First quarter update
March 2020

TrustedImpact
PROTECTING DIGITAL

The bad guys don't "self-isolate" – so neither will we! It's business as usual for our team (albeit, from a safe distance!). We're consultants, so we're used to working wherever needed to help clients with hard cyber issues. We're here and able to help.

They say every disaster movie starts with a high-level official ignoring the advice of a scientist...

Try not to let that happen to your organisation. In other words, try not to let the CEO be that high-level official and make an edict to "stop spending across the board". Don't misunderstand us; it's absolutely vital to react quickly and decisively to our new global business environment. And try not to let the CIO be the scientist who gets ignored...

We now work in a world where many businesses must desperately determine how to use technology to combat the disruption from the pandemic. If they weren't yesterday; today your digital channels will likely be the difference between success and failure. For many organisations no digital channel can mean no business. Your sales force can't meet with clients, so your digital channels must take the load, and if you can't take orders, you'll have bigger issues than cutting overheads. With COVID-19, digital 'availability' is key and threats to your digital channels can be existential.

So, what does this have to do with that strange movie analogy? Last week someone said "We absolutely must assess the health of our digital channel, but I just heard the CEO froze all spending". If your digital channels are keeping you afloat, you must do what's needed to make sure they're open, vibrant and resilient. That could mean anything from websites to factory processing machines. It's all about **resilience**. If you want help thinking through what that might be for you, just call – we can help.

Working (remotely) in the new normal.

From an organisation's perspective, good COVID-19 and remote working advice comes from the Australian Cyber Security Centre. If you're responsible for the security of an organisation consider the following nine proactive strategies;

1. Review your business continuity plans and procedures.
2. Ensure that your systems, including Virtual Private Networks and firewalls, are up to date with the most recent security patches (see guidance for Windows and Apple products).
3. Increase your cyber security measures in anticipation of the higher demand on remote access technologies, and test them ahead of time.
4. If you use a remote desktop client, ensure it is secure.
5. Ensure your work devices, such as laptops and mobile phones, are secure.
6. Implement multi-factor authentication for remote access systems and resources (including cloud services).
7. Ensure that you are protected against Denial of Service (DoS) threats.
8. Ensure that your staff and stakeholders are informed and educated in cyber security practices, such as detecting socially-engineered messages.
9. Ensure that staff working from home have physical security measures in place. This minimises the risk that information may be accessed, used, modified or removed from the premises without authorisation.

"Such remote working at scale is unprecedented and will leave a lasting impression on the way people live and work for many years to come. China, which felt the first impact of the pandemic was an early mover in this space. As home to some of the world's largest firms, it offers lessons for those that are just now starting to embrace the shift." McKinsey's "Blueprint for remote working: Lessons from China" is insightful from a management perspective.

From a cyber safety perspective, keeping remote workers safe will be another challenge. If you need free material because money is tight, our partners at Terranova have kindly pulled together a Working From Home Cyber Safely Kit that you can share with your team. There's a free online learning module and other resources. SANS also has a content rich 'Working From Home – Deployment Guide" here.

There's lots to do, so we suggest you start by keeping it simple – it's hard enough getting remote workers to operate effectively. For example, instil the basics such as strong password hygiene – we do lots of "password cracking" and you'd be amazed at just how bad it is in ALL organisations. There's some good password advice here. Also, if you're not using Multifactor Authentication for ALL external access or your cloud assets, you're extremely exposed.

Scams social engineering and phishing threats!

These days, miscreants are exploiting 'virus anxiety' for social engineering attacks. Therefore, one of the most important things to do is try to raise your staff's awareness of these threats. StaySmartOnline has collated some good examples and resources specifically relating to malicious COVID-19 scams here. Our partners, Terranova have also put together some useful tips to protect yourself from cyber scams that you can also send your team.

Unfortunately, cyber awareness and behaviour change takes education, measurement and time and we don't have a lot of that when urgently deploying a remote workforce. Therefore, simple instructions to reduce their phishing risk is to ask them to:

1. Validate the actual email address (not just the name).
2. Hover your 'mouse pointer' over links to confirm the address looks correct and be careful of shortened links.
3. Pick up on the warning signs like generic greetings, poor grammar and misspelled words.
4. Be wary of urgent calls to action.
5. Never give out passwords, usernames, birth dates or personal information unless you're confident it's legit.

One of the best ways to understand and measure this risk to your organisation is to conduct a fake phishing test to measure the level of staff response. We help clients do that a lot and it can make it 'real' to measure progress. We understand that some feel it's not an appropriate time to do this now. That might be true, but the bad guys don't worry about those things. Therefore, if you'd like us to run a quick (free) phishing test – get in touch here. It can be a meaningful and factual way to measure your risk.

Rampant Raucous Ransomware

This quarter it's also worth a quick note about ransomware (again). It's big and will get bigger ($7.5 Billion in the US alone), and it's becoming stealthy and dangerous (FBI says attackers may lurk for months seeking to lock up everything). In fact, just before Christmas ransomware destroyed a company of 300 employees and there are similar cases. As a rule of thumb, "Keep THREE copies of mission critical data, on TWO kinds of media, and keep at least ONE copy offsite". Do it for your own good. Also, do you have 'local' copies of your cloud-based data or do you assume they've got it covered? Ask the question.

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