COLIN BIGGERS & PAISLEY LAWYERS

Practical cyber risk management checklist

TOBY BLYTH
Partner
T +61 2 8281 4440
E toby.blyth@cbp.com.au

Malicious cyber activity against Australian individuals, businesses and government agencies is on the rise, with the Australian Cyber Security Centre (ACSC) noting that cybercrime is one of the most pervasive threats facing Australia, with self-reported losses topping $33 billion in the last financial year (with real losses widely predicted to be far greater).

Do not just rely on insurance - once you are at that stage the damage is done. Remember the three lines of defence that apply to any organisation: Tech, People and Insurance.

In this checklist we outline our top tips to mitigate the risk of malicious cyber incidents.

WHAT CAN YOU DO?

Train your employees to look for red flags in suspicious emails.	
The sender may be someone in a position of authority, particularly if such a person wouldn't normally issue payment requests.	☐
The email requests urgent payment or threatens consequences if payment isn't made. (often from an email that looks like the client's email — but say with an exttra letter added — see what we just did there?).	☐
A vendor has provided new bank details.	☐
The sender requests payment of an invoice outside of the usual payment cycle or the invoice amount is larger than usual.	☐

Always confirm account details over the phone before processing funds transfers.	
Employees should always keep note of call details including the date, the name of the person calling and confirmation of account details. These details ensure reasonable steps were taken to avoid the risk of misappropriation in the unfortunate event that funds are lost.	☐
Ensure multi-factor authentication (MFA) is enabled.	
MFA can be incorporated into most essential programs and is an existing feature on systems like Office 365. If MFA is not enabled on your organisation's computer network, we encourage you to contact your IT security provider.	☐
Ensure regular software updates and patching occurs.	
Regular software updates and patching is important to guarantee that security flaws are removed, ensuring the ongoing effectiveness of your IT security systems.	☐
Conduct regular cybersecurity audits.	
These audits should involve penetration and awareness testing, security review and ensuring back-up systems and protocols are functioning effectively. Whilst security audits can be handled internally, best practice is to have external IT consultants conduct the audit to accurately test the strength of existing systems.	☐
Formulate a cyber incident and privacy breach response plan.	
These plans should clearly outline the immediate steps which should be taken in response to a cyber incident, including: • appointment of IT consultants to assess the extent of the incident identification of important data and critical systems; • key roles and responsibilities, including internal notification protocols stakeholder communication protocols (public relations and media management) reporting obligations (particularly under the Privacy Act).	☐

Any cyber incident response plan or privacy breach response plan should include notification to your cyber insurer (if applicable) and a hard copy should be kept on site. APRA's CPS 234 on information security provides a good planning tool (even if you are not a financial institution).

It is essential that organisations institute training and workflow procedures that ensure their employees are aware of the threats faced from cybercrime and the steps they must take to avoid it.

This checklist was first published in volume 31 issue 4 of Risk Management Today and relies on extracts from an article, Practical cyber risk management for SMEs, that first appeared in this issue.

BRISBANE

Level 35, Waterfront Place
1 Eagle Street
Brisbane QLD 4000
Australia

+61 7 3002 8700

MELBOURNE

Level 23
181 William Street
Melbourne VIC 3000
Australia

+61 3 8624 2000

SYDNEY

Level 42
2 Park Street
Sydney NSW 2000
Australia

+61 2 8281 4555

ALTERNATIVE CONTACTS:

Katherine Jones | Special Counsel
T: +61 2 8281 4990 E: katherine.jones@cbp.com.au

John McGirr | Special Counsel
T: +61 3 8624 2068 E: john.mcgirr@cbp.com.au

This checklist was first published in volume 31 issue 4 of Risk Management Today and relies on extracts from an article, Practical cyber risk management for SMEs, that first appeared in this issue.