# Cyber checklists

BREACH RESPONSE

wotton kearney

A founding member of LEGALIGN GLOBAL

delta

## Guide to Cyber Breaches

Responding to cyber breaches is a comprehensive process, but the three key elements are:

- Step **1**: Follow your incident response plan
- Step **2**: Notify your insurer
- Step **3**: Comply with your legal obligations

The below chart provides a basic framework for responding to a cyber breach.

## Step 1: Follow your incident response plan

Immediately following a cyber breach, the key focus should be to contain the breach and remove the attacker from your systems. Your incident response plan (as outlined in our cyber readiness guide **here**) should provide a clear process for this and the personnel in charge of each step.

## Step 2: Notify your insurer

As part of your incident response plan, you should notify your insurer and get their advice on incident management. This will often involve obtaining legal representation to assist you in responding to the incident and engaging third party experts such as forensic IT providers, to stop the breach.

Notifying your insurer early in the breach process will additionally assist you if you need to make a later claim for restoration costs, business interruption costs or third-party losses, as they will be able to track your losses and expenditure across the entirety of the incident.

## Step 3: Comply with your legal obligations

This is the most intricate step in responding to a data breach is complying with your legal obligations under the Privacy Act and Notifiable Data Beach Scheme (NDB scheme). To understand your legal obligations, refer to our guides on the **NDB Scheme** and **Cyber Readiness**.

If you have no obligations under the NDB Scheme, you aren't required to notify your customers/ clients or the OAIC about the breach. However, you may consider making a voluntary notification.

If you are covered by the NDB Scheme you need to form a view, perhaps with the assistance of legal advice, as to whether you've suffered an eligible data breach. An eligible data breach occurs when:

1. there is unauthorised access to, unauthorised disclosure of, or loss of information where it is likely to be accessed or disclosed; which
2. a reasonable person would conclude would likely result in serious harm to any of the individuals to whom the information relates; and
3. you are unable to take remedial action to prevent the risk of serious harm.

If, following a cyber incident, you have reasonable grounds to suspect a data breach may have occurred but are unsure whether the relevant circumstances meet the criteria, you have 30 days to investigate the breach and make a reasonable assessment about whether it was an eligible data breach. You will need to identify, as far as possible, what information was accessed during the breach and which individuals were affected. Forensic IT providers will be able to help you with this assessment process

If, during that investigation, you have reasonable grounds to believe that a cyber incident amounts to an eligible data breach, you must notify the Office of the Australian Information Commissioner (OAIC) and affected individuals as soon as possible.

If notification is required, the Privacy Act requires a statement to be prepared that at the very least includes:

1. your organisations or agency's name and contact details;
2. a description of the data breach;
3. the kinds of information involved; and
4. recommendations about the steps individuals should take in response to the data breach.

# Privacy for Small Businesses – Does the NDB Scheme Apply to Me?

For the Notifiable Data Breach Scheme (NDB Scheme) to apply to your business, you must be covered by the Privacy Act 1988 (Cth). Only certain businesses are covered by the Act and subject to the NDB Scheme.

To determine whether the NDB Scheme applies to your business, follow the checklist below.

Q1.

## Does your business handle personal information?

Personal information is information or an opinion about an identified person or a person who could reasonably be identified from the information. Even if the information you handle is anonymous or you use pseudonyms, you may still handle personal information if the information could be combined with other publicly available information to identify the person.

**Yes** Proceed to Question 2.

**No** The NDB scheme does not apply to you.

Q2.

## Have you had an annual turnover of more than $3,000,000 in any financial year since 2002?

This includes all income from all sources, but does not include assets held, capital gains or proceeds of capital gains.

**Yes** The NDB Scheme applies to you in relation to all of the kinds of personal information you hold.

**No** Go to Question 3.

Q3.

## Do you trade in personal information?

Trading in personal information means you provide a benefit or service in order for you to collect personal information or you disclose personal information for a benefit or service without the individual's consent and without being required or authorised by law. This benefit could be a payment of money, concession, subsidy or another service.

**Yes** The NDB Scheme applies to you.

**No** Go to Question 4.

Q4.

## Are you a health service provider?

This includes medical practitioners, private hospitals, IVF and fertility clinics, gyms, private schools, childcare centres and disability service providers. You will be a health service provider if you provide a health service, which includes recording and managing and individual's health, diagnosing illnesses or disabilities and dispensing prescription or other medication. Note this can be broader thank you think so think about what health information about individuals (such as customers or members) that you hold.

**Yes** The NDB Scheme applies to you.

**No** Go to Question 5.

Q5.

## Are you related to a larger body corporate covered by the Privacy Act?

If your business is under a holding company, a subsidiary, or a subsidiary of a holding company, or related to another body corporate under the Corporations Act 2001 which has obligations under the Privacy Act. Please check with the related or larger body corporate to confirm if it is covered by the Privacy Act.

**Yes** The NDB Scheme applies to you.

**No** Go to Question 6.

Q6.

## Are you providing services under a Commonwealth contract?

If you provide services to, or on behalf of, Australian Government agencies or the Norfolk Island administration under a Commonwealth contract or subcontract, you are considered a Commonwealth contracted service provider. Please check the terms of any Commonwealth contract and confirm the extent to which you are required to comply with privacy laws, including the NDB Scheme.

**Yes** The NDB Scheme applies to you.

**No** Go to Question 7.

Q7.

## Are you a reporting entity or authorised agent of a reporting entity under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006?

If you provide services to, or on behalf of, Australian Government agencies or the Norfolk Island administration under a Commonwealth contract or subcontract, you are considered a Commonwealth contracted service provider. Please check the terms of any Commonwealth contract and confirm the extent to which you are required to comply with privacy laws, including the NDB Scheme.

**Yes** The NDB Scheme applies to you.

**No** Go to Question 8.

Q8.

## Do you operate a residential tenancy database?

If you provide services to, or on behalf of, Australian Government agencies or the Norfolk Island administration under a Commonwealth contract or subcontract, you are considered a Commonwealth contracted service provider. Please check the terms of any Commonwealth contract and confirm the extent to which you are required to comply with privacy laws, including the NDB Scheme.

**Yes** The NDB Scheme applies to you.

**No** Go to Question 9.

Q9.

## Are you a credit reporting business?

You are a credit reporting business if your business involves collecting, holding, using or disclosing personal information about individuals for the purpose of providing companies with information about the credit worthiness of an individual for a profit or reward.

**Yes** The NDB Scheme applies to you in relation to the information you hold about individuals' credit, including their consumer credit liability, repayment history, the type of credit sought and identifying information about the individual. Please ensure you check your answers to the other questions in this checklist to determine if you have obligations in relation to other personal information you hold as well.

**No** Go to Question 10.

Q10.

## Are you a credit provider?

You are a credit provider if a substantial part of your business involves issuing credit cards or providing credit to individuals.

**Yes** The NDB Scheme applies to you in relation to the information you hold about individuals' eligibility for credit. Please ensure you check your answers to the other questions in this checklist to determine if you have obligations in relation to other personal information you hold as well.

**No** Go to Question 11.

Q11.

## Do you hold Tax File Numbers (TFNs)?

You are a credit provider if a substantial part of your business involves issuing credit cards or providing credit to individuals.

**Yes** The NDB Scheme applies to you in relation to the tax file numbers you hold. Please ensure you check your answers to the other questions in this checklist to determine if you have obligations in relation to other personal information you hold as well.

**No** Go to Question 12.

Q12.

## Are you an employee association registered or recognised under the Fair Work (Registered Organisations) Act 2009?

**Yes** The NDB Scheme applies to you.

**No** Go to Question 13.

Q13.

## Do you conduct protected action ballots under Part 3-3 of the Fair Work Act 2009?

**Yes** The NDB Scheme applies to you.

**No** Go to Question 14.

Q14.

## Are you a service provider required to comply with the data retention provisions in Part 5-1A of the Telecommunications (Interception and Access) Act 1979?

**Yes** The NDB Scheme applies to you.

**No** Go to Question 15.

Q15.

## Have you voluntarily opted into the Privacy Act?

The NDB Scheme applies to you.

**Yes** The NDB Scheme applies to you in relation to the tax file numbers you hold. Please ensure you check your answers to the other questions in this checklist to determine if you have obligations in relation to other personal information you hold as well.

**No** The NDB Scheme does not apply to you. However, please ensure you check whether your business' website contains a privacy policy which states that you comply with the NDB Scheme or Privacy Act. Your privacy policy may represent to your customers that you will comply with the NDB Scheme or Privacy Act even though you may not need to.

# 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**

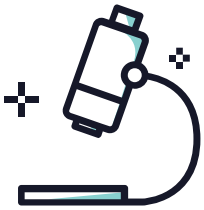
- What systems and technologies do you rely on most heavily?
- Who is responsible for checking whether detected threats are legitimate, or false positives?
- How often are servers going to be backed up? Who will monitor that these backups are being completed and stored successfully?
- How often are you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



# Health

As a healthcare provider you hold highly sensitive private information that may be the target of cyber-attacks. Making sure your organisation is cyber ready is imperative to reducing your risk as a business. It is important that you:

1. understand what data you hold;
2. understand general cyber risks and those specifically relevant to your industry;
3. take steps to reduce your cyber risk; and
4. be prepared to respond to cyber-attacks if that occur.

## Understand your data

Understanding the data you hold is an important part of effectively assessing and reducing your cyber risk. As a healthcare provider you are likely to not only hold financial information for your clients, but also medical records, which are of an extremely personal and sensitive nature. You should aim to be aware of the volume and type of information you hold for each client and whether that is their complete medical file or only isolated records, in order to effectively assess breaches and whether you need to notify clients, and what you need to notify them about. You should also have a policy about how long you retain your clients' information and where that information is stored.

In the event that sensitive data is compromised in a data breach, a number of risks can potentially arise for your organisation and your clients, including financial, physical, psychological and reputational harm. Depending upon the depth of information you hold about your clients, they may also be exposed to financial harm arising from identity theft. You will need to consider whether this amounts to a risk of "serious harm" and whether the incident is notifiable under the Notifiable Data Breach Scheme set out in the Privacy Act (click **here** for more information).

## Understand your risks

You should be particularly wary of cyber-attacks in the form of ransomware and data scraping. Ransomware is malware which encrypts the data on your systems and then demands money in exchange for being decrypted or unlocked, whereas data scraping is where an attacker enters your network to access and export your data. Sometimes, these attacks can occur at the same time, meaning the hacker is able to exfiltrate your data while before your data is encrypted and you are unable to access your systems.

These attacks usually start through phishing attacks, where fraudulent emails are used to trick users into revealing their login information or giving access to their network account or getting them to download malware through a document attachment or link.

## Reduce your risk

There are two major areas to focus on to reduce your cyber risk: security systems and employee training.

### Security systems

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

+ 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

The single biggest cause of cyber breaches is human error – be it inadvertently downloading malware from email attachments or handing over credentials via genuine looking websites. Therefore, a critical 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.

See our comprehensive guide on cyber readiness **here**.

## Respond to attacks

Responding to cyber-attacks is a three-stage process, outlined in our **Guide to Cyber Breaches**.

As a healthcare provider you will be required to notify the OAIC and affected clients of eligible data breaches under the NDB Scheme, which supplements the mandatory data breach reporting requirements of the My Health Record system for branches that occur outside of the My Health Record system.

Breaches that occur within the My Health Record system should be notified and dealt with through the Australian Digital Health Agency. You may also have additional obligations to report to the Commissioner under the National Cancer Screening Register Act.



# Finance

As a financial services provider you hold highly sensitive private information that may be the target of cyber-attacks. Making sure your organisation is cyber ready is imperative to reducing your risk as a business. To ensure you're across your cyber obligations and responses, you need to:

1. understand what data you hold;
2. understand general cyber risks and those specifically relevant to your industry;
3. take steps to reduce your cyber risk; and
4. be prepared to respond to cyber-attacks if that occur.

## Understand your data

Understanding the data you hold is an important part of effectively assessing and reducing your cyber risk. You likely hold sensitive financial information about your clients which may include their bank account, credit card and tax details. You need to be aware of the specific type of financial information you hold for each client and what can be done with it.

Financial information carries with it a risk of financial harm (e.g. credit card information) and usually, identity theft. Depending upon the information you hold, for example if you hold information about a customer who is in financial distress, a data breach may also carry the risk of reputational or psychological harm. In the event of a data breach, you will need to consider whether this amounts to a risk of "serious harm" and whether the incident is notifiable under the Notifiable Data Breach Scheme set out in the Privacy Act (click **here** for more information).

## Understand your risks

You should be particularly wary of cyber-attacks in the form of ransomware, business email compromise and data scraping. Ransomware is malware which encrypts the data on your systems and then demands money in exchange for being decrypted or unlocked, whereas data scraping is where an attacker enters your network to access and export your data. Sometimes, these attacks can occur at the same time, meaning the hacker is able to exfiltrate your data while before your data is encrypted and you are unable to access your systems.

Business email compromise involves a hacker gaining access to one or more of your employees' email accounts and using their email account to imitate your employees and, in most cases, trick your clients into paying money into a fraudulent bank account or providing their login details.

These attacks usually start through phishing attacks, where fraudulent emails are used to trick users into revealing their login information or giving access to their network account or getting them to download malware through a document attachment or link.

## Reduce your risk

There are two major areas to focus on to reduce your cyber risk: security systems and employee training.

### Security systems

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

+ 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

The single biggest cause of cyber breaches is human error – be it inadvertently downloading malware from email attachments or handing over credentials via genuine looking websites. Therefore, a critical 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.

See our comprehensive guide on cyber readiness **here**.

## Respond to attacks

Responding to cyber-attacks is a three-stage process, outlined in our **Guide to Cyber Breaches**.

As a financial services provider you will be required to notify the OAIC and affected customers of eligible data breaches involving their financial information under the NDB Scheme.

If you an APRA regulated entity under the Prudential Standard CPS 234, you will also have APRA related obligations and be required to report to APRA any cyber breaches that materially affect, or have the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers. If you have notified OAIC of a breach, you will also be required to notify APRA no later than ten business days after you become aware of a breach.

You may also consider notification to ASIC, AUSTRAC and the ATO depending on the financial services you provide and the type of information which was accessed.

# Not for Profit

As a not-for-profit organisation you hold highly sensitive private information that may be the target of cyber-attacks. Making sure your organisation is cyber ready is imperative to reducing your risk as a business. To ensure you're across your cyber obligations and responses, you need to:

1. understand what data you hold;
2. understand general cyber risks and those specifically relevant to your industry;
3. take steps to reduce your cyber risk; and
4. be prepared to respond to cyber-attacks if that occur.

## Understand your data

Understanding the data you hold is an important part of effectively assessing and reducing your cyber risk. You will likely hold sensitive information about your clients or other individuals, for example if your not-for-profit engages in research activities or community outreach services. That sensitive information could be financial information, including bank account, credit card and tax details, information about individuals' social or political opinions, race, sexuality or religion, or even health information depending upon the types of services and activities your not-for-profit participates in.

You need to be aware of the scope of information you hold about individuals and the risks which are likely to arise in the event of a data breach, which may range from financial harm (including identity theft) to reputational harm and psychological harm. You will also need to consider whether such a breach needs to be reported under the Notifiable Data Breach Scheme set out in the Privacy Act (click **here** for more information).

## Understand your risks

You should be particularly wary of cyber-attacks in the form of ransomware, business email compromise and data scraping. Ransomware is malware which encrypts the data on your systems and then demands money in exchange for being decrypted or unlocked, whereas data scraping is where an attacker enters your network to access and export your data. Sometimes, these attacks can occur at the same time, meaning the hacker is able to exfiltrate your data while before your data is encrypted and you are unable to access your systems.

Business email compromise involves a hacker gaining access to one or more of your employees' email accounts and using their email account to imitate your employees and, in most cases, trick your clients into paying money into a fraudulent bank account or providing their login details.

These attacks usually start through phishing attacks, where fraudulent emails are used to trick users into revealing their login information or giving access to their network account or getting them to download malware through a document attachment or link.

## Reduce your risk

There are two major areas to focus on to reduce your cyber risk: security systems and employee training.

### Security systems

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

+ 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

The single biggest cause of cyber breaches is human error – be it inadvertently downloading malware from email attachments or handing over credentials via genuine looking websites. Therefore, a critical 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.

See our comprehensive guide on cyber readiness **here**.

## Respond to attacks

Responding to cyber-attacks is a three-stage process, outlined in our **Guide to Data Breaches**.



# Professional Services

As a not for profit organisation you hold highly sensitive private information that may be the target of cyber-attacks. Making sure your organisation is cyber ready is imperative to reducing your risk as a business. To ensure you're across your cyber obligations and responses, you need to:

1. understand what data you hold;
2. understand general cyber risks and those specifically relevant to your industry;
3. take steps to reduce your cyber risk; and
4. be prepared to respond to cyber-attacks if that occur.

## Understand your data

Understanding the data you hold is an important part of effectively assessing and reducing your cyber risk. You will likely hold sensitive legal and financial information about your clients which may include their bank account, credit card and tax details. You need to be aware of the specific type of legal and financial information you hold for each client, and the level of individual identification that can be gained through it.

This types of information, in the event that it is compromised, carries risk of financial (including identity theft), emotional and reputational harm, which may need to be notified under the Notifiable Data Breach Scheme set out in the Privacy Act (**click here** for more information).

## Understand your risks

You should be particularly wary of cyber-attacks in the form of ransomware, business email compromise and data scraping. Ransomware is malware which encrypts the data on your systems and then demands money in exchange for being decrypted or unlocked, whereas data scraping is where an attacker enters your network to access and export your data. Sometimes, these attacks can occur at the same time, meaning the hacker is able to exfiltrate your data while before your data is encrypted and you are unable to access your systems.

Business email compromise involves a hacker gaining access to one or more of your employees' email accounts and using their email account to imitate your employees and, in most cases, trick your clients into paying money into a fraudulent bank account or providing their login details.

These attacks usually start through phishing attacks, where fraudulent emails are used to trick users into revealing their login information or giving access to their network account or getting them to download malware through a document attachment or link.

## Reduce your risk

There are two major areas to focus on to reduce your cyber risk: security systems and employee training.

### Security systems

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

+ 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

The single biggest cause of cyber breaches is human error – be it inadvertently downloading malware from email attachments or handing over credentials via genuine looking websites. Therefore, a critical 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.

See our comprehensive guide on cyber readiness **here**.

## Respond to attacks

Responding to cyber-attacks is a three-stage process, outlined in our **Guide to Data Breaches**.

# Cyber contacts

## AUSTRALIA + NEW ZEALAND

Delta Insurance Australia is a specialist underwriting agency and part of the Delta Insurance Group. Established in 2014, the Delta Insurance Group challenges the status quo by embracing technology, transparency and integrity, introducing niche products into new markets and delivering exceptional service.

Wotton + Kearney has a dedicated team of cyber specialists across Australia and New Zealand. We have worked on many cyber breach responses for insurers, brokers and their customers in Australia and New Zealand. We also draw on our knowledge of each jurisdiction and our excellent relationships with local regulators to effectively work together on cross-border breaches.

### DELTA

**Stephen Carey**
Delta Founder and Director

stephen@
deltainsurance.com.au

**Oliver Gilmore**
Underwriting Manager – Casualty

oliver@
deltainsurance.com.au

**Jacqui Warwick**
Underwriting Manager – Professional Indemnity, Technology & Cyber

jacqui@
deltainsurance.com.au

### AUSTRALIA

**Kieran Doyle**
Partner (Sydney)
Australian Cyber Leader

kieran.doyle@
wottonkearney.com.au

**Nicole Gabryk**
Special Counsel (Sydney)

nicole.gabryk@
wottonkearney.com.au

**Magdalena Blanch-de Wilt**
Special Counsel (Melbourne)

magdalena.blanch-dewilt@
wottonkearney.com.au

### NEW ZEALAND

**Joseph Fitzgerald**
Partner (Wellington)

joseph.fitzgerald@
wottonkearney.com

**Laura Bain**
Senior Associate (Wellington)

laura.bain@
wottonkearney.com

**David Smith**
Associate (Auckland)

david.smith@
wottonkearney.com

For a full list of W+K's cyber contacts, click **here**.