WHY THE 'CYBER-DRILL' IS NOW THE NEW 'FIRE DRILL'

RSM Australia was proud to recently sponsor a Boardroom Hypothetical presented by the theresolution.com.au around a major cyber incident. The Board was made up of Lindsay Tanner, Graeme Samuel AC and Chaired by Sue O'Connor – three very accomplished directors. A key take-away from the event was the readiness of organisations to deal with a major cyber event, both in crisis and as a business-as-usual.

Put cyber-security 'front and centre' in your company

Recent and malicious global cyber-attacks of 2017 such as "Wannacry" and "Petya" ransomware, have targeted both large corporates and small businesses in Australia. This has highlighted that cyber-security needs be a front and centre issue and not just a 'top-ten' issue to be addressed at 'some stage'. No company is exempt from these risks.

Andrew Walduck, Executive General Manager Trusted eCommerce Services and Group Chief Digital Officer for Australia Post explained, if you do have a policy in place, does it take a "whole organisation" approach with cyber-protocols in place that all staff understand and follow? In other words, how has your organisation prepared for managing a cyber event.

Don't wait for a crisis to happen. Prepare for it now.

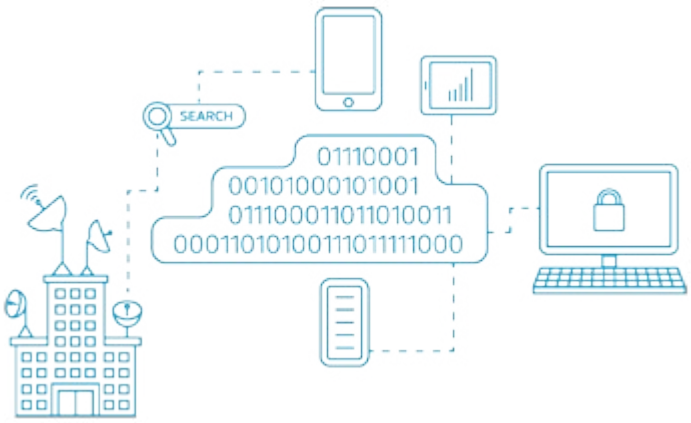
Just as employees know where the exit door is when the fire alarm goes off in the office, cyber security crisis plans and procedures should be clearly understood and embedded in your organisation. The board should be confident that management and staff know what to do right now if e.g. a malware attack occurred right now!

In 2017, cyber-security should be no different as 'business as usual' areas such as health and safety. The 'cyber-drill' is the new fire drill according to Graeme Samuel AC saying that every single staff member should feel confident in what they have to do and how they have to do it in the case of a cyber-attack or hacking incident.

How to create a 'security-aware' work culture

A key take-out from the day was "don't wait for a cyber crisis to work out how to manage the event".

It's only recently that organisations are 'shining a torch' on cyber security according to Michael Shatter, RSM. If your culture is 'security-aware' then a key defence is how your staff become cyber-responsible, alert to potential risks and know how to react. Every person in your organisation has a part to play – not just the IT Team.



RSM

Get comfortable with the risks and avoid the 'black-boxing'

No company can be 100% invulnerable to cyber-attacks, explained Andrew Walduck. This is the new reality of business. The risk of systemic and persistent, cyber threats will never go away, but they will eventually become embedded in business as usual processes.

Richard Tait recommends adopting a 'whole of organisation approach' where the control management of potential cyber-risks is not just outsourced or 'black-boxed' but understood internally and faced head-on. Again, this is why being 'cyber-smart' should be an intrinsic and 'business as usual approach' within your organisation.

Being Cyber-smart: Run a cyber-drill and test your response to these six tests

Graeme Samuel AC recommends hypothetical tests of your organisation's cyber incident response frameworks and the robustness of cyber security policies and procedures in circumstances of a crisis.

How will your company's brand, share price, and reputation hold-up? How can you recover quickly and prove your responsiveness once the attack has occurred or is unfolding to avoid being given a black mark in the media, your community, and industry sector.

Being Cyber-smart: Be resilient and recover well.

Final thoughts...

Organisational resilience and recovery is essential in being 'Cyber-smart' says Sue O'Connor, FAICD.

> The risks will always be there, but it is how your company responds and recovers that is crucial.

As part of your procedures, your organisation must have in place 'recovery techniques' to respond to the crisis and recover proactively and expediently. These techniques must consider a broad organisational risk perspective that manages the impact of a major cyber event. As with any other whole-of-business matter, broad stakeholder managment is a key requirement for successfully responding to a cyber crisis issue.

SIX COMMON SENSE TESTS TO CONSIDER A CYBER INCIDENT AGAINST

1. The 'Morning Newspaper' Test
2. The 'Community Reaction' Test
3. The 'Reputation Test'
4. The 'Shareholder Test'
5. The 'Customer Test'
6. The 'Internal Communication Test'

For further information, please contact:

Michael Shatter
Director, Risk Advisory, Security and Privacy Services
T 03 9286 8166
E michael.shatter@rsm.com.au