Thanks for joining us this quarter. Our approach with this newsletter has always been to be 'short, sharp and salient': Just 2 pages, only once a quarter, and not just "what" happened, but the important 'so what' or insights behind the headlines. Please tell us if we hit or missed here – we'd like to know if we're getting it right for you!

Rampant Raucous Ransomware

This quarter, ransomware was high on the list. Someone will fall victim to ransomware every 14 seconds in 2019. Municipalities (ie, Councils), Schools, and Healthcare are top victims in the US. In fact, at US schools there's "one new publicly-reported incident every three days of the calendar year" and in July, Louisiana's Governor declared a 'State-wide Emergency' over cyberattacks targeting schools. Really? We'd suggest that we should try to declare less emergencies and just start doing the basics of Business Continuity or Disaster Recovery!

The situation should be enough to convince everyone to run at least one exercise to really assess how well their organisation would cope against ransomware.

1) TEST back-ups to ensure they work (be honest – when was the last time you actually tested it?),

2) Ensure back-ups are removed or DISCONNECTED from the network. Hackers often get access to internal systems or email (easy if you're not using "Two Factor Authentication"). If back-ups are network connected, they target those too, making reinstalling back-up impossible. And finally,

3) Think about files that may reside LOCALLY on those (desktop/laptop) computers that may not be a part of an application database back-up regime – is there anything there that would be sorely missed if it was lost?

Capital's Cloud Consternation

As they say "It's not the cloud, it's just somebody else's computer". In July, Capital One disclosed one of the "biggest breaches of a major financial institution ever". 106 Million Credit Card applications (btw, that's over FOUR TIMES the entire population of Australia!), and a cornucopia of other juicy or exploitable information. This was interesting from three different angles:

First, the hacker was a former employee of the cloud provider where the data was stored (AWS). Don't misconstrue our point - the cloud can provide a significant improvement in one's security posture – a good move for many. But don't be lulled into thinking that your data in that database cannot be read or accessed by a "System Admin" at the cloud provider if it isn't encrypted or masked in some manner.

Second, the hacker "allegedly exploited a misconfigured firewall". We do lots of security testing and often the 'traditional Penetration Test' often does NOT also evaluate configuration issues. The rise of CONFIGURATION issues causing vulnerabilities has skyrocketed in the past few years. Make sure this aspect is considered if you're testing, or go to the CIS benchmarks if you want deep technical insight on how to secure your cloud.

Finally, "Capital One says the misconfiguration lay in its own infrastructure, rather than AWS". Make sure you know what you are responsible for and what your cloud provider is responsible for – don't simply assume that it's all taken care of in terms of patching your application for known vulnerabilities, etc.

Bad Biometric Blunders

In March we wrote about "what nobody is talking about", or the unique issues of using biometrics for passwords. Then we hear that Suprema's "BioStar 2" platform, a web-based biometric security smart lock. It's apparently used by over 5,700 organisations in 83 countries, and leaked "27.8 million records and 23 Gigabytes worth of data including admin panels, fingerprint data, facial recognition data, face photos of users, unencrypted usernames and passwords, logs of facility access, security levels and clearance, and personal details of staff".

Measurements of unique human features (or 'biometrics') are digitally recorded and matched to the person trying to access the device. But if these measurements – whether facial features, voice or fingerprints – exist as digital records they can be stolen. And if they are stolen, they cannot be changed or replaced like a credit card number, password or PIN.

Apparently when the researchers who found the issue tried to proactively contact Suprema, it was largely shrugged off. Shame! Hopefully, Cisco's recent $8.6 million first-ever security software whistle-blower payout will motivate organisations who ignore the significance of these issues.

If you run a business that's considering biometrics, or if your business works with other organisations that do, it's worth conducting a review of the security practices surrounding their use. Also, if someone took your biometric data, consider whether you'd detect if it was being used fraudulently, and consider other 'factors' of authentication.

Phishing Phrenzie Phever

However you pronounce your Ph's or F's, our Security Awareness partner, Gartner-recognised Terranova is orchestrating a global phishing simulation event in October. The Gone Phishing Tournament is an annual, cyber security initiative run as part of the North American National Cyber Security Month (which coincides with Australia's **Stay**Smart**Online** week).

Statistics show that unaware employees are your cyber program's weakest link. Any meaningful program must involve the human aspect, and effective programs must focus on creating a sustainable shift in culture. Participating can be an easy way to create your "baseline" and also see how your human security compares to organisations all over the world. It's free and uses one common template over the same time period to facilitate a comparison of results. Register directly, or we'd be delighted to assist you if you'd like to participate. Just contact us here, and do it soon so you don't miss out – space is limited!

Local Lessons Learned

It's good to hear that Landmark White (ASX:LMW) may survive the impact of several security breaches that began in February this year. If you're not across it, you should be because there are lots of lessons. It's a gripping tale of how a small, local, listed company learned how important cybersecurity is when information and customer trust is essential. The CEO, and two Directors stepped down, and for months the company's financial viability was in question. It isn't over yet and it will be a good case study for a long time to come. In short, some key lessons are:

Cyber is a leadership challenge: make it yours – ASIC has repeatedly stressed boards and executives must take ownership of cybersecurity. The tone and priorities of an organisation are set and reinforced at the top. Cyber isn't a technical problem, but a business challenge that needs to be faced head-on and with open eyes. The story of LMW isn't theoretical – particularly for those unfortunate execs who learned the hard way.

Also, don't think cyber is just a problem for 1) large companies, or vulnerabilities are 2) perpetrated by savant, Nation State hackers. Think about what might be at risk and take steps to identify issues and RESOLVE them. Apparently, LMW knew of the issue before the incident for over a year. Sticking to the (often boring) basics like patching, managing tight access, passwords, etc. can keep you from becoming a headline.

Significant Salient Statistics

Each quarter we see lots of stats on the size and scale of cyber. When used sparingly and in the right context, they can improve your discussions. The best (and scariest) statistic this quarter is that 'Business E-mail Compromise (BEC)' scams are now a $26 **BILLION** problem over the last 3 years. Details and practical advice from the US FBI is found here.

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