It's fair to say that most organisations are still trying to figure out what 'normal' looks like this quarter. It is also funny how there are times in one's life when – at the time of a major change or event –you often don't grasp how significant it is and how different your life will be going forward. It mostly happens on a small, individual level like choosing a school, changing jobs, or having a child. As obvious as it may sound, we think COVID-19 is one of those moments, but on a massive, global scale never before seen. What 'normal' will look like is still unclear as we take it one step at a time.

One (of the few) things that is clear however, is just how crucial and important 'digital' is and will continue to be in the future. If you're not engaging with customers or suppliers via digital channels, it'll likely be the difference between flourishing and merely surviving (if not worse).

And if you're re-thinking your digital strategies, it's time to 'BUILD IN' security! Consider the risks associated with your digital tools and BUILD IN meaningful approaches to minimise risks and issues – NOT simply identifying vulnerabilities via a "Penetration Test" once your digital tools are ready to go.

Build in Security

When seeking ways to operate digitally, we must also recognise and protect "first time digital" users by building in approaches to protect them. First time digital users connotes those who previously never considered digital channels, but because of isolation, have finally taken the leap and will continue to use them. McKinsey found that "Fully 75 percent of people using digital channels for the first time indicate that they will continue to use them when things return to 'normal'. Companies will need to ensure that their digital channels are on par with or better than those of their competition to succeed in this new environment".

Not only is it a competitive imperative to engage digitally, but these new digital users are likely the most vulnerable – those who are less aware of cybersecurity risks and may not know basics such as patching or not re-using passwords. But you must try harder to protect them and build in features such as two-factor authentication, password complexity checking, using geolocation techniques, or even provide simple videos of the do's and don'ts when setting up an account. Frictionless commerce does NOT mean removing all protection. Pay it forward and help your first time users be more secure – it'll pay off for both them and you.

And as previously mentioned, a "Penetration Test" can woefully fall short if you haven't thought about potential issues such as cloud-based configuration errors that often leave the doors open to your databases. Building in security also involves important considerations like how access is provided (from the perspective of both developers and users), logging & monitoring, use of (proper) encryption, etc. Drop us a note if you want a simple list of things to consider and why it's relevant to address.

The Government says we're being hacked!

We were pleased to see an increased level of discussion after Prime Minister Scott Morrison publicly announced both government and the private sector were the target of malicious attacks by state-based actors. We were asked what we thought the motivation was behind the announcement. This advisory was purportedly the main impetus behind the announcement.

Two specific issues were highlighted, which you should confirm that you have addressed well. They are: 1) using multi-factor authentication (MFA) for ALL cloud-based systems and remote access. Simply stated – do it, and do it now – **make no more excuses**. And 2) 'Patching' your systems – something that, at first blush, we thought couldn't be more basic...

That was until we read a great rant aptly titled "If a Cyber Security Report Falls in the Forest, Is Anyone Listening". Last month the US released stats on the 'Top 10 Routinely Exploited Vulnerabilities". The author eloquently noted that "It's amazing to me that at the top – the top being the operative word here – most exploited vulnerabilities we have one vulnerability that is eight years old and one that is five years old.... [and] all of the "Top Most Exploited" [vulnerabilities] have patches available".

In addition, we recently saw someone say in an email that 'since you've got Office 365, you don't have to worry about patching'. True on one hand, but be very clear as to who's got what responsibility when it comes to all things cloud. And don't forget your other technology assets like your website – if it's doing anything important, you still need to keep it updated! Patching – sometimes it can be tricky in old environments but it's about as fundamental as it gets.

The other 'top 3' things you should do is 1) user education. Staff need to be alert to phishing attacks and other cyber basics (it's about changing behaviour and culture, not just doing one phishing test – drop us a note if you'd like some help), 2) have a comprehensive, regularly tested, back-up approach – a good rule of thumb is "Keep THREE copies of mission critical data, on TWO kinds of media, and keep at least ONE copy offsite", and 3) build (and exercise) an Incident Response Plan – the old saying is true: 'a stitch in time saves nine'. Think through how you'd respond and recover (to an almost inevitable event). We can help here too and have access to an excellent tool to assist - just send us a note.

Need more justification? Just reference the latest news about the beer shortages because of Lion's recent ransomware problem.

Politically motivated announcement?

We need to lift our game against not just nation state actors, but also the miscreants and criminals who are doing it on a fulltime basis too. This was highlighted when the "Internet Crime Complaint Center" turned 20 years old this quarter! They noted "The more prevailing trend is that those early, rudimentary scams have given way to more destructive and costly data breaches and network intrusions..."

This was further reinforced here by Tim Watts, Shadow Assistant Minister for Cyber Security (we're not sure who he's actually shadowing since no one is in the first chair!). He released a great paper on "National Cyber Resilience – Is Australia ready for a computer COVID-19?" We applaud the report and there's a lot of useful Australian statistics to help you engage with senior Executive's on the Cyber topic.

There's no doubt that the updated Federal Cybersecurity Strategy is woefully past due. We hope that the Morrison announcement was the prelude to its release. In fact, this morning's announcement of additional funding to 'go offensive' is another positive step given the challenges we've experienced helping clients who have been victims of cybercrime. Improvement opportunities are abound - one just needs to look at Patrick Fair's Australian updated Cyber Security Landscape to understand the confusion at the Federal-level cyber space. Just imagine how complex it would be if the state-level was overlayed!

_____

Our sincere thoughts and wishes go out to those who have lost, or who may lose, family and friends in these difficult times. Try to keep positive – together we are strong.

Thanks again 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