This quarter marked the 30th anniversary of the World Wide Web. While working at the European Organization for Nuclear Research (or CERN) in the 1980s Tim Berners-Lee became frustrated with the inefficiencies and difficulties of finding information on the early internet, and proposed a better system for finding information that eventually became 'the Web.'

Thirty years on, more than half the world's population is now online. The social, industrial, commercial and political changes that have been sparked by the internet's widespread use have been the equivalent of a 'Digital Industrial Revolution.' Whether via the web, email, text messaging, social media or internet-enabled phones and other smart devices, businesses have an unprecedented range of channels with which to engage with customers. These developments have in turn led to new and surprising ways of doing business.

You may have heard the adage that in the digital age, the world's largest source of information - Google - can be searched without visiting a physical library. The world's largest taxi business Uber owns no vehicles, and the world's largest accommodation provider Airbnb does not own or lease any of the inventory it offers. Digital has become the 'new normal.' But not all the changes have been positive. As Berners-Lee wrote in Wired:

"…while the web has created opportunity, given marginalised groups a voice, and made our daily lives easier, it has also created opportunity for scammers, given a voice to those who spread hatred, and made all kinds of crime easier to commit."

With digital opportunities come cyber security risks

A constantly evolving range of digital security threats has grown as fast as the business opportunities offered by the 'Digital Industrial Revolution.' And businesses of all sizes are vulnerable, not just large ones. Often the vulnerabilities arise as businesses transition from pre-digital to digital operations. Operational processes using assets and technology purchased for pre-digital, steady and predictable operations, often struggle to cope with the demands of the fast-moving and unpredictable 'agile' digital operating environment.

Previously, most threats were mainly physical and could be stopped at the 'periphery' of a business with good physical security and risk management procedures. The most significant threats generally came from physical theft by malicious employees, robberies or events such as fires and floods.

In today's hyper-connected world businesses now have to contend also with the threats that do not require physical access to a business. These cyber infiltrations can emanate from anywhere in the world. As a result, domestically-focused businesses now have to 'think global' when considering their security. Even businesses which are digital 'from the ground up' are not immune from cyber threats. Whilst built on foundations imbued with digital processes and management nous, they remain vulnerable to well-executed fraudulent criminal activities such as email phishing.

Cyber attacks – the growing threat to businesses

Proof of the likelihood of cyber threats to business came thick and fast this quarter when:

- The computer systems of a specialist cardiology practice renting offices at the Cabrini Hospital in Melbourne was hacked and 15,000 patient records were digitally locked and held to ransom for more than three weeks;
- Toyota Australia's staff were locked-out of their emails for several days due to a cyber attack;
- Landmark White had 137,500 unique valuation records stolen which included names, residential and business addresses, email addresses and phone numbers of the property owners, as well as commentary relating to the valuation of particular properties. It's interesting to note the listed ASX company continues to be in a voluntary trading suspension since February 19th, and
- There was an attempt to hack into the computer network at Parliament House in Canberra.

We also learned this quarter that cyber attacks occurred last year to the Catholic Archdiocese of Melbourne, as well as the Telstra employees' superannuation fund. In February it was also reported that a director of Judo – one of Australia's emerging fintech ("financial technology") lenders – had their email compromised. The hackers used

this information to contact potential Judo clients in an attempt to exploit them too. Significantly, most if not all, of this criminal activity occurred without needing to physically infiltrate their targets. It is likely that many of these criminals may not even be physically located in Australia.

Emerging threats to healthcare and patient information

The scope for further threats continues to expand. Health-related industries in particular are becoming more attractive to hackers due to the rising value of stolen health information. Information stolen from hospital management systems, patient record systems, and medical devices has been used to 'ransom' major healthcare providers by threatening the integrity of their patient records and consequently the care they provide. Significant events of this nature continue to occur overseas and in Australia.

Being secure means being 'permanently ready' to respond

The diverse and unpredictable nature of cyber threats means that businesses can no longer simply patrol their peripheries. In the digital age it is not a matter of 'if' but 'when' a cyber attack will occur. Therefore, businesses need to be 'permanently ready' to respond. They first need to know what information and technology assets are valuable and in need of protection. Then they need the people, processes and technologies in place which allow them to not just protect, but detect, respond and recover from malicious activity that will inevitably occur. Businesses that adopt this approach will be better able to manage cyber breaches.

Work that Trusted**Impact** did in recent years found that success using this approach depends on the right combination of process, technologies and most importantly people. While Australia's looming cyber skills shortage means that finding the right mix of cyber security and risk management skills will not be without challenges, businesses do not need to do everything in-house. Strategic partnerships with security specialists like Trusted**Impact** means they can access expertise well beyond their 'periphery,' while benefiting from an ongoing relationship in which the strategic partner is as vigilant about their clients' security as their clients are. Contact us if you'd like to explore this.

Significant Salient Statistics

Each quarter a wealth of statistics from diverse sources is published. When used sparingly and in the right context, they can improve a discussion with senior executives. This quarter the Office of the Australian Information Commissioner (OAIC) released its report on data breaches between October and December 2018:

- Over 1 million people were affected by data breaches during this period.
- 262 data breaches were reported during the quarter, up from 245 the previous quarter.
- 168 breaches were malicious, while 85 breaches were caused by human error.
- Health service providers reported the most breaches, 54 for the quarter. The next worse were finance with 40 breaches and legal, accounting and management services with 23.
- Theft of health information alone accounted for 71 breaches.

Thank you for being part of our community. Please 'follow us' on LinkedIn or Twitter to keep connected. Also, don't hesitate to send this to others, or simply have them subscribe here.

TrustedImpact
PROTECTING DIGITAL

we're **independent** consultants – it's about **your** business and **your** success
with a **singular focus** – cyber security is all we do
leveraging **experienced** professionals – credentials, not checklists