INCIDENT RESPONSE SOLUTIONS

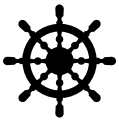
Data Breach Response

2020 Edition

Our Data Breach Response Services at a Glance

Incident Response Solutions can assist you through all phases of the Data Breach Response process.

PREPARE



Cyber Security and Privacy Frameworks and Controls

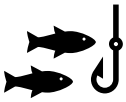
Our experts will help you implement best practice frameworks and controls in order to assess and improve upon your current level of cyber security and privacy maturity.

Incident Response Preparation

We will help you create a cyber incident response plan and a data/privacy breach response policy/playbook, so your team are ready to respond should a crisis strike.

Crisis Resilience

We will test your resilience by simulating a data breach in a controlled environment, which will assist your incident response team and other key parties identify gaps in current processes.



Training and Awareness

We offer online cyber security training and phishing simulations so your staff can learn how to identify potential cyber risks and avoid becoming victims of a cyber-attack.

RESPOND

Incident Controllers

We have extensive experience in managing incidents and will guide you through all stages of a data breach, either at your site or from our dedicated incident response control room.

Forensic Technology Experts

Our forensic technology experts are experienced in responding to data breaches in situations such as business email compromise and ransomware.

Specialist Data Breach Software

We use advanced forensic software to examine the source of the compromise and the extent that confidential information has been breached, including PII.

RECOVER

Mandatory Notifications

Our notification services are compliant with the NZ Privacy Act 2020 via either a third party email tool, a tailored website, postal mail, or our contracted call centre.

Ongoing Monitoring

We use leading technology to search the ‘Dark Web’ for credential compromises, the Open Web and Social Media for your ‘Brand Reputation’, as well as Credit Monitoring.

Reliable Resources

Subscribe to our Alerts and Bulletins and view our resources to keep up to date with the latest threats in order to reduce your cyber risk.

OVERVIEW

As experienced incident responders and forensic examiners, we know that time is of the essence in a crisis. In the event of a data breach, customers expect to be kept up to date as to how it may impact them and what steps they should take.

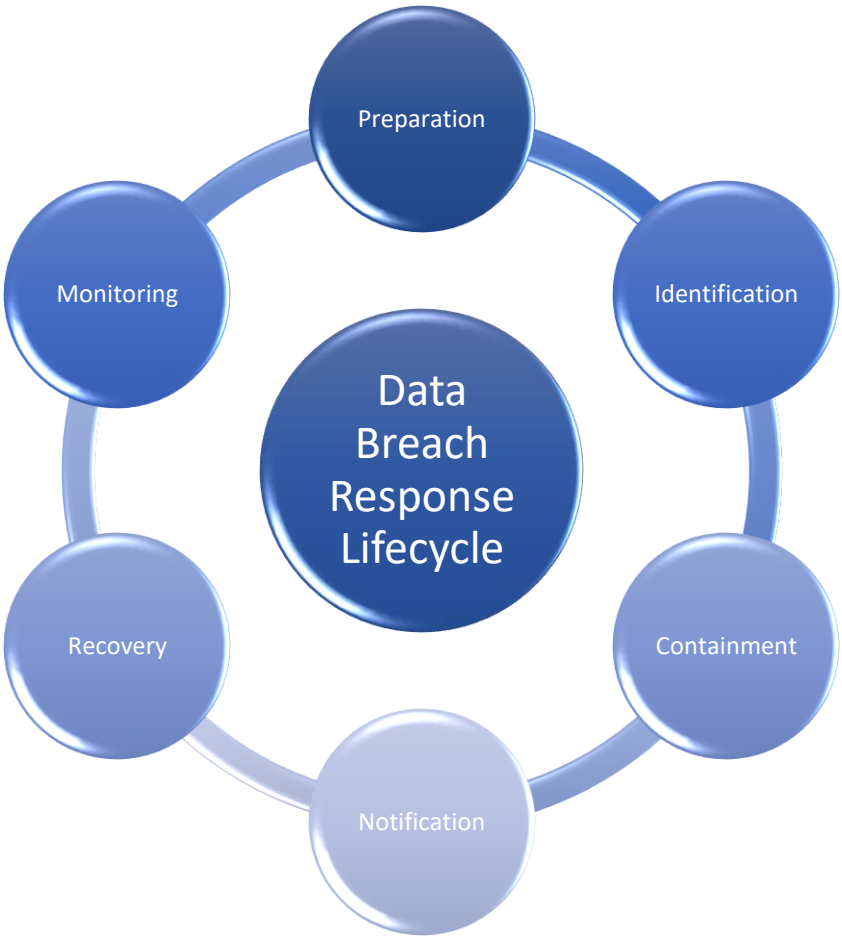
We specialise in the forensic collection and examination of data from a wide variety of sources and have the proven experience in applying advanced investigative and analytical techniques when responding to a data breach.

Our Data Breach Response service (also Privacy Breach Response) is tailored to support organisations prepare for, respond to, and recover from a data breach. The core of our business is to provide you with the confidence you require in a crisis, to a forensic standard, i.e. the highest level of proof. We strive to make you look good, even in times of crisis.

This guide contains ten factors to consider in order to be better prepared for a potential data breach, including:

- References to the recently updated Privacy Act 2020
- Resources to help you improve your level of preparedness
- Practical steps such as creating plans and playbooks
- Tools to recover from a breach such as dark web monitoring

Let Incident Response Solutions help you manage your entire data breach response lifecycle.



PREPARE

1. Cyber Security and Privacy Frameworks and Controls

Cybersecurity Framework

Our Cybersecurity Advisory Programme is aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which organisations can use to:

- Describe their current cybersecurity posture
- Describe their target profile for cybersecurity
- Identify and prioritise opportunities for improvement
- Assess progress towards the target profile
- Communicate amongst internal and external stakeholders about cybersecurity risk

Our automated self-assessment tool allows you to complete an initial assessment so you can immediately start making improvements.

Privacy Framework

New Zealand's Privacy Act 2020 came into force on 1 December 2020, creating new responsibilities for organisations in New Zealand. A privacy breach occurs when personal information is lost, stolen, or accessed without permission. Common examples include the theft or inadvertent loss of documents or devices, business email compromises and ransomware attacks.

The new Act introduces a number of changes concerning how the privacy principles are enforced and regulated including:

- Mandatory notifications for privacy breaches. If a privacy breach poses a risk of "serious harm" to affected individuals, the Privacy Commissioner and affected individuals must be notified. In determining "serious harm", consideration factors include actions taken by the agency to reduce the risk of harm, the sensitivity of the personal information, the nature of harm to any recipients, the party that has the information and whether the information is protected by a security measure.
- Increased powers for the Privacy Commissioner. The Privacy Commissioner can require agencies to comply with the new legislation with penalties of up to $10,000.
- Criminal offences. New criminal offences carry a maximum fine of $10,000, including offences for agencies that either fail to notify a privacy breach appropriately or obstruct the Privacy Commissioner. Notifications can be sent to the Office of the Privacy Commissioner via the NotifyUs tool.

Our Privacy Advisory Programme is also aligned with the NIST Privacy Framework, which organisations can use to:

- Take privacy into account as they design and deploy systems and services
- Communicate their privacy practices
- Encourage cross-organisational workforce collaboration

We also offer an automated privacy self-assessment tool which is complementary to the NIST Cybersecurity Framework as per above.

Your conformance with both the Cybersecurity and Privacy Frameworks can be re-assessed using these tools as often as you like without the need to re-produce time intensive reports.

2. Incident Response Preparation

We recommend developing a tailored incident response plan and privacy breach playbook so that in the event of a crisis, you are better prepared to respond.

We can assist you in drafting these documents that will include the following phases:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

3. Crisis Resilience

We will help you test your resilience in the event of a data breach by conducting a cyber incident simulation to evaluate both your executive and technical level of preparedness.

The key outcome of a cyber incident simulation, or tabletop exercise as it is often referred, is that your organisation will have greater confidence to prepare, respond and recover in a crisis.

By conducting a simulation, you will:

- establish your current state of readiness
- gain a better understanding of the cyber risks you face
- practice your decision making in a safe environment
- identify areas for improvement.

We combine our experience in responding to actual cyber incidents, along with realistic and engaging tools, to help make your simulation real.

4. Training and Awareness

We can help reduce your cyber risk by scheduling our online cyber security training and phishing simulations programmes for your staff on a regular basis.

Cyber Training and Awareness

The time and cost spent on security awareness training significantly reduces your business' vulnerability to cyberattacks. This could prove to be priceless when avoiding long-term costs such as lost customer trust and damage to your business' reputation because of a data breach.

Incident Response Solutions can help you with your cyber training and awareness program, delivered via an online course or in person workshop.

Phishing Simulations

A Phishing simulation is a training tool that organisations can use to send realistic phishing emails to employees in order to test their level of awareness of such attacks, as well as advising them on what to do with phishing emails when they receive them. A Phishing simulation is typically conducted in coordination with cyber security training that educates employees about how these attacks work and how to avoid them.

Incident Response Solutions run carefully planned simulated phishing attacks to help you find out how vigilant your employees are and how they can be trained further.

RESPOND

5. Incident Controllers

We have extensive experience in managing incidents and will guide you through all stages of a data breach.

We adhere to official guidance from:

- The New Zealand National Cyber Security Centre (NCSC)
- The New Zealand Government's Coordinated Incident Management System (CIMS)
- The Ministry of Justice (MoJ)
- Australia New Zealand Forensic Science Society (ANZFSS)
- International Association of Computer Investigative Specialists (IACIS)

6. Forensic Technology Experts

Our forensic technology experts have responded to a large number of data breaches across a wide range of issues, such as insider theft, business email compromise and ransomware.

We use leading forensic hardware and software to collect, examine and report on your electronic evidence requirements. Our offering includes computer forensics and eDiscovery (including cloud hosting).

Our expertise helps you determine the extent of the compromise so you can target your notifications and avoid causing unnecessary concern to those that may not be affected.

We have significant experience in providing expert witness reports and in delivering expert witness testimony at trial.

7. Specialist Data Breach Software

We use advanced forensic software to examine the source of the compromise and the extent that confidential information has been breached. We specialise in finding Personally Identifiable Information (PII) using tools such as Nuix and Magnet Axiom to locate Passports, Drivers Licences, and other sensitive information, that if breached, may lead to serious harm.

RECOVER

8. Mandatory Notifications

Our Data Breach Notification services are compliant with the NZ Privacy Act 2020 and will assist you in determining:

- Whether your data breach constitutes "serious harm" and requires mandatory notifications
- When and how to notify your customers
- Who should notify your customers and what to tell them?

We can manage your entire breach notification process. Our team are trained to:

- Produce notifications via email tracking tools, a tailored website, or by physical mail
- Process large volumes of emails including standardising email addresses and deduplication
- Providing reports showing the results of the notification process
- Providing direct support to answer customers queries via our contracted call centre

9. Ongoing Monitoring

We use leading technology to search the 'Dark Web' for credential compromises, the Open Web and Social Media for your 'Brand Reputation' as well as Credit Monitoring.

Dark Web Monitoring

Cyber-criminals are increasingly offering compromised information for sale on the Dark Web, which in turn can be used to launch an attack on your information systems. Our Dark Web Monitoring service detects compromised credentials in real-time and notifies you immediately when these critical assets are compromised, minimising the risk of them being used for identity theft, data breaches, or other crime. Our Dark Web Monitoring services uses human & machine intelligence to shine light on the Dark Web including:

- 640,000+ botnets
- Hidden chat rooms
- Unindexed, private and black market sites
- Peer-to-peer (P2P) networks
- IRC (internet relay chat) channels
- Social media platforms

Social Media Monitoring

We offer a comprehensive social media monitoring service to identify any published information that may require brand management. We combine our incident response and forensic expertise to pin-point data from over one billion sources across the web daily, including press articles, review sites, forums, and blogs.

Credit Monitoring and Reporting

We can assist in arranging credit monitoring and reporting via our partnership with New Zealand's leading information management portal. Credit information can affect how companies treat your customers, for example when they want to borrow money or get insurance. Reports typically include payment history for credit cards, mortgages, car finance and hire purchases.

10. Reliable Resources

Subscribe to our Alerts, Bulletins and view our resources to keep up to date with the latest threats in order to reduce your cyber risk. Keep up to date by visiting and subscribing to the following:

Alerts and Tips

The Alerts and Tips published by Incident Response Solutions are intended to be a high-level summary containing some of the most important information that has been published on Forensic and Cyber Security matters as it comes to hand.

NZ Incident Response Bulletin

The NZ Incident Response Bulletin is a monthly high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month. Each Bulletin also includes a section of our own content, based on a trending theme.

Incident Response Resources

Visit our Incident Response Resources web page to obtain free useful guides and references to assist you in a wide range on incident response activities.

Incident Response Retainer

With our Incident Response Retainer, you can take comfort knowing that when you need us, you will quickly have access to Incident Response experts, along with a comprehensive network of associated professionals. We can tailor a plan to meet your requirements, including the following:

- A welcome pack and initial consultation to explain how to maximise the service
- Access to a panel of experts who are ready to help
- Support desk for ad-hoc queries
- Our monthly forensic and cyber bulletin
- Yearly forensic readiness assessments
- Yearly assistance in drafting or revising your cyber incident response plan
- Board briefing packs and deep dive presentations
- Access to our incident response service desk tool for managing incidents
- Facilitation of a yearly cyber incident tabletop simulation
- Discounted rates on our forensic technology expert services

To find out more, please give us a call, send us an email, or visit our website.

Incident Response Solutions
Plaza Level
41 Shortland Street
Auckland 1010
New Zealand

Phone	0800 WITNESS or 021 779 310 (24 Hour Support)
Email	support@incidentresponse.co.nz
Website	https://incidentresponse.co.nz

Incident Response
FORENSIC & CYBER

INCIDENT RESPONSE SOLUTIONS