Industry 4.0: Security imperatives for IoT — converging networks, increasing risks

Received (in revised form): 15th May, 2017

Shaun Bligh-Wall

is a global security infrastructure and end point strategy advisor within the Security Consulting team of DXC Security. He has worked in a number of information security roles over the last 20 years. Currently, his primary responsibility is research and development of DXC's security consulting portfolio. This includes working closely with clients, other DXC teams and technology partners to define and provide a cohesive approach to delivering consulting services that align with corporate and DXC security services strategy and market trends.

DXC, 2 Kelvin Close, Warrington, WA3 7PB, UK
Tel: +44 560 1094724; E-mail: shaun.bligh-wall@dxc.com

Abstract This paper discusses the security challenges and inherent risks that result from the Internet of Things and Industry 4.0 within the context of digital transformation. It discusses the explosive growth of devices and data, lack of standards, and ubiquitous adoption without due understanding of the need to consider the shift in implications. IoT and Industry 4.0 will accelerate the convergence of cloud, legacy IT and Operational Technology (OT) security. Securing data will be an organisational imperative, as will a top-down approach to information security from governance to the individual, one that ensures it is a business enabler aligned to wider business strategy. Businesses will be driven by the potential rewards offered by adopting IoT and this paper offers insights into achieving them securely.

KEYWORDS: Internet of Things, IoT, Industry 4.0, cybersecurity, standards, governance

THE NEXT INDUSTRIAL REVOLUTION IS HERE

There is a buzz within the IT and manufacturing industries about the so-called 'Fourth Industrial Revolution' — or as it is more commonly known, Industry 4.0. Currently, the excitement seems to be centred in Europe, but there is evidence that the concept is beginning to spread around the world.

There are many articles on the internet that describe the Fourth Industrial Revolution, but a reminder of each industrial phase may be useful. In addition to providing a refresher on the Industry 4.0 concept, this paper also provides some context.

Figure 1 provides an overview of the four industrial development phases:

1. **Mechanisation:** The first industrial revolution saw the introduction of steam power to speed up and improve the manufacturing process. It is widely understood to have begun around the year 1760, and the effects of steam-powered mechanisation on industrial productivity are well documented and recognised.
2. **Electrification:** The second industrial revolution is believed to have occurred when electricity was introduced to factories and manufacturing. Joel Mokyr

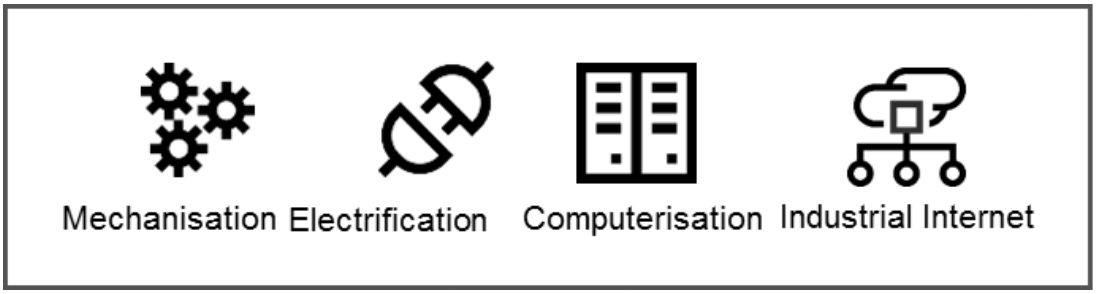

Figure 1: Four stages of industrial development

reports[1] that the second industrial revolution took place between 1870 and 1914.

3. **Computerisation**: The computer or digital revolution followed the electrification of the manufacturing floor, but it didn't start until the 1950s. The use of computers in manufacturing began with accounting and record-keeping systems; it has developed since the 1970s to include automation and communications.
4. **Industrial Internet:** Also referred to as Industry 4.0, the latest industrial revolution has seen the interconnection of sensors, devices and services (commonly known as the Internet of Things or IoT) to integrate and enhance industrial value chains.

THE IOT EXPLOSION

It has been widely reported that there will be ubiquitous adoption of the Internet of Things as companies and other organisations seek to transform into a digital business. The use of IoT will enable them to take advantage of the rich data streams that can be collected and analysed from myriad inexpensive sensors and devices. Estimates of the growth in IoT devices vary by billions, but you simply need to look around for proof points. You may even be wearing one.[2]

The adoption of these sensors and devices will have a significant impact on traditional Operational Technology (OT) environments. Businesses are finding that IoT can deliver a shorter time to value and enable the organisation to reach digitisation objectives in a way that could not be imagined previously. A 2014 PWC Industry 4.0 white paper[3] states that companies surveyed expect more than 18 per cent higher productivity as a result of adopting Industry 4.0 projects. This is expected to result in €110bn in additional revenues for the European industry sector.

Digitising the manufacturing business won't be cheap; most likely, it will have a few casualties along the way — when businesses fail to plan properly and invest unwisely in Industry 4.0 projects. It is estimated that some manufacturing organisations will allocate as much as 50 per cent of their planned capital investment to Industry 4.0 projects, hoping to make significant gains in productivity and improve competitiveness on the world stage. Unwise IoT investments, therefore, carry a significant risk to an enterprise's future well-being. That's why prudent planning in keeping with wider business strategy and imperatives is paramount.

The rise of the Industrial Internet will deliver real business value as organisations find their 'digital feet' and begin to see returns on their IoT investments. For some organisations, this time to value may take up to two years. But there is recognition that the fundamental value of IoT comes from the data produced by the population of deployed

IoT devices and the organisation's ability to analyse and take action on it. Businesses that currently depend heavily on data, such as those in the retail sector, are natural candidates for IoT projects.

Planned maintenance of plant and equipment has previously been a 'dark art' for some organisations. It requires maintenance teams to have the tools, skills and parts to replace faulty components just before they fail and keep mission equipment and processes running. It is not unusual for maintenance teams to plan to replace equipment parts based on manufacturer recommendations or to rely on team members to identify components that may or may not be near the point of failure. This can lead to unnecessary expense being added to the balance sheet — especially when the replaced part is still serviceable.

Industry 4.0 can address this problem. Sensors can be integrated within manufacturing equipment to monitor critical performance factors. Data analysis is performed as close to the network edge as possible, so only actionable data is sent back to management systems that assess the data to identify signs of stress and potential failure. Replacement parts can be automatically ordered at the right time and maintenance teams deployed with the part to support plant and factory efficiencies. This allows for a more efficient operation that makes optimum use of human and technical resources.

IoT and Industry 4.0 projects can generate huge amounts of data that need a great deal of computing power to analyse. In the past, this could have been a barrier to adoption for some organisations. But the advent of cloud computing has provided many businesses the ability to quickly move from pilot project to full deployment.

Of note: The use of cloud computing introduces new business and security challenges of which some businesses may not be aware. We will discuss these later in this paper.

IOT AND INDUSTRY 4.0 SECURITY: THE CHALLENGES

The proliferation of IoT and adoption of Industrial Internet projects has given security professionals the opportunity to evaluate the new risks and vulnerabilities that are being introduced into organisations around the world. IoT and cybersecurity intersect with a number of existing security disciplines. These disciplines include: 1) Information Technology (IT Security) for protecting information systems; 2) Physical Security to protect buildings, offices, facilities and the like; and 3) Operational Technology (OT) security to protect operational systems for plant automation and environmental monitoring systems. Securing IoT environments will require drawing from each of these three disciplines. The combination of the elements shown in Figure 2 can be described as *digital security.*

Unfortunately, it is not unusual for new technologies to be introduced to the market without a robust set of security features, and it may take some time before these are integral to IoT technologies.

So what security challenges are hampering widespread adoption of IoT?

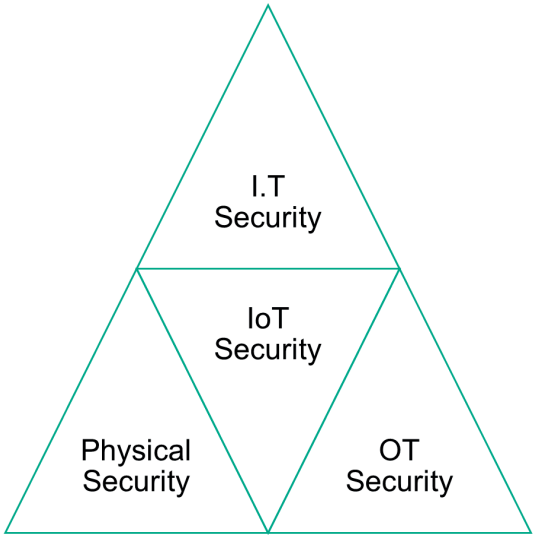

Figure 2: Elements of digital security

Wanted: Credible IoT security standard

The first glaring problem is a lack of standardisation when it comes to IoT security features. A number of vendors and IoT developers are working on potential solutions, but there isn't a standardised solution yet that can apply to all devices and infrastructures. The problem is largely due to the limited processing power and capabilities of the devices; 'traditional' computers tend to use standardised operating systems and software and can be secured using tried and tested methods, but sensors and other IoT devices are not governed by a common set of software tools and applications. This makes deploying standardised, robust security measures more difficult.

Historically this would have been a smaller problem because the devices would have used proprietary protocols to communicate with each other, and they operated in a contained and/or isolated environment. Most IoT devices today make use of the standard Internet Protocol (IP) to communicate with other devices and the outside world. Using standard networking protocols with insufficient security controls to protect data means many IoT devices are vulnerable to attack.

Press-ganged attackers

Recent reports in the media have already illustrated how seemingly innocuous devices with little computing capabilities can become instruments of a distributed denial of service attack. Home user devices such as internet-connected cameras and baby monitors are not the only unwilling recruits for the dark enterprise. Other devices that have business-critical functions can also be compromised and used to deliver targeted attacks.

It is reasonably common knowledge that some IoT devices are easily used as unwitting foot soldiers in a distributed denial of service attack because of weak or missing security controls. The most common failure reported is the use of known or weak administrator passwords, many of which are not changed at the time of installation. There are other security problems, too. And some of these can be attributed to older legacy equipment where digital security was not an important requirement during design and installation.

Of course, the use of the Industrial Internet of Things (IIoT) to attack other networks and systems presents a number of new challenges, besides the fact that they could be used to attack other systems. For example, what would the impact be to manufacturing processes if scarce device computing resources were not available for intended purposes? What would the legal and business risks be if a DDoS forensic investigation appears to suggest that the compromised network of an organisation has been used to deliberately attack another? Would there be grounds for litigation and compensation?

Naturally, most customers and vendors will respond to these challenges with technical solutions. Some of the technical answers to the problem will require further capital investment. They also can be disruptive to manufacturing processes and the business because they require new, up-to-date equipment to be installed and commissioned. Other solutions may be more temporary or inadequate in nature and, while cheap, may not be sufficient to support future needs. The key to the secure deployment and use of IoT infrastructure lies in the combination of a sound digital security strategy, comprehensive design and robust technical controls. Strategy needs to fundamentally acknowledge and address business and technical risks but also safety. In the digital age of the Fourth Revolution, security and technical controls must be designed into systems from the beginning; when IoT controls devices that may result in physical damage and potential loss of life, the risks are too high to 'fix it later'.

A new breed of factory worker

A new breed of information worker needs to be created and trained in the ways of information security. Factory workers and engineers will be working with data, networks and systems in ways that are unfamiliar to them. They will be unaware of the risks associated with gathering, handling and analysing that data. But they will be expected to use computing power and secure data-handling techniques in ways that their office worker colleagues have been developing over many years. They will need to be security-savvy in much less time.

Security governance, risk and compliance management must embrace this new dimension to ensure a balanced and effective approach in the management of distributed risks that have the potential to alter critical outcomes. Awareness training and education is also essential to allow each employee to become a proactive security agent.[4]

New model, new risk

A key concept of Industry 4.0 and IoT is that of the cyber-physical system (CPS).[5] A CPS is a machine that is controlled or monitored by computer software and is also connected to an external network such as the Internet. We have seen numerous examples of CPS in mainstream media — such as the medical robot that is controllable via the Internet or even a robotic gardener[6] at MIT in the United States.

As illustrated in Figure 3, the use of sensors enabled the development of cyber-physical systems, which in turn has led to the creation of the 'factory-as-a-service' (FaaS) model, by which service providers can provide virtual factories for their clients. And by providing a network of machines along with information analytics, service providers can offer specialist manufacturing facilities to customers who may not want to make major investments in similar plant and equipment. This could result in a client selecting multiple service providers in diverse geographic locations to manufacture the components for their company's product.

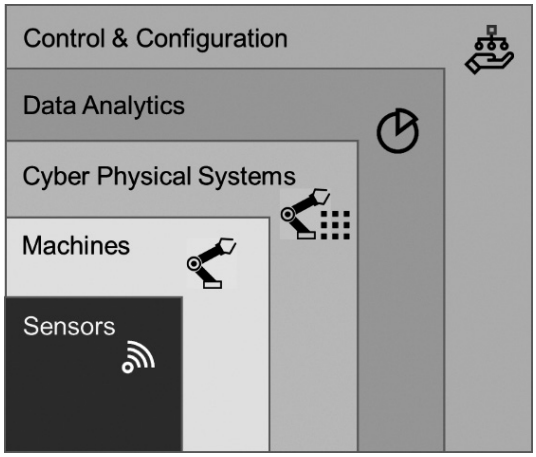

Figure 3: Role of sensors in creating 'factory-as-a-service' model

FaaS and CPS could also allow manufacturing equipment to be reconfigured remotely for a new client. The data collection and analytics features of the FaaS model mean that sensitive and potentially market-leading manufacturing processes could be vulnerable to theft by competitors. Entire manufacturing runs could be ruined through sabotage if an attacker gains remote access to CPS infrastructure.

IoT data breach challenges

A data breach involving IoT equipment will occur after the adversary recognises the potential for reward. The challenge for the organisation that makes use of IoT and the Industrial Internet is how best to identify a breach when it occurs on the factory floor and, more importantly, how to respond to and recover from it.

The limited processing power and storage capabilities of IoT devices means that data is overwritten on the device or transferred to external systems frequently — making the traditional digital forensics approach of device isolation for data preservation challenging. The question of human safety and costs associated with disabling an IoT

device for forensic investigation must also be considered. Some devices, such as those functioning on an oil rig, cannot simply be disabled without significant impact to the company and its employees.

The external systems that gather and process IoT data may be cloud services or third-party data centres. The distributed nature of this model will make the process of identifying and containing the source of a breach difficult. The issue of infrastructure boundaries and ownership will also complicate a digital forensic investigation. Companies that are already moving their business operations to the cloud should understand this problem and have an answer for it.

All of the preceding comments consider the impacts and challenges of identifying, handling and responding to a data breach that involves IoT infrastructure. Similar consideration should also be given to the use of IoT-generated data that can be used to support crime investigations of 'traditional' law enforcement.

IoT sensors and devices bridge the digital world and our physical environment. It follows that these devices can provide vital evidence that can lead to solving a non-IT-related crime (such as equipment theft). There are no known demands by governmental or law enforcement agencies for preserving and handling IoT sensor data for crime investigation, but we cannot discount the possibility of these requirements being made in the future.

INDUSTRY 4.0 SECURITY: THE SOLUTIONS

Organisations that have either embarked on Industry 4.0 projects or are planning them may be forgiven for thinking that the prognosis for a secure IoT infrastructure is poor. There are many challenges to address. Some of the technical security problems will take time to be resolved by vendors seeking to gain market advantage by offering a secure IoT product.

Top-down approach

Security professionals and organisations with more established information security capabilities recognise that IoT and Industry 4.0 security require much more than traditional technical security controls. Defending the business IoT investment and other digital assets from attack requires a layered approach that includes business strategy and extends to people, process and technological defences.

Effective and efficient defences require implementing a reference architecture that addresses all of these needs. It should also enable the organisation to adapt and grow as it follows its digital transformation strategy.

The model shown in Figure 4 provides a conceptual view of this approach. IoT projects should begin at the business layer where strategy, policy and directives are defined and introduced to the rest of the organisation. Next, enterprises must address the need to secure critical data within the data processing layer. This is the greatest challenge many firms experience in their digital journey, according to an EIU survey of 700 firms.[7]

A data security strategy must be designed not for the present but for the future business and the projected level of threats. This requires a new degree of flexibility and scalability in security strategies, as threat landscapes and technologies advance at pace.

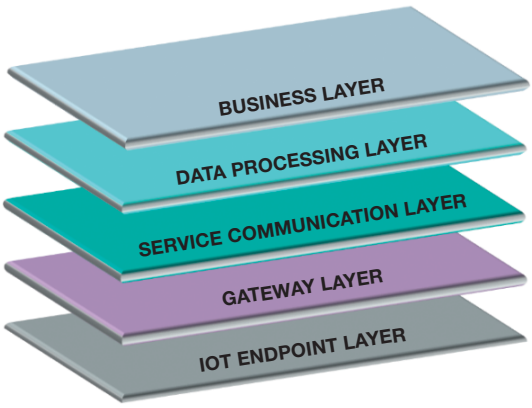

Figure 4: Conceptual view of top-down approach

From that point, additional layers for systems and infrastructure can be designed to take into account enterprise needs for security and functionality. The model also allows for the right vendors to be selected before a single piece of equipment is purchased or installed. It also ensures that third-party risk is identified and managed.

Security architects will be able to deliver designs that address the demands of each layer according to the reference architecture. This will ensure a consistent approach where business needs are met and risks are maintained at an acceptable level. It will also address the crucial aspects of how the enterprise should respond when a data breach is discovered.

Consequently, leaders must plan for security defences that can scale to meet the demands of the new digital business era and which are focused on data rather than infrastructure or perimeter.

Data security as standard

Most controls needed for the security operation of an Industrial Internet environment should be implemented with the view to protect the data while ensuring human and equipment safety objectives remain intact. Businesses will have to deal with the challenges associated with data being dispersed over the vast collection of sensors and systems. When this happens, data storage and management can introduce higher levels of risk and vulnerability, so a robust data security plan must be defined, tested and implemented.

A strategy to protect mission-critical data naturally begins with a discovery phase. This is an exercise designed to find all of the distributed data across an organisation and then classify it according to subject, sensitivity and its location. (Other categories may also be required.) An effective data classification strategy is essential to ensure that the right controls are applied to data and the organisation complies with local and international laws and regulations.

Data collection management is also important from the perspective of spotting irregularities and possible cyberattacks. 'Traditional' intrusion detection systems are unlikely to be effective in an environment that includes a large number of data-generating sensors. Advanced data analytics and security event monitoring are the most effective methods by which irregular activity and possible cyberattack can be identified and managed.

The vast amount of data that can be collected from IoT sensors and devices will often lead to the adoption of cloud computing capabilities. Here we find the merging of networks and subsequent blurring of the traditional boundaries most organisations have built over many years. Cloud computing will be part of this equation; it is a natural choice for organisations that need a cost-effective and flexible way to capture and process large volumes of data. It also introduces a dynamic and fluid boundary between the enterprise and service provider, which calls for a robust enterprise risk management strategy.

It is likely that the enterprise will face a nexus of strategies as a result of these trends. Consequently, no single strategy can be developed in isolation. Traditional information systems risk management, cloud risk management and IoT adoption strategies will have to be cognisant of each other and ultimately dovetail to prevent gaps that could leave the business at risk.

WRAPPING IT UP

IoT and the Industrial Internet are here to stay. Organisations will continue to accelerate their efforts to transform to the digital enterprise, and this will result in the widespread adoption of IoT, where previously unthought-of benefits will be realised and converted into profit, accelerating adoption rates.

Many business leaders will recognise that Industry 4.0 projects will accelerate the convergence of cloud, legacy IT and OT security. Securing company and customer data will be imperative, especially in an age when data can be distributed around the world and held by multiple service providers.

An organisational imperative is a top-down approach to information security that ensures it is a business enabler aligned to wider business strategy. Business investment will be driven by the potential rewards offered by adopting IoT. But security as a key consideration will only be taken seriously after the first few high-profile IoT breaches occur.

References

1. Mokyr, J. (September 1998), 'The Second Industrial Revolution, 1870–1914'. Available at https://www.researchgate.net/publication/228781185_The_Second_Industrial_Revolution_1870-1914 (accessed 15th May, 2017).
2. DXC.technology (March 2017), 'Securing the Internet of Things'. Available at http://assets1.dxc.technology/security/downloads/DXC-Security-Securing_the_Internet_of_Things-4AA6-3369ENW.pdf (accessed 15th May, 2017).
3. Strategy& (September 2016), **'**Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused'. Available at http://www.strategyand.pwc.com/reports/industry-4-0 (accessed 15th May, 2017).
4. Hewlett Packard Enterprise (2015), 'Awareness is Only the First Step'. Available at: http://riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf (accessed 15th May, 2017).
5. J. Lee, J., Bagheri, B. and Kao, H-A. et al (January 2015), 'A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems'. / *Manufacturing Letters*, Vol. 3, pp. 18–23. Available at http://www.sciencedirect.com/science/article/pii/S221384631400025X (accessed 15th May, 2017).
6. The Distributed Robotics Garden. Available at http://people.csail.mit.edu/nikolaus/drg/ (accessed 15th May, 2017).
7. Enterprise Forward (22nd February 2016), 'The Path to Self-disruption: Nine Steps of a Digital Transformation Journey'. Available at https://hpe-enterpriseforward.com/eiu-pace-of-disruption/ (accessed 15th May, 2017).