Curry, J. and Drage, N. (2017) 'IoT: the internal and external threat.' *ITNOW*, 59 (1), pp. 30-31.

The New Threat from the Internet of Things, What Should the CISO do?

John Curry, Senior Lecturer in Computing, Bath Spa University. j.curry@bathspa.ac.uk
Nick Drage, Specialist in Cyber Security.

Internet of things (noun) *- A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data. If one thing can prevent the Internet of things from transforming the way we live and work, it will be a breakdown in security.*

Oxford English Dictionary

When the gatekeepers for the English language defined the IoT in the summer of 2013, they highlighted IT security in their example sentence.

The threat of other businesses using the IoT is no different from the existing *external* threats. While the size of DDoS attacks in the future may be larger, as there are even more potential devices to add to the botnet, the widespread use of IoT online does not introduce any new threats to you or your network.

Opportunity

With the right frame of mind, the IoT actually represents a similar opportunity to that provided by PCI: a specific and quantifiable threat regularly in the news, that will enable you to attract and maintain the attention of stakeholders. The possible introduction of unauthorised IoT on your watch and into your estate, and the increased awareness amongst your threat actors of IoT vulnerabilities, gives you an opportunity to reinforce those security practices you need to bolster. Perhaps even to finally obtain the buy-in from the relevant stakeholders to have those security practises implemented.

From Sun-Tzu, to the SANS Critical Security Controls, and arguably everyone in-between, the first step in any situation is to be aware of the environment. Use your existing network inventory and vulnerability scanning capability to determine what's on the network, and what state it's in; from there you can assess your current exposure to risk, and where improvements are required.

Arguably, the main cause of "Shadow IT" is the inability of the organisation to process IT requests through approved channels within timelines that the rest of the business finds acceptable. Due to its overall ease of installation, the IoT in general is intended to be "plug and play", and so repeats the potential risk represented by easy to use cloud services. Ensure your security team are seen as *the* experts in IoT, and are easy to communicate with, so they're seen by users as the first people to speak to, not the key people to avoid.

To reinforce this message, keep an eye out for issues with domestic IoT products, such as children's toys, webcams, light bulbs, thermostats, and cars. These can be used to not only keep your staff safe at home, which may be their main place of work, but also to improve their security mindset, and keep IoT issues in their thoughts.

Use this as an opportunity to revisit existing IoT services, such as your CCTV and HVAC (Heating, Ventilation, Air Conditioning) systems, and all of the security controls around those. This can be used to justify regular scanning and interrogation of both your internal network and its perimeter.

In addition, while examining your network connected infrastructure, consider improving the restrictions on third party access to your systems. We all need third party support, but do you really want them to be able to turn off your burglar alarm or the temperature controls in the server room? While we have taken a wide definition of IoT for the purpose of this article that's to your benefit, when you're asked about new IoT implementations explain that it's already in place, and what plans you have to improve security around it.

IoT tends to have simple administration controls in place which re-emphasises the importance of network segmentation, and network monitoring. Use the current or future installation of IoT to finally get that network segmentation in place, or to introduce the VLAN based controls you've been waiting to implement since you took the position. Not only will this reduce the probability of your IoT being compromised, it will reduce the impact of any such compromise.

Use security of devices as a factor in the procurement process, and emphasise this to vendors. In the short to medium term, it appears best to assume the worst of the IoT and to build a secure infrastructure around any existing devices that are already in place. Improving the security and secure development of IoT devices is a necessary long term aim, but your security needs to be put in place now than some distant point in the future.

Now turn to your external threats, which is primarily DDoS. Any mention of IoT must consider the threat demonstrated by for example the Mirai botnet. Use this to confirm:

- That your DDoS protections are in place.
- Are up to task they would expect to face.
- You have implemented and tested any backup communication methods required to talk to the relevant third parties if you under such an attack.

Once these basics are covered, then examine the "Hollywood" scenarios that are starting to become a possibility due to the introduction of IoT: such as hackers setting off fire alarms to clear your buildings before they sneak in, and tracking and hijacking your shipments because of GPS notifications to your company or RFID in your packaging, and so on. This is an excellent subject for your security team to brainstorm on a Friday afternoon, especially as it'll give them something to ponder over during the weekend.

Be Positive

It can be easy to be disheartened about cyber security, a battle you can never decisively win, but where survival is just failing to lose on a daily basis. It can be easy to be persuaded by the security nihilists, we all know pessimists like those, who see the IoT as the inevitable victory of "cheap and fast" over "good" in the project management triangle.

However, as we hope we've shown, with the right frame of mind the rise of IoT can be dealt with through the reinforcement of existing practices, and can provide an opportunity for CISOs to obtain the resource they may have been failing or struggling to obtain until now.