Clock ticks toward data breach notification; six steps to take right now

A collective chill scuttled across the nation in late 2017 when the Australian Cyber Security Centre's latest Threat Report assessed the risk of cyber compromise as "high" for local organisations.

It had already recorded a 15 per cent increase in cyber incidents in the previous 12 months – rising to 47,000 – with 56 per cent of the incidents affecting industry rather than the public sector. But only 58 per cent of those incidents were self-reported; the ACSC identified the remainder itself.

This apparently relaxed approach to cyber compromise is about to face its biggest challenge ever with the introduction from early 2018 of mandatory data breach notification for companies when they endure a serious compromise. And companies will have just 30 days to alert the authorities. Under the Privacy Act, there is some leeway for organisations that turn over less than $3 million per year, however any organisation that holds potentially harmful information is not exempt.

In its 2017 investigation into the cost of data breaches, the Ponemon Institute found that organisations were able to identify data breaches much faster than previously; however it still took organisations 191 days on average to identify a breach – well outside the 30 day notification envelope.

Organisations which also trade with Europe, and hold personal data about EU residents – be they suppliers, partners or customers - also need to comply with the new General Data Protection Regulation – and will have just 72 hours to alert authorities to breaches classed as serious.

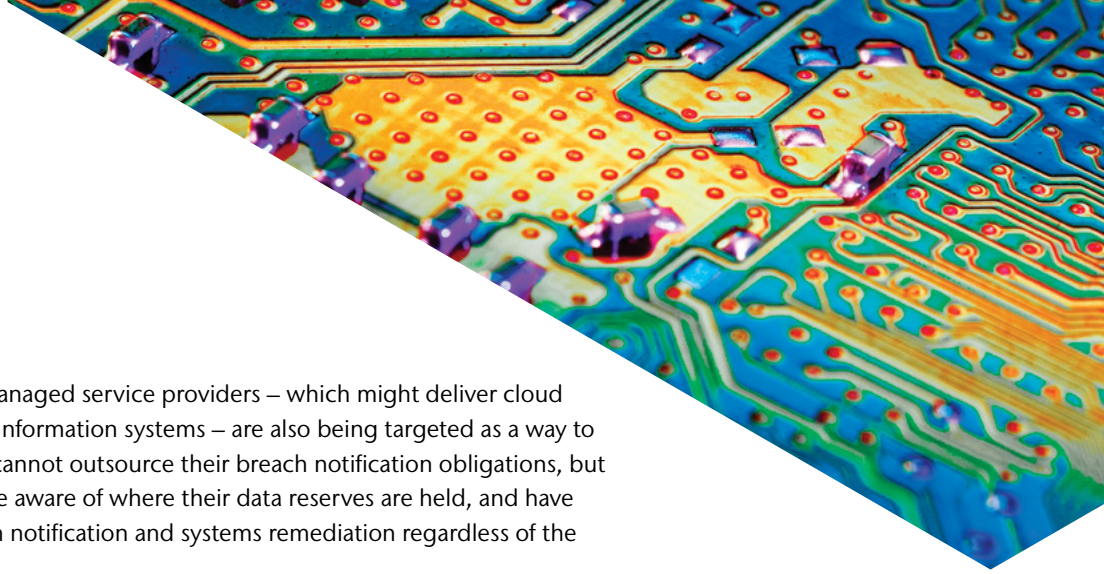
Failure to comply with both sets of regulations risks significant fines. Australian organisations which fail to meet the local data breach regulations risk a fine of $360,000 for individuals and $1.8 million for organisations. Flouting the GDPR rules risks fines of €20 million or 4 per cent of global turnover. Perhaps even more challenging to navigate are the stormy seas of public perception associated with a data breach.

The Ponemon report noted that rapid identification of a breach helps rein in the costs associated with remediation, and also reduces the reputational impact that a breach might have.

Having a current, tested cyber incident identification and response plan which allocates responsibilities, expedites notification and remediation, and leverages appropriate cyber insurance coverage is essential in this emerging era of mandated notification.

Certainly the threat of data breach is not declining; attacks on personal identifiable information and the use of credential harvesting malware are on the rise according to the ACSC's threat report.

AON
Empower Results®



The ACSC report also noted that managed service providers – which might deliver cloud computing services or outsourced information systems – are also being targeted as a way to access customer data. Companies cannot outsource their breach notification obligations, but instead need to ensure that they are aware of where their data reserves are held, and have systems in place to expedite breach notification and systems remediation regardless of the location of data.

With the clock ticking for both the Australian data breach notification and the GDPR regime, organisations need to immediately assess their exposure, risk mitigation opportunities, processes and procedures to ensure they can respond to the very tight notification schedules in both Australia and Europe and, as much as possible, contain the impact of a cyber incident.

Six steps to preparing for breach notification

1. Get across the detail of the legislation and implications for your organisation.
2. Understand what data you have, where and how it is stored - review and test your existing systems for managing and storing data and ensure they are compliant/robust.
3. Ensure you have a plan on how to address the legislation. This plan should be integrated with your cyber risk plan, cyber incident response plan and overall crisis management and business continuity plan.
4. Consider implementing the Australian Signals Directorate's Essential Eight guidelines for cyber-attack mitigation and incident management.
5. Communicate the plan with key leaders across the organisation and get their buy in and educate employees.
6. Do any work required to prepare for legislation and review your current insurance arrangements with your broker to ensure you have adequate insurance and a response team at the ready.

Contact Us

Fergus Brooks
National Cyber Risk Practice Leader
+61 2 9253 7835
fergus.brooks@aon.com

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

ARS0289A 1117

Empower Results®