Enterprise Internet of Things:
Balancing the value versus vulnerability equation

The average Australian home has 13.7 internet connected devices today while two in five homes has at least one Internet of Things (IoT) sensor or appliance according to recent research from Telsyte.

We may use that device to control the lighting or heating at home, or to keep an eye on the dog in the backyard or baby in the nursery. The chances are that each of our PCs, tablets or smartphones has some form of password control, a firewall, or virus protection – but are we sure that the IoT appliance such as the backyard camera or baby monitor is as secure?

Are we sure that it could not become the vector for an attack on our other devices?

Segue what we have in our homes to the IoT devices we are now deploying in offices, in factories, in shops, and smart cities and the security question becomes even more pronounced.

Critically this is an issue that does not just impact businesses that are technology focussed or data driven. If your business uses a smart IoT device to monitor your energy usage or has an internet connected camera to monitor your shop or warehouse, you have potentially opened up the door to a cyber-attack if that device isn't properly secured and regularly patched.

And it may not even be your IoT device that creates the problem – remember the Target hack in the US? Hackers found their way into the company's network through systems used by the air conditioning contractor.

IoT devices massively extend the perimeters of any organisation. How well protected are yours?

It's a fast expanding perimeter too. IDC Australia says that by 2020 Australia will have 2.7 million connected commercial vehicles and 1.8 million connected healthcare appliances. Globally Gartner says there will be 21 billion IoT devices in use by 2020 – Forbes' estimate is even higher at 50 billion.

The challenge for users of Enterprise IoT is to manage the value versus vulnerability equation.

The information gathered by IoT devices can deliver unprecedented volumes of very valuable data to an organisation, that data can be turned into insight to steer decision making. It can be used to identify business patterns – traffic flow in a supermarket for example so that displays can be optimised. It can rein in costs by shutting off lighting and air conditioning in offices and boardrooms when people depart.

That's the value. The vulnerability arises because there are few standards in IoT device manufacture today, security is often bolted on as an afterthought with varying success, and each device potentially offers entre to the broader enterprise network. There is already IoT specific malware such as Mirai and Hajime targeting these IoT networks.

Aon's recently released Global Risk Management Survey reveals that cyber threats are now ranked a top five business risk by organisations all over the world – and it became a top five risk in Australia for the first time ever in the 2017 report. That study particularly highlights the rising risk of cyber criminals hijacking IoT devices to act as botnets to then attack critical systems.

As the report notes: "Cyber threat has now joined a long roster of traditional causes such as fire, flood and strikes that can trigger business interruptions - because cyber-attacks cause electric outages, shut down assembly lines, block customers from placing orders, and break the equipment that companies rely on to run their businesses."

How fast is this risk rising? In 2016 businesses ranked cyber risk at number nine – it's jumped four places in a year.

The Australian Centre for Cyber Security recently noted that around seven out of ten Australian organisations now has a cyber response plan – but only 46 per cent have tested it. Does enterprise really want to find out the plan's limitations when the cyber marauders are already in the network?

It could prove a costly approach. Lloyd's has already estimated that cyber related business interruption could cost organisations as much as $US 400 billion each year.

And the impact on brand and reputation of a poorly handled cyber incident can't just be measured in dollars.

The cyber-attack on last year's online census wasn't handled well. It earned the ABS its own Twitter handle, #Censusfail, and even now the ABS' reputation is bruised. Compare that with the relatively benign impact on the Red Cross which handled its 2016 data breach in text book fashion – alerting affected individuals and calling in experts to support it.

Preparing for a cyber-attack is even more important because of the imminent introduction of legislation which requires most Australian organisations to notify the authorities and affected customers if they suffer an eligible data breach. That ratchets up the challenge and costs associated with a cyber-attack considerably.

Enterprise IoT deployments dramatically extend the internet perimeter of an organisation and potentially offer cyber attackers new routes into corporate networks.

Any organisation deploying Enterprise IoT needs to weigh value versus vulnerability.

To promote the value and rein in the vulnerability organisations need to create and test a cyber response plan; to educate employees and contractors about cyber risk and the actions to take if there is a breach; and to explore the opportunity to transfer associated financial risk through cyber insurance.

Contact

Fergus Brooks
Cyber Risk Practice Leader
+61 2 9253 7835
fergus.brooks@aon.com

Michael Parrant
Cyber Insurance Practice Leader
+61 3 9211 3485
michael.j.parrant@aon.com