gadens

pesel & carr

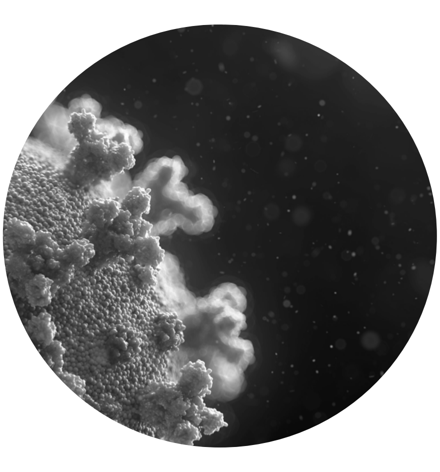
Stay Cyber Safe

Managing your privacy obligations and communications effectively during the COVID-19 pandemic.

There has been an uptick of reports of bad actors using the COVID-19 pandemic for scams, online frauds, and phishing campaigns.

With new remote working arrangements and workplace disruptions that could be exploited by bad actors to infiltrate business accounts and networks, businesses are operating in an environment with heightened cyber security risks.

What You **Need to Know**



COVID-19 Cyber Related Statistics

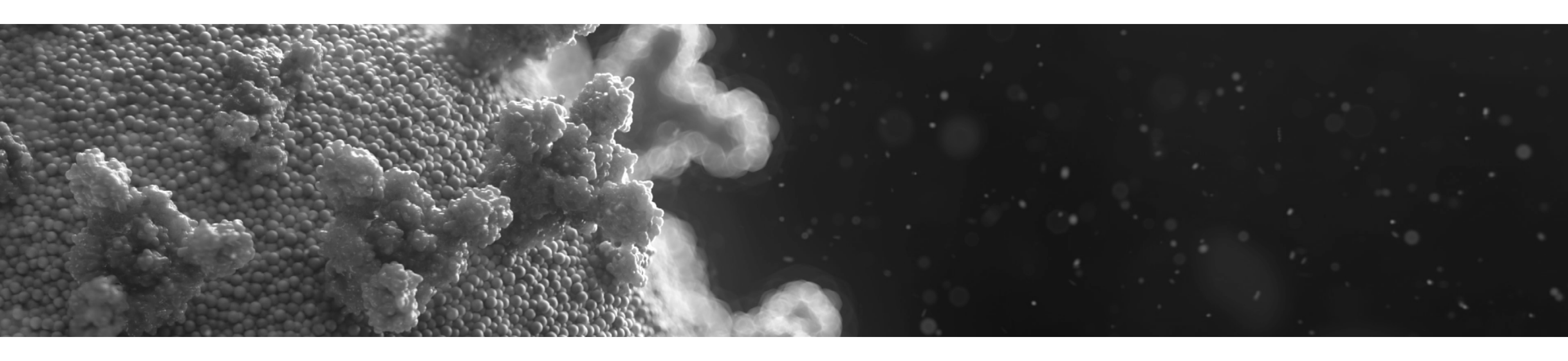
How To Mitigate Cyber Security Risks

How To Communicate When A Data Breach Occurs

How To Prepare For A Data Breach

What To Do When A Data Breach Occurs

Five Post Crisis Steps



COVID-19 Cyber-Related Statistics

Scamwatch has received over 1,000 corona-virus related reports since the COVID-19 pandemic outbreak. Common scams relate to phishing for personal information, ecommerce and online shopping, and superannuation.

The Australian Signals Directorate's Australian Cyber Security Centre has:

- Received more than **95 reports** since 10 March 2020 about Australians losing money or having their personal information compromised due to COVID-19 pandemic scams, online frauds, and phishing campaigns.
- Responded to **20 cyber security incidents** affecting COVID-19 response services and major suppliers.
- Disrupted over **150 malicious COVID-19 pandemic-themed websites**.

Cyber security risks increase the likelihood of a data breach occurring. A data breach occurs when information is compromised, lost, or accessed or disclosed without authorisation. Data breaches are one of the biggest future crisis concerns for businesses.

A global study of non-executive directors showed 73% named reputation as the single greatest crisis vulnerability, yet only 39% had a plan for it.

69% of business leaders have experienced at least one corporate crisis in the last five years — with the average number of crises experienced being three.

Five proactive steps you can take to **mitigate the current cyber security risks:**

Tighten up network access and **bolster security measures**. Consider limiting access on work devices only, implementing a VPN solution to create an encrypted network connection or enabling multi-factor authentication.

Engage a cyber security consultant to **undertake a cyber security audit**, particularly in relation to your remote working arrangements, to identify any vulnerabilities, as well as provide advice on how to address them.

If your business is subject to the Privacy Act 1988 (Cth), **undertake a privacy impact assessment** to evaluate and mitigate risks to personal information, noting the higher security requirements for health information.

Update your cyber security policy, including processes and procedures in handling personal information (including health information).

Update your workers re changes to your cyber security policy.

How to **effectively communicate** when a data breach occurs:

In the event of a data breach, effective crisis communications can minimise impact to reputation and business. It is critical to have a plan! If you do not, your first step should be to knock on the door of your senior execs and explain the risks of breaches and their damaging impact to your company, your clients, and the broader community.

A **plan** must:

Provide a step-by-step roadmap to follow	Simplify decision making	Ensure stakeholders are managed appropriately
Inform and equip employees	Disseminate information quickly	Have a dedicated team of people to activate it

Five essential steps to **prepare for a data breach**:

Consider all potential breaches and understand the impact they would have on your stakeholders and rank them in respect to impact on reputation as well as finances.

Map out all the different scenarios, along with respective responses.

Work out in what order stakeholders need to be contacted and the best method of communication for each.

Pre-prepare any materials for the different scenarios such as holding statements, Q&As, client scripts and email, social media responses and scripts for reception staff or call centres.

Test your plan and make sure your team knows and understands their roles.

To **minimise the impact** of a data breach you need to:

Effectively Manage Stakeholders	Build Capability	Respond Appropriately

Five essential steps **if a data breach occurs:**

Take the immediate, appropriate steps to **contain the data breach.**

Organise a meeting to establish facts and **prioritise issues**. Activate the plan, adapting templates and materials such as holding statements, emails and Q&As to be in line with the data breach.

Assess any risks associated with the data breach, including harm to individuals whose personal information may have been affected, and whether an 'eligible' data breach has occurred within the meaning of the Privacy Act 1988 (Cth).

If your business is subject to the Privacy Act 1988 (Cth) and an eligible data breach has occurred, you must **notify the affected individuals** and the Office of the Australian Information Commissioner. You may also need to notify other government organisations and law enforcement authorities.

- Make sure you **own the conversation**, to prevent external voices from owning it such as the media or your clients. Communicate simply and directly, without jargon. Drive people to your website for more information.
- **Be sensitive, measured, and honest**, cover ups are always uncovered and if you don't know a fact don't guess!
- **Monitor**, monitor monitor…**internal channels, social and traditional media**, right wrongs on social media and respond promptly.

Continue to **communicate** – what's been learnt, what's been done to respond, how it is progressing – it takes approximately four positive pieces of news to right one negative.

Five **post crisis** steps:

The most important – **evaluate and learn how you handled the breach** – what went well, what worked, what didn't work!

Investigate the cause of the data breach and develop a plan to mitigate its recurrence.

Report and assess response.

Refine and re-test.

Hold yearly review of response plan to ensure it is still relevant. Remember… cyber security is one of many risks that should be mapped out into an overall incident response plan and crisis communications plan and playbook.

Contact us:

pesel & carr

Level 1, 47 Elgin Street, Carlton,
VIC, Australia 3053
T: +61 3 9036 6900
E: barbara.pesel@peselandcarr.com.au
W: www.peselandcarr.com.au

gadens

Level 25, Bourke Place, 600 Bourke Street,
VIC, Australia 3000
T: +61 3 9252 7748
E: dudley.kneller@gadens.com
W: https://www.gadens.com

Other **resources:**

https://www.peselandcarr.com.au/index.php?mact=NewsManager,cntnt01,frontend_article_detail,0&cntnt01article_id=412&cntnt01returnid=62
https://www.peselandcarr.com.au/index.php?mact=NewsManager,cntnt01,frontend_article_detail,0&cntnt01article_id=409&cntnt01returnid=62
https://www.gadens.com/legal-insights/covid-19-managing-privacy-during-a-pandemic-practical-steps-and-considerations-for-businesses/
https://www.gadens.com/news-covid-19-response/
https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams
https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity-20-apr-2020