



Cyber incident response planning – the critical components

Nine out of ten Australian organisations faced an attempted or successful cyber-attack in the 2015-16 financial year according to the Australian Cyber Security Centre. Three out of five experienced tangible business impacts as a result of an attempted compromise, and if the attack was successful that rose to 82 per cent.

How would your organisation fare if attacked?

Do you have a cyber incident response plan? Has it been tested recently? Are you confident your people know what to do and when? Or are you at risk of your business grinding to a halt and your reputation being severely bruised as a result of a cyber incident?

US retailer Target was famously hacked in the lead up to Thanksgiving 2013, and around 40 million credit card details were siphoned off by hackers. The damage to the company's brand and reputation continues today, several years after the event and reports suggest that the company is facing 90 plus lawsuits as a result.

In late 2016 Aon surveyed up to 2,000 global organisations about risk management. The [Aon 2017 Global Risk Management Survey](#) reveals that damage to brand and reputation is the most acute risk faced by organisations around the world.

And, for the first time cyber risk entered the top five ranked risks. For the aviation, education and government sectors cyber risk is ranked number one. On the local front, 45 per cent of Australian organisations surveyed indicated cyber-crime as a top risk with 12 per cent confirming that they have experienced financial loss at an event of an attack.

The report also notes that cyber crimes have evolved rapidly from stealing personal information and credit card details to more co-ordinated attacks on critical infrastructure. For example, a series of cyber-attacks on the distribution systems of three energy companies in Ukraine had devastating consequence for industry and individuals, and the detonation of the WannaCrypt ransomware malware across the world in May created widespread problems for multiple sectors.

The critical components


To protect brand and reputation and to contain the impact of business interruptions, organisations of all sizes, in every sector need a well-crafted and regularly tested incident response plan. It forms part of a matrix of good governance and risk management planning requiring organisations to craft, test, and regularly review their;

- Business Incident Plan
- Business Continuity Plan
- Crisis Management Plan, and
- Cyber Incident Response Plan.

Although the Australian Cyber Security Centre has reported 71 per cent of local organisations now have a cyber incident response plan, fewer than half of the businesses regularly review or test them. An alarming 15 per cent have never tested their plans and 24 per cent report they test their incident response plan less frequently than once a year.

Yet new threats are emerging daily. Good governance and effective risk management requires greater diligence with regard to crafting and testing these plans.

Australian organisations also need to be mindful of the new mandated data breach notification which will from next year oblige organisations to report any eligible data breaches to the Office of the Australian Information Commissioner and affected individuals. Does your cyber incident response plan clearly articulate how that needs to be tackled?



Developing a cyber incident response plan requires whole-of-business attention, it cannot be offloaded to the IT department. In larger organisations, its formulation should be led by the risk and audit committee while support from an external consultant may bring additional clarity to discussions and planning.

With a clearer understanding of the information assets, the organisation can start developing response plans. These should include details of how the business can resume operations as quickly as possible in order to minimise business interruption, and identify the business roles responsible for specific actions required by the plan.

The plan requires regular review and testing, at least every quarter to reflect changing business or cyber conditions.

A well thought through and tested cyber incident response may benefit the sort of cyber insurance policy your organisation is able to negotiate in order to financially transfer the associated risk. It will also help you sleep at night.

With the largest team of dedicated cyber risk consultants and brokers exclusively engaged in delivering a range of cyber assessment, mitigation, transfer, and response solutions for our clients, Aon is uniquely positioned to assist organisations to improve their overall cyber risk profile and readiness.

If you would like Aon to assist with any of these cyber services for your organisation, please contact us today.

aon.com.au/cyber

Contacts:

Fergus Brooks

Cyber Risk Practice Leader
T +61 2 9253 7835
E fergus.brooks@aon.com

Michael Parrant

Cyber Insurance Practice Leader
T +61 3 9211 3485
E michael.j.parrant@aon.com

AON
Empower Results®