Allens > < Linklaters

Cyber Security

What should businesses do to avoid, minimise or remedy the damage caused by a cyber breach?

1. Ensure you have a formal, up-to-date policy covering your organisation's approach to data security.
2. Assess how much information, and the type of information, that you need to retain in your databases for your business. Don't retain more information than you really need and consider de-identifying information wherever practical.
3. Ensure there is a cultural awareness amongst your staff of the need for data security, confidentiality and privacy compliance. Develop education plans that address any gaps in staff awareness and train teams to implement your data security and compliance plans.
4. Implement best practice physical, computer and network security measures, including in relation to:
   - firewalls
   - enhanced encryption
   - software monitoring
   - password security
   - intrusion detection systems

   Consider following the recommendations from the Defence Signals Directorate's 'Strategies to Mitigate Targeted Cyber Intrusions' (ie application of whitelisting, minimising administrative privilege and immediate patching of operating system and applications) and the Office of the Australian Information Commissioner's 'Guide to Information Security'.
5. Monitor and review compliance with your data security policy and test all parts of your systems regularly.
6. Ensure that staff travelling to high-risk jurisdictions take adequate precautions for the safety of the data and devices that they carry with them.
7. Ensure your systems will allow you to identify if, and the extent to which, information may have been affected by any cyber breach so that you can act quickly if you suffer a breach and identify any affected individuals.
8. Develop a data breach response plan with practical, up-to-date and easy-to-follow steps, including a series of response plans for different scenarios. Appoint a data breach response team which includes individuals from across the organisation – senior management, IT, public and investor relations, legal and privacy compliance.
9. Maintain appropriate records of any suspected breaches, including all steps taken to rectify the situation and a summary of decisions made (this is useful to mitigate future data breaches based on previous experience).
10. Consider cyber protection insurance options to mitigate financial loss.

Contacts

Niranjan Arasaratnam
Partner
T +61 3 9613 8324
Niranjan.Arasaratnam@allens.com.au

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

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

Michael Pattison
Partner
T +61 3 9613 8839
Michael.Pattison@allens.com.au

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

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

Allens is an independent partnership operating in alliance with Linklaters LLP.

www.allens.com.au