The Industrial Internet of Things: assess and manage the risk

Apart from human capital, the most important asset that any organisation has is data.

Access to real time information and analysis injects significant operational efficiencies into any business, particularly utilities, manufacturers, mining and other critical industries. Greater insight helps digitally transform industry, streamlines supply chains, schedules predictive maintenance, optimises traffic flow and strips out costs.

In the past information was collected by workers with clipboards, or meter readers, and fed back into central information systems. Increasingly that data collection is automated with connected sensors constantly monitoring equipment, temperature, water and electricity use, traffic flow.

Analyst Gartner has forecast that this year 8.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020. Forbes has estimated it could be even higher – 50 billion devices by 2020.

A significant proportion of these devices will be integrated into industrial internet of things (IIoT) networks running Australia's mines and ports. They facilitate the development of smart cities, are essential to autonomous vehicles or SmartGrids, and widely deployed in agritech solutions.

At a national level these connected information networks form the critical data fabric that underpins the economy.

One of Australia's utilities giants and a lynchpin of regional energy stability has deployed 200,000 sensors to measure temperature, pressure and a range of other factors. Each sensor is connected to the cloud, streaming data to 6,000 analytics models performing 3 million calculations a day.

The resultant insights allow it to schedule preventative maintenance, monitor plant performance and boost efficiency and safety. But it also expands the organisation's attack surface for cyber villainy – each IIoT device offers a potential route into the organisation. A computer virus or Ransomware attack can bring a business to a standstill for a day or two. An attack against critical systems can have national implications with the risk of extensive power cuts, contaminated water supplies, large scale transport failures or catastrophic industrial incidents.

Efficiency dividend v efficiency risk

The Australian Cyber Security Centre's (ACSC) most recent threat report acknowledges that connected sensors streamline management and optimise operation of systems supporting critical infrastructure. It notes however that this creates a new vector for cyber adversaries to attack companies and critical infrastructure.

It warns that "with adequate access, knowledge and capabilities, a sophisticated adversary could modify Industrial control systems (ICS) to achieve a disruptive effect on critical infrastructure. These effects could include manipulating the production and supply of energy and power, the creation of outages, damage to industrial systems, and manipulation or theft of information utilised by infrastructure owners and operators."

In December 2015 just such an attack was launched against Ukraine's power network, taking down 30 substations and leaving more than 225,000 Ukrainians without power for several hours. Continued interference delayed Ukraine's restoration efforts.

According to the ACSC's 2016 security survey 44 per cent of Australian respondents had deployed industrial control systems – significantly expanding the technical perimeters of organisations.

Weapons of attack

Malware is often considered as computer viruses that can lock up or corrupt computers. But it can also corrupt or enslave IIoT devices.

Stuxnet was one of the first computer worms specifically developed to target SCADA (supervisory control and data acquisition) networks which are widely used in industry, and brought Iran's nuclear operations to a standstill in 2010.

Mirai1 and Hajime1 are two more recent forms of malware which have been deployed to seize control of sensor networks. These scan the internet for poorly secured IoT devices and then compromise them, creating a route into the industrial network and an opportunity for attack.

Prevention

Organisations which deploy IIoT solutions need comprehensive assessments of the systems currently deployed and in use to understand the risk landscape. They should be vigilant about the security settings of the technology and ensure there is proper communication between operational technology and information technology departments. The IoT Alliance of Australia has developed security guidelines for IoT deployments[1] offering a high level guide for CEOs and chief information officers and recommending security is prioritised during network design and selection. Proper attention to cyber hygiene is critical for IIoT networks.

Respond

Organisations operating critical infrastructure need to be prepared for the worst with a well-designed and tested robust cyber incident response strategy. In its 2016 Threat Report the ACSC noted that CERT Australia had responded to 418 incidents involving systems of national interest and critical infrastructure[2]. The energy and communications sectors had the highest numbers of compromised services while the energy and mining resources sectors had the highest number of malicious emails received.

Regardless the efforts taken to prevent an attack IIoT users need to develop robust response plans that ensure they are able to rapidly tackle any attempted systems compromise. The ACSC reports that about seven out of ten Australian organisations currently has a cyber response plan – but only 46 per cent have tested it. It's too late to test the plan when a cyber-attack has already taken place.

Recover

Following any form of IIoT compromise organisations need to recover and repair their networks, working with specialist third parties skilled in recovery and remediation. This may extend beyond the technical into areas including brand recognition and consumer relations.

Organisations may need access to highly specialised forensic skills to facilitate recovery and remediation. Finding those skills after a compromise may take too long – organisations need for forge relationships with key specialists in advance.

"There is rarely an an air gap between IIoT and information technology networks now – as a result the risk of cyber incident is real and extensive. Organisations need to properly assess their IIoT vulnerabilities, develop robust protection, response and recovery plans and use these to sensibly transfer risk where possible to ensure critical networks and industry are not permanently or catastrophically disabled."

–Fergus Brooks,
National Practice Leader, Cyber Risk

Transfer

Organisations cannot insulate themselves from every cyber event – however careful evaluation may help transfer various risks via insurance and other well-crafted risk management solutions.

As part of an holistic security response plan, organisations with IIoT networks need to carefully assess whether insurance policies would cover business interruption prompted by IIoT compromise. What support is provided for any regulatory fines or remediation work? In the event of an IIoT attack causing physical property damage, which policy would provide coverage, if any?

Taking these steps to protect your business is essential. It is an issue no industry can ignore.

1 http://www.iot.org.au/resources/
2 https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf

Aon Contacts:

Paul Pryor
Global Mining Practice Leader
T +61 3 9211 3052
E paul.pryor@aon.com

Fergus Brooks
National Cyber Risk Practice Leader
T +61 2 9259 7835
E fergus.brooks@aon.com