CYBER INCIDENT/DATA BREACH RESPONSE

YOUR EMERGENCY CHECKLIST

The first 24 hours after you discover a data breach are critical to restoring security, minimising harm, obtaining and preserving evidence and complying with contractual and legal obligations. This Emergency Checklist provides executives and in-house counsel of organisations with prioritised key steps to take (i.e. what to do) in response to a cyber incident/data breach and key warnings as to what not to do.

WHAT IS A DATA BREACH?

Though legal definitions vary, a data breach is any unauthorised acquisition or release of or access to information which usually exposes the information to an untrusted environment, whether an organisation stores and manages its data directly or through a contractor, such as a cloud service provider. A data breach is, nowadays, often a result of or related to a cyber incident but data breaches come in all shapes and sizes: paper files or documents stolen from an office or car; lost laptops, mobile devices or tablets; compromised servers or email accounts; hacked computers or social media accounts; advanced persistent threats (APT) (i.e. persistent stealthy hacking attacks directed at an organisation).

"Insider threats" or threats coming from within the organisation are common (accounting for more than 40% of incidents) and often involve employees accidentally, unknowingly or maliciously mishandling, exposing or losing personal information and/or business sensitive data.

In some cases, a cyber incident may not lead to the compromise of (i.e. unauthorised access to) personal information, even if control of the organisation's IT systems has been lost temporarily. In such an instance the organisation must determine whether to treat the incident as a full scale data breach or simply as an inadequate security practice requiring (immediate) rectification.

WHY BE PREPARED?

A data breach places your organisation in crisis management mode. While this crisis cannot be avoided, your organisation can plan for it and significantly reduce the impact that a data breach/cyber incident has on the organisation (both financially and on its reputation).

Data breaches can cost your organisation millions of dollars in mitigation and remediation, as well as causing significant harm to your brand and reputation and potential personal liability for directors/officers. In Australia, cyber incidents have increased 48% in the last 12 months and the annual cost to Australian and New Zealand business of data breaches alone is $1.6 billion. Across the Asia Pacific (including Australia) in 2014 the average cost of data breaches for affected organisations was between US$2 million and US$3 million per breach. In 2014 the average cost of cyber incidents/data breaches for affected organisations in Australia was AU$2.8 million per breach.[1]

In addition to being good risk management and significantly reducing the costs of a cyber incident/data breach (see below), some organisations are required by regulation or contract to implement a cyber incident response plan. For example, the PCI Data Security Standard requires that all organisations that accept credit cards create and maintain an emergency response (and communication) plan for data breaches involving the loss of credit card data.[2]

Organisations which have an appropriate cyber risk management plan in place before an incident occurs, including having established an incident response team and incident response plan, can save millions of dollars and significant reputational harm when the inevitable cyber incident/data breach occurs. A recent study found that having strong security ($14), establishing an incident response plan and team in advance of any data breach ($13) and appointing a CISO ($7) could reduce the average per record costs of a data breach by the amounts noted. Given data breaches in Australia usually impact hundreds of thousands (if not millions) of records, these are very significant potential cost savings and reward for being prepared!

[1] This average cost is expected to double, at least, once mandatory breach notification is introduced in Australia.

[2] In addition, APRA regulated financial services licensees have IT security and data management obligations which require them to have and maintain a cyber incident/data breach response plan and see also ASIC's Report 429 "Cyber resilience: Health check" (March 2015) which requires cyber resilience for all entities regulated by ASIC.

CHECKLIST

DO:

- ✓ Activate the incident response team (IRT)
- ✓ Establish a "privileged" reporting and communication channel
- ✓ Use independent cyber security and forensic experts
- ✓ Stop additional data loss
- ✓ Secure evidence
- ✓ Preserve computer logs
- ✓ Document the data breach
- ✓ Consider possibly involving law enforcement and/or regulators
- ✓ Determine your legal, contractual and insurance notification obligations
- ✓ Interview personnel involved
- ✓ Change security access and passwords

DO NOT: (unless a cyber security/forensic expert)

- × Ignore the incident
- × Probe computers and affected systems
- × Turn off computers and affected systems
- × Image or copy data or connect storage devices/media to affected systems
- × Run antivirus programs or utilities
- × Reconnect affected systems

WHAT TO DO!

Activate the incident response team (IRT)[3]	The makeup of the IRT for a specific data breach incident (i.e. selected from those in the wider established IRT) will depend on the kind of breach, what information/data was lost and what the threat is. Generally, **the IRT should include:** ■ An executive with decision-making authority. ■ A team leader responsible for response coordination, contacting outside counsel and the forensic team and addressing any press inquiries. ■ "First-responder" security and IT personnel with access to systems with all necessary permissions. ■ Representatives from key departments including IT, legal, human resources, customer relations, risk management, communications/public relations, operations (for physical breaches) and finance (for breaches involving loss of company financial information). ■ The Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Information Technology Officer (CITO) and/or other relevant C-level stakeholder. ■ Outside resources including legal, forensic, IT and/or advisory/management consultants, as necessary.
Establish a "privileged" reporting and communication channel	Establishing a **privileged reporting channel** (ideally before a breach occurs) **maintains the confidentiality of the investigation**. Legal counsel (in-house and/or external) should provide legal advice, retain forensic/cyber security experts and direct responses every step of the way to protect the privilege of the investigation and of applicable internal communications. Legal counsel should receive all incident reports (initial, draft and final), including IT-related communications, for the purposes of providing legal advice. External legal counsel are often the best resource to work with regulators, law enforcement and forensic experts as they should have established relationships. Also, external legal counsel experienced with data breaches are often best placed to assist in assessing risk and providing guidance on remediation, disclosure and notification efforts.

[3] If an incident response team has not already been established prior to an incident occurring then urgently assemble the team. However, we recommend that an incident response team and plan is established prior to the incident occurring.

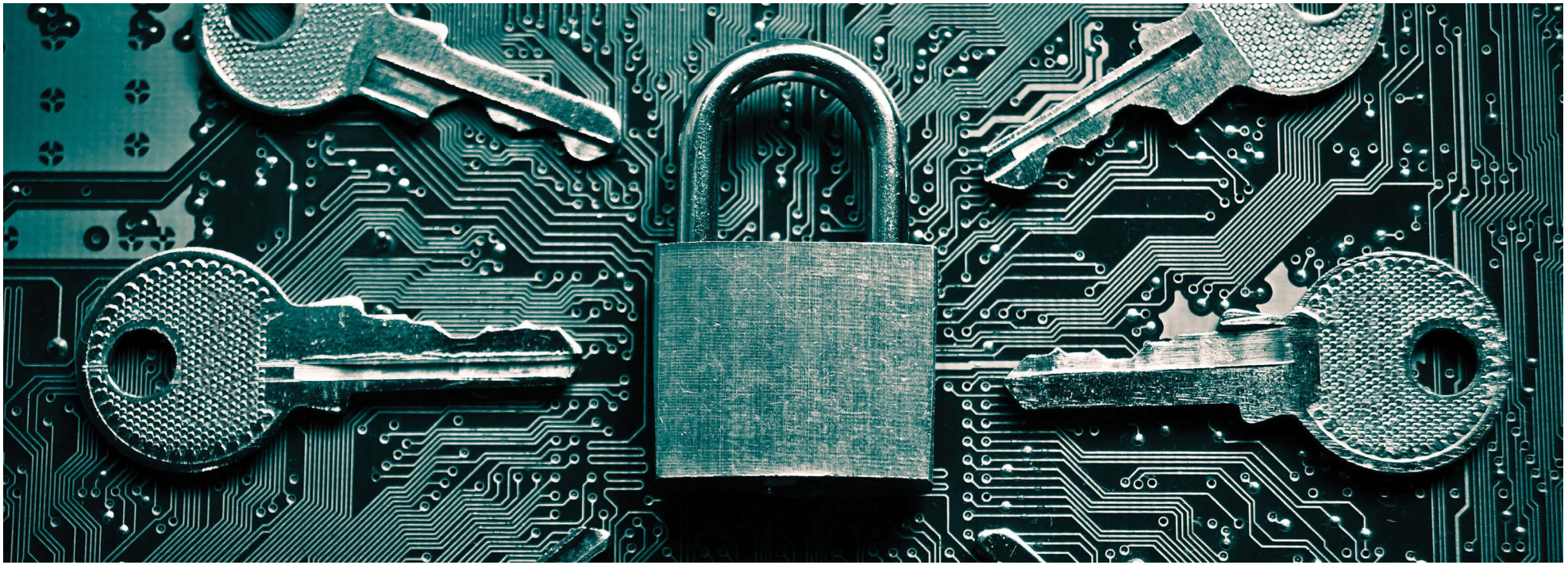
Use independent cyber security and forensic experts	In the rush to mitigate a data breach in-house security and IT personnel are often not in the best position to verify the depth and extent of the breach, especially when an APT is involved or if hackers have left back doors to give themselves future access. **Independent forensic experts, retained and directed by legal counsel,** bring perspective and experience to investigations and are free from any (real or perceived) conflicts that might arise in respect of internal IT and security personnel who manage the affected systems day to day.[4] Forensic experts can (via the legal counsel) advise your organisation how to stop data loss, secure evidence and prevent further harm. They are also trained to preserve evidence (including that which may exist only in temporary memory) and manage the chain of custody, minimising the chance that evidence will be altered, destroyed, lost or rendered inadmissible in court.
Stop additional data loss	**If the breach is ongoing**, consult with forensic and cyber security experts and trained IT staff about taking affected systems offline by disconnecting them from the network and using tools to dynamically image affected systems to preserve evidence prior to any such action.
Secure evidence	**Secure and prevent physical access to affected systems** such as servers and workstations to maintain the integrity of the evidence and ensure that only selected forensic experts and law enforcement (if applicable) have access. Preserve all security access devices (tokens, badges, key cards, etc), logs and surveillance tapes. Work with legal counsel to send evidence preservation letters to service and cloud providers. Track the chain of custody for all physical and digital evidence and take an inventory of any missing hardware. **Determine:** Who had contact with the affected system? What did they do? Who was the next to touch the affected system?
Preserve computer logs	**Preserve** all affected system log files including firewall, VPN, mail, network, client, web, server and intrusion detection system logs. These logs are critical for assessing the origins of the attack, its duration and the volume of data exfiltrated during the breach.
Document the data breach	**Record** in as much detail and as precisely as possible the date and time of the data breach, the personnel who discovered the breach, the nature of the breach, the kinds of data stolen/lost, when the response efforts began and all of the employees who had access to the affected systems. Document all data and/or devices and other hardware affected by or lost in the breach. Given that a high percentage of data breaches are often traced to former employees, collect the names and contact information for all employees terminated within the last 120 days and confirm whether their security access was terminated.

[4] As noted above, by retaining these experts via legal counsel the communications prepared for or by the experts may be protected by lawyer-client privilege.

Involve law enforcement and/or regulators (possibly)	After consultation with legal counsel and management, determine whether involving law enforcement and/or any regulator is necessary, prudent or valuable. More serious cyber attacks/data breaches resulting in the unauthorised access, modification or impairment of your organisation's technology including theft of data, ransom or damage to equipment or software must (in New South Wales, at least) be reported to law enforcement. In New South Wales, failure to report is a criminal offence with a penalty of 2 years' imprisonment on conviction. Law enforcement's expertise in evidence gathering and forensics may be leveraged to ensure that the evidence can be used in any future court proceedings against wrongdoers. In some cases, even without a mandatory notification obligation under Australia privacy law, it may be prudent to notify the Australian privacy regulator (and possibly the individuals affected, see below).[5]
Determine your legal, contractual and insurance notification obligations	Australian financial services licensees will (and certain healthcare providers may) have mandatory data breach reporting/notification obligations (separate to privacy law requirements) requiring notification of their industry regulator in certain cases. In addition to any industry specific obligations (i.e. financial services and healthcare) and even though there is no mandatory data breach notification under current Australian privacy law, if there is a likelihood of financial loss, serious harm or embarrassment (i.e. where sensitive information is involved) to the individuals affected by the data breach your organisation would be wise to seriously consider notification of those individuals (and, possibly, the regulator), especially where such notification may assist to reduce such loss, harm or embarrassment. Remember that other jurisdictions with mandatory breach notification may be involved in/affected by the data breach. Your organisation may have notification obligations under the laws of other countries if data collected outside of Australia is lost or improperly accessed as part of the data breach. The legal notification requirements of other countries will often vary depending on the types of data held, what data has been "lost" and the form in which the data is stored. For listed companies consider whether the data breach may have a material effect on your company's share price or value of at least enough to trigger your continuous market disclosure obligations. With guidance from legal counsel, determine whether there are also obligations to notify service providers, payment card networks or other contractual parties. Additionally, review insurance policies (ideally with the assistance of your broker and an experienced insurance lawyer) to determine whether insurers should be notified to preserve coverage rights.

[5] It is expected that mandatory breach notification will be introduced in Australia before the end of 2015.

Interview personnel involved	**Identify** all of the **individuals involved in the discovery and initial investigation of the breach**. Conduct interviews to create a complete record of all efforts taken to stop data loss, secure systems and mitigate damage and harm. Determine whether legal counsel (in-house or external) should participate in the interviews or be present if law enforcement also requests interviews with relevant personnel.
Change security access devices and passwords	Increasingly cyber attacks are aimed at gathering log-in credential and password combinations. After a cyber/data breach personnel should be required to **change passwords and be issued new physical authentication/access devices** (tokens, badges, key cards). Your organisation's personnel should also be encouraged to change passwords for their personal banking, credit cards, web mail and social media accounts as hackers often glean the personal information of an organisation's employees as well as that of its customers.



WHAT NOT TO DO!

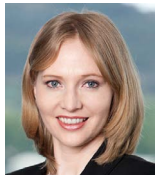
Do Not ignore the problem	Cyber incidents/data breaches do not fix themselves or go away on their own. Failure to act swiftly and decisively (and in accordance with the pre-established incident response plan) will result in significant additional costs and reputational harm to the organisation. It may lead to personal liability for the directors/officers of the organisation for breach of the privacy law and/or their director's duties.
Do Not probe computers and affected systems	**Evidence could be accidentally altered or lost** or hackers could be alerted to your activities, causing them to take measures to hide their trail, damaging your systems in the process. So, unless under the direction of a cyber security/forensic expert, do not probe affected computers or systems.
Do Not turn off computers and affected systems	Valuable information can be stored in temporary memory that could be lost if you simply turn off a running system. If an affected system is on and connected, **leave it on and connected**. Work with forensic experts to determine whether the system should be dynamically imaged before disconnecting it to avoid tipping cyber criminals to the fact that you are aware of the breach and to preserve evidence that the hackers might destroy to conceal their tracks. If the system is off, unplug it.
Do Not image or copy data or connect storage devices/media to affected systems	**Imaging and copying** of affected systems should be **left to forensic experts and/or law enforcement** who are equipped with state-of-the-art forensic toolkits and imaging utilities. Copying data without the right protocols and tools (even for the purpose of providing it to law enforcement) can alter or destroy important evidence and render evidence inadmissible in court.
Do Not run antivirus programs or utilities	Running antivirus programs or utilities on the affected systems could result in the **accidental loss or destruction of evidence**.
Do Not reconnect affected systems	Affected systems should be preserved until forensic expert or law enforcement examination and remediation efforts have been completed. **A "cleaned" system is not always clean**. Backdoors and APTs are designed to lull an organisation into a false sense of security. All affected systems should go through rigorous testing and verification before being reconnected to the network.

WE CAN HELP!

DLA Piper's dedicated Australian Privacy & Security Team can help with all your cyber and privacy needs. For more information on your legal obligations and cyber risk/data breach incident response planning, please do not hesitate to contact:

Alec Christie
Partner
T +61 2 9286 8237
alec.christie@dlapiper.com

Jacques Jacobs
Partner
T +61 2 9286 8284
jacques.jacobs@dlapiper.com



Sharon Rowe
Partner
T +61 2 6201 3417
sharon.rowe@dlapiper.com

"They certainly have the global footprint."
Chambers Global 2015

"Very responsive, pragmatic and practical."
Chambers Global 2015

"…lauded by clients for excellent advisory work in privacy." Who's Who Legal, World's Leading Information Technology Lawyers, 2014

"Deals with a range of data protection matters, including cyber security audits, Big Data, compliance and data transfers."
Chambers Global 2015

This checklist is intended as a first point of reference and should not be relied on as a substitute for professional advice. Specialist legal advice should always be sought in relation to any particular circumstances and no liability will be accepted for any losses incurred by those relying solely on this Checklist.

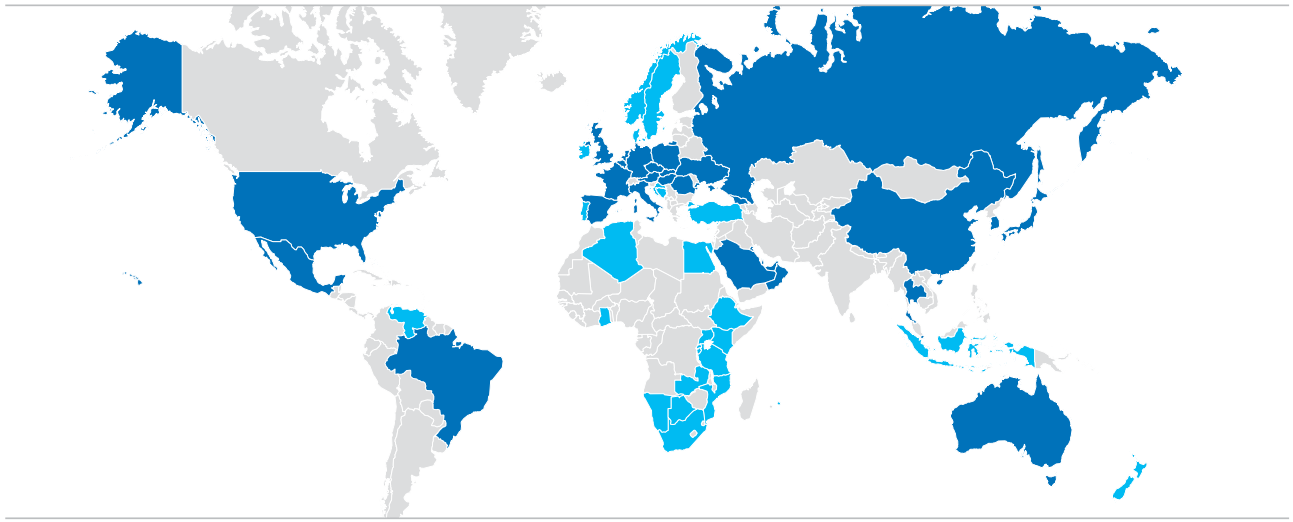
ABOUT DLA PIPER

DLA Piper is a global law firm with 4,200 lawyers in the Americas, Asia Pacific, Europe and the Middle East, positioning us to help companies with their legal needs around the world.

We strive to be the leading global business law firm by delivering quality and value to our clients.

We achieve this through practical and innovative legal solutions that help our clients succeed. We deliver consistent services across our platform of practices and sectors in all matters we undertake.

Our clients range from multinational, Global 1000, and Fortune 500 enterprises to emerging companies developing industry-leading technologies. They include more than half of the Fortune 250 and nearly half of the FTSE 350 or their subsidiaries. We also advise governments and public sector bodies.



DLA PIPER

AUSTRALIA
Brisbane
Canberra
Melbourne
Perth
Sydney

AUSTRIA
Vienna

BAHRAIN
Manama

BELGIUM
Antwerp
Brussels

BRAZIL
São Paulo

CHINA
Beijing
Hong Kong
Shanghai

CZECH REPUBLIC
Prague

FRANCE
Paris

GEORGIA
Tbilisi

GERMANY
Berlin
Cologne
Frankfurt
Hamburg
Munich

HUNGARY
Budapest

ITALY
Milan
Rome

JAPAN
Tokyo

KUWAIT
Kuwait City

LUXEMBOURG
Luxembourg

MEXICO
Mexico City

NETHERLANDS
Amsterdam

OMAN
Muscat

POLAND
Warsaw

QATAR
Doha

ROMANIA
Bucharest

RUSSIA
Moscow
St. Petersburg

SAUDI ARABIA
Riyadh

SINGAPORE
Singapore

SLOVAK REPUBLIC
Bratislava

SOUTH KOREA
Seoul

SPAIN
Madrid

THAILAND
Bangkok

UKRAINE
Kyiv

UNITED ARAB EMIRATES
Abu Dhabi
Dubai

UNITED KINGDOM
Birmingham
Edinburgh
Leeds
Liverpool
London
Manchester
Sheffield

UNITED STATES
Albany
Atlanta
Atlantic City
Austin
Baltimore
Boston
Chicago
Dallas
Houston
Los Angeles
Miami
Minneapolis
New York
Northern Virginia
Philadelphia
Phoenix
Raleigh
Sacramento
San Diego
San Francisco
Seattle
Short Hills
Silicon Valley
Tampa
Washington, DC
Wilmington

RELATIONSHIP FIRMS

ALGERIA
Algiers

BOSNIA-HERZEGOVINA
Sarajevo

BOTSWANA
Gaborone

BURUNDI
Bujumbura

CROATIA
Zagreb

DENMARK
Copenhagen

EGYPT
Cairo

ETHIOPIA
Addis Ababa

GHANA
Accra

INDONESIA
Jakarta

IRELAND
Dublin

KENYA
Nairobi

MAURITIUS
Port Louis

MOZAMBIQUE
Maputo

NAMIBIA
Windhoek

NEW ZEALAND
Auckland
Wellington

NORWAY
Oslo

PORTUGAL
Lisbon

RWANDA
Kigali

SOUTH AFRICA
Cape Town
Johannesburg

SWEDEN
Stockholm

TANZANIA
Dar es Salaam
Mwanza

TURKEY
Ankara
Istanbul

UGANDA
Kampala

VENEZUELA
Caracas

ZAMBIA
Lusaka

www.dlapiper.com