

# Incident Response Retainer



**We help you Prepare, Respond  
and Recover from Forensic and  
Cyber Incidents**



**Incident  
Response**

FORENSIC & CYBER

# How we help you

We can help you at any stage during your time of need. As there is no magic formula for technology, we've made it a little easier for you by creating this handy little guide to help us explain...

PREPARE



### Strategy and plans

We develop and improve **incident response plans**, we can also help with your security strategy and policies.



### Testing through simulations

Using forensic and cyber experts, we facilitate robust **tabletop exercises** to test and **improve** your incident response plan.



### Panel of experts

We establish a suitable panel of **experts** including a breach coach, forensic, security, legal and public relations specialists who are **ready to assist** in your time of need.

RESPOND



### Forensic technology expert witness

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



### Electronic investigations and eDiscovery

We love finding needles in haystacks, using our **analytical** and **investigative** techniques to a **Forensic standard**. Our **eDiscovery expertise** is also recognised by the Courts.



### Risk mitigation

We help you to **identify**, **contain** and **eradicate** risks from your business, e.g. if a staff member has stolen your IP, we can wipe it from their electronic devices and cloud storage.

RECOVER



### Return to business as usual

You may require **data breach notification** services, assistance with your **cyber insurance** requirements, or general security **recommendations**.



### Post-incident review and improvement plans

Following an incident, we **evaluate** your response to **correct** any weaknesses and **build** on your strengths.



"I don't think we've even seen the tip of the iceberg. I think the potential of what the internet is going to do to society, both good and bad, is unimaginable."

David Bowie in 1999

"I don't think anything is getting better, that much is pretty clear."

Troy Hunt - Security researcher who maintains  
'Have I Been Pwned?'

"The knock-on effect of a data breach can be devastating. When customers start taking their business elsewhere, that can be a real body blow."

Christopher Graham, former Information Commissioner, UK

"In the very near future, cybersecurity exercises are going to be absolutely expected of all companies by regulators."

Michael Vatis, founding Director of the FBI's National  
Infrastructure Protection Centre, USA

## Thinking Ahead. Being Prepared

In October 2018, the New Zealand National Cyber Security Centre (NCSC) published the results of its survey of 250 nationally significant organisations.

### Key findings include:

- i. An area of good practice that was identified is:  
**Readiness – Preparing the organisation to detect, respond and recover from a cyber-security incident.**
- ii. When an organisation becomes aware of an incident, being **ready** to respond can **reduce** its impact of a compromise.
- iii. Having an **up-to-date plan** allows an organisation to react **quickly and decisively** when an incident occurs and serves as a framework to **preserve evidence** in the event legal action is sought following an incident.
- iv. 63% of New Zealand's Nationally Significant Organisations have an incident response plan, but 33% have not **tested their plan** in the last year.

*We are proud to be a 100% New Zealand  
owned and operated business.*

## Our Incident Response Retainer

When dealing with your health, you know in advance who your Doctor is.

For Forensic Technology and Cyber Security matters, you should also have a professional provider on an **0800 Speed Dial**.

With our Incident Response Retainer, you can take comfort knowing that in your time of need, you will quickly have access to Incident Response experts, along with a comprehensive network of associated professionals.

---

### Retainer options

1. *A welcome pack and an initial consultation to explain how to maximise the service*
2. *Access to a panel of experts who are ready to help*
3. *Support desk for ad-hoc queries (up to 30 mins per month)*
4. *Our monthly Forensic and Cyber Bulletin – Premium Edition*
5. *Yearly forensic readiness assessment to prepare*
6. *Yearly assistance in drafting or revising your cyber incident response plan*
7. *Board briefing packs and deep dive presentations*
8. *Access to our Incident Response Portal and suite of Ops tools for managing incidents*
9. *Facilitation of a yearly cyber incident tabletop simulation*
10. *Discounted rates on our forensic technology expert services*

### Benefits to you



*24/7 on call support*



*Forensic collection and  
examination of data*



*Faster outcomes during  
your crisis*



## **#1 - A welcome pack and an initial consultation to explain how to maximise the service**



We know that you significantly invest in and rely on technology to serve your users and facilities. You don't need us to tell you that information security should therefore be a critical function within your organisation.

We also know that you face targeted cyber-attacks, and that these are only going to increase in frequency and intensity. When faced with a need to respond to an incident, you will occasionally require extra assistance.

We differ from other security providers as we are forensic experts with a long-established proven track record in responding to actual incidents.

We are here to help you prepare for, respond to and recover from an incident.

## #2 - Access to a panel of experts who are ready to help



Our panel is comprised of experts from Incident Response Solutions and our wider network of specialists.

Incident Response Solutions forensic technology and cyber security experts will be your initial points of contact when you require incident response support. We will facilitate the activation process in the event of an incident and provide ongoing support. We will then confirm your requirements with you, record the scope of work and provide an estimate of costs. We will only proceed on your written approval.

Where required, we will assist you in locating available specialists from the panel.

### #3 - Support desk for ad-hoc queries



The Retainer provides you with occasional ad-hoc support. Simply call or email us and we will endeavour to answer any queries you may have.

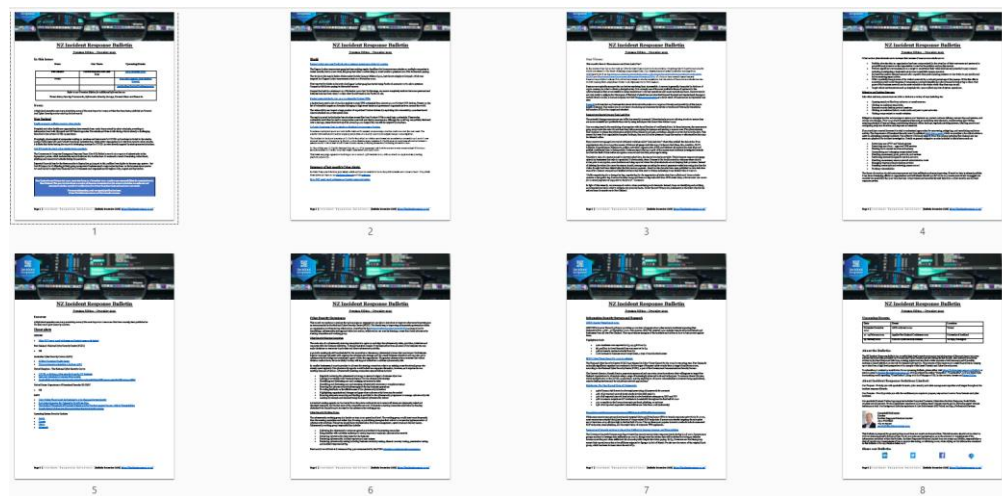
This service is provided on a best endeavours approach. Please note that additional time or expertise may be required to answer queries to your satisfaction. We will notify you of any additional time and expertise required to answer your query.



## #4 - Our monthly Forensic and Cyber Bulletin – Premium Edition



**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.

We will give you a brief summary of each article and a link to more information. Why do we publish this bulletin? To keep you up to date with the latest forensic and cyber security news, so that you aren't caught by surprise – and so that you will know about risks and changes before they become problems.

<https://incidentresponse.co.nz/bulletin>

## #5 - Yearly forensic readiness assessment

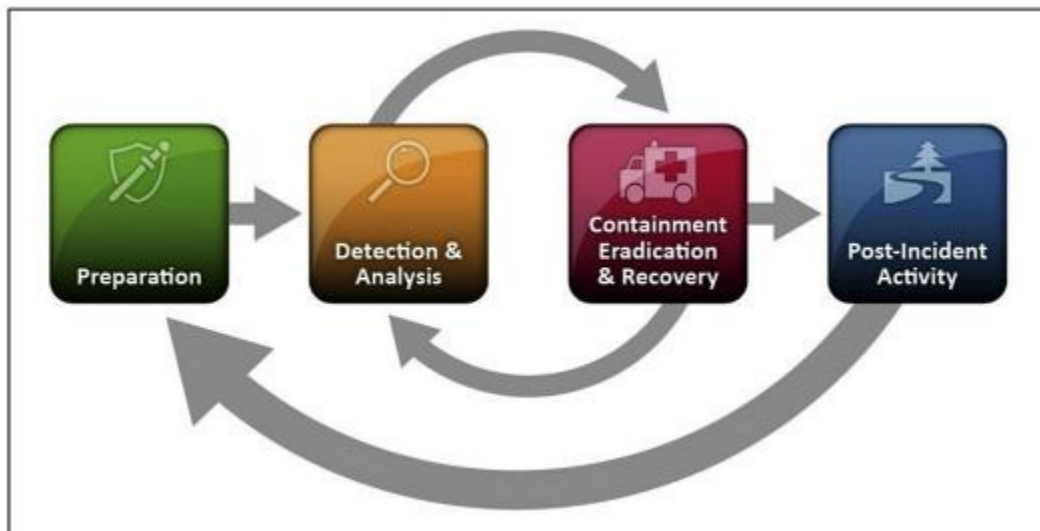


From our experience having worked on numerous and complex incidents, we have a deep understanding of what steps are required to work through an incident.

Our forensic readiness assessment evaluates the following:

- Identification of critical digital assets
- Logging and detection technologies
- Ability to contain an incident
- Evaluation of first response capabilities
- Forensic collection requirements
- Recommendations for areas of improvement

## #6 - Yearly assistance in drafting or revising your cyber incident response plan



Referencing the SANS Institute "Information Security Reading Room Incident Handler's Handbook" and the NIST "Computer Security Incident Handling Guide", we will review or draft your current 'Cyber Incident Response Plan'.

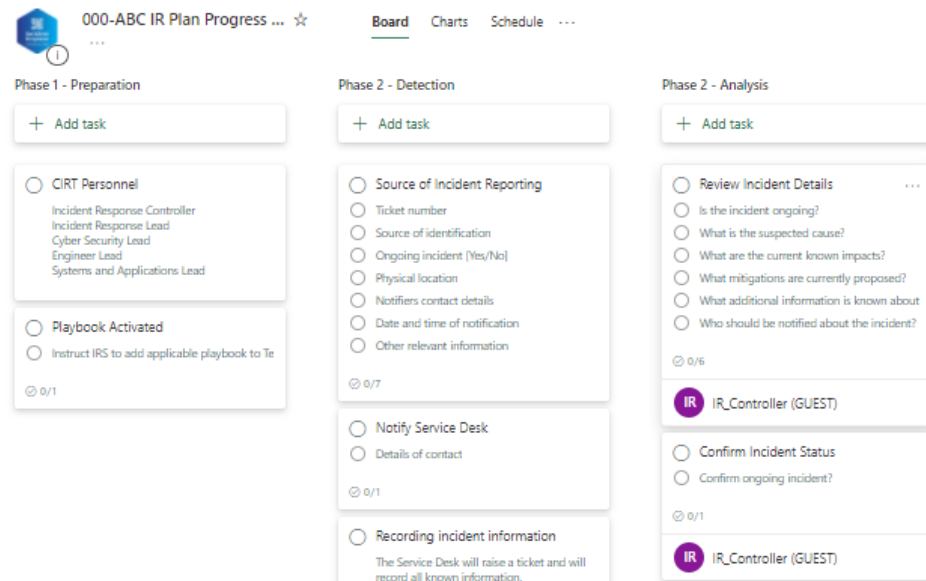
## #7 - Board briefing packs and deep dive presentations



We will review any cyber related content within your board briefing packs and provide feedback.

We will also attend, either in person or by conferencing, meetings to present a deep dive on a cyber topic of your choice.

## #8 - Access to our Incident Response Portal and suite of Ops tools for managing incidents



Should an incident occur, if required we will provide you with access to our suite of Ops tools which include

- Incident Service Desk
- Electronic Task Boards loaded with IR Plans and Playbooks
- Dark Web Monitoring
- Social Media Monitoring
- Credit Monitoring
- and more



## #9 - Facilitation of a yearly cyber incident tabletop simulation



A cyber incident simulation evaluates your organisation's level of preparedness both from an executive and technical perspective.

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.

## #10- Discounted rates on our forensic technology expert services



We specialise in the collection and examination of data from a wide variety of sources e.g. laptops, desktops, servers, mobile devices and cloud.

We adhere to global forensic standards and have the proven experience in applying advanced investigative and analytical techniques to help our clients solve their problems.

Acting as an expert witness, we specialise in electronic investigations, cybercrime incident response and eDiscovery matters.

Campbell McKenzie is recognised by the District and High Courts of New Zealand as a forensic technology expert and has also been appointed as an independent expert by the High Court.

Thank you

**Campbell McKenzie**

0800 WITNESS

[campbell@incidentresponse.co.nz](mailto:campbell@incidentresponse.co.nz)

[incidentresponse.co.nz](https://incidentresponse.co.nz)

We help you Prepare, Respond and Recover  
from **Forensic** and **Cyber** Incidents

