IT | PARTNERS

INCIDENT RESPONSE GUIDE

Cyber incidents happen. Even with the best prevention measures in place, no business is immune. That's why being prepared to respond is just as critical as your efforts to protect.

A well-structured Cyber Incident Response Plan gives your team the tools and confidence to act quickly, reduce downtime, and minimise the overall impact of an attack.

Based on real-world experience, here are some key elements to consider when building or refining your response strategy.

How to start & what to consider

First, it's important to recognise that Incident Response Planning is not a one-time task - it's an ongoing, iterative process. If you haven't started yet, the most valuable step you can take today is to initiate the conversation within your business.

Before diving into specific steps to take during an incident, start by identifying who you would contact in the event of a cyber incident. Next, build a solid baseline by taking stock of your technical environment and understand your existing technical debt by mapping out your application landscape. Which systems are business-critical? How do they integrate and interact? Our Application Landscape Guide can help you build a clear and holistic view of your environment.

From there, turn your attention to the different phases outlined in this document. This guide offers a glimpse into how we guide clients through this process, helping them build resilience and confidence in the face of cyber threats.

High Level Process Overview

Prepare

Develop and implement incident response policies, procedures, and tools. Train the incident response team, who's key roles are outlined in the next section, and conduct regular exercises to ensure operational readiness. Ensure all necessary resources, including hardware, software, and communication channels, are available and functioning effectively.

Detect, Investigate, Analyse & Activate

Monitor systems and networks for signs of incidents using various detection tools and techniques. Analyse alerts and logs to confirm incidents and determine their scope and impact. Document findings and gather evidence for further investigation.

Contain, Collect Evidence & Remediate

Implement short-term and long-term containment strategies to prevent the incident from spreading. This may involve isolating affected systems or networks. Then identify and remove the root cause of the incident, such as malware or unauthorised access. Ensure that all traces of the threat are eliminated.

Recover & Report

Restore affected systems and services to normal operation. This may involve restoring data from backups, applying patches, and conducting thorough testing to ensure that systems are secure and functional.

Learn & Improve

Conduct a thorough review of the incident and the response actions taken. Perform a root cause analysis to identify underlying issues and implement corrective measures. Update incident response plans, policies, and procedures based on lessons learned. Share findings with relevant stakeholders and provide additional training if necessary.

Communication

Internal communications during a cyber security incident should clearly outline the situation, business impact, response actions, and how personnel can assist while ensuring business continuity. External communications should address the needs of customers, stakeholders, and regulatory bodies, detailing affected systems, response efforts, available support, and expected timelines tailored to the recipients' role. Both communication streams should include clear contact points and support information where appropriate.

Process Example: Phishing Attack

Prepare

- Conduct regular phishing awareness training and simulated phishing campaigns.
- Ensure MFA (multi-factor authentication) is enforced for all systems.
- Maintain up-to-date email filtering, domain reputation, and anti-spoofing (e.g. SPF, DKIM, DMARC).
- Define a rapid escalation path for suspected phishing reports.
- Keep IR playbooks and communication templates for credential-based phishing updated.

Even with strong controls in place, no business is immune to human error. Here's an example of a common phishing scenario that highlights how easily a breach can begin: A staff member receives a convincing email from what appears to be the company's HR system, prompting them to "log in" to review updated leave policies. The link leads to a fake login page and captures their credentials.

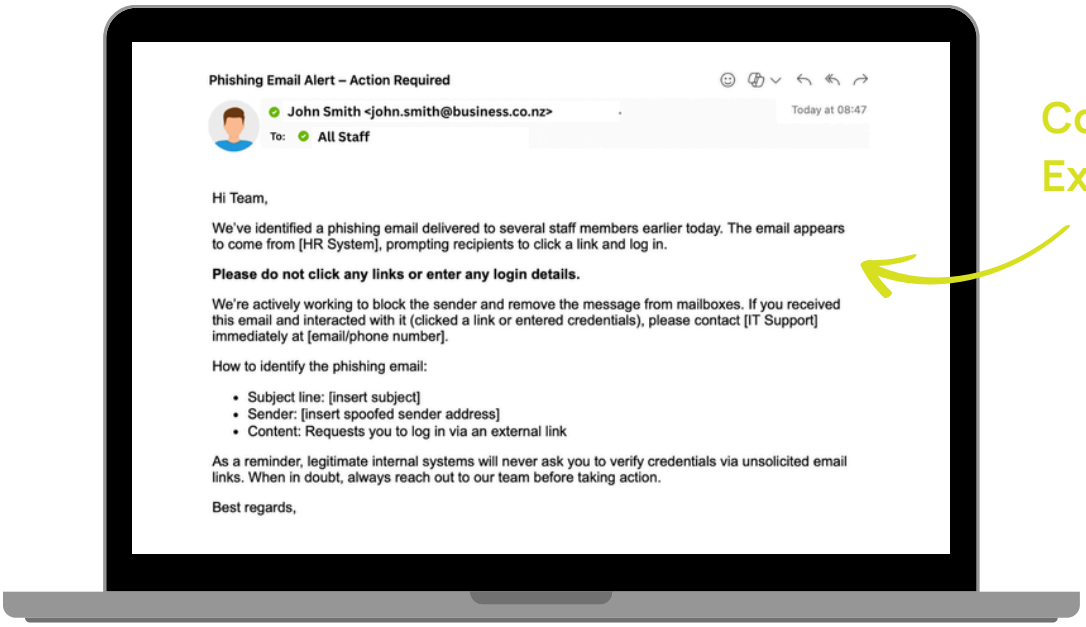
Detect Email user reports suspicious link to IT. Following this, IT identifies other recipients of the email using mail logs. Unusual login attempts are flagged from offshore IPs.

Contain Immediate password reset for affected user(s). Disable any active sessions. Block the malicious domain in email gateway, firewall and DNS systems

Eradicate Confirm no other accounts accessed. Search SIEM and endpoint logs for other indicators of compromise (IoCs).

Recover Educate affected user on phishing awareness. Confirm MFA is enabled. Restore any altered mailbox rules or settings.

Learn Update email filters. Include scenario in future phishing simulation. Brief executive team and update comms templates.



Communication Example

Key Roles

These roles and responsibilities ensure a comprehensive and coordinated approach to incident response, enabling businesses to effectively manage and mitigate the impact of incidents, making up the Incident Response Team (IRT).

Incident Response Commander (IRC)
Leads the incident response team, makes critical decisions, coordinates response efforts, and communicates with stakeholders.

Communication Coordinator
Manages internal and external communications, provides updates to stakeholders, and ensures clear and consistent messaging.

Legal Advisor
Provides legal guidance on incident response actions, ensures compliance with regulations, and handles legal aspects of the incident.

Financial Advisor
Provides financial guidance on incident response actions. Ensuring visibility on the financial implications of the effects of the incident and response activities are considered.

Public Relations Officer
Manages public communications, handles media inquiries, and maintains the business's reputation during and after the incident.

Technical Security Lead
Directs the technical response and integrates threat intelligence to guide detection, containment, and recovery while ensuring actions are accurate, documented, and compliant.

Incident Responder
Provides technical support to the incident response team, assists with system recovery, and ensures the availability of necessary tools and resources.

Human Resources (HR)
Manages employee-related issues during incidents, provides support to affected staff, and ensures adherence to HR policies.

Core Questions for IR Planning

To ensure your business is prepared to respond effectively to a cyber incident, consider the following key questions:

- [ ] Who is responsible for coordinating the incident response?
- [ ] Has an Incident Controller been formally appointed?
- [ ] Where will the response team convene during an incident?
- [ ] Is there an alternative location or virtual "war room" if the primary space is unavailable?
- [ ] Is the list of key internal and external contacts up to date?
- [ ] Have we pre-developed scripts for:
  - [ ] Internal communications during likely scenarios?
  - [ ] External communications for clients, partners, and stakeholders?
- [ ] Have we conducted a response simulation or tabletop exercise:
  - [ ] With the senior management team?
- [ ] What are our most significant risks?
- [ ] Are there known areas of technical debt?
- [ ] Could insider threats pose a concern?
- [ ] What controls or strategies are currently in place to mitigate these risks?
- [ ] How are our systems interconnected, and could a single point of failure impact multiple services?

Building Confidence Through Preparedness

Cyber incidents are an ever-present risk, but they are manageable with the right planning, structure, and mindset. A strong incident response capability is not just about tools or procedures - it's about creating a culture of preparedness, clarity, and collaboration across the business.

This guide has outlined the essential components of a mature incident response strategy:

- ✓ Clear roles and responsibilities across the business
- ✓ Defined processes for detecting, containing, and recovering from incidents
- ✓ Strong internal and external communication practices
- ✓ Regular testing and continuous improvement to keep your response relevant and effective

Whether you're just starting or refining your approach, the most important step is to keep the conversation active and evolving.

If you're unsure where to begin, start with:

1. Mapping your critical systems
2. Confirming your key contact list
3. Running a tabletop exercise

And remember: incident response is not just an IT issue. It's a shared responsibility that protects your people, your operations, and your reputation.

Let's build resilience, together.

IT | PARTNERS

Making Each Day Better Through Technology

GROWING NEW ZEALAND'S PRODUCTIVITY AND PLACE IN THE WORLD

IT Partners are more than just your IT support team; we're your business partner, and we are here to challenge you to think differently, improve outcomes, and help manage business risk.

We're mid-market experts working with companies headquartered in or around the Waikato. With specialist knowledge in digital transformation, systems operations, cyber security, business analysis and strategic thinking, we will work with you to deliver a technology roadmap that aligns with your business objectives.

www.itpartners.co.nz

Panama East
469 Grey Street
Hamilton, 3216

07 957 2650

hello@itpartners.co.nz