Cyber risk: why it matters and how to develop resilience

Cyber security is often seen as a remote, nebulous problem, yet the impact of recent events lies firmly in the real-world. We asked Ed Parsons from information security specialists, MWR Infosecurity, to give his perspective.

In February this year, Verizon Communications Inc. announced a reduction in the price it will pay to acquire Yahoo's operating business by $350 million, following a number of cyber incidents exposing over half a billion customer records. Many organisations could soon face similarly large penalties for failing to protect data: under the European General Data Protection Regulation (GDPR) from May 2018, companies that fail to comply with statutory obligations could face fines of up to 4% of global annual turnover.

The risk is not new, although threats have increased in scale and sophistication. Despite spending more than ever on security, data breaches and system outages continue. Analysis of these incidents suggests organisations are failing to effectively prevent or even detect attacks. Arguably we are reaching a state of 'breach fatigue', where the number of incidents, the incomprehensible amount of exposed data – and perhaps media focus itself – has led businesses and their customers to view cyber-attacks as an inevitability. With such a bleak picture it's little wonder security wonks are telling their superiors to 'assume compromise'.

It begs the question 'how did it all get so bad?' Part of the answer is our exposure to cyber risk has drastically increased. We are increasingly societies that live and conduct business online. Digitisation is transforming businesses and increasing their reliance on networked technology susceptible to remote attack: the replacement of high street branches with mobile applications is just one example. This trend is only likely to continue with the drive towards interconnectivity, automation and artificial intelligence across industries.

Businesses also struggle to weigh long-term, remote risks with more immediate benefits. In the rush to market, security can be perceived as an obstacle, adding 'friction' to internal processes or – even worse – user experience. In the wake of the Yahoo data breaches, an employee claimed that Chief Executive Marissa Meyer had "emphasised a cleaner look for services and new products over security improvements", adding that "the security team often clashed with other parts of the business, because of concerns that the inconvenience of added protection would make people stop using their products." If true, the decision now appears costly.

Finally, many businesses lack an accurate understanding of how they might be attacked; knowledge that is essential to build effective defences. High profile leaks speak of omnipotent government surveillance regimes, and newspapers revel in stories of the proverbial teenager damaging major businesses from the comfort of their bedroom. Technology companies and service providers within the security industry have little incentive to provide a clearer view, instead exploiting their information advantage to continue selling ineffective solutions. Little wonder therefore that things aren't getting better.

There are several strategic imperatives that businesses should think about addressing to enhance their resilence to modern cyber-attacks, as discussed below.

Cover the basics

A number of key security controls effectively mitigate modern attack techniques, improving an organisation's chances of preventing low-sophistication attacks, whilst increasing the effort for more determined adversaries. Implementing these controls effectively at scale is a significant challenge but one any organisation serious about security should rise to, or accept the risk. SANS, an information security training institute, has produced a list of critical security controls. The Australian Signals Directorate, a government intelligence agency, has produced an even shorter list of four key controls – application whitelisting, application patching, operating system patching and privilege access management – it claims will mitigate at 85% of known intrusion techniques.

Shift focus from prevention to detection and response

Modern attacks focus on abuse of legitimate access and processes – things businesses depend on. Rather than focusing exclusively on preventing 'known bad' events, organisations should balance investment and efforts between prevention, detection and response. Gartner predicts that by 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 20% in 2015. Traditional technical controls (including those mentioned above) should be interpreted as methods to reduce the opportunities for attack; to raise the – perceived or real - cost to the attacker, and increase the chances of detection. The case for this shift in focus is underlined by GDPR requirements that data breaches must be reported to the Supervisory Authority within 72 hours, and timely reporting relies on effective detection.

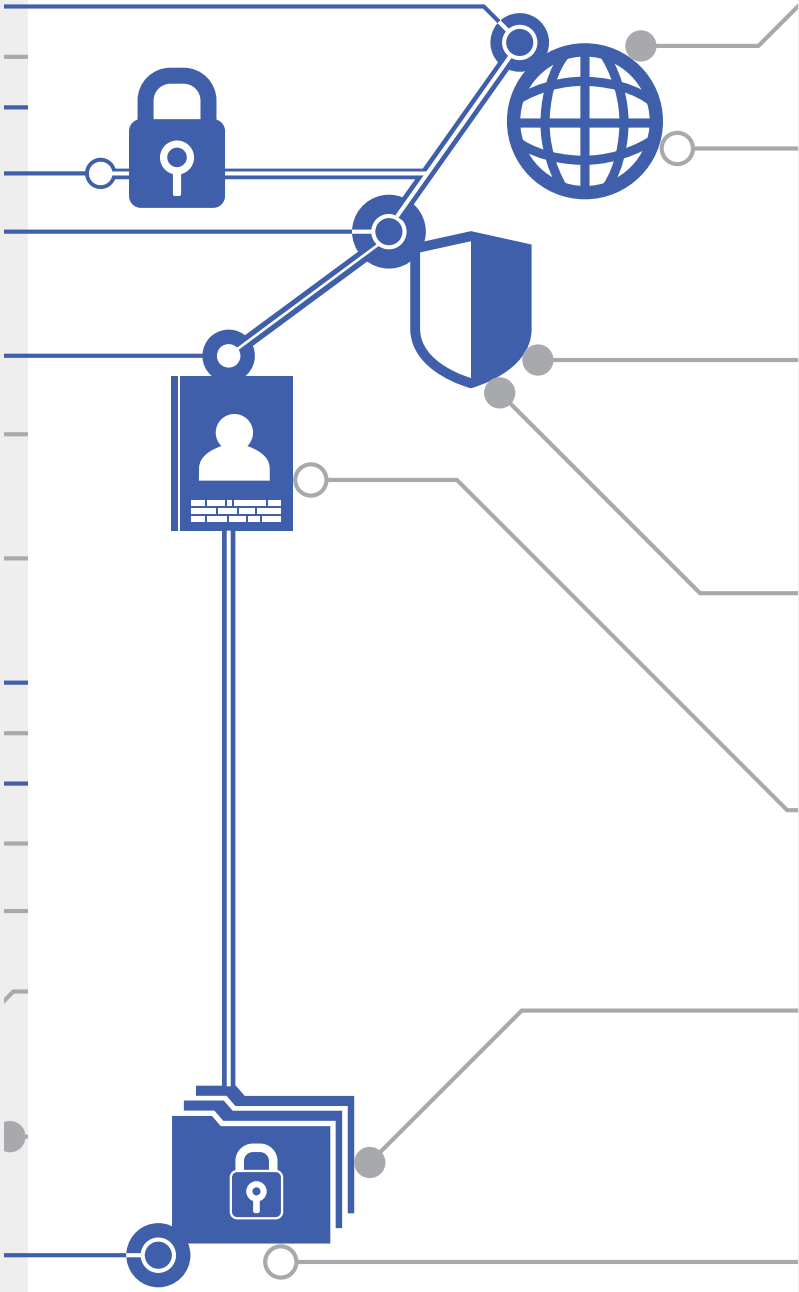
Design and test defences against modern attack techniques

A leading security researcher recently claimed 'designing the battlefield' was the single advantage we hold over cyber adversaries, given the asymmetric nature of the threat. Organisations need to consider the context, or environment in which modern attacks occur, in order to determine the right balance of preventive and detective controls. With modern attackers 'living off the land' – using tools and resources available within target environments, organisations should use scenario-based testing as a realistic measure of their resilience, and use the results to identify appropriate mitigations, saving time and money wasted on controls that don't materially alter the risk.

Recognise that security is becoming application security

Digitisation is turning many organisations into technology (even software) companies. Cyber security therefore plays an increasing role in enabling business strategies and objectives, and managing the attendant risk. As businesses move online and into mobile applications, and embrace virtualisation, cloud and continuous delivery models, organisations must also develop sufficient agility within security functions to adapt to foreseeable future risks, including those created or exacerbated by innovation. Secure software development will play an increasingly important role: As infrastructure is becoming code, so is security. Software teams are taking responsibility for security of (virtual) hardware and larger scale systems, and must be supported to bake security in rather than belatedly testing for vulnerabilities.

Ed Parsons
Associate Director, MWR InfoSecurity



MWR InfoSecurity

MWR Infosecurity is a global provider of world class research-led cyber security solutions with a range of products and services for clients worldwide.
www.mwrinfosecurity.com

The Berkeley Partnership
www.berkeleypartnership.com