The first quarter update
March 2021

There's optimism in the air this quarter as the global vaccine rollout gets a bit of traction and has finally reached our shores. Without a doubt, the last twelve months has challenged our resilience on all levels from personal to professional, thus, the smell of optimism is sweet and most welcome – let's hope it continues.

It's all about resilience

All things 'digital' will remain a priority for many organisations and building resilience into your digital channels must also be a priority. While "UX" (user experience) and scalability are important, consider 'left of centre' cyber concerns, such as the risk of ransomware to these channels. Today, the bad guys invest considerable time and effort to get on the inside to learn how your organisation sets up its Disaster Recovery (DR) process so that they can wreak havoc with maximum impact. Develop and execute 'thoughtful' DR plans that reflect the possibility that someone might actually know your DR processes. And not just recovering the data, but reflecting the need to rebuild essential systems where 'availability' is critical such as what Channel Nine learned just this last weekend.

Also left of centre is the possibility that if you are using the 'cloud', it's configured in risky or insecure ways. During COVID many organisations shifted quickly to the cloud, often without appreciating the nuances of those features, functions and other security configuration settings that can leave your cloud exposed. CIS benchmarks are always valuable – either get on top of those or ask us for help. We review cloud configurations all the time and have NEVER, NOT found major opportunities to improve.

… and speaking of the cloud

We're very proud to have released our latest Security Leadership Series paper this quarter: Cloud Migration – the Sky is the Limit. It was developed in partnership with the Australian Information Security Association (AISA). This paper synthesised some great insight from thirty leaders in technology, security and cloud computing. We gratefully appreciate their involvement and input (you know who you are!). The paper (here) was summarised well in AISA's Cyber Today digital magazine (here), and we were honoured that AISA hosted an interactive Webinar Panel Discussion with four of the leaders.

The key "take-aways" from the research were:

1) Information Security is a 'leadership challenge.' Boards and Executive suites need to 'lift their game' by adjusting and realigning the organisation's investments, priorities, policies and processes to be more reflective of the use of cloud technology and its unique risks.

2) Organisations must accelerate their security and cloud-specific risk awareness programs to improve ineffective policy compliance so the organisation can more sensibly adopt cloud technology. It's about going beyond the traditional "don't do it" mindset in order to create long-lasting behavioural change and to minimise the use of 'rogue' or potentially risky cloud services across the organisation.

3) It is essential that organisations go beyond the simple responses of 'yes' to critical questions on essential security processes or controls, and begin to seek evidence that controls not only exist but that they are also effective, and

4) Even when organisations know that the measures implemented by their Cloud Providers are effective, they shouldn't always rely on Cloud Providers' measures ONLY, especially for Disaster Recovery.

These last two items rang true this quarter when the "OVHcloud data centre' went up in flames. Check out our 'cloud nine' recommendations (page 16) if you'd like some thoughts on how to improve your cloud position.

Beyond the hype

This quarter's been a big one for major cyber issues. Accellion, SolarWinds, Microsoft Exchange, and SITA (multinational IT company providing shared communications networks for numerous airlines).

Granted the headlines 'our staff made a stupid mistake' doesn't read as powerfully as 'hacked by sophisticated nation state enemies', but the implication that an organisation is helpless against cyber threats is simply wrong. If we look beyond the typical news headline hype, we find some simple basics that are worth thinking about for your organisation.

The first important 'basic' is appreciating your risk of third parties, cloud providers and your 'supply chain'. Simply stated, it's paramount your organisation appreciates the 'others' who may store or process your sensitive data, or who may have access to or be part of your technology ecosystem. Our Security Leadership Series research paper will provide you with 9 recommendations to consider for your organisation's cloud providers. Also don't forget those 'outsourcers' that look after various aspects of your technology environment (eg PABX's, copiers, building management systems, security cameras, etc.) who may also have the ability to log into your organisation to fulfil their ongoing maintenance requirements. Analogously, give a gardener the key to the tool shed, not your front door and tell them they can enter any time of the day or if you're not there.

Keeping systems 'current' is the second theme. The Accellion File Transfer System (read 'system to send large, important files') used by the Reserve Bank of New Zealand and the Australian Securities and Investments Commission was 20 years old and had been replaced by another system in 2014. The iPhone isn't even 20 years old… analogously, don't use an 'old clunker' car if driving or hauling things is an important part of what you do (or not expect it to break down).

Third. with 5.1 billion internet users, good passwords / passphrase use is paramount (as is using Multi-Factor Authentication for everything that is internet-connected). Simply throwing the unnamed Intern under the bus and saying it was 'against policy' to use 'solarwinds123' is poor form. Consider analysing your company's Active Directory to see just how bad (and against policy) it is (we can help if you want). That insight from that should then be used as a 'burning platform' to initiate a 'change management' cyber program that goes beyond the "don't do it" mantra to actually adjusting behaviour. It isn't just about simple phishing or training, but trying to change behaviour. Email us if you want help there too.

The final basic to comes from the MS Exchange issue. We often say "a cyber incident is inevitable – but becoming a headline doesn't have to be'. Digital is here to stay and adoption isn't going to slow down. Does your executive team (not just IT) have a Cyber Incident Response Plan? That's a good first step, but don't forget that it's really about practice. A successful sporting team doesn't just have a plan – they practice their positions, roles, responsibilities and step through it so that when the proverbial 'game day' hits, they are comfortable knowing what to do, Drop us an email – we can help there too.

Significant Salient Statistics…

Each quarter we trip across a wealth of statistics. Used sparingly and in the right context, they can often improve a conversation with executives. This quarter, the US FBI noted an increase of nearly 70% in internet crime from 2019 to 2020 and reported losses exceeding $4.2 Billion. Big numbers to demonstrate a big problem. Also, if you need help getting 'cyber' embedded in your Board, have a look at the World Economic Forum's new six principles for Board Governance of Cyber Risk.

Thanks for being part of our community. Please 'follow us' on LinkedIn or Twitter, and don't hesitate to send this to others or 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