Internet Of Things And Cybersecurity

Introduction

The “Internet of Things” (IoT) is the developing web of objects embedded with microchips capable of allowing sending and receiving data, and so connecting them to the network we call the Internet. In an article in the Harvard Business Review late last year, Michael Porter and James Heppelmann explained that the “smart, connected products” constituting the Internet of things consisted of three basic components – the physical component that gave them their function, the smart component consisting of sensors and software, and the connectivity components, including antennae, radios and connection protocols. Those connections can be one-to-one (in which the product connects a user, the manufacturer, or another product), one-to-many (a central system that connects to many products), or many-to-many (where multiple products connect other products and data sources).

Business Considerations

The IoT has a huge potential for business. A McKinsey Global Institute report, published in June 2015 sees value not only in business-to-business applications but also in consumer applications, ranging from fitness monitors and self-driving cars to medical devices. Indeed, in terms of medical devices alone, McKinsey foresees that the value of improved health of chronic disease patients through monitoring could be as much as $1.1 trillion per year by 2025. The McKinsey report predicts a potential economic impact – including consumer surplus, of as much as $11.1 trillion per year in 2025 for IOT applications in nine specific settings – home automation and security, office security and energy, factory operations and optimization, retail environment automated checkout, worksite operation and health and safety, human health and fitness, logistics and navigation, public health and transportation, and commercial vehicles.

Security Considerations

Where there is profit there is risk. In the case of the Internet of Things, that risk is not merely financial. The IoT poses huge privacy and security issues, all the more so because many intended IoT applications are themselves security applications, as the McKinsey report makes clear. Even outside of IoT security applications – in the realm of consumer products and transportation – system security is a fundamental issue. This was made clear in mid-July, when Wired Magazine reported that two hackers demonstrated that it was possible to seize wireless control of certain functions of a vehicle, via its Internet connected entertainment system. The vehicle manufacturer

took immediate action by applying network level security measures to prevent remote manipulation reported, by blocking remote access to certain vehicle systems. No injuries resulted. The vehicle manufacturer conducted a voluntary safety recall.

System security is obviously critical. Indeed, in a near future world in which medical devices become part of the IoT, one can imagine scenarios in which system security is supercritical. It will not be long before hackers can target the security of systems of given individuals, in the same way that they can, and do, today target the data of given individuals. We may at that point enter a world in which hackers can exact physical harm, on an individualized basis.

As Dominque Guinard recently reported in an article in The Guardian, data is the lifeblood of the IoT. Users contribute to the IoT by allowing companies to access their information to better understand and predict behavior, and to anticipate needs. While often mundane, the kind and quality of data which will be and is being produced in the IoT can be much more private than the kind of identification and financial data with which we have been historically concerned. Your car, fridge, and smart watch know a good deal more about you than you think. The sheer interconnectedness of the IoT raises profound issues about who controls the data which is its life's blood.

Governance and Legal Considerations

Businesses need to approach the IoT with their eyes open. Data and system security need to be at the forefront of any IoT Business Plan – they are not issues that one can "come back to later." Put in different terms, it is cheaper to plan system and data security into a product or offering than it is to revise the product or offering or, worse still, recall or cancel it.

Organizations should determine their strategy in relation to IoT security at a corporate level. Businesses need to ask themselves the essential questions. What data are we collecting or transacting in? Do we really need the data? What are the implications of its loss? Who suffers? What are the risks of loss of the system? What are the consequences of system loss? Knowing what is at risk is half the battle. Knowing how to address that risk, in both technological and legal terms, is the other half.