For our team who are in Melbourne's Stage 4 restrictions, we're starting to feel a bit like that great 1993 Bill Murray movie 'Groundhog Day'… last quarter we noted that it was "fair to say that most organisations are still trying to figure out what 'normal' looks like this quarter". Well, hit that alarm clock again – the same seems true this quarter.

This quarter (August) the Federal Government released its (somewhat past due) Australian Cyber Security Strategy. Overall, the Strategy aims to invest $1.7 billion to build new cyber security and law enforcement capabilities, assist industry to protect themselves and raise the community's understanding of how to be secure online. The legal firm Allens has a good summary here.

A quick pareto analysis of that spend sees two thirds of that going to hire more Australian Signals Directorate people, building an intelligence capability and program administration, bolstering law enforcement, and a nebulous category called data science. Even though a big 'theme' of the strategy is protecting small to medium enterprises and vulnerable Australians, it's sad to see it accounts for a meagre 4.5% of the total spend. And as aptly reported at InnovationAus, "If anyone were waiting on the…Strategy… to include a set of industry policies [to] grow the local cyber security sector, they will have been massively disappointed".

Defining what 'critical infrastructure' actually means is a major part of the Strategy and close on the heels of its release, the Dept of Home Affairs released a discussion paper on Protecting Critical Infrastructure and Systems of National Significance. The pandemic has given us all a clearer view on critical 'supply chains' and infrastructure that we didn't previously appreciate, such as our food supply.

Like most things, there's likely to be both positives and negatives as they try to define what critical infrastructure really means. For some it may mean the ability to tap into cyber resources when needed. For others, greater reporting obligations. Under proposed reforms, some organisations may be given legal exemption to fight threats, but it's interesting to note that "if the federal government itself identified an 'immediate and serious cyber threat' against a piece of critical infrastructure, it would be given the power to declare an emergency and take control of the systems and networks to take direct action". Sometimes in business, you should be worried when someone jumps in saying "we're here to help"!

Cyber Incident Response Planning is a major theme in both the strategy and discussion paper. This is one reason we're really excited to announce a new Partnership to assist clients with that issue.

The BeST Incident Response Plans are EXERCISED

Are you sure your Incident Response Plan will work? We've partnered with Israeli built "BeST" (Be-Strategic) – an innovative and insightful software platform to run simulations and table-top exercises.

The old school approach was to write a Plan and file it away; hoping you'd never need it. A few organisations practiced it, but again, the old school was to bring everyone together for a half day 'gabfest' in the boardroom – much of which was forgotten the day after the exercise.

Simply stated: Cyber incidents are inevitable – becoming a headline doesn't need to be. Having a plan makes a big difference, but real success lies in the ability to test and EXERCISE that plan! As Benjamin Franklin once said "by failing to prepare, you are preparing to fail".

BeST is practical, engaging and based on real data, real procedures and real scenarios. Our "TrustedResponse" partnership allows us to combine senior level cybersecurity craftsmanship with a world leading tool to enable you dramatically improve your ability to respond and recover from an incident. Learn more here.

ASIC sues for cyber failings?

In August, the Australian Securities and Investments Commission (ASIC) took RI Advice Group to court for cyber security failings that led to its systems being hacked for months on end and on multiple occasions.

These attacks are nothing new. However, the action from ASIC is an entirely new development, as this sets a precedence that organisations will be held accountable for their 'detection and response' failings!

While many organisations 'log' certain system actions, few ever look at those logs, and even fewer have ever thought about what connotes a real threat across multiple system events. Therefore, don't just buy a 'SEIM' or 'SOC' product – start with a simple, but thoughtful strategy. For example, assess what threat types you might face, understand what logs or events would indicate a concern, and put a simple, but meaningful process in place to monitor and alert your organisation to something nefarious happening.

Then don't just stop there – develop an Incident Response Plan so you can respond to a threat and EXERCISE it to avoid attracting the attention of ASIC – then again, we already mentioned that above.

A sobering sign & new strategies needed for ransomware

Unfortunately this month, a woman in Germany became the first [known] healthcare cyberattack death after a hospital was unable to admit her because its systems had been the target of a ransomware attack. That's (arguably) the first time a death has been directly attributed to something cyber.

In fact, we believe that today's ransomware threats have moved the goal posts and that many cybersecurity strategies are yet to catch up. We used to plan for events such as an outage of one or a few systems - perhaps the loss of one site. But what many are NOT planning for is someone using trusted network credentials to spend time learning about an organisation's network and critical systems and then wiping (encrypting) all of it at once, across geographical locations. Leaving it nearly impossible to login, access email, files, chat services, phone systems, web sites, finance systems etc. That takes a higher level of planning and preparation.

Therefore, we think it's worth reviewing the Mitre Att&ck Framework, which has mapped many recent flavours of ransomware, from initial entry point – to lateral movement within a network – to encrypting critical systems.

Assessing your ability to withstand these types of attacks and developing a layered defence which includes technology, people, policy and process can be hard because it often involves multiple teams and disciplines within in an organisation. Drop us a note if you'd like to improve your posture.

It is sobering and sad to read this week the worldwide death toll from COVID-19 passed one million. It's easy to get impatient with our COVID-19 constraints, but we're fortunate to be in a country where social distancing is possible (for most) and which has been relatively lightly impacted by deaths.

Irrespective, 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 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