Internet of Things (IoT) Thought Paper

Introduction

The purpose of this paper is to provide insights to what the Internet of Things (IoT) is and the security issues associated with the use of current IoT solutions, to enable informed decision-making for the BC public sector organizations on the adoption of IoT.

Background

The first IoT device was a toaster that could be turned on and off over the internet in 1990.[1] The growth in IoT has been exponential since the launch of IPV6 on the internet in 2011.[1] The power of cloud computing further fuels this growth.[4] The International Data Corporation (IDC) predicts the global market for IoT solutions to grow to $1.7 trillion by 2020.[2]

IoT provides opportunities for more direct integration of the physical world into computer-based systems that can result in improved efficiency, accuracy, cost savings and automation. It redefines the way humans and machines interface and how they interact with the world around them.[4] It represents a world where smart objects are seamlessly integrated as part of a global network; where smart objects interact without human intervention to deliver new services or improved processes beyond the silos and across the business.[4] The value from adopting IoT comes from enabling data to be transformed into information that improves productivity, decision-making and the customer experience for the whole enterprise.[4]

IoT is often introduced into the enterprise environment without the enterprise's knowledge and this introduces hidden risks for the enterprise since IoT vendors usually put profit and speed to market before anything else, with cybersecurity very low down on the list of priorities[3]. Despite the risks associated with IoT, it offers too many benefits to ban outright, and therefore, it is essential that a risk assessment is performed before introducing it into the enterprise environment.

Benefits

IoT brings together all sorts of technology developments that enable actionable insights from the data generated by things[Δ], to transforming how people interact with machines and how machines interact with each other.[4] These actionable insights will enable a fundamental change in how business and society operate:[4]

- **Proactive and preventive.**[4] A change from health to asset maintenance will cause a fundamental shift as people look proactively for causes of issues (insights) and take early-stage action to prevent, where possible, a larger issue.[4] For instance, IoT can transform society's infrastructure by providing a single holistic approach to transport management and enable logistics operators

Footnote [Δ] *The term 'things' is used to represent sensors, actuators, devices and machines that are connected through the Ethernet, Powerline, QR codes, proprietary open access multicast wireless sensor network technology (ANT) , Wi-Fi, radio-frequency identification (RFID), Bluetooth, near-field communication (NFC), ZigBee, cellular 4G, etc. (see Reference #12 for more details) that are part of the IoT technology.*

[1] https://www.postscapes.com/internet-of-things-history/ [accessed 3/9/2018]
[2] https://www.nist.gov/news-events/news/2016/07/nists-network-things-model-builds-foundation-help-define-internet-things [accessed 3/5/2018]
[3] http://www.zdnet.com/article/internet-of-things-security-what-happens-when-every-device-is-smart-and-you-dont-even-know-it/ [accessed 3/5/2018]
[4] CGI: The Internet of Things for Dummies - https://www.cgi-group.co.uk/article/internet-of-things-for-dummies [accessed 3/6/2018]

to proactively adjust the provided capacity as well as the routes and services offered to the public and business.[4] It can also enhance future healthcare systems by enabling users to orchestrate complex clinical and organizational processes across multiple platforms to improve patient safety, reduce cost and improve the health of populations.[4]

- **Data-driven business models**.[4] Business will migrate from a subscription or 'flat-fee' based model to ones based on usage, time, duration, load, risk and so on, fundamentally changing how people buy and consume products and services.[4] For example, smart meters in the home will provide energy suppliers with significant insights to enable proactive demand management by offering consumers things such as demand-based tariffs.[4]
- **Interconnectivity and collaboration**.[4] A move from 'siloed' datasets to an interconnected world in which trusted parties subscribe to published data will shift businesses to a position where they learn from other people and organizations to enhance their own performance.[4] For instance, in building management, IoT will enable a single view of building operation, allowing operators to visualize how one system or event is impacting others, that will result in improvements in energy consumption, maintenance schedules, and how real estate properties are offered for lease based on footfall.[4] It can also enable building owners to maximize the use of their building throughout the day, enabling access and billing to companies in the daytime and to social groups in the evenings.[4]

Challenges

In order to gain the many benefits IoT can bring, the challenges its rapid emergence presents first need to be addressed:

- **Information security**.[5] The IoT brings risks inherent in potentially unsecured information technology into the environment where it is used; be it in homes, corporate offices, factories, and communities. IoT devices, networks or cloud servers where the IoT data is generated, transmitted, processed or stored can be compromised in a cyberattack.[6] Given the variety of differences between enterprise IT and IoT, standard enterprise security tools and practices (e.g. authentication, encryption, ID management, security patching, etc.) may not be viable or applicable and will need to be rethought and reworked to address the challenges posed by IoT.
- **Privacy**.[5] Certain data elements in the IoT ecosystem can become personal information even though, on the surface, they may not appear to fit traditional understanding of personal information.[7] Also, smart devices that monitor public spaces may collect information about individuals without their knowledge or consent.[5] Forethought on privacy is a must in the design and/or implementation of IoT solutions as it will be difficult, if possible, to retrofit privacy measures after the fact.
- **Safety**.[5] An IoT security breach does not just present a traditional loss of data, but a physical attack that might involve human casualties or fatalities.[8] Researchers have demonstrated that IoT devices such as connected automobiles and medical devices can be hacked, potentially endangering the health and safety of their owners.[5] Careful consideration is a must on what, where and how IoT is adopted until security is integrated into the design and development of IoT.

[4] *CGI: The Internet of Things for Dummies - https://www.cgi-group.co.uk/article/internet-of-things-for-dummies [accessed 3/6/2018]*
[5] *US Government Accountability Office: IoT Technical Assessment - https://www.gao.gov/assets/690/684590.pdf [accessed 3/5/2018]*
[6] *http://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/ [accessed 3/5/2018]*
[7] *Office of the Privacy Commissioner of Canada: The Internet of Things - https://www.priv.gc.ca/media/1808/iot_201602_e.pdf [accessed 3/5/2018]*
[8] *A Computer Weekly Buyer's Guide to Internet of Things Security [accessed 3/5/2018]*

- **Standards**.[5] There is currently no single universally recognized set of standards or definitions for the IoT, nor a commonly accepted definition among various standards organizations. Due to the complex nature of IoT, there are numerous standards* that address different aspects of IoT, especially in communications and networking[5]. This can create a potential issue of standards incompatibility and prevent interoperability between devices. Unproven standards can also increase integration and implementation complexity as well as security risks. It will also be necessary to consider the life-span of the IoT, its potential integration and where it is planned to be used to ensure the long-term viability of the adopted IoT.[ø]

Recommendations to Public Sector Organizations

The following recommendations are geared towards the public sector organizations and are advised to be enacted sooner than later:

1. Ensure a policy[¥] is created or the existing updated for the adoption and governance of IoT to ensure that the same rigor around procurement, implementation, operations and management of enterprise IT is applied to any device or object embedded with IoT connectivity (e.g. domestic appliances, TVs, security cameras, light bulbs, elevators, automobiles, bridges, etc.) installed in the enterprise environment.
2. Develop a framework for secure adoption of IoT solutions and ensure both operational technology[†] (OT) and cyber security teams are involved in the adoption lifecycle of IoT solutions/devices i.e. procurement, use/implementation and disposal of IoT solutions/devices since enterprise IoT today is often a convergence of IT systems for data-centric computing and OT systems for monitoring events, processes and devices and making automatic adjustments in enterprise and industrial operations.
3. Develop an IoT adoption standard to support the IoT adoption and governance policy (**Recommendation #2**) to ensure that IoT is implemented securely. For example, the adoption standard can specify that IoT devices or objects with embedded IoT connectivity are segmented and isolated based on their business purpose and function, require that the IoT device is configured securely, supports authentication and changing of default passwords, allows disabling unnecessary features and functions, etc. The standard can also specify how to manage the IoT supply chain risks.
4. Invest the necessary skills and resources in big data analytics that harnesses the data generated by IoT that can be used to inform and transform policy development, program and service delivery.
5. Develop the necessary policies and frameworks to guide the use of big data analytics to ensure compliance with existing legislative frameworks that protect privacy and security of personal information.[7]
6. Be an active participant in the IoT space to influence the developments of IoT.

Footnote: ** Institute of Electrical and Electronic Engineers (IEEE) has more than 350 standards that can apply to IoT, and more than 110 IoT-related standards in development.[5] NIST has developed a number of standards and frameworks related to IoT and is working on several more as well. Other groups like International Telecommunication Union (ITU), Industrial Internet Consortium, the Thread Group, Apple and Google have also developed standards and frameworks.[5]*

[ø] Unlike traditional IT systems, an IoT device like an IoT enabled pacemaker may not be as easily replaced when it fails or upgraded as quickly as needed to address a security vulnerability.

[†] Operational Technology (OT) is a category of hardware and software that monitors and controls how physical devices perform. Example of an OT is a SCADA system.

[¥] Contact InfoSecAdvisoryServices@gov.bc.ca for further guidance.

[5] *US Government Accountability Office: IoT Technical Assessment - https://www.gao.gov/assets/690/684590.pdf [accessed 3/5/2018]*

[7] *Office of the Privacy Commissioner of Canada: The Internet of Things - https://www.priv.gc.ca/media/1808/iot_201602_e.pdf [accessed 3/5/2018]*

References

1. *National Institute of Standards and Technology (NIST) SP 800-183 – Networks of 'Things' - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf [accessed 3/5/2018]*
2. *National Institute of Standards and Technology (NIST): Demystifying the Internet of Things - http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=921822 [accessed 3/6/2018]*
3. *Forrester: The State of IoT Security 2018 [accessed 2/13/2018]*
4. *Gartner: Leading the IoT – Gartner Insights on How to Lead in a Connected World - https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf [accessed 3/12/2018]*
5. *451Research: Secure all the Things: tackling the challenges of IoT security [accessed 3/5/2018]*
6. *TechTarget: IoT Agenda E-guide – Prevent Enterprise IoT Security Challenges – Your expert guide to preparing your security program for IoT - http://media.techtarget.com/digitalguide/images/Misc/EA-Marketing/Eguides/Prevent-Enterprise-IoT-Security-Challenges.pdf [accessed 3/5/2018]*
7. *Fortinet: FORTIGUARD 2018 THREAT PREDICTIONS - https://dbac8a2e962120c65098-4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/2018-threat-predictions-pdf-2-w-4005.pdf [accessed 3/9/2018]*
8. *Industrial Internet Consortium: Industrial Internet of Things Volume G4: Security Framework - http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf [accessed 3/6/2018]*
9. *Cyber Physical Systems Public Working Group: Framework for Cyber-Physical Systems Release 1.0 - https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf [accessed 3/6/2018]*
10. *https://dataflog.com/read/internet-of-things-iot-security-privacy-safety/948 [accessed 3/9/2018]*
11. *https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program [accessed 3/9/2018]*
12. *https://www.postscapes.com/internet-of-things-technologies/ [accessed 3/19/2018]*