PROTECT+/ kinetic IT

# CYBER SECURITY
# INCIDENT RESPONSE SUCCESS

Effective cybersecurity incident management ensures your people are prepared and empowered to respond to even the most sophisticated of cyberattacks. A comprehensive incident management capability involving the right people, processes, tools and standards should give you the confidence that your business and your data are secure and protected.  In addition to addressing potential risks and threats to your ICT systems, your organisation's incident management plan should incorporate overall business requirements to ensure informed and contextual decisions underpin the containment and eradication of threats, and the recovery and restoration of information and systems.  We also recommend you adopt a comprehensive cyber security training and education program to increase your employees' cyber security awareness and strengthen the effectiveness of your organisation's incident response capability.

YOUR **PEOPLE**

YOUR **DATA**

YOUR **BUSINESS**

YOUR **CONFIDENCE**

YOUR **AWARENESS**

**PREPARATION** | **DETECTION AND ANALYSIS** | **CONTAINMENT AND ERADICATION** | **RECOVERY** | **POST INCIDENT ACTIVITIES**

## +NIST FRAMEWORK

The National Institute of Standards and Technology (NIST) provides industry standards and guidelines to assist public and private sector organisations in protecting their data and information systems. For effective Incident Response practices, Kinetic IT adopts and endorses the application of the globally-recognised NIST Cybersecurity Framework in conjunction with other industry security frameworks including ISO 27001 and the Australian Cyber Security Centre (ACSC) Essential Eight. **Find out more here.**

## YOUR PEOPLE

Your people are your organisation's first line of defence. Strengthen your resilience by building their cyber awareness capabilities and clarifying your incident response protocols.

## YOUR DATA

Protect your critical data first. Focus on securing your organisation's most sensitive and high risk data as a priority rather than trying to apply the same levels of protection to non-critical data.

## YOUR BUSINESS

Your organisation's incident response program should be dynamic and evolve with your business. As new technologies and working practices are adopted, your incident management plan should be updated.

## YOUR CONFIDENCE

A sound incident management program should include engagement plans for customers, suppliers, partners and subcontractors as well as employees.

## YOUR AWARENESS

Cybersecurity awareness training helps reduce the volume of security incidents you respond to, while educating crew and customers on good cyber hygenine and demonstrating commitment to keeping information safe from hackers.

## PREPARATION

## DETECTION AND ANALYSIS

## CONTAINMENT AND ERADICATION

## RECOVERY

## POST INCIDENT ACTIVITIES

Incident response preparation is crucial in ensuring the business swiftly and confidently handles any kind of digital or physical threat. Preparation includes stakeholder engagement plans, reporting mechanisms, tracking systems, war room establishment, digital forensics planning, and digital evidence gathering tools.

## YOUR PEOPLE

Everyone in your organisation is a possible target. Ensure your people know how to identify a cyber attack and what actions they must take to escalate for action.

## YOUR DATA

New technologies and ways of working will result in different network and system activity profiles. Recognising these new profiles will enable you to apply more targeted data protection mechanisms.

## YOUR BUSINESS

Threats from hacking and phishing damage businesses every day. The earlier your organisation can identify, contain, eradicate and return to normal operations, the faster you can restore your stakeholders' confidence.

## YOUR CONFIDENCE

It's important to be aware of your suppliers, partners and contractors threat detection and response processes to ensure they are adequete and aligned to your own organisation's processes for targetted cyber attacks.

## YOUR AWARENESS

Consider your organisation's supply chain as an extension of your own business and educate them on how they can better detect and respond to incidents and the criticality of informing your business of notable events.

PREPARATION

**DETECTION AND ANALYSIS**

CONTAINMENT AND ERADICATION

RECOVERY

POST INCIDENT ACTIVITIES

Detection is only possible when the attack vectors are understood and your incident response team has the tools and telemetry to identify and validate threats targeting information or data assets. Detection capabilities include intrusion detection and prevention systems, antivirus software, and threat intelligence and response tools such as a Security Information and Event Management (SIEM) system. Analysis includes disciplines such as network and system profiling, behavioural analysis, log analysis, event correlation, and machine learning.

## YOUR PEOPLE

In the event of a breach, timing is critical. Your people should be aware and capable of undertaking immediate containment or risk mititgation activities before reporting the incident to your cyber security team.

## YOUR DATA

Information and data assets are targets for cyber attacks. Correspondingly, your organisation's incident response program, including threat management, incident detection, containment and eradication, should be data-driven.

## YOUR BUSINESS

Your organisation's service management team should be able to differentiate between high priority incidents and major incidents and apply the correct triage and containment processes to quickly mitigate further risk.

## YOUR CONFIDENCE

Patient threat actors hide in target systems for weeks or months before attacking. Use threat hunting to detect digital evidence of hidden threats that would otherwise go unnoticed.

## YOUR AWARENESS

Incident responders should be educated on how to execute your organisation's incident response process during a crisis. Tabletop exercises and cyber drills will ensure they have practical experience using your systems come crunch time.

PREPARATION

DETECTION AND ANALYSIS

**CONTAINMENT AND ERADICATION**

RECOVERY

POST INCIDENT ACTIVITIES

Containment is the process of stopping an incident from escalating before it can cause more damage or overwhelm your incident response team's capacity. The aim of the containment phase is to provide your team with adequate time to tailor the remediation strategy. After containment, eradication eliminates the threat from your systems to restore them to a clean state.

## YOUR PEOPLE

Effective and efficient recovery from an incident involves many stakeholders across the business. Your people should understand their individual or team's roles, responsibilities and requirements in your organisation's business continuity plan.

## YOUR DATA

Recovery of critical business data over transient data should be prioritised and this should done in consultation with the approproate business stakeholders. Recovery processes should focus on data integrity and availability and ensure no further possibility of compromise.

## YOUR BUSINESS

A company-wide cyber attack is highly complex and an effective recovery program requires collaboration between your organisation's security team and business stakeholders to identify and prioritse recovery activities.

## YOUR CONFIDENCE

Incident managers should be experienced in handling a varity of cyber incidents and possess the communicartion skills required for effectivly handling enquiries from external stakeholders e.g. regulators, the media, and supply chain.

## YOUR AWARENESS

Incident response training should be extended to a large contingent of staff members across the business, making sure the material is contextual, relevant and appropriate to their roles and responsiblities.

PREPARATION

DETECTION AND ANALYSIS

CONTAINMENT AND ERADICATION

**+RECOVERY**

POST INCIDENT ACTIVITIES

In the recovery phase, systems are restored to normal operation and information assets are recovered from backups or offline storage to ensure users can return to work. Containment and eradication is closely related to the recovery stage (they are combined under NIST) and should be carried out in a phased approach so that remediation steps are prioritised and recovery steps are dependent on the threat being eradicated.

## YOUR PEOPLE

A strong cyber security culture is built on trust, honesty and respect. Your people must be encouraged and feel confident to participate in incident investigation and analysis activities without fear of retribution.

## YOUR DATA

Your organisation's incident response team must be capable in effectively handling investigation artefacts including digital evidence and chain of custody records.

## YOUR BUSINESS

Business stakeholder participation in post-incident activities is recommended as they often provide contextual insight and strategic direction beyond technical solutions for service improvements.

## YOUR CONFIDENCE

Following an incident, your organisation may be criticised by customers, government departments (OAIC) and the media. How you respond to the incident and how you commit to improvements afterwards will define your ability to recover from public scrutiny and loss of confidence.

## YOUR AWARENESS

Providing annual incident response refresher training demonstrates your commitment to keeping your organisation and its stakeholders safe and ensures you can effectively respond to even the most sophisticated of attacks.

PREPARATION

DETECTION AND ANALYSIS

CONTAINMENT AND ERADICATION

RECOVERY

**POST INCIDENT ACTIVITIES**

One of the most important elements of incident response is the post-incident review which allows identification of learning and improvement measures to reduce the likelihood or impact of a similar incident in the future. Reviews should engage key business stakeholders and occur immediately after a major incident and/or examples of smaller but frequent incidents, with key lessons learned and identified improvement measures to be included in your organisation's continual service improvement plan.