Cyber checklists

CYBER READINESS

wotton kearney

A founding member of LEGALIGN GLOBAL

Cyber Readiness

Having steps in place to protect your business against breaches and respond to incidents effectively are crucial to limiting your exposure and liability in the event of a cyber breach. We set out below four crucial steps that can assist you being cyber ready:

1. Safeguard your systems;
2. Know your obligations;
3. Have an incident response plan; and
4. Make sure you're covered.

Step 1. Safeguard your systems

There are two major steps you can take to prevent cyber risks: security systems and employee training.

Security systems

External cyber risks can be reduced through protection and detection software, as well as security techniques such as multi-factor authentication.

Accepting that not all cyber risks cannot be eliminated, there are steps you can take to reduce your risk. You should consider seeking the assistance of your IT provider about:

- Know where your business-critical data is (your crown jewels) and ensure the security architecture for these systems (at least) are high
- Setting up alert systems for suspicious or abnormal email activity.
- Turning on comprehensive audit logging in your email systems.
- Requiring employees to update their passwords regularly.
- Locking user accounts after 3 failed password attempts.
- Enabling multi-factor authentication.
- Configuring regular back-ups of your data and regularly testing those back-ups. Ideally, these back-ups will be disconnected from your main server in case your main server is attacked.
- Regularly updating firewall and anti-virus software.
- Application whitelisting.
- Patching applications immediately when a patch is available.
- Configuring macro settings.
- Restricting administrative privileges.

Employee training

One of the biggest causes of cyber breaches is human error, so a crucial element in safeguarding your systems is employee training.

Training should be organised through your IT provider and be regular and customised according to your systems and internal structures. Training ensures that every employee understands that cyber safety is part of their responsibility and that individuals are on the alert for external threats. Have specific cyber training for employees identified as incident responders in your incident response plan (Step 3).

Step 2. Know your obligations

It's important that you're aware of your legal obligations in the event of a cyber breach and know what steps to take when responding to incidents.

If you have had a turnover of more than $3,000,000 in any financial year since 2002 or are an eligible small business (see our checklist **here**), you are covered by the Privacy Act.

This means you're subject to the Notifiable Data Breach Scheme and the Australian Privacy Principles. You need to make sure that your business is actively complying with the Australian Privacy Principles (able to be viewed **here**) or you may be liable for penalties for a breach of the Privacy Act.

You also need to consider privacy breach notifications in your incident response plan (Step 3). This is because, under the NDB Scheme, you may be required to notify the Office of the Australian Information Commissioner and your clients in the event of a data breach.

If you experience a suspected data breach, you should seek legal advice about how to comply with your obligations under the Privacy Act.

Step 3. Have an incident response plan

An incident response plan helps you meet your obligations under the Privacy Act, limit the consequences of a cyber breach and preserve and build public trust. It sets out exactly want you need to do in the event of a cyber breach. You should regularly review and test your plan to make sure it is effective, and employees are aware of their roles in executing the plan.

Your plan should set out:

1. What a cyber breach is;
2. Your strategy for containing, assessing and managing a breach;
3. How you will fulfill any legal notification obligations you have;
4. Who is responsible for what steps in the plan;
5. How you will document breaches; and
6. How you will review your systems after a breach has occurred.

Your incident response plan should be catered to the technologies your organisation uses and what IT resources and staff you have access to. You may create particular incident response plans for different kinds of security breaches, for example malware or tampering with payment terminals.

Your response plan should also set out the contact details and responsibilities of all key personnel, including internal staff, IT consultants, legal advisors and server hosting providers, as applicable.

Incident response plan check list

- What systems and technologies do you rely on most heavily?
- Who is responsible for checking whether detected threats are legitimate, or false positives?
- How often are servers going to be backed up? Who will monitor that these backups are being completed and stored successfully?
- How often are you going to check detection software notifications?
- Who is responsible for reviewing incidents reported by employees?

Step 4. Make sure you're covered

A fourth step in cyber readiness is making sure that, not only are you insured for cyber breaches, but you know exactly what cyber incidents you are covered for and who to contact if your business is affected by a cyber incident.

See our industry checklists **here** to see what attacks you are most vulnerable to, and make sure you have coverage for those risks. Also check what sub-limits you have for specific incidents e.g. ransomware, and what types of losses are covered in your policies e.g. business interruption costs.

Cyber insurance should act as the final frontier in your cyber protections, to supplement the protections and processes you already have in place, providing extra support in responding to attacks.