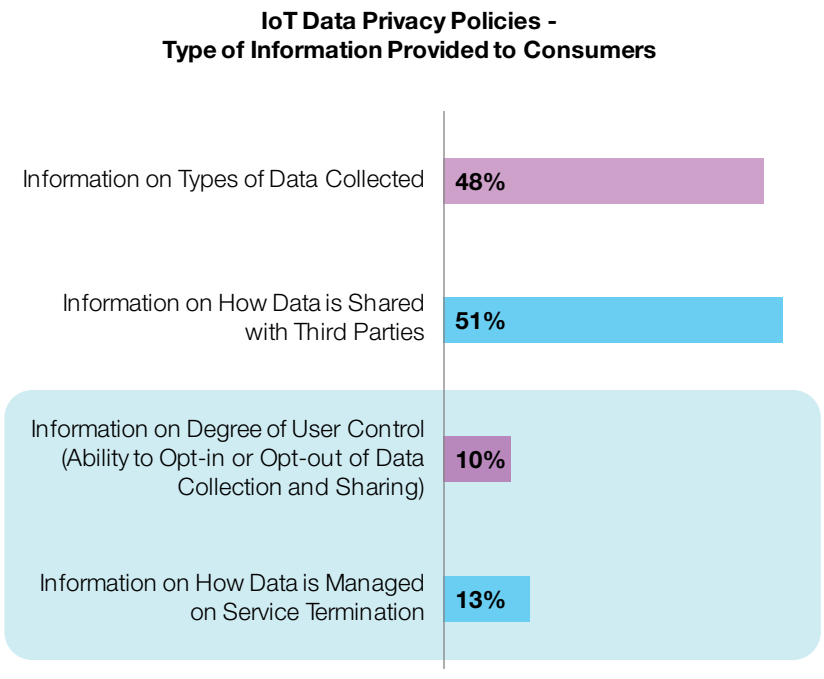
> *Only 10% of companies allow consumers to either opt-in or opt-out of data collection and sharing.*

Of the 100 startups and traditional organizations that we studied, 47% do not provide any privacy related information regarding their IoT products. Even when they do, organizations rarely enable consumers to control the collection and sharing of data from their IoT devices. For instance, only 10% of companies allow consumers to either opt-in or opt-out of data collection and sharing (see Figure 4). AliveCor, a startup that provides a remote cardiac health monitoring service, is a notable exception. AliveCor asks users for their explicit consent before sharing any data with a healthcare professional. In addition, AliveCor's privacy statement clearly informs users about how they can withdraw from sharing data if they wish to[15].

Another significant omission in most privacy statements is the absence of information on how customer data is dealt with once a service is terminated. Our research revealed that only 13% of companies provide this information. However, there are some exceptions. Automatic, a startup that offers a telematics device for connected cars, informs customers that it may permanently delete customer data at its own discretion, upon termination of service[16]. Fitbit, the fitness tracking device manufacturer, lets consumers know that it stops storing data once the consumer terminates a contract[17]. Such information enables consumers to take a more informed decision about whether to opt for a service or not.

> *AliveCor, a startup that provides a remote cardiac health monitoring service, asks users for their explicit consent before sharing any data with a healthcare professional.*

Figure 4: Data Privacy Information Provided by Organizations



N = 100

Source: Capgemini Consulting and Sogeti High Tech Analysis

Why are Organizations Lagging behind in Securing their IoT Products and Systems?

A number of factors are affecting organizations' ability to put in place rigorous security. These include an expanded attack surface, inefficiencies in the IoT product development process, the weak security architecture of the entire IoT system, lack of specialized security skill-sets, and insufficient use of third-party support.

The IoT Presents an Expanded Attack Surface and Multiple Points of Vulnerability

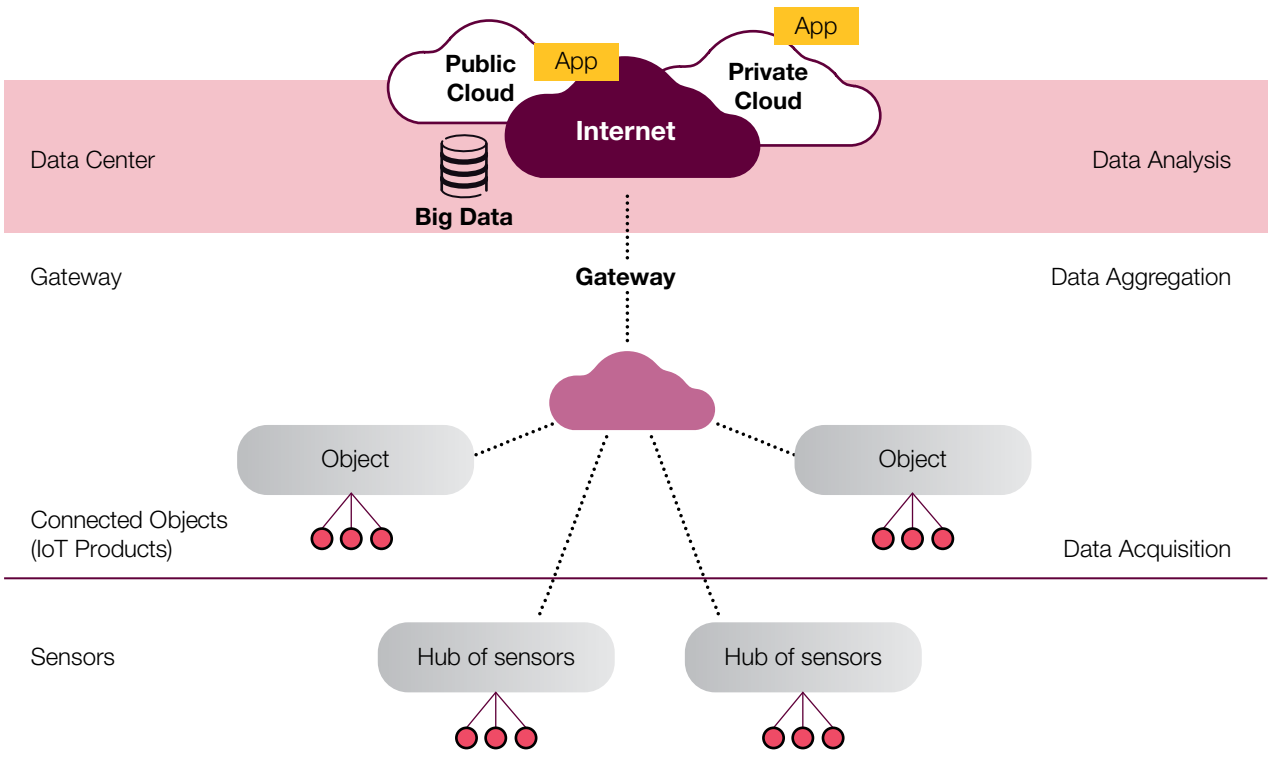
Securing an IoT system is a challenge because of its multiple points of vulnerability. These include the IoT product, and the embedded software and data residing within it. They also include the data aggregation platform, data centers used for analysis of sensor data, and communication channels (see Figure 5).

Securing all of these surfaces is a major challenge for organizations (see Figure 6). As a senior executive at a leading European industrial manufacturing firm explains, it involves a wide-ranging response: "Securing an IoT system involves securing the IoT product and implementing multiple features at the system level, such as access control and account management, segregation of networks and accounts, the use of secure protocols for data transmission, and the management of firewall and antivirus updates.[18]"

The security of the IoT product is a key element of the overal security of an IoT system. Figure 6 illustrates the key challenges to securing an IoT product.

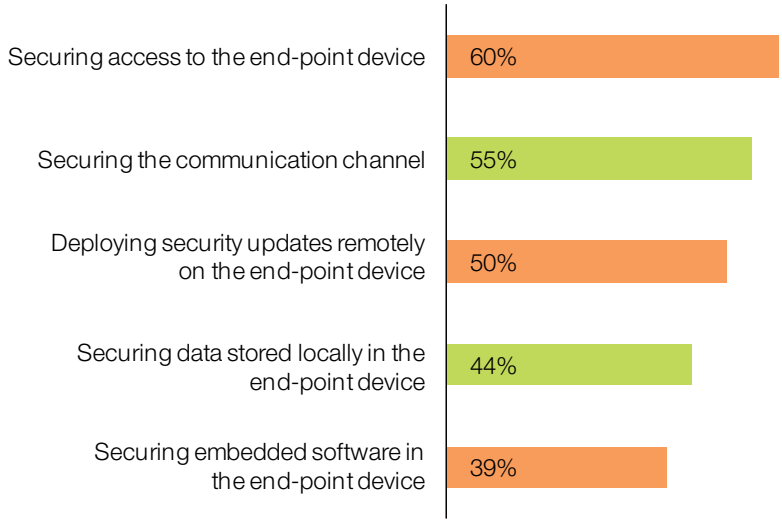
> *"The focus on security can get lost if organizations rush to launch their IoT products, prioritizing speed-to-market over security."*

Figure 5: The Expanded Attack Surface of an IoT System



Source: Capgemini Cybersecurity Service Line

Figure 6: Key Challenges to Securing IoT Products



Source: Capgemini Consulting and Sogeti High Tech, "Security in the Internet of Things Survey", November 2014
N=109

For Most Organizations, Security is not the Core Focus of the IoT Product Development Process

Securing a product from cyber attacks is a critical element of the product development process in an IoT world. Michael Murray, the Director of GE Healthcare's Cyber Security Consulting and Assessment division highlights this when he says, "It's all about building these sensitive medical systems and devices with cyber security in mind, rather than as an afterthought." Murray's team is responsible for overseeing the development of the company's remote patient monitoring, medical imaging and diagnosis systems right from the design phase[19].

However, this focus on security can get lost if organizations rush to launch their IoT products, prioritizing speed-to-market over security. Our survey showed that only 48% of companies focus on securing their IoT products from the beginning of the product development phase. In addition, only 36% are working towards modifying their IoT development process to focus more on security from the earliest stages of product design (see "Cyber Insecurity: Why IoT Product Security Is Lagging").

Organizations have not set up Mechanisms to Remotely Patch Connected Devices

Connected products need to be updated regularly for their defenses to be watertight to existing and emerging threats. If patches are not updated frequently, the risk of cyber security attacks increases. Despite this, our survey revealed that only 49% of organizations provide remote updates for their IoT devices (see "Cyber Insecurity: Why IoT Product Security Is Lagging").

There are many reasons for this. Since most IoT products are built using inexpensive, low-margin chips, chip manufacturers are not adequately incentivized to provide patches for them. At the same time, vendors of IoT products, unlike PC and smartphone manufacturers, may not necessarily have the technical expertise required to develop patches[20]. In some cases, the issue lies in the absence of channels to deliver patches remotely, as organizations rely on users to manually download and install them. However, consumers may not be aware of updates or have the expertise to install them. 67% of respondents in our survey cited lack of awareness among consumers regarding security best practices as a major cause of security breaches. Despite this, 41% of respondents reported that they release updates online and require consumers to download and install them.

> *"Only 49% of organizations provide remote updates for their IoT devices."*

> *Only 48% of companies focus on securing their IoT products from the beginning of the product development phase.*

Most Organizations are not Focusing on Acquiring Specialized Security Skills for their IoT Products

Despite growing awareness about the risk of cyber attacks, most organizations are not working towards building specialized security skill-sets. Securing an IoT product requires multiple skills to cover the app, device, infrastructure and the communication channel. 35% of respondents in our survey cited the shortage of specialized security experts in their organizations as a key challenge to securing IoT products. Despite this, only 20% reported that their organizations are hiring IoT security experts in order to improve security. Companies like Tesla, however, are exceptions. Tesla hired Kirstin Baget, a hacking expert with prior experience in companies such as Apple, Google, eBay and Microsoft, to lead its vehicle security team (see Exhibit 1, "Tesla: Liaising with the Hacker Community to Develop Secure Connected Cars").

Most Organizations are Not Leveraging Third-Party Support to Accelerate the Process of Strengthening Security

Few organizations are taking proactive steps to strengthen security by partnering with, or acquiring, specialized security firms. Our research revealed that only 35% of companies are partnering with specialized security firms and only 19% are acquiring specialized security firms as part of their IoT security strategy (see "Cyber Insecurity: Why IoT Product Security Is Lagging").

Exhibit 1 - Tesla: Liaising with the Hacker Community to Develop Secure Connected Cars

Tesla Motors, the leading American electric car maker, makes some of the most digitally advanced cars in the world. Tesla's cars are equipped with over-the-air software updates and provide an infotainment screen that can be used to control everything from navigation to the door locks. But this also opens up the possibility of Tesla's cars being vulnerable to cyber attacks.

Making Tesla Sit Up and Take Notice

The possible consequences of cyber hacking for Tesla's cars were brought to the fore by two instances involving Tesla's Model S electric car. In the first, the owner of a Model S was able to hack into the car's system and bring up a non-standard web browser on its infotainment display. In the second, participants in a Chinese security conference were able to remotely operate the car's lights, horn and sunroof.

Courting Hackers to Develop Secure Systems

Tesla's initiative to make its cars more secure against much more serious hacks started with the hiring of Kirstin Baget, a hacking expert with prior experience in companies such as Apple, Google, eBay and Microsoft, to lead its vehicle security team. Tesla also attended the Def Con, an annual security conference held in Las Vegas, in order to hire 20 to 30 hackers to develop security systems for its current and future vehicles.

Tesla is also courting freelance security researchers and hackers. The company actively encourages people to report vulnerabilities, and offers factory tours in exchange. So far, 20 confirmed vulnerabilities have been exposed in this manner. Tesla adds the names of hackers who are able to successfully point out security flaws to a "Hall of Fame" list on its website.

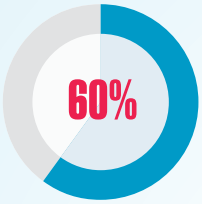
Source: Wall Street Journal, "Tesla Invites Hackers for a Spin", August 2014; Jalopnik, "Tesla Looking To Hire Up To 30 Hackers To Prevent Pwning", August 2014; CleanTechnica.com, "Tesla Motors Snags "Hacker Princess" From Apple", February 2014

> *35% of respondents cited the shortage of specialized security experts in their organizations as a key challenge to securing IoT products.*

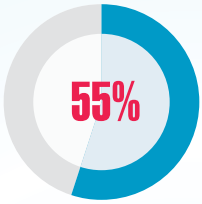
Cyber Insecurity: Why IoT Product Security is Lagging

An Expanded Attack Surface Increases the Challenge of Securing IoT Products

Key Challenges to Securing IoT Products: *% of respondents*



Securing access to the **end-point device**

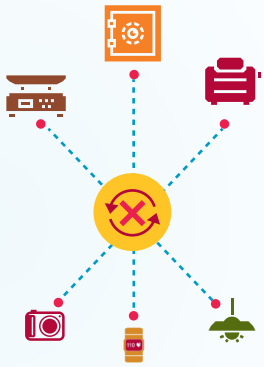


Securing the **communication channel**

Deploying **security updates remotely on end-point devices**

Security is not a Priority While Developing IoT Products

Only **48%** of organizations focus on securing their IoT products from the beginning of the product development phase



Organizations have not set up Mechanisms to Remotely Patch Connected Devices

Only **49%** of organizations provide remote updates for their IoT devices

IoT Security is in the Slow Lane

Ignoring the importance of building in-house capabilities to secure IoT products

% of respondents:

Hiring IoT security experts – 20%

Appointing a team to look into the development of **data privacy policies for IoT products – 35%**

Modifying the IoT product development process **to focus more on security** from the earliest stages of product design – **36%**

Increasing **IoT R&D spending on security – 43%**

Not exploring external expertise to secure IoT products

% of respondents:

Acquiring **specialized security firms – 19%**

Inviting third parties such as **hackers to identify vulnerabilities** in IoT products – **28%**

Partnering with **specialized security firms – 35%**

Gold-Standard Security: Making Security the Core of the IoT Value Proposition

> *Organizations should set up an integrated team structure for IoT product development, comprising business executives as well as security specialists.*

Set up an Integrated Team of Business Executives and Security Specialists

The first step in securing an IoT system is to treat security as a fundamental element of the product value proposition. This means that product managers and security specialists must work together to plan the IoT product roadmap and conceptualize the defining features and functionality of the product. To achieve this, organizations should set up an integrated team structure for IoT product development, comprising business executives as well as security specialists. This will enable greater collaboration between business executives and security specialists and, in turn, help ensure that business and security considerations related to IoT product development are well-balanced.

Integrate Security Best Practice with the IoT Product Development Process

Product Planning Should Begin with a Detailed Risk Analysis

The IoT product planning process should begin with a detailed risk analysis so that organizations have a clear view of the cyber threat landscape and a firm basis for choosing the right security features for their IoT products (see Figure 7). The analysis should include a study of disruptive attack scenarios, especially those arising from new and advanced types of threats. In addition, organizations must quantify the financial and non-financial impact of potential attacks on the organization as well as end-users. The results of the risk-analysis should feed into the IoT business plan, so that decisions on proceeding with product development and launch are based on a strong understanding of the potential risk factors.

A cyber security expert from a leading European research organization highlighted the importance of this analysis. "The technical measures for improving security – such as authentication and cryptography – are a second level problem," he explained. "The first level is to understand the risks. Organizations need to know what they want to protect against and then choose a solution depending on their analysis.[21]"

> *The results of the risk-analysis should feed into the IoT business plan, so that decisions on proceeding with product development and launch are based on a strong understanding of the potential risk factors.*

Embed Security throughout the IoT Product Design Process

This includes the design, coding, testing and evaluation:

- **Secured design.** Security mechanisms must be defined and implemented in the hardware and software architecture, during the design phase of the product. Organizations must also pay special attention to the implementation of cryptographic mechanisms.

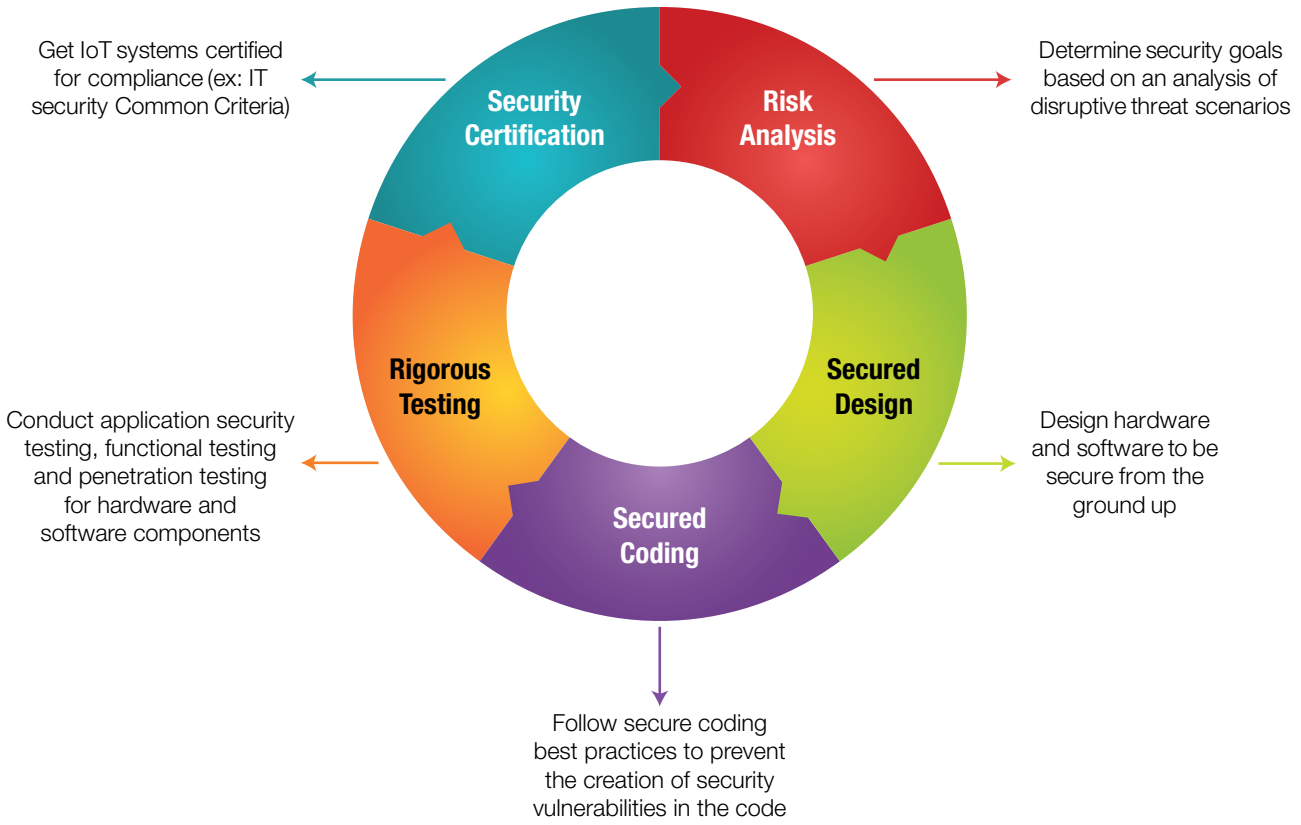
> *A significant number of software vulnerabilities can be addressed if organizations adhere to secure coding standards and best practices.*

- **Secured coding.** A significant number of software vulnerabilities can be addressed if organizations adhere to secure coding standards and best practices. Specific mechanisms such as code obfuscation should be implemented to prevent the reverse engineering of source code.
- **Rigorous testing.** IoT products should be subject to stringent security testing – including application security testing, functional testing and penetration testing – for the hardware as well as software components of the IoT system.
- **Security evaluation.** As the final step of securing their IoT products, organizations should liaise with specialized third-party security firms that have an Information Technology Security Evaluation Facility (ITSEF)[a] to ensure that these products go through a formal security evaluation process, such as Common Criteria[b]. Such an evaluation from a certified lab could in turn enable an organization to obtain an international security certificate for its IoT products.

[a] An accredited laboratory for security evaluations

[b] Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard for the security evaluation of computer products and systems

Figure 7: Revamp the IoT Product Development Process to Comprehensively Address Security Issues



Source: Capgemini Consulting and Sogeti High Tech Analysis

Educate Consumers as well as Front Line Staff in Security Best Practice

Including strong security features is only one part of securing an IoT product. The security of an IoT product also depends on the manner in which it is operated. To prevent cyber attacks, organizations must ensure that they educate consumers about the correct security procedures to be followed. This includes coaching on seemingly elementary issues, such as changing passwords regularly, which still remains one of the most common causes of security breaches. A senior executive at a leading European industrial manufacturing firm affirmed this view: "There are ways to counterbalance new kinds of threats from a technical standpoint. But that is not enough. It is also absolutely critical that the right procedures are laid down to operate a system. For example, customers need to change passwords regularly and manage access control appropriately.[22]"

At the same time, organizations must also train technical support staff so that they are better able to coach customers on security issues. An executive at a leading equipment manufacturer highlighted the need for such training, saying: "Our front line function, which is responsible for maintenance and spare parts, is made up of old-school technology specialists. They now need to understand the security features of our connected equipment so that they can respond to customer queries on security issues.[23]"

> *"To prevent cyber attacks, organizations must ensure that they educate consumers about the correct security procedures to be followed while using an IoT system."*

Address Privacy Concerns with Transparent Privacy Policies

To protect consumers from potential data privacy breaches, organizations must develop privacy policies that clearly detail how data from IoT devices is collected and used. Privacy policies should be readily accessible to consumers and easy to understand. Further, guidelines for opting into a service (or opting out) should be clearly described so that consumers can make informed choices about sharing data. In a post-Snowden world, where consumers are growing increasingly concerned about data privacy issues, a transparent privacy policy can be a key differentiator for an organization, signaling its commitment to protecting the interests of consumers.

While few organizations today seem to recognize security as a source of competitive advantage in the IoT world, BlackBerry is a notable exception. The smartphone manufacturer is aiming to establish itself as a leader in the IoT market, based on the platform of security (see Exhibit 2, "BlackBerry: Making Security the Foundation of an IoT Offering").

Cyber attacks are a grim reality in an increasingly connected world. However, despite mounting evidence of the potential human and material impact of such attacks, organizations have not yet trained all their guns on security threats. Building a secure IoT system begins with the recognition that security needs to be as much of a priority as the features and functionality of an IoT product.

As the world economy struggles to escape from stagnation and slowing growth levels, the IoT is a massive opportunity for organizations to achieve new levels of efficiency and to develop innovative new services and products. However, like Achilles, whose strength was compromised by one telling vulnerability, organizations must act on IoT security. Organizations that recognize this imperative are the ones who will lead this new IoT revolution.

Exhibit 2 - BlackBerry: Making Security the Foundation of an IoT Offering

BlackBerry, the once-iconic smartphone manufacturer, is betting on IoT to script a turnaround story. A major part of BlackBerry's transformation strategy involves leveraging its strengths in network security to become a leader in the IoT market. BlackBerry aims to achieve this by building an IoT platform that allows its customers to develop secure IoT applications. BlackBerry's IoT platform will provide various device management features that include over-the-air software updates. It is built on the "Project Ion" initiative that BlackBerry launched in May 2014 and leverages technologies that have made BlackBerry a leader in mobile data security and embedded systems. BlackBerry plans to initially target the shipping and automotive sectors with its platform. In future, it plans to extend the platform to other industry verticals such as healthcare and energy.

Project Ion: Laying the Foundation of a Secure IoT Platform

BlackBerry's Project Ion initiative comprises multiple efforts designed to promote the development of the IoT. This includes a secure application platform to gather data from across a range of devices and operating environments, and building relationships between partners, carriers and application developers. It also aims at building strategic partnerships with industry organizations such as the Industrial Internet Consortium and the Applications Developers Alliance.

QNX Systems: Bringing the Expertise in Embedded Software

QNX, bought by BlackBerry in 2010, is an operating system for embedded devices. QNX already powers mission-critical systems in cars, industrial applications and medical devices. It has a market share of more than 50% in the infotainment market and more than 50 million vehicles use QNX. In addition to infotainment systems, QNX also powers the "H Box" - a device used to capture and transmit secure medical data between patients, doctors and healthcare providers.

Source: Financial Post, "How BlackBerry can become the Google or Twitter of the Internet of Things", August 2014; BlackBerry Website; Forbes, "A Look At BlackBerry's Internet of Things Strategy", January 2015; Techcrunch, "BlackBerry Reveals Project Ion, Its QNX-Powered Effort To Underpin The Internet Of Things", May 2014; Forbes, "A Look At BlackBerry's Internet of Things Strategy", January 2015

> *"Privacy policies should be readily accessible to consumers and easy to understand."*

Research Methodology

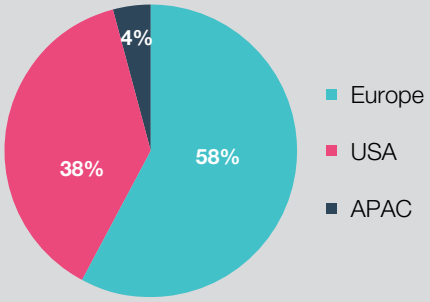
Capgemini Consulting and Sogeti High Tech conducted extensive research to understand the current state of security for IoT products. The research spanned two areas: the main survey concerning the security of the IoT and a benchmarking assessment of organizations' privacy policies. We surveyed more than 100 large enterprises and startups, interviewed industry executives and cyber security experts, and evaluated the data privacy policies governing the use of IoT devices in 100 organizations.

The Security of the IoT Survey

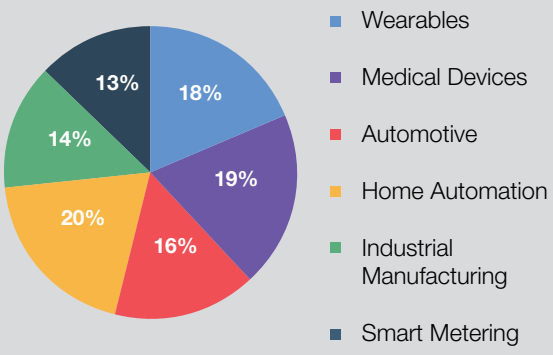
The survey was conducted in November 2014 and covered more than 100 industry executives involved in the development of IoT products. Survey respondents came from a range of industry segments, including Wearables, Medical Devices, Automotive, Home Automation, Smart Metering, and Industrial Manufacturing. The survey focused on gathering opinions on the following areas – the current levels of security in IoT products, key challenges that organizations face in securing their IoT products, and the approach to securing IoT products.

Survey Demographics

Region-wise Distribution of Respondents



Industry-wise Distribution of Respondents



Privacy Policy Benchmarking Assessment

We researched the IoT data privacy policies of 100 companies across the Wearables, Medical Devices, Automotive, and Home Automation segments. We evaluated the policies based on the level of transparency that they provided to users on the manner in which data from IoT devices was collected, used and shared with third parties.

About the Capgemini Cyber Security Service Line

Capgemini and Sogeti are experts in IT infrastructure and application integration. Together, we offer a complete range of cybersecurity services to guide and secure the digital transformation of companies and administrations. Our 2,500 professional employees support you in defining and implementing your cybersecurity strategies. We protect your IT and industrial systems, and the Internet of Things (IoT) products & systems. We have the resources to strengthen your defenses, optimize your investments and control your risks. They include our security experts (Infrastructures, Applications, Endpoints, Identity and Access Management), and our R&D team that specializes in malware analysis and forensics. We have ethical hackers, five multi-tenant security operation centers (SOC) around the world, an Information Technology Security Evaluation Facility, and we are a global leader in the field of testing.

References

1 Capgemini Consulting, “The Internet of Things: Are Organizations Ready For A Multi-Trillion Dollar Prize?”, May 2014

2 Bloomberg, “Target’s Data Breach: The Largest Retail Hack in U.S. History”, May 2014

3 ComputerWorld, “Target attack shows danger of remotely accessible HVAC systems”, February 2014

4 The Economist, “Home, hacked home: The perils of connected devices”, July 2014

5 Gartner.com, “Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020”, December 2013

6 Pew Research Center, “Digital Life in 2025: Cyber Attacks Likely to Increase”, October 2014

7 Capgemini Consulting and Sogeti High Tech Interview

8 Capgemini Consulting and Sogeti High Tech Interview

9 Washington Post, “Data breach hits Target’s profits, but that’s only the tip of the iceberg”, February 2014

10 LinkedIn.com, “Berg Insight says 3.0 million patients worldwide are remotely monitored”, 2014

11 HP.com, “HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack”, July 2014

12 Forbes.com, “Zubie: This Car Safety Tool ‘Could Have Given Hackers Control Of Your Vehicle’”, July 2014

13 FTC.gov, Federal Trade Commission, “Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers’ Privacy”, September 2013

14 CIO Today, “Internet of Things Growing Despite Privacy, Security Concerns”, December 2014

15 AliveCor.com, “AliveCor Privacy Notice”, September 2014

16 Automatic.com, “Terms of Service” (as on October 10th, 2014)

17 Fitbit.com, “Fitbit Privacy Policy”, August 2014

18 Capgemini Consulting and Sogeti High Tech Interview

19 InformationWeek Dark Reading, “Hiring Hackers To Secure The Internet Of Things”, December 2014

20 Wired.com, “The Internet of Things Is Wildly Insecure — And Often Unpatchable”, January 2014

21 Capgemini Consulting and Sogeti High Tech Interview

22 Capgemini Consulting and Sogeti High Tech Interview

23 Capgemini Consulting and Sogeti High Tech Interview

Authors

Franck Greverie
Corporate Vice President and
Global Head of Cyber Security
franck.greverie@sogeti.com

Jerome Buvat
Head of Digital Transformation
Research Institute
jerome.buvat@capgemini.com

Roopa Nambiar
Manager, Digital Transformation
Research Institute
roopa.nambiar@capgemini.com

Didier Appell
Director, Sogeti High Tech
didier.appell@sogeti.com

Ashish Bisht
Senior Consultant, Digital
Transformation Research Institute
ashish.bisht@capgemini.com

Digital Transformation Research Institute
dtri.in@capgemini.com

*The authors would like to acknowledge the contributions of **Melle van den Berg** from Capgemini Consulting Netherlands, **Johan Williamson** and **Karl Bjurstrom** from Capgemini Consulting Sweden, **Florian Knollmann** from Capgemini Consulting Germany, and **Erik van Ommeren** from Sogeti Group.*

The authors would also like to acknowledge the numerous executives who took time out of their schedules to share their views on security in the Internet of Things with us.

For more information contact

Capgemini Consulting

Germany/Austria/Switzerland
Guido Kamann
guido.kamann@capgemini.com

France
Cyril François
cyril.francois@capgemini.com

Spain
Christophe Jean Marc Mario
christophe.mario@capgemini.com

Sweden/Finland
Ulf Larson
ulf.larson@capgemini.com

United Kingdom
Richard Bowler
richard.bowler@capgemini.com

Netherlands
Onno Franken
onno.franken@capgemini.com

United States
Jeffrey T Hunter
jeffrey.hunter@capgemini.com

Sweden
Karl Bjurstrom
karl.bjurstrom@capgemini.com

Sogeti High Tech

Didier Appell
didier.appell@sogeti.com

Philippe Meleard
philippe.meleard@sogeti.com

Capgemini Consulting is the global strategy and transformation consulting organization of the Capgemini Group, specializing in advising and supporting enterprises in significant transformation, from innovative strategy to execution and with an unstinting focus on results. With the new digital economy creating significant disruptions and opportunities, our global team of over 3,600 talented individuals work with leading companies and governments to master Digital Transformation, drawing on our understanding of the digital economy and our leadership in business transformation and organizational change.

Find out more at: www.capgemini-consulting.com

Rightshore® is a trademark belonging to Capgemini

With more than 25 years of experience, Sogeti High Tech makes its skills and know-how available to industry in Aeronautics and Space, Defense, Energy, Telecoms & Media, Railway and Life Sciences sectors. To be more responsive to market needs, Sogeti High Tech has developed a range of expertise based on its R&D department, High Tech Labs, a real innovations incubator. In close partnership with its customers, Sogeti High Tech develops and manufactures solutions with a high added value in the areas of Internet of Things, collaborative multi-agents systems, Big Data and cyber-security. Subsidiary company of Capgemini Group, Sogeti High Tech is a center of excellence in System Engineering, Physical Engineering, Software Engineering, Testing and Consulting services.

Learn more about us at www.sogeti-hightech.fr

About Capgemini and the Collaborative Business Experience

With more than 130,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2013 global revenues of EUR 10.1 billion. Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at www.capgemini.com