There were some important cyber developments in the 'nation state' space this quarter. Israel took a major step with a lethal cyber response, by shooting rockets into a building that was purportedly the source of a cyber attack. In a similar vein, the US apparently launched cyber attacks on Iran as a response to their physical shooting down a surveillance drone. Thus, the delineation between physical and cyber is blurring very quickly.

From another lens, the lines between national interests and commercial interests are also blurring after the US (and friends) turned up the head on Huawei's network business over cybersecurity worries that "half its kit has at least one potential backdoor', and then pulled software and hardware support for Huawei's consumer smartphones – currently the No. 2 smartphone builder in the world.

But try not to get overwhelmed or distracted by the nation state activity – it's advanced, always been there, and will continue to be there. It's the miscreants who try to take advantage of our businesses (and citizens) that we should not lose sight of... It's not futile, and focusing on executing well on the basics that will help to protect your organisation from becoming a headline.

Cyber crime rising – 61% of incidents are criminal

In May, the Office of the Australian Information Commissioner (OAIC) reported that criminal or malicious activity was behind 61% of breaches during the first quarter of 2019. Over 130 incidents involved the digital equivalents of fraud, break-ins, thefts, industrial sabotage, criminal impersonation and ransoms.

The Health sector reported the highest number of breaches, followed by professional services firms like accountants and lawyers. These sectors rely on the exchange of intimate personal information or confidential business data to deliver most of their services – hence, because their data can be monetised, criminals are motivated. Health data often has a longer 'shelf-life' for thieves because it can't be easily changed like a credit card number. This quarter's report from Carbon Black did a good job actually detailing why health and patient data is worth more on the black market than credit cards or similar financial data.

Cyber success is about "leadership"

Cyber has been traditionally seen as an "IT problem". The severe impact of cyber incidents is a serious BUSINESS problem that can no longer be relegated to junior ranks or IT teams alone. Chairs, Directors, CEOs, and senior executives need to take a leadership stance because cyber incidents has been shown to:

- **Threaten the viability of long established businesses**, such as ASX-listed property valuer Landmark White which forecast an $11.50 million or 21% fall in annual revenues following the theft of 137,500 unique valuation records earlier this year. After this breach trading in the company's shares were suspended, severely limiting its ability fund its operations. Shortly after share trading resumed in May, another data breach was discovered, threatening the viability of the business as it lost key customers.
- **Severely damage the trust and reputation organisations take decades to build**, as seen loss of personal details of customers (at Westpac), patient records (at a cardiology practice in Melbourne's Cabrini Hospital), and student details (at Australian National University).
- **Threaten to derail new ventures**, such as Australia's new national e-conveyancing platform PEXA (launched in 2013). Last year criminals broke into a conveyancer's computer systems and subsequently impersonated that conveyancer on the PEXA platform. By doing so they were able to steal the $250,000 proceeds from the sale of a Melbourne family's home. This incident was a contributing factor to the company abandoning a planned listing on the ASX.

The C-suite must LEAD. An organisation's culture and organisational priorities are set at the top. If CEO's do not 'walk the talk' and highlight the role of cyber to the entire organisation, it exposes it to potentially significant, escalating risk. This 'leadership' can take the simple steps like:

1. Clarifying and discussing the cyber-based risks the organisation faces, and developing practical mitigation strategies across the business, its key suppliers, and even customers (which, by the way, should not involve acronym-laden technology solutions as the answer);
2. Ensuring the organisation (re)prioritises its limited resources to minimise or transfer major risks; and

3. Setting a culture (ie, “walk the talk”) to instil “Secure Thinking” across the workforce.

Postcards from the Front-Lines

Cyber is challenging but not futile. We thought it might be useful to share a few simple, hands-on insights gained from real client assignments that might help you in your situation. For example:

- Use “2-factor” authentication on all external systems (especially email). It’s now become pretty easy to do and the excuse ‘you’re keeping us from being productive’ doesn’t hold water any more. Employees use bad passwords, and it’s child’s play to ‘credential stuff’ and get inside your systems. Trust us: do it - do it now!
- If you’ve got Microsoft Office 365 email, configure simple alerts to find potentially nefarious activity like as ‘email forwarding rules’. It’s a common tactic we’re seeing far too often to steal confidential information.
- These days we’re seeing so many frightening issues relating to how a web application is CONFIGURED in the cloud (eg, AWS, Azure) that will likely not be picked up in a ‘traditional Penetration Test”. Consider undertaking a ‘configuration review’ to assess if that system is exposed because a configuration option hasn’t been considered.

Significant Salient Statistics

Each quarter we see a wealth of diverse industry statistics. Used sparingly and in the right context, they can improve a discussion with executives or those less exposed to the industry. This quarter Verizon released its latest annual *Data Breach Investigation Report* based on 41,686 confirmed security incidents and 2,013 data breaches spanning 86 countries. It revealed the growing threats on many fronts:

- Senior executives were 12 times more likely to be the target of security incidents and nine times more likely to have been the victims of data breaches compared to last year (are your exec’s trained to identify common scams?)
- 43% of all breaches occurred at small businesses (don’t kid yourself by thinking it’s just large banks).
- Over half (56%) of data breaches took months or longer to discover (think about how you could detect a breach)
- While external threats remained dominant (69% of breaches), incidents involving insiders (either by accident or malice) accounted for a third of breaches (have you considered this to be a practical risk?)

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.

Kind regards,

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