Welcome to the first quarter review for 2022. This years' started with a twist when Russia invaded Ukraine in late February. Financial markets are shaky, currencies are shifting, supply chain's are floundering, and there are some strong inflation flags waving. Omicron continues to hold on, but fortunately at greatly reduced mortality rates as Australia's strong vaccination position helps us slowly get back to 'normal' – however that's defined in today's world!

Priorities & Investments – an Outcome-Driven Approach

Last quarter we were proud to bring together a number of seasoned experts from key industries such as health, financial services, education, logistics, academia, information technology and consulting. They shared their insights during our Leadership Series on The Reboot Show providing practical guidance on the journey to developing Cyber Maturity and achieving Cyber Resilience.

This quarter, these sessions were summarised into an 'e-book' titled "Cyber Security Priorities and Investments with An Outcome-Driven Approach" which you can download here. We'd love any feedback (positive or negative), and would value your opinion on future topics – just drop us a note here.

Are you now defined as 'critical infrastructure' and are you ready?

The US passed legislation this month requiring critical infrastructure operators to alert Homeland Security within 72 hours of a breach and 24 hours if an organisation makes a ransomware payment.

It has similarities to Australia's own, amended Security of Critical Infrastructure (SoCI) Act which is gaining a lot of momentum, and was just endorsed by a the bipartisan Parliamentary Joint Committee on Intelligence and Security (PJCIS). A good summary of the business implications is here.

In short, the definition of Critical Infrastructure is expanding. If you fall within that definition, the implications are a) mandatory reporting of incidents (and penalties if you don't), and b) possible Federal Government 'intervention' in response to a cyber security incident. Penalties -- including imprisonment – for those who fail to comply. You should consider the implications to your organisation.

Ransomware is still the headline

Ransomware continues to be a big topic this quarter – you should expect it to 'knock on your front door'. A sound (and tested) back-up regime goes a very long way to mitigate this risk. But don't forget what JBS and Channel Nine realised which was that it's **ALSO** about being able to recover bespoke systems and 'Operational Technology' as well as data. That 'purpose built' system needs to be recoverable too – most can't simply be 'reinstalled' like the traditional Microsoft Office reinstall CD.

The statistics also tell us that over half (54%) of ransomware is delivered via Spam/Phishing emails, and 1 in 3 employees will click on a initial baseline phishing test. So, if you're not running an awareness program focused on adjusting your entire staff's behaviour (not just sending phishing emails), you really should be. If you'd like to discuss what that might look like for your organisation, just drop us a note.

Sobering as well this quarter, we read from Sophos that, on average, ONE THIRD of data was never recovered, even though the ransom was paid.

Why a cyber incident is a C-suite problem.

Whether it's a data breach, or ransomware attack that locks your data or systems from your ability to use them (or both), having an 'incident response' plan these days is about as fundamental as it gets. As we've said for a long time, having an incident is inevitable but becoming a headline doesn't have to be. While many organisations have some sort of plan, we regularly see two areas where most fail.

The first, is to think a Cyber Incident is just a problem for the IT department to deal with. The second is the hesitancy to PRACTICE that plan with the entire executive team. Still true is the decade old comment from Mckinsey that "a poor response can be far more damaging than the attack itself".

Responding well includes the ENTIRE executive team including HR, Finance, Legal, Operations, Communications, etc.

For example, sizable fines (like Equifax's recent settlement of US$425 Million) and lawsuits for data breaches are becoming commonplace - your **LEGAL** team must be involved and prepared. Particularly if the question of paying a ransom comes up... "for an organisation under attack the decision to pay or facilitate payment of a ransom can be further complicated – and pressured – as the **legal position is unclear**. At worst, payment of ransomware may be unlawful and involve committing a criminal offence." You should probably have a legal position BEFORE you find yourself pressured for a decision.

And it's more than just legal that needs to be involved in the planning and throughout an incident. PWC's post-incident review of Ireland's health system has a wealth of lessons highlighting the role of **OPERATIONS** and **HR** when 31 acute hospitals had to cancel services ranging from surgery to radiotherapy. The operational challenge of shifting patients, nurses, doctors, and all of the support services for that would be daunting. JBS also learned that when supply lines had to be redirected and shifts were cancelled when ransomware impacted its different regions and 47 facilities in Australia.

FINANCE is often your insurance liaison – Mondelez found their insurance provider wouldn't cover their $100M bill for 2017 NonPetya attack and it's still under legal dispute. Closer to home, when Frontier Software's ransomware attack left 330 employers without their 'Software as a Service (SaaS)' automated payroll system, they recommended employers implement "contingency provisions for alternative payroll processes". Does your **ACCOUNTING** team have alternative payroll processes? As highlighted in our Leadership Series paper, just because your data sits 'somewhere else' in the cloud, it's better to be safe than sorry, and developing a Recovery Plan in the event of a cloud disaster could keep you from becoming that headline.

Finally, the role of **MARKETING, COMMUNICATIONS** and **PR** is the 'Achilles heel' for many. Simply identifying and establishing relationships with the important industry, regulatory, government, and police bodies is a list that few have put together. Having a pre-considered position on how to communicate to stakeholders is important. Harvard Business Review summarised it best: **"…don't forget to dust off and revisit your plan often. Hackers are constantly trying to stay one step ahead of you. So, keep running simulations… Your brand and your company's livelihood depend upon it."**

Cyber Politics

Things are heating up for an election. The Opposition leader resonated when he summarised his cyber position: "…cyber attacks represent a threat to our way of life… (and) costs the Australian economy $33 billion per year. Our security agencies are very good at what they do… but true national cyber resilience is a whole-of-nation endeavour… Cyber security needs to be someone's day job, not the last item on another Minister's to do list." Irrespective of your political views, he's spot on. The budget pledge of $10B to REDSPICE is good, but it takes resources and LEADERSHIP to make a difference.

_____

Thanks for investing the time to catch up with us this quarter. If you're not already, please 'follow us' on LinkedIn and/or Twitter, and feel free 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