Security and the Internet of Things (IoT)

Analysis and Recommendations for IoT Manufacturers and IT/Business Executives

Wei (Weslay) Xu
Tuck School of Business at Dartmouth
03/20/2015
High Level Description

There have been three revolutionary waves in the development of the Internet. The first wave, back in the 90s, was user devices (mainly desktops) connecting to businesses via wired Internet connections (dial-up, DSL, etc.).

The second wave, back in the 2000s, was mobile devices (Smartphones, tablets, etc.) connecting to businesses and each other via wireless Internet.

The third wave that is happening now, which we would discuss in this whitepaper, is "things" connecting to businesses and each other via both wired and wireless connections. The “Things” we referred to here can be categorized into the following two sectors:

1. Industrial devices – Devices used in critical industrial infrastructure, such as sensors used in power plants, manufacturing facilities, transportation, etc.

2. Personal devices – Devices used in people’s everyday personal and business life, such as mobile devices, fitness and medical devices, home automation devices, automobile accessories, etc.

By nature, these IoT devices can gather, store and exchange very sensitive personal data and information, such as social security numbers and banking information. As a result, they can become potential high priority targets for cyber-attacks, identity theft and fraudulent activities. In addition, as the number of IoT devices now increases at an unprecedented speed, security concerns also multiply exponentially. Furthermore, the paradigm change and shift led by the emergence of IoT have posed significant challenges to both IT and business professionals in today’s organizations, and will force them to re-evaluate the current IT environment and re-consider the current IT strategies.

In this whitepaper, we will mainly focus on Internet of Things (IoT) devices, the underlying challenges for IoT device manufacturers, as well as IT and business executives at corporations, and the recommended action plans and strategies.

Key Challenges

The new wave of the rapid adoption of IoT devices, both in personal and business environments, has brought tremendous challenges for IoT device manufacturers, as well as CIOs and CISOs.
Device Manufacturers

According to a 2014 Gartner report, IoT install base will surpass 5 billion connected devices by 2015 and will grow to 25 billion connected devices by 2020. However, based on a research conducted by Hewlett-Packard in 2014, an alarmingly high average number of vulnerabilities per device HP examined were identified:

1. Privacy concerns: A large number of IoT devices collect some form of sensitive personal information such as name, address, credit card numbers, etc. In addition, these concerns are multiplied as many of these devices are connected via cloud services and mobile apps. These sensitive information can be transmitted on your home network unencrypted and subsequently attacked by hackers via the Internet, leading to serious privacy concerns and issues.

2. Insufficient authentication and authorization: A majority of IoT devices don’t require strong password for users to access their local management interface and/or have insecure password recovery mechanisms. Furthermore, many of these devices use the same weak passwords on their cloud websites and/or mobile apps, thus leaving the door wide open for hackers or malicious software to gain access to these devices remotely.

3. Lack of transport encryption: Transport encryption is critical given that many of the IoT devices are collecting and transmitting sensitive personal data. However, based on the HP research, a majority of the devices failed to encrypt network data transmission both on local network and the Internet.

4. Insecure web interface: The IoT devices HP examined had raised serious security issues such as persistent cross-site scripting, poor session management, and weak default credentials. Considering many of the devices offer access via the cloud, these issues are of more significant concerns.

5. Insecure software and firmware: Over 60% of the IoT devices HP examined had issues including no encryption when downloading software and firmware updates. Therefore malicious software and firmware could be installed into the original system via system updates.
CIO/CISO

With the adoption of IoT devices in the corporate environment, the landscape of the business environment changed fundamentally. In addition to dealing with the day-to-day operations of traditional IT devices, CIOs and CISOs now need to simultaneously manage both devices and make sure not to cause any business interruptions. Based on a 2014 Gartner Report, CIOs and CISOs should pay special attention to the following 4 areas:

1. The evolving adoption of IoT devices have fundamentally changed the business environments. CIOs and CISOs need to redefine the scope of their security efforts beyond their present responsibilities.

2. CIOs and CISOs need to understand the impact brought by the adoption of IoT devices. This does not necessarily mean that they should replace the current security strategies and solutions. On the contrary, in many cases, there are potentials to integrate new security solutions with the existing ones. Therefore CIOs and CISOs should carefully evaluate their current security options first.

3. There is currently no definitive guide to securing IoT available. In addition, the adoption of IoT devices can be of vast number of different combinations of technologies and services. Therefore, the task to secure these IoT devices is dynamic and constantly changing.

4. The requirements for securing IoT devices are very complex. CIOs and CISOs must take into consideration multiple aspects, including but not limited to: mobile and cloud architectures, industrial control, automation and physical security.

Industries / Groups Impacted

A wide range of industries and groups are impacted by the rapid adoption of IoT devices. In general, IoT can be broken up into five key verticals of adoption: Connected Wearable Devices, Connected Cars, Connected Homes, Connected Cities and the Industrial Internet.

Many participants, including device manufacturers, consumers, corporations, security vendors, infrastructure providers and governments will be engaged in this adoption process, and play their different roles, ranging from manufacturing, securing to managing, consuming and regulating.

In addition, different industries/groups can harness tremendous gains from the adoption of IoT devices. The following chart from Cisco report shows four industries with most to gain from IoT adoption:
Best / Representative Practices

Device Manufacturers

Considering the increasing number of IoT devices being deployed both in personal and business environment, the findings by Hewlett-Packard we talked about earlier have raised red flags for device manufacturers, consumers and corporations. In order to minimize and mitigate the risks, the actions below are recommended for the device manufacturers:

1. **Conduct a security review of devices and all associated components**

   Use automated security tools provided by established security companies to test and scan the products, software, firmware and network activities of all IoT devices. Review the results and take necessary steps to fix the vulnerabilities and bugs in the products.

2. **Implement security standards across all products before production**

   Although there are no established global standards for IoT security, IoT device manufacturers should use recommendations and guidelines published by security companies and organizations (such as OWASP’s Internet of Things Top Ten Project, [https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project)) to carefully plan and design the devices before they are put into production.

3. **Ensure security is incorporated throughout the product lifecycle**

   Security is not a one-time effort. Instead, from product planning to product support, throughout the entire product lifecycle security should be considered as one of the top priorities for manufacturers. In addition, when the IoT products come to the end-of-life, manufacturers still should provide best efforts support to minimize the future security impact of these products.

CIO/CISO
Because of the complexity of IoT devices, as well as the different combinations of technologies and architectures involved, CIOs and CISOs should leverage their existing security solutions and resources on specific use cases:

1. Re-examine and re-evaluate the current IT security plans, processes and strategies to incorporate new technologies and architectures used by adopted IoT devices and platforms.

2. Evaluate the IoT devices being used in the IT and business environment, and understand the possible combinations of technologies (mainframe, client/server, Web, Cloud and mobility) in specific use cases.

3. Instead of trying to solve all the IoT security issues all at once, CIOs and CISOs should instead try to develop initial security solutions based on specific IoT interactions within specific business use cases. Consequently, they should seek to define ownership and responsibility areas for IoT security projects.

4. CIOs and CISOs should work with their staff to carefully monitor the following technologies to better understand security requirements:
   a. Wireless technologies and standards, such as ZigBee and Modbus
   b. Hardware platforms, such as Arduino and TMote Sky
   c. Connected-device software platforms, such as TinyOS and Android
   d. Cloud application software platforms, such as ThingWorx and Evrything

**Business Benefit**

Although it brought a lot of challenges in terms of management and security, the adoption of IoT devices can also provide tangible business benefits and values:

1. Cost savings: Cost savings can be achieved through improving asset utilization, process efficiencies and productivity.

2. Improved asset utilization: With IoT devices, the tracking of assets can become much more accurate and in-time. These real-time insights and visibility into the assets can provide tremendous benefits to the business.

3. Efficient processes: By using real-time operational insights, organizations can make smarter business decisions and thereby reduce operating costs and minimize human intervention.

4. Improved productivity: IoT improves organizational productivity by offering employees just-in-time training, thereby reduces unnecessary and unmatched skills, improving labor efficiency.
Case Examples

A good example is Bosch, a German manufacturer of consumer and industrial products. They are trying to build the next wave of manufacturing with IoT-enabled systems. In the process of setting up this system, security was the most oft-cited obstacle to setting up their smart factories.

As part of their solutions, they took carefully evaluated steps to secure their environment:

1. Operations managers ensured that safeguards are built into the solution including security procedures such as hardware encryption, physical building security and network security for data in transit.

2. The network is also designed to allow secure remote access to systems. Security and networking solutions are engineered to withstand harsh environmental conditions, such as heat and moisture, that aren't present in typical networks.

3. Identity and authentication structures are also updated to support “things” as well as people.

Conclusion

As explored in this whitepaper, we are now in the process of seeing a wide range of IoT devices quickly being adopted both in personal and business environment. IT and business executives should be fully aware of this trend, and actively seeking to apply best practices and strategies in terms of protecting both the security of the corporate environment, as well as the privacy concerns of their customers and employees.

CIOs and CISOs should examine the existing security solutions and strategies, understand the technologies and architectures used by incoming IoT devices, define ownership and responsibility areas for IoT security projects, and then leverage on the existing resources to develop initial security solutions based on specific IoT interactions within specific business use cases.

Footnotes:

1 The Internet of Things: Making sense of the next mega-trend, Goldman Sachs, Sep 2014

2 Gartner Says 4.9 Billion Connected “Things” Will Be in Use in 2015, Gartner, Nov 2014

3 Internet of Things Research Study 2014 Report, Hewlett-Packard, Sep 2014

4 What Securing the Internet of Things Mean for CISOs, Gartner, Apr 2014

5 The Internet of Everything: How More Relevant and Valuable Connections Will Change the World, Cisco IBSG, 2012

6 Building Smarter Manufacturing With The Internet of Things (IoT), Lopez Research, Jan 2014
About the Center

The Glassmeyer/McNamee Center for Digital Strategies at the Tuck School of Business focuses on enabling business strategy and innovation. Digital strategies and information technologies that harness a company's unique competencies can push business strategy to a new level.

At the center, we foster intellectual leadership by forging a learning community of scholars, executives, and students focused on the role of digital strategies in creating competitive advantage in corporations and value chains. We accomplish this mission by conducting high-impact research; creating a dialog between CIOs and their functional executive colleagues; and driving an understanding of digital strategies into the MBA curriculum.

We fulfill our mission by concentrating on the three following areas:

**Scholarly Research**
Connecting practice with scholarship anchored on IT enabled business strategy and processes.

**Executive Dialog**
Convening roundtables focused on the role of the CIO to enable business strategy.

**Curriculum Innovation**
Bringing digital strategies into the classroom through case development and experiential learning.