Are you ready for the industrial internet of things?

Wake up and smell the coffee

The term internet of things (IoT) first emerged in 1999 – coined for an internal presentation to grab the attention of executives. Invented at a time when anything associated with the web was a red hot business topic, the speaker knew that talking about linking RFID tags to the internet[1] would guarantee his audience's interest. But despite its origins in business machine-to-machine (M2M) communication, the media became obsessed with its potential to replenish milk. The concept of a fridge sensor automatically reordering dairy products before they ran out became the poster child example for connected devices. Perhaps this is why, unless an enterprise drank a lot of coffee, the exponential growth and associated risk of connected devices may not have registered with every information security professional – until now.

Since 1999

52% OF FORTUNE 500 COMPANIES HAVE GONE BANKRUPT, BEEN ACQUIRED OR CEASED TO EXIST

Move forward just over a decade and Costa Coffee, the second-largest coffee shop chain in the world after Starbucks, has over 2,500 connected Costa Express machines in locations such as schools, hospitals and offices.[2] These machines not only aim to give users the sights, smells and sounds of the coffee shop, but scan customers to try to predict and suggest individualized products. They also offer real-time, comparative reporting on menu items' popularity and sensor-triggered automatic product replenishment, therefore reducing operational costs. Forget milk – global business is now competing for places within the industrial IoT – exploiting connected devices to offer new services, driving performance improvement, reshaping experiences and entering new markets – and quickly.

Since 1999 and, coincidentally, the invention of the term IoT, 52 percent of the companies in the Fortune 500 have gone bankrupt, been acquired or ceased to exist[3]. This has largely been attributed to disruption of traditional industry models by new, often digital ways of doing business. As with most technology innovations, the IoT creates great opportunity. But with this opportunity comes new risk: that the data, devices and systems we rely upon for new and innovative services, will be compromised in ways that are increasingly difficult to detect or defend against.

The internet of everything

So what do we mean by the internet of things? IoT enables objects, devices, animals and even people with unique identifiers (IP addresses) to transfer collected data over a network without human-to-human or human-to-computer interaction. IoT's growth has evolved from the convergence of the internet with micro-electromechanical systems and wireless technologies. Its acceleration is driven by the reduction in the size and cost of sensors, cheaper computing power, big data analytics and the increased availability of IP addresses through IPv6. For the IoT, a 'thing' could be a car with embedded devices that alert the driver to changes in tire pressure; an app that allows you to set your home heating system remotely while driving home; a farm animal with a biochip transponder that can diagnose and alert the farmer to specific health issues; a chip monitoring a medical condition within a person; or a manufacturer's machine that can self- diagnose potential failures, in order to minimize production interruption during maintenance.

In 2017

THE FIELD SERVICE INDUSTRY ALONE WILL SAVE $1 BILLION BY ADOPTING CONNECTED SMARTGLASSES

As we move to the internet of everything, where we have the capacity to assign an IP address to anything on the planet, industries such as financial services, pharma and energy are joining manufacturing and logistics in seeking ways to exploit the IoT potential. That is, the ability of connected devices to collect new data that can be turned into actionable insight.

1. RFID Journal 2. Reuters 3. Cap Gemini: When Digital Disruption Strikes: How Can Incumbents Respond?

Using techniques such as deep machine learning, cognitive computing technologies, speech and image recognition and reasoning capabilities means that industry analysts such as IDC predict an explosion in devices – 32 billion by 2020.[4] They also predict that IoT devices will generate 10 percent of the 44 zettabytes of data that will exist in the same timeframe.

By 2018

THE WEARABLE TECHNOLOGY MARKET IS ESTIMATED TO BE WORTH $12.6 BILLION

Amongst all this excitement – information security professionals are taking a hard look at the risks of IoT concerning not only data privacy, data sovereignty and security, but also wireless infrastructure required to deliver the levels of connectivity and availability.

Creating a secure wireless infrastructure for industrial IoT

As we create network and communications infrastructures to support the industrial IoT globally, a vast number of different wireless technologies will be used to connect devices to the internet.

As IoT services are distributed to more users and endpoints, often located in remote areas or subject to tough environmental conditions, enterprises must ensure their wireless LANs are bolstered by the right networking solutions to handle the additional number of clients sending and receiving data. Whatever approach an organization takes to IoT deployment, a robust, secure wireless network is an essential component, as is wireless connectivity management, controllers to manage traffic, a secure system to integrate wireless and wired networks, and the right appliances to maximize the value of data centre or cloud deployments.

Wireless networks are increasingly an extension of an organization's internal network and IoT will further accelerate demand. Failure to establish industry best practice levels of protection in a wireless access point or to connected clients can result in a potential breach of your internal network. For example, IoT connected device policies would need to be in place for things such as BYOD (Bring Your Own Device) in order to protect crucial access points to corporate data.

Protecting the business value of IoT

Industry analysts such as Gartner have made some bold predictions as to the business value of IoT. Forecasts suggest, for example, that by adopting connected smartglasses, the field service industry alone will save $1 billion by 2017[5]. The wearable technology market which includes products such as Google Glass and the Apple Watch as well as other medical connected devices is estimated to be worth some $34 billion[6] by 2020. For the healthcare industry, connected devices offer the potential to transform areas such as epidemiological studies by integrating lifestyle data with genetics data to analyze predispositions to certain diseases. The policies around collecting, storing and accessing this type of sensitive data will need to be carefully considered and integrated with an organization's security strategy and compliance standards. Patients and clinicians will need support from information security advisors to give them confidence that appropriate data protection and governance controls are in place, while avoiding protocols that unnecessarily limit the beneficial use of new information.

By 2020

IDC PREDICTS THERE WILL BE 32 BILLION CONNECTED DEVICES ON THE PLANET

IoT has the potential to create value in other public services as well as in health. For example, in Los Angeles, IoT has enabled the city to create 7,000 smart parking spaces. Embedded road sensors provide real-time parking information via a smartphone app. Everyone appears to win from this innovation, with space utilization up by 11 percent and parking revenues up by 2 percent – yet the average cost of parking for consumers reduced by 11 percent.[7] What this example highlights is that IoT services often rely upon sharing data across partner organizations – in this case the city, parking companies and consumers. This requires an understanding of expected software and security controls, clear communication to IoT stakeholders and potentially new governance frameworks to verify compliance. Establishing mechanisms to understand what data is being collected and accessed and by whom is also a critical part of maintaining trust. This is particularly important as we adopt intimate smart devices such as self- monitoring pacemakers and in-home heating and lighting controls.

By 2020

IOT DEVICES WILL GENERATE 10% OF THE 44 ZETTABYTES OF DATA THAT WILL EXIST GLOBALLY

Managing risk in context – establishing the Visibility of Things

As the IoT landscape evolves to exploit rapidly emerging commercial opportunities, information security professionals are faced with re-examining the impact of these developments upon their risk exposure. Evaluating how this explosion of additional endpoints and data sits within an organization's core risk and security strategy, as well as the active management of corporate policies, is necessary to ensure the long term confidentiality, integrity and availability of IoT services. Ironically, although the core of IoT is automatic data exchange – very few organizations have dynamic information security infrastructures that could deliver comprehensive visibility and control of every connected device. For example, within Siemens' electronics manufacturing plant in Amberg, Germany, machines and computers handle 75 percent of the value chain autonomously, with some 1,000 automation controllers in operation from one end of the production line to the other.[8]

"For most organizations, integrating 1,000 additional endpoints into core security processes such as identity and access management, asset monitoring, device management, data loss prevention and incident management would be a profound challenge"

Greg Hampton, VP Product Management, NTT Security

Many organizations may not even be aware of how many connected devices are already in use within internal or external processes or services that would need to be incorporated into their enterprise security architecture.

4. IDC's Worldwide Internet of Things Taxonomy, 2015, Worldwide Internet of Things Forecast, 2015–2020 5. Gartner Says Smartglasses Will Bring Innovation to Workplace Efficiency', press release, 2013 6. Forbes: Wearable Tech Market To Be Worth $34 Billion By 2020 7. Accenture Technology Vision 2015 – Digital Business Era: Stretch Your Boundaries 8. Siemens: Defects: A Vanishing Species? Pictures for the Future

The NTT Security point of view: the value of an intelligence-based approach

Connected devices help organizations offer new services, reshape experiences and enter new markets. But with these opportunities come risks that the data, devices and systems we need for new ways of doing business, will be compromised with new and unforeseen consequences - such as your fridge not ordering milk thus indicating to criminals that your house is unattended; your car launching a denial of service against the local traffic lights; or an implant not delivering the correct dose of medication.

In our experience, wireless networks have often been neglected as part of operational testing programs and therefore have become easy targets for those seeking to compromise an organization's network. This is why as part of any IoT deployment, NTT Security recommends that organizations conduct penetration testing from both within and outside company premises. Only by doing this will an organization be able to see themselves as an attacker would in attempting to gain access to wireless networks.

So how can organizations get ready to embrace the opportunities of the IoT securely?

IoT is driving connectivity on a scale never before seen – as well as requiring organizations to make good security practice supported by robust system design an essential part of everyday life.[9]

As part of the digital transformation of business, new applications will demand new models and security controls and IoT offers the chance to bake in security at the outset, rather than reactively.

At NTT Security, we are working with organizations to establish what IoT devices already exist in the work place, the value of the data these devices generate or exchange in a business context – and how to maintain the long-term, sustainable visibility of things necessary for continuous risk management.

Our R&D labs are working every day to develop and practicalize reliable security technologies that protect against the misuse, runaway, or disclosure of data in rapidly advancing fields like connected cars and medical devices.

One IoT concept is to enable flexible, secure, and scalable collaboration among IoT services and devices. Applications could include enabling a personal healthcare service to safely and securely collaborate with other services; determining, for example, a dynamic auto insurance premium based on the driver's personal health data and driving data obtained from the car.

For more information on how NTT Security can help you to take practical steps to anticipate the challenges of IoT for your business and build and implement processes and controls for agile, secure adoption, visit **www.nttsecurity.com**

About NTT Security

NTT Security is the specialized security company of NTT Group. With embedded security we enable Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of consulting and managed services for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more.

To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information.

9. UK Government Office for Science: The Internet of Things: making the most of the second digital revolution