FACTCHECK: THE CYBER SECURITY ATTACK SURFACE

DEBI ASHENDEN,
CRANFIELD UNIVERSITY

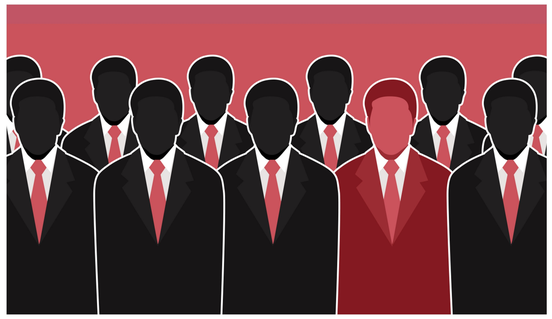
It isn't just your bank account criminals are seeking to access. We give an insight into the size and complexity of systems and devices that are vulnerable to attack.

1
INCREASING COMPLEXITY AND SHORTAGE OF STAFF

By 2020 there will be 35 billion devices connected to the internet, six billion of these devices will be able to request support for themselves. The amount of data on the internet will increase to 44 zetabytes (roughly the equivalent of streaming the entire Netflix catalogue more than 3,000 times). Technology fixes for security will not be able to keep up and there is a shortage of suitably qualified and experienced security staff. The qualities most valued in security staff are agility, responsiveness and trustworthiness.

2
MARKET FORCES

In an ideal world software would be written securely but in the real-world market forces don't allow for it. Microsoft, Google and Facebook are examples of companies that run bug bounty programmes where they will pay individuals who find bugs and exploitable vulnerabilities in their software. There are also companies, however, who trade in bugs and vulnerabilities and will sell them to the highest bidder. There are some that specialise in buying zero-day vulnerabilities (these are vulnerabilities that haven't been publicly reported previously). The highest bug bounty currently being offered is $1.5m for zero-day vulnerabilities in Apple's iOS 10 operating system.

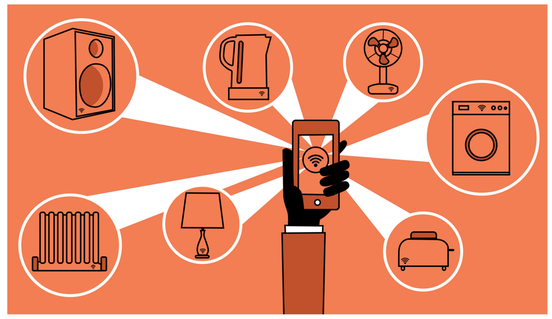


3
INSIDER THREAT

At the moment an average large organisation can expect to see 81 million security events over the course of a year. These are alerts on a system that may or may not indicate an attack has occurred. Technology can currently filter out 11% of these. While only a proportion of these will turn out to be attacks the incident to attack ratio is rising. In the region of 55% of security breaches are caused by insiders – individuals with legitimate access to an organisation's systems.

4
INDUSTRIAL CONTROL SYSTEMS

In the US the Department of Homeland Security has said that the energy sector faces more cyber attacks than any other industry. In December 2015, the Ukraine suffered a power outage caused by a cyber attack. In May 2016, the G7 Energy Ministers highlighted their concerns about the cyber security threat to energy systems and their commitment to developing resilience against attacks.

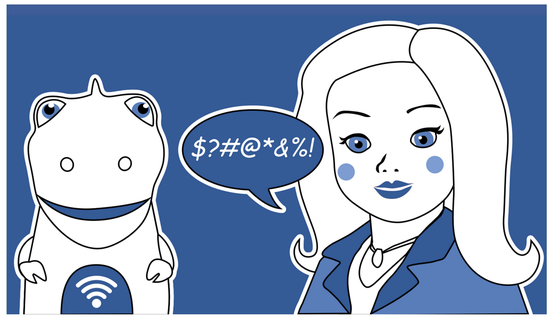


5
THE INTERNET OF THINGS

By the end of 2018, 20 percent of smart buildings will have suffered from digital vandalism. This could be in the form of attacks on digital signage, heating, air conditioning or lighting for example. The cyber attack on the US retailer Target in 2014 was through their HVAC (heating, ventilation and air conditioning). Smart buildings are often connected to the internet with weak or non-existent password protection. Physical security processes will need to be integrated with cyber security processes.

6
PERSONAL DATA

The biggest personal data breach to date is probably that experienced by Yahoo who recently admitted that names and phone numbers from more than 500m accounts had been stolen in 2014. The CEO of Yahoo apparently rejected the idea of requiring customers to change their passwords when the breach was discovered because she believed it would have an adverse effect on the business. 93% of data protection breaches are due to human error.



7
IMPACT ON FAMILY LIFE

We have seen instances of baby monitors being hacked but toys for children (such as the 'My Friend Cayla' doll) are also now wifi-enabled and speech-enabled. CogniToys Dino is a soft toy dinosaur and has advanced language processing algorithms that enables two-way speech-based interaction and uses the IBM Watson learning machine. 'My Friend Cayla' has already been hacked and instructed to recite lines from '50 Shades of Grey' and to quote Hannibal Lecter.