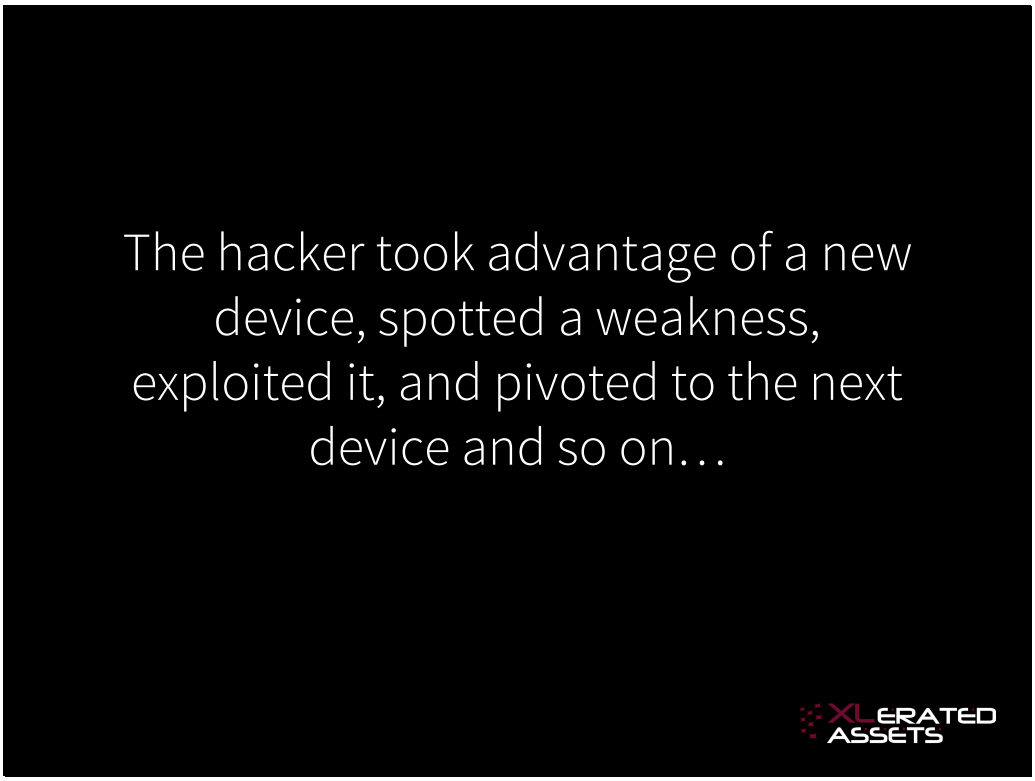
Slide 1

- A friend of mine that works at the company that discovered this told me a story of an unusual data breach. The target was a major hotel casino, to remain nameless, who had their entire high-roller database stolen by hackers.
- This casino thought they had a fool-proof security system. So how did the hackers get access? Turns out, they were able to break in through a thermostat in the fish tank in the hotel lobby.
- This Internet of Things thermostat was installed as a new attraction and used hi-tech sensors to monitor temperatures and feeding schedules.

Slide 2

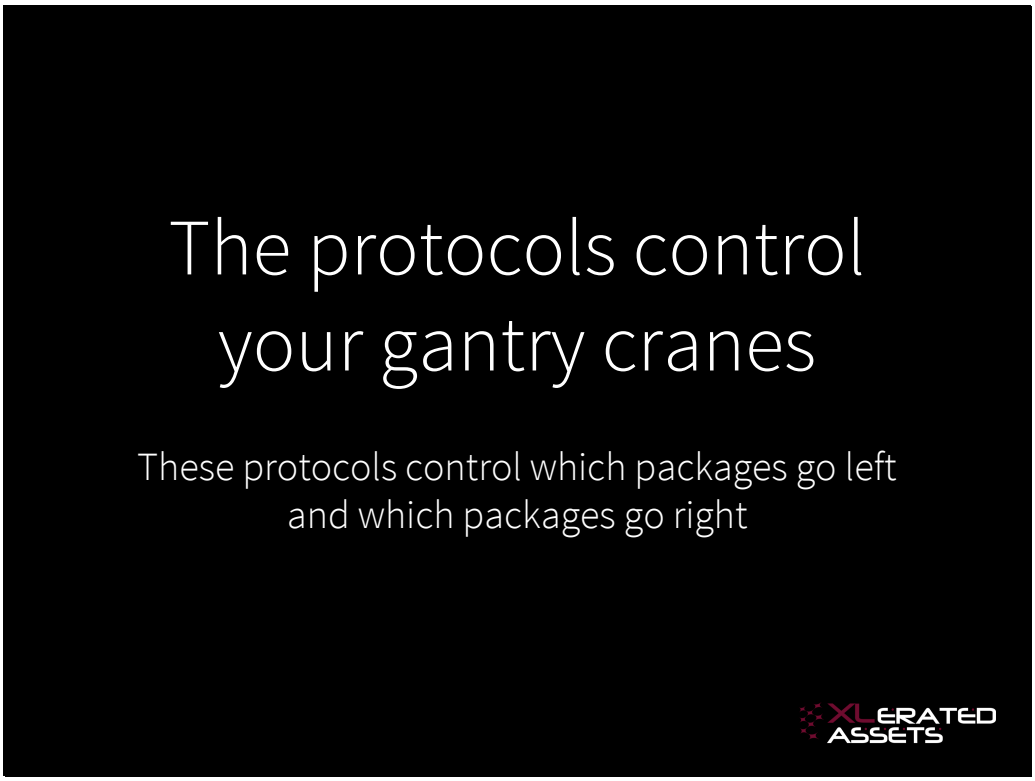


- The hackers were able to pivot to other parts of the network find a database of high rollers and steal their credentials.
- The casino used a configured VPN, the company that detected the breach noticed that there was a large amount of data, 10gb, that was using a protocol that was usually reserved for audio and video conferencing. This was transferred to an address in Finland for data exfiltration.
- I think the key here is that the hacker took advantage of a new device, spotted a weakness, exploited it, and then pivoted to the next device and so on.
- One thing that is becoming more evident is importance of monitoring a network to spot unusual patterns of activity and data transfer. In the fish tank example, there is no need for that amount of data to be associated with the thermostat.

Slide 3

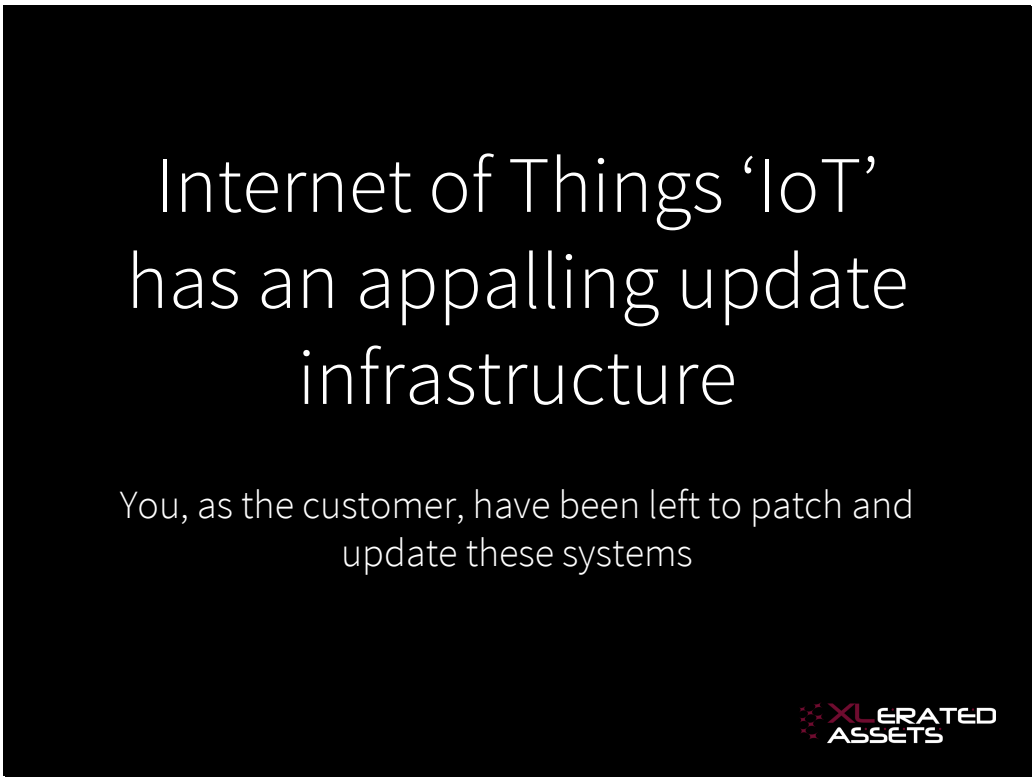
- This might seem like a niche threat. But these devices are remarkably similar to the IoT, Industrial control systems that run your ports and logistics facility.
- These protocols run your gantry cranes and control which packages go right and which packages go left

Slide 4



- If that's the damage that can be done with a thermostat, think what could happen when a hacker accesses an automated piece of heavy machinery.

Slide 5

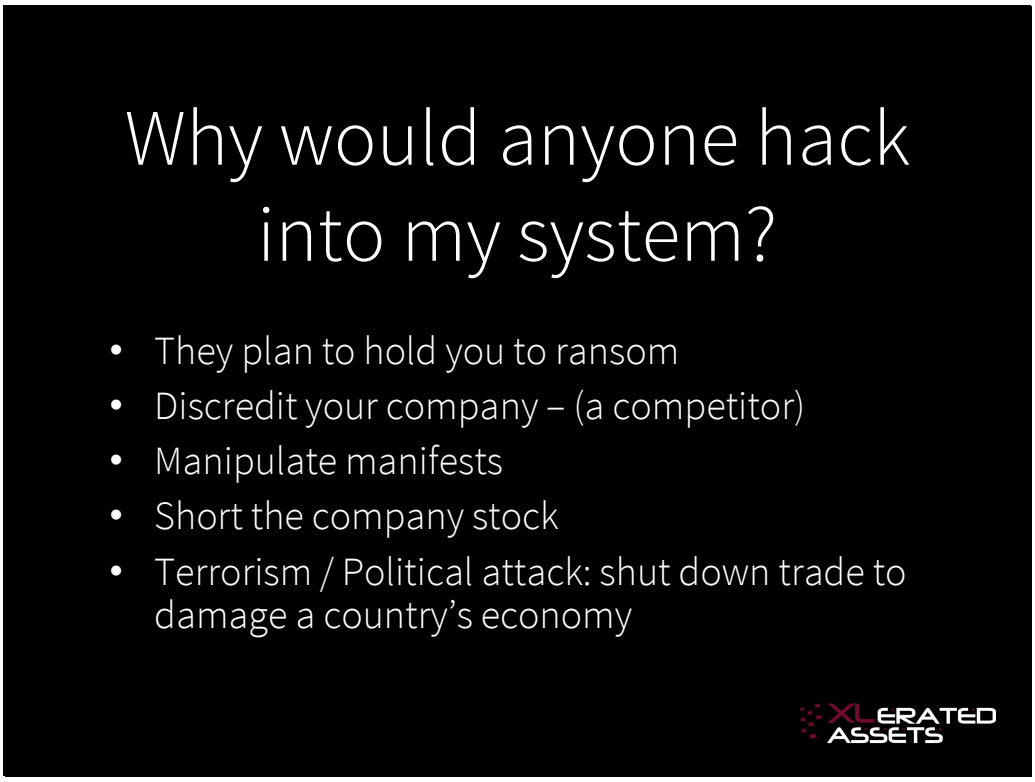


- Internet of Things 'IoT' has an appalling update infrastructure: you as the customer have been left to patch and update these systems. In some cases, the vendor no longer exists or only supports the current version of Windows. In other cases, the vendor is suggesting or 'pushing' you to a multi-million dollar upgrade.
- IoT devices also tend to use open source software which is known to have serious bugs.

Slide 6

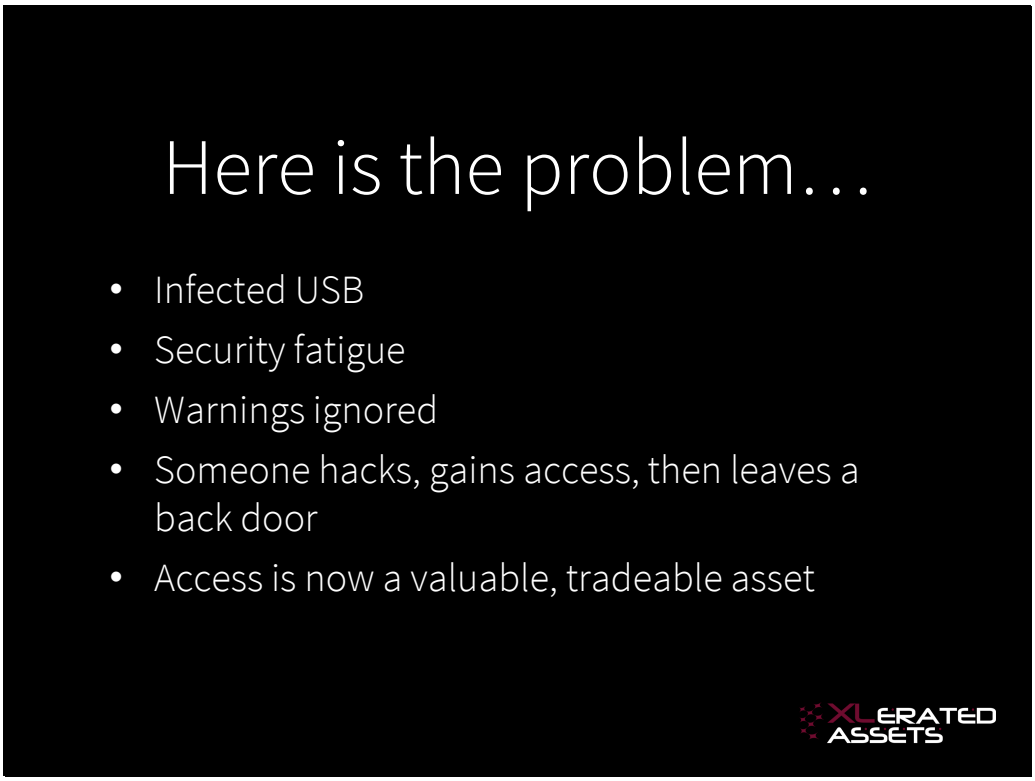
- Here is a staggering statistic… 80%
- Why is that? That is a high number.

Slide 7



- If you are already inside the company environment (known as 'being owned'), you can search for the container number, then decide to move it to another stack
- My article in the *Across Borders* magazine, outlined that there are specialist companies, that will find weaknesses in your systems, report back, short your stock and go public.
- Company in question 'Muddy Waters'
    - Just google 'Muddy Waters short selling
- Insurance companies are also interested in how well you are doing.
- If you already take up Cyber insurance, the insurance companies are checking your security posture, so if your premiums go up, this could be why.

Slide 8



- Imagine this: the captain of a ship hands over an infected USB stick to the Port Authority person (e.g. harbour master)
- The captain may be an inadvertent insider, who has been deceived into providing a way in for hackers. The captain might have received warnings in the past, but due to ‘security fatigue' or just not knowing what to do, these warnings are ignored. The Port Authority guy plugs in the USB and the network becomes infected.

Here is what could have been done to solve it.

- The captain needs to have some endpoint software installed to take care of the ship’s manifest computer
- The Port Authority needs to have a solution in place that can detect, quarantine, alert and respond to any possible scenario like this. You can’t reduce the risk of infection to zero, but if you have a response plan in place you can make a huge difference by minimising damage.

- Right now, a lot of companies focus on prevention but not damage control. If you only plan for the probable and not the possible, the consequences of getting caught by a freak event, like the mass NotPetya infection last June, are enormous.
- Someone hacks, gains access, then leaves a back door. They then they have that capability on the dark web and when there is a requirement, someone will buy that capability. Access is now a valuable, tradeable asset.
- Could take years before someone needs it, and the hackers have an incentive to remain stealthy until they have a buyer.
- They are now leaving a back door and patching the systems, so this would go undetected in a regular Vulnerability Scan.

Slide 9

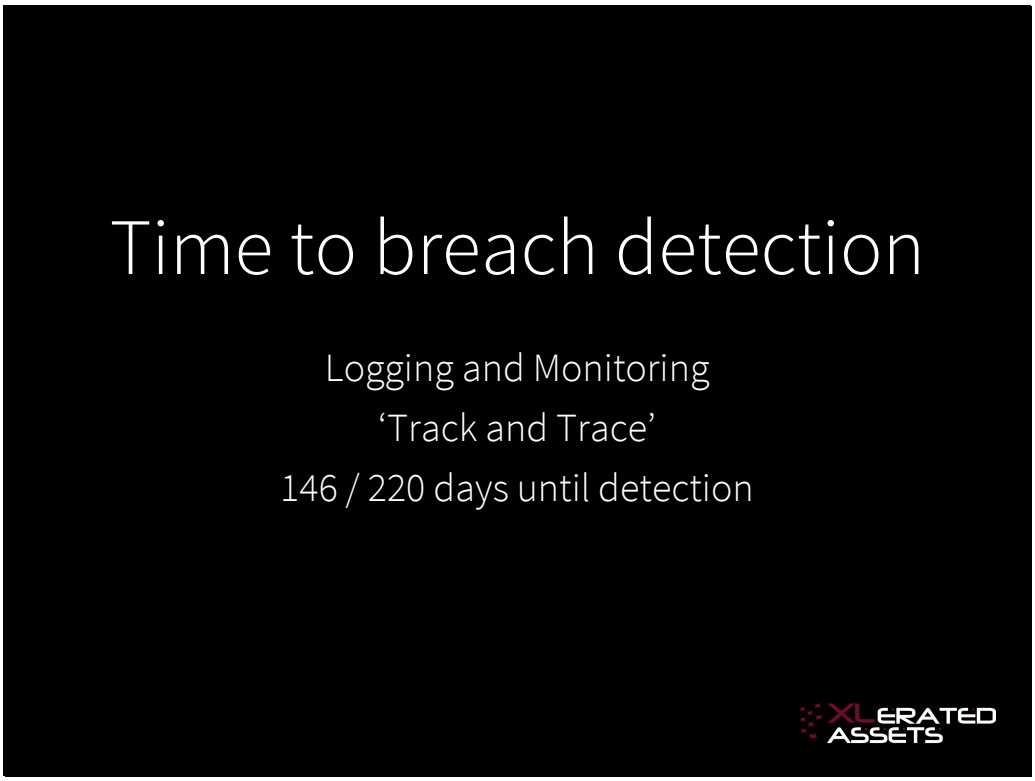
Shadow IT (this is an interesting one)

- This refers to IT solutions which are developed by employees / users within a company, without planning or approval by the IT department.
- This could involve employees automating processes themselves using Excel macros, or firing up a new cloud service to manage a group's shared tasks.
- The users are often well meaning, but can accidentally open up vulnerabilities if they don't have any security training.

Slide 10

- DDOS attacks and spamming, etc… your business can be taken offline

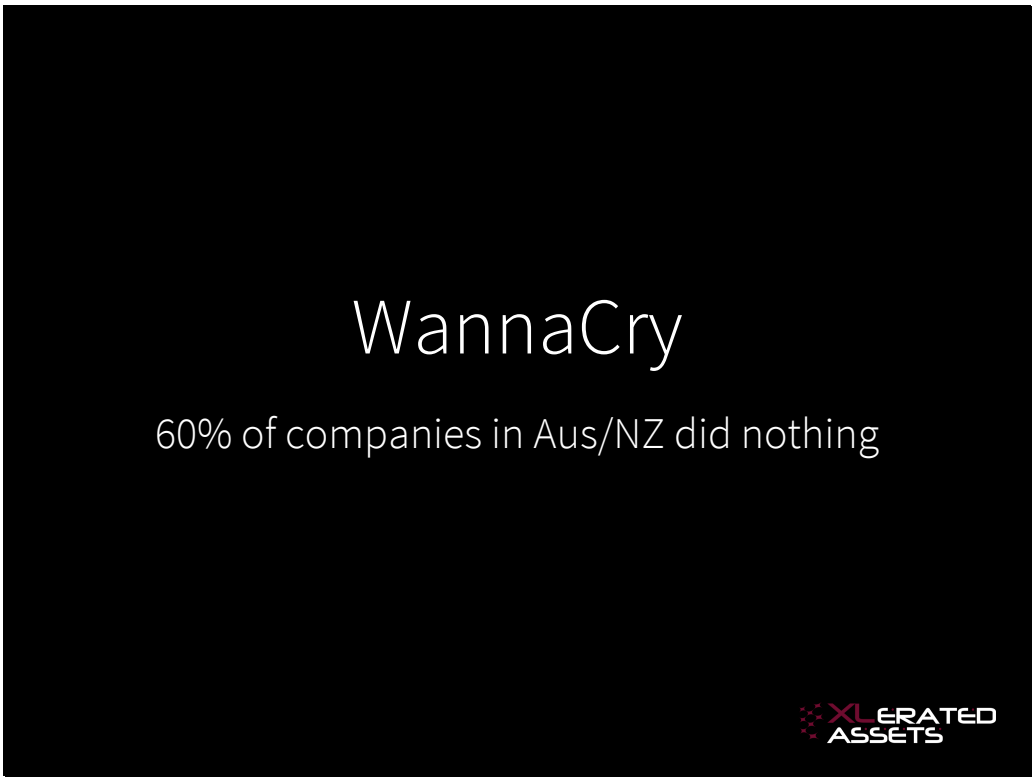
Slide 11



- These situations are common, as there is very little information collected on computer use and behaviour.
- Between 2016 and 2018, hundreds of companies and government agencies in the American energy, nuclear, aviation and water industries were breached. This breach remained undetected for almost 2 years until it was identified by the Department of Homeland Security and the FBI.
- To be able to identify these breaches faster, companies need to get much better at analysing the information being produced by their IT systems.
- For example, when I plug in a USB or login to the network, information is collected and stored in a file or database. Mostly this is just routine documentation of what is going on behind the scenes in the computer – but if you're trying to find anomalies which could point to a breach, that information becomes vital.

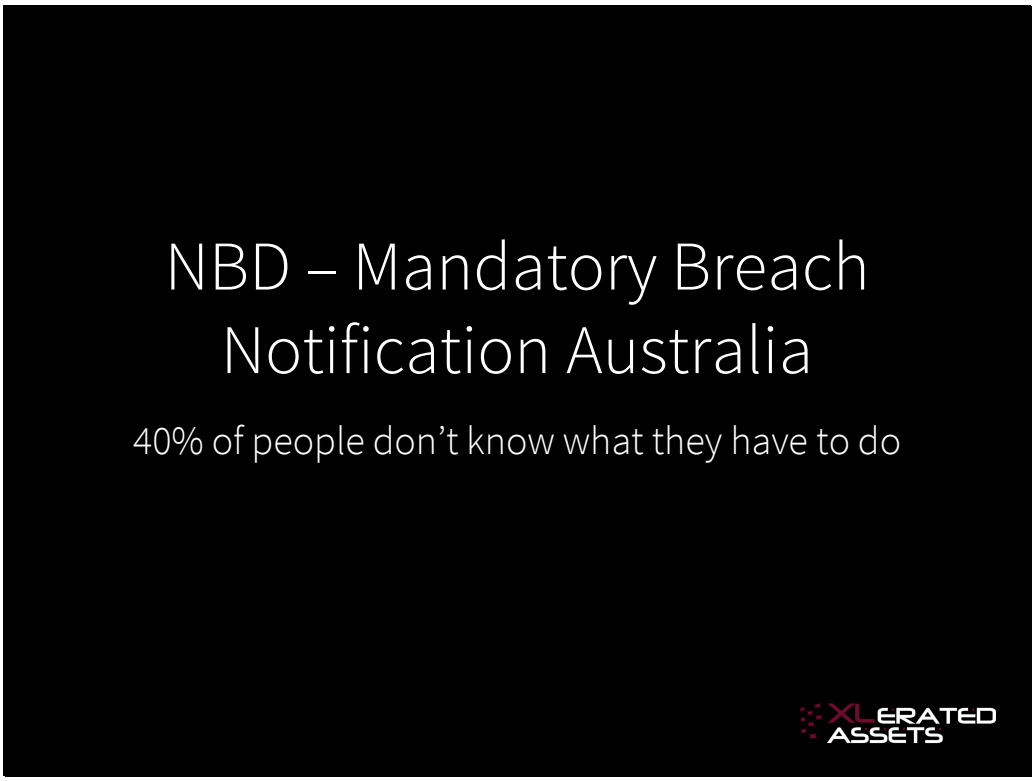
- A large company can send circa 8,000 messages per second, so for the untrained IT security guy, this is far too much noise, and the messages and events get ignored.
- Your IT guys don't have time, but I can show you something that will provide you with your top 10-20 priorities.
- It can be like panning for gold, sifting through thousands of rocks to try to find that one golden nugget.
- You need to be able to have a strategy to detect this hidden anomaly and have a plan of action in place when it is found.
- Thought this might be a good concrete example highlighting time to breach detection, leading into need for better analysis of logs.

Slide 12



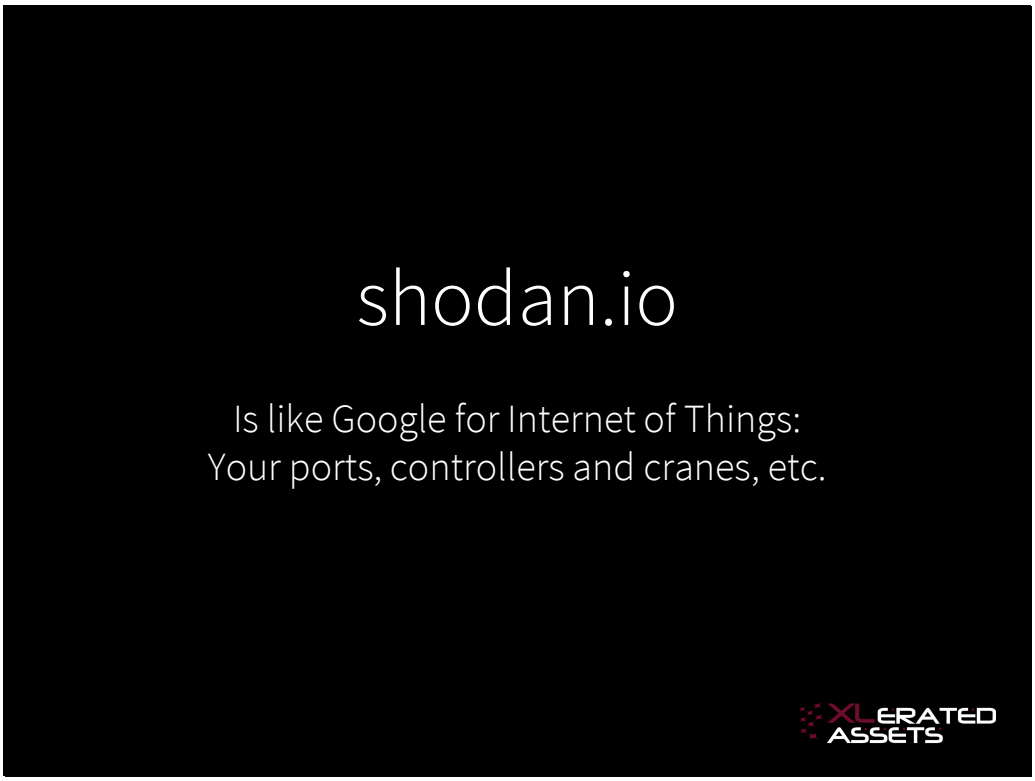
- How long do you think Wannacry was around for?
- Eternal Blue was a 10-year-old exploit
- Researchers have now shown it can be exploited to Windows 10

Slide 13



- NBD and the number of cases reported: already up to 63 as of a month ago
- About half of these were malicious attacks, and half were caused by human error.
- Point to take away: give staff basic security training.

Slide 14



- It exists, and as I speak is scanning and reporting back to a central site (like Google) and will display all your network, unpatched systems and vulnerabilities.
- It is very detailed, an example would be

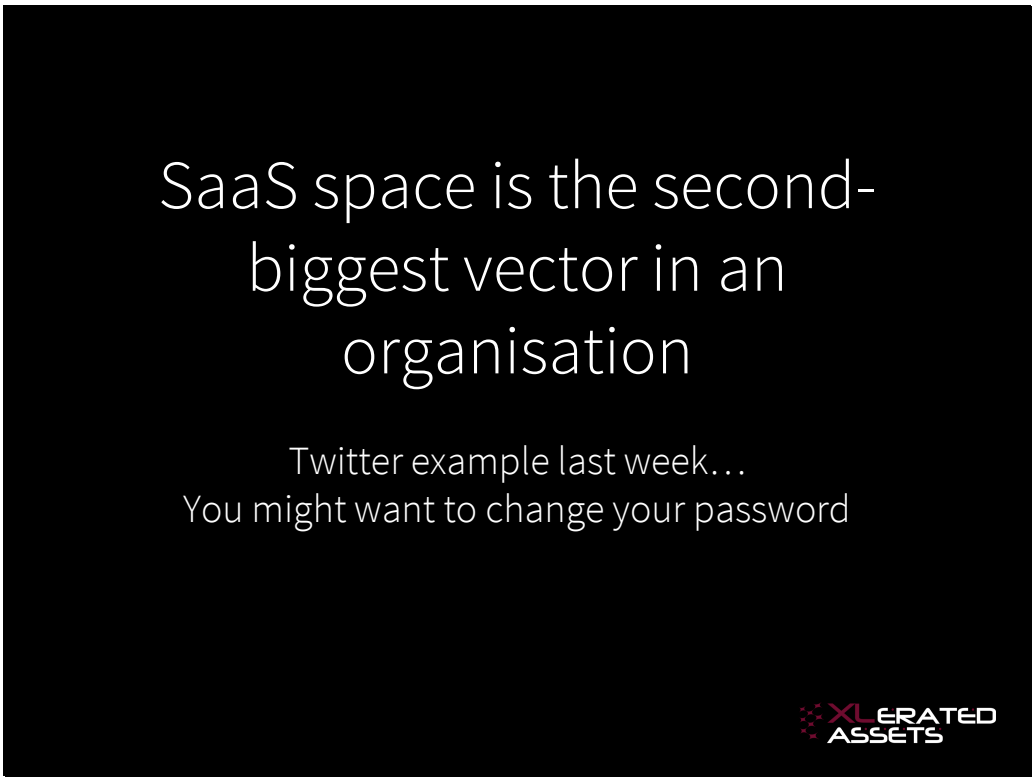
  search for ‘scada melbourne’

Slide 15

75% of organisations in Aus/NZ top 10 companies have no Incident Response

- What happened when you are breached, compromised or… taken offline
- GDPR requires an IR plan
- If the CFO is on a plane to New York and uncontactable, he won't be able to sign-off some forensic work
- Who will be in the initial meetings and how will you communicate?

Slide 16



- Employees can and do use the same password for everything

Slide 17

A huge fear statistic: 1 in 10 people now have home assistants

- People are now bringing consumer devices from home and asking the ‘echo’ to help them at work
- This is a huge risk, and can open networks up to cross-contamination from infections on employees’ home networks
- Unprotected consumer devices should not be plugged onto the network, but often policies to prevent this have not kept up with changing tech

Slide 18

So what can you do?

- To mitigate attacks, don't allow unencrypted protocols, change default passwords.
- Turn off legacy protocols and anything that is not required.
- A useful report to read is the Australian Signal Directorate's (ASD) Top 4 Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirement Explained. This is easy-to-follow advice that will give you an initial strategy to implement the most effective security controls to prevent over 85 percent of intrusions.

Slide 19

- NDB, GDPR and Privacy Act NZ amendments. Companies working across borders are going to have to adapt to privacy laws across their whole networks, particularly with regulations such as the GDPR in the EU, requiring fundamental shifts in how companies handle data privacy.
- Shortage of skill sets:
    - It can be really hard for a company to keep a single skilled cyber security expert. Security people like to sit and hang out with other security people, and they'll often move into a specialist company if they get the chance. Using a trusted partner to manage cyber security can help you get the best people working on your system.
    - Is my interpretation correct here / match with what you were going for?

Slide 20

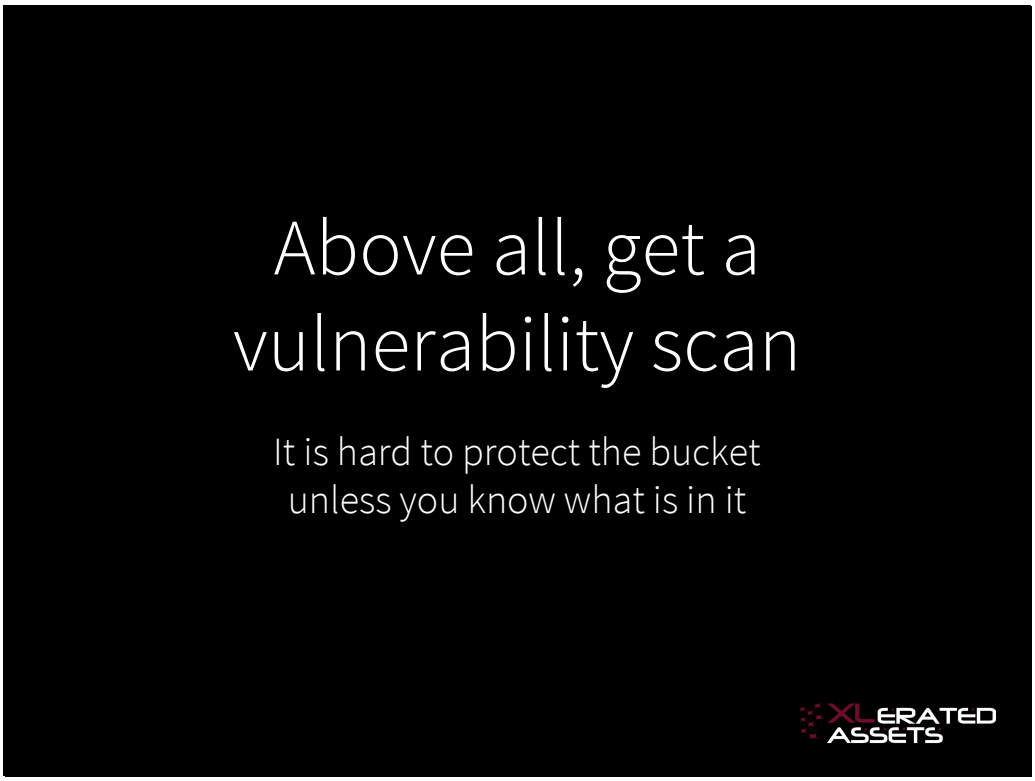
- This is the free option. It only costs time.
- Some things cannot be patched, or it is extremely difficult (ICS Industrial control systems), so get some advice.
- I'm working with the vendors so can help provide some guidance here; there is no need for it to end up in the too-hard basket.

Slide 21

Phishing Attacks

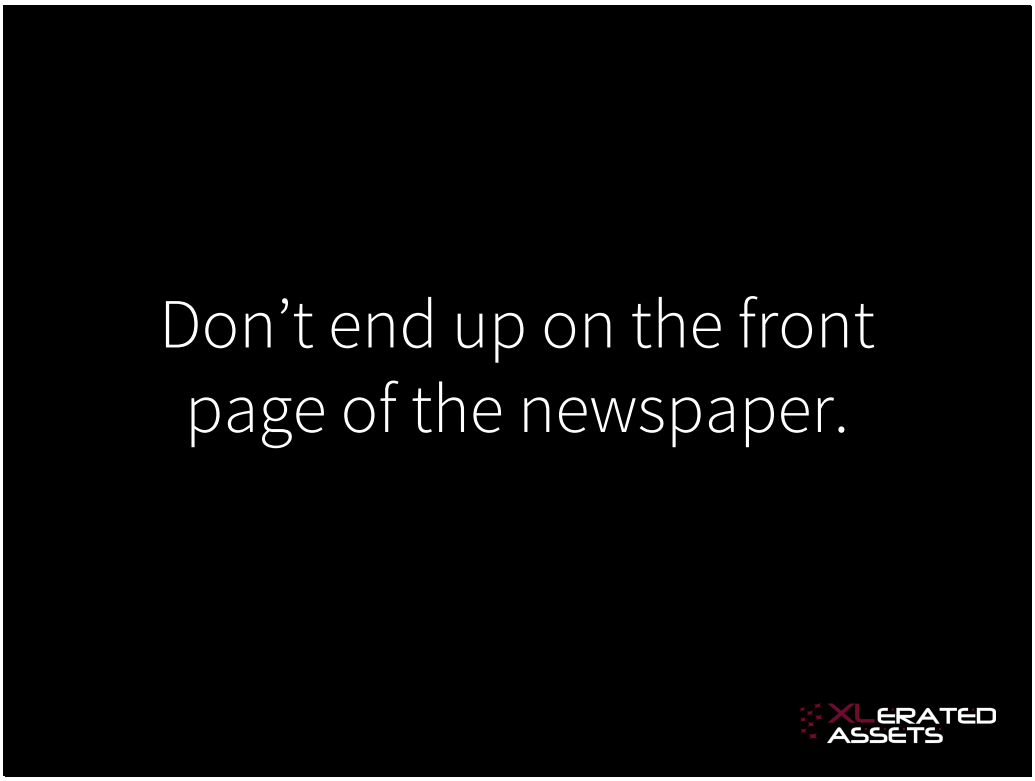
- 82 percent of boards are concerned with email fraud and more than half (59%) consider it a top security risk
- Hackers love the human element
- Wedding photos or Company Christmas party… most people are expecting the photos

Slide 22



Above all, get a Vulnerability scan: it is hard to protect the bucket unless you know what is in it.

Slide 23



Slide 24

White paper https://bit.ly/2FMYYAp