Allens › ‹ Linklaters

Cyber Security Tip Sheet

Preparing for a cyber breach

1. **Ensure that you have an up-to-date IT and data security policy**
2. **Develop a data breach response plan**
3. **Ensure that the board understands the cybersecurity risks that are applicable to your business.** Ensure that your staff understand the need for data security, confidentiality and privacy compliance. Identify any gaps in awareness and train staff to implement your plan.
4. **Monitor compliance** with your IT and data security policy and regularly test your systems.
5. **Implement the latest best practice physical, computer and network security measures – don't 'set and forget'.** Consider the OAIC's *Guide to Information Security*.
6. **Ensure that your systems can identify any information affected** by a cyber breach so that you can act quickly and identify affected individuals.
7. **Don't retain more information than you need.** Know what data your organisation holds, consider what information it actually needs to retain and de-identify that information wherever practical.
8. **Appropriately manage third party providers.** Imposing contractual obligations (eg a requirement to comply with certain IT security industry standards and relevant legislation, and to notify your organisation of any cyber breach) may not be sufficient. You may need to undertake due diligence and audits.
9. **Consider taking out a cyber insurance policy**
10. **Ensure staff travelling to high-risk jurisdictions take adequate precautions** for the safety of the data and devices that they carry.

Your data breach response plan should...

1. **Be practical, up-to-date and easy-to-follow**
2. **Identify a data breach lead and response team** comprising senior management, IT, public and investor relations, legal and risk / compliance and consider how that team will be activated.
3. **Include direct contact details for an external PR team and legal team** and, in case you need to seek an injunction, counsel.
4. **Include plans tailored to specific scenarios, eg:**
   - **different types of breaches** a data breach arising from information leaked by a disgruntled employee vs a hack by an external third party.
   - **different types of detection** via your organisation's internal systems, an external tip-off or from contact by the media.
5. **Include processes for tracing and securing your data**
6. **Consider how you will assess whether to notify affected individuals and other stakeholders and what you will say if you do.** Include a list of stakeholders and their direct contact information.
7. **Consider whether any national security issues will be involved.** If so, what, if any, additional steps are required in relation to that information.
8. **Include a process for recording breaches,** including all steps taken to rectify the situation and a summary of any decisions made.

Responding to a cyber breach

1. **Appoint a data breach lead and response team** comprising senior management, IT, public and investor relations, legal and risk/compliance. The lead should have sufficient authority to investigate and make recommendations to the business.
2. **Contain the breach and undertake a preliminary assessment of exposure.** Speed is critical. Stop the unauthorised practice, recover the records, shut down the breached system and/or revoke or change access privileges. Check whether the relevant data has been made available online (eg on the dark web).
3. **Evaluate the risks** associated with the breach. Consider what personal information is involved, the context of the information, the cause and extent of the breach, the risk of harm that could result to individuals and any other harms that could arise.
4. **Consider whether it is mandatory under the *Privacy Act 1988* (Cth) to notify the OAIC and affected or at risk individuals.**
   - **Are there reasonable grounds to believe that there has been an 'eligible data breach'?** Has there been unauthorised access to, disclosure of, or loss of personal information? If so, is it likely to result in serious harm to individuals? Make this assessment expeditiously and within 30 days of becoming aware of the incident.
   - **Does the remedial action exception apply?** Have you taken action early enough for serious harm not to have occurred or still be likely to occur?
   - **Consider applying for a declaration from the OAIC** as to whether you have to notify individuals, particularly if you think that notification should be delayed (e.g. to prevent interference with a law enforcement investigation) or may increase the risk of harm to affected individuals.
5. **If it is not mandatory to notify, consider whether to voluntarily notify the OAIC and affected individuals.** Consider the OAIC's *Data Breach Notification Guide*. Notification may still be appropriate, but only once your organisation has completed its risk assessment and determined that notification is appropriate. In some circumstances, notification of affected individuals may need to be delayed or not undertaken at all (e.g. where small low risk breaches have been contained).
6. **Be careful not to destroy evidence. Maintain appropriate records of any suspected breaches,** including all steps taken to rectify the situation and a summary of decisions made.
7. **Prevent further breaches.** Investigate the cause of the breach, identify key learnings and update your prevention and response plans accordingly. Audit updated processes and security measures.

Contacts

Gavin Smith
Partner
T +61 2 9230 4891
Gavin.Smith@allens.com.au

Michael Morris
Partner
T +61 7 3334 3279
Michael.Morris@allens.com.au

Ian McGill
Partner
T +61 2 9230 4893
Ian.McGill@allens.com.au

Michael Park
Partner
T +61 3 9613 8331
Michael.Park@allens.com.au

Valeska Bloch
Partner
T +61 2 9230 4030
Valeska.Bloch@allens.com.au

David Rountree
Senior Associate
T +61 2 9230 4773
David.Rountree@allens.com.au

Samantha Naylor Brown
Associate
T +61 2 9230 4458
samantha.naylorbrown@allens.com.au

Allens Cyber Breach Hotline
T +61 2 9230 5300