INCIDENT MANAGEMENT.

BE RESILIENT, BE PREPARED.

NATIONAL CYBER SECURITY CENTRE
A PART OF THE GCSB

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

New Zealand Government

Incident Management: *Be Resilient, Be Prepared* sets out five key steps designed to help business leaders and cyber security professionals strengthen their organisation's ability to manage and respond to cyber security incidents.

This resource accompanies the NCSC's guidance on enhancing organisational cyber security governance[1].

[1] https://www.ncsc.govt.nz/guidance/charting-your-course-cyber-security-governance

Every year in New Zealand, hundreds of organisations are affected by cyber security events.

The impact and severity of these events is determined by the complexity of each incident, how rapidly it was detected, and the ability of the affected organisation to respond.

In a National Cyber Security Centre (NCSC) study[2], New Zealand's nationally significant organisations showed a need for greater focus on readiness. The NCSC has identified the ability to respond to incidents as a key cyber security readiness challenge for New Zealand organisations.

[2] https://www.ncsc.govt.nz/newsroom/nationally-significant-organisations-cyber-resilience-report-released/

Contents

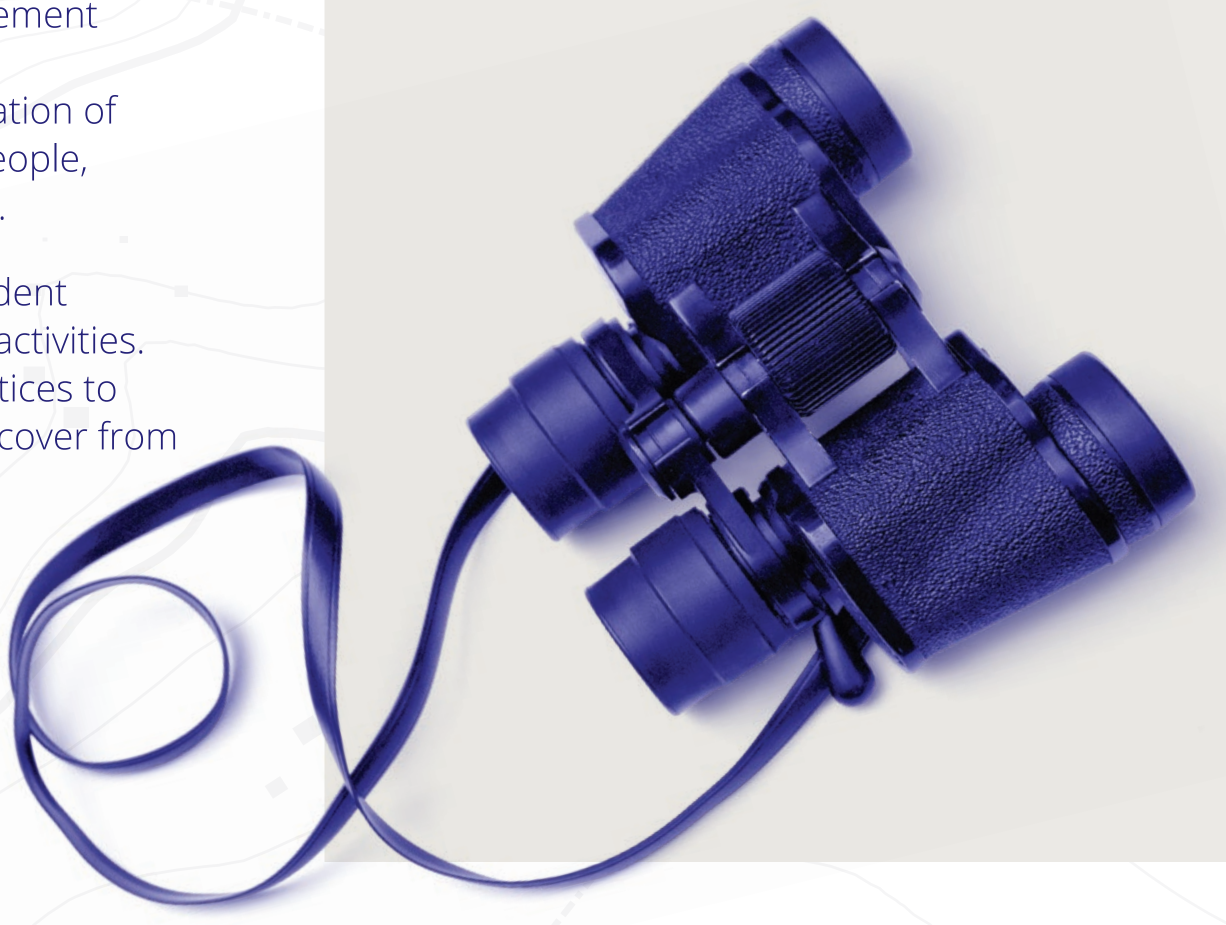
WHAT IS INCIDENT MANAGEMENT?

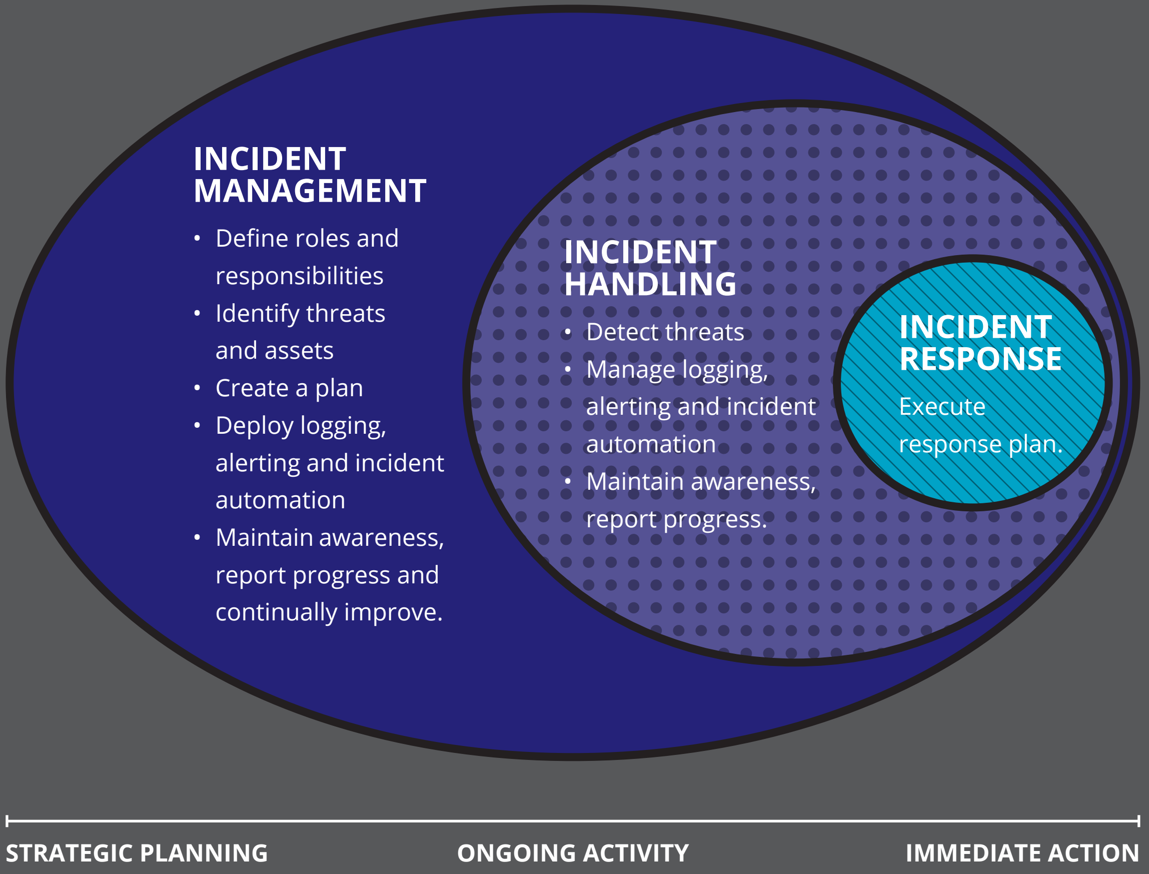
Incident management is the overall practice of managing cyber security incidents. Incident management involves the development, implementation and operation of capabilities that include people, processes and technology.

Incident handling and incident response are operational activities. These involve tactical practices to detect, respond to, and recover from cyber incidents.

Information systems are critical assets for most organisations. Jeopardising the secure operation of these systems, and the business processes they support, constitutes an unacceptable organisational risk.

The risk of a cyber security incident cannot be managed with preventative measures alone. A difficult but accepted reality in the cyber security profession is the unattainability of perfect prevention at an acceptable cost. Good frameworks recognise this and highlight detection and response as being fundamental to achieving cyber resilience.





INCIDENT MANAGEMENT

- Define roles and responsibilities
- Identify threats and assets
- Create a plan
- Deploy logging, alerting and incident automation
- Maintain awareness, report progress and continually improve.

INCIDENT HANDLING

- Detect threats
- Manage logging, alerting and incident automation
- Maintain awareness, report progress.

INCIDENT RESPONSE

Execute response plan.

Is your organisation ready?

Time is an important factor in determining the impact of an incident. The longer an incident lasts, the more likely it is to cause major disruption and inflict significant cost. The key to reducing the duration of an incident is prompt detection and response. Readiness is fundamental to efficient and effective incident management.

One readiness indicator is the preparation of an incident response plan. With a documented plan in place, an organisation can react quickly and decisively when an incident occurs. Every organisation should have an incident response plan and test it at least yearly to ensure it's understood and fit for purpose.

Only one third of organisations surveyed by the NCSC possessed and tested an incident response plan in the previous year. 41% of organisations were either 'mildly confident' or 'not confident' in their ability to detect a cyber intrusion.

Who is this guidance for?

Executives and business leaders can use this guidance to inform an assessment of their organisation's incident management readiness. This document describes the key elements of incident management, then demonstrates their application using a fictional scenario. For information security managers or those with some knowledge of incident management already, this guidance will help to reaffirm your understanding of the subject.

By reviewing and applying this guidance, organisations will be able to enhance their incident management capabilities, strengthen their cyber resilience, and enable:

- increased confidence when pursuing new business opportunities reliant on digital tools or processes;
- effective management of cost, disruption, and other impacts when an incident occurs, and:
- improved organisational robustness and an ability to respond to challenges.

Conversation Starters are highlighted throughout this document. These are designed to enable senior leaders to start useful conversations with specialists or responsible managers. Executives and boards may not play hands-on roles in most incidents, but it’s still their responsibility to understand incident management and ensure the capability is in place.

INCIDENT MANAGEMENT: THE FIRST FIVE STEPS

The first five steps are fundamental to establishing an incident management capability. They are the initial areas for an organisation to focus on when commencing this process. Taking these first steps will enable a foundational ability to identify, respond and recover from cyber security incidents.

Incident management capabilities and maturity levels vary widely between organisations. Two organisations of similar sizes may have differing approaches that reflect their risk appetites, business objectives and cultures. There is no simple one-size-fits-all process for incident management; each case is unique and requires continuous refinement.

STEP ONE

Define Roles and Responsibilities

During an incident, an organisation must know who needs to be involved, what their responsibilities are, and at what point in the process they should assist. Staff members should understand which actions they are authorised to perform and when to escalate an issue.

STEP TWO

Identify Threats and Assets

Every organisation must understand its assets and the potential threats these face. Assets—the services and information your business relies on—will be more vulnerable to some threats than others. Defining threat scenarios and doing so in a consistent way is fundamental to cyber resilience. Identifying threats and assets gives scope to your incident management programme.

STEP THREE

Have a Plan

At the core of effective incident management is a well-established and tested plan. This plan describes the actions required when something does go wrong, and details the resources needed to resolve the incident. Creating a plan should be the primary focus for improving incident management.

STEP FOUR

Logging, Alerting and Incident Automation

Rapid detection and response relies on having the right data. An architecture and capability to manage logs, events, alerts, and incidents should be defined. Identifying sources of data and determining their value ahead of an incident will expedite the processes of detection, containment, and remediation.

STEP FIVE

Maintain Awareness, Report Progress and Continually Improve

All organisations should maintain an ongoing programme of work to develop and improve incident management. Through a committed and continual process, even organisations with limited resources can steadily improve their capacities.

STEP ONE:

DEFINE ROLES & RESPONSIBILITIES

The speed and effectiveness of an initial incident response will be increased by clearly establishing who should perform which tasks, and when.

Incidents often arrive out of the blue and develop quickly, so it's necessary for those involved to have an immediate awareness of the situation and be authorised to quickly perform the correct actions. It's crucial to have a guide in place describing who can make key decisions on behalf of the organisation, and when issues need to be escalated.

Organisations may not have the resources to dedicate individuals or teams to specific incident management roles. In New Zealand, staff members often have many different tasks to perform. However, roles and responsibilities should still be defined, even if they are additional to other duties. If an organisation relies on outsourced IT services, clarify and make explicit any assumed role and responsibility performed by a third party. The most effective way to do this is by capturing them in a RASCI chart. The process of defining a RASCI (Responsible, Accountable, Supporting, Consulted, and Informed) is explained in the NCSC's Cyber Security Governance Guidance[1]. Key roles you should consider are listed in this section.

CONVERSATION STARTERS:

- When will the leadership team be informed if a cyber incident has occurred?
- What are the thresholds for notifying different stakeholders?
- Who is involved in our organisation's cyber incident response?
- Who will lead the coordination and response?
- What authority does the incident manager require to effectively respond to incidents?

[1] https://www.ncsc.govt.nz/guidance/charting-your-course-cyber-security-governance

Key Incident Management Roles

Primary Contact

The initial contact for any suspected security incident, whether it's reported from outside the organisation, by a staff member, or by a dedicated detection capability. This point of contact needs to be clearly defined and communicated within the organisation. Typically an email contact for this role is also published on the website and a phone number is communicated to all staff. Ideally there should also be an after-hours contact method.

Incident Manager

The escalation process is covered in the incident response plan but there needs to be a clear understanding of who manages an incident. The incident manager coordinates response and recovery activities. In a smaller organisation this role might be shared between several people, or there might be a roster system to designate who is responsible after-hours. The incident manager doesn't necessarily have to be a cyber security expert; they need to be able to coordinate the response and ensure there's a single person with a complete situational view. For ongoing incidents, this role may be passed from one person to another to provide staff with breaks and a chance to rest.

Technical Specialists

It is important that technical specialists for the different business areas are designated, since they may be vital in helping to identify and communicate what has occurred during an incident. This includes roles such as infrastructure engineers, network specialists and software developers.

Business Services Owners

The owners of business services delivered by the organisation should be identified. If an incident occurs the service owners will often be required to make decisions about changes to the availability or configuration of their services, and they will have the best understanding of potential business impacts.

Communications Lead

Even small organisations should nominate a person who can manage communications. External communications tasks should be limited to the authorised staff. In a major incident this responsibility may include communications with customers and the media. Ensuring that this point of contact has been identified and has knowledge of media handling is very important.

Third Parties and Service Providers

Many organisations utilise service providers (including cloud service providers) or outsourcing partners. These may well be central to the management and response of any incidents, depending on the scope of their services and support. It is vital to understand how to contact them, what their obligations are, and what response time is expected. The right support contracts should be in place to receive the assistance required.

Privacy

The issue of privacy is increasingly being scrutinised, and many New Zealand organisations have a nominated or dedicated privacy lead. If an incident involves personally identifiable information it is important that a member of staff manages the privacy implications. This includes ensuring relevant legislation is adhered to (for example, the Privacy Act), the correct authorities are informed, and impacted individuals are appropriately notified.

Legal Counsel

Smaller organisations may not employ an in-house legal counsel but they usually have an agreement with an external agency. In any case, there must be a representative to assist with any legal queries as part of incident response. These tasks may include evidence gathering or disclosure requirements, through to management of third parties to assist with incident response. In many organisations the legal team will also advise on interactions with suppliers, such as insurance providers.

Insurance Provider

It is increasingly common for organisations to include some level of cyber security cover in their insurance policies. Understanding when and how to engage the insurance provider is critical because there are often conditions and requirements on invoking insurance claims. Some insurance policies list pre-approved vendors you must use for incident response. This engagement strategy can have a significant impact on how an organisation responds to an incident, and what they can communicate about the incident. It is often important to decide early on in an incident whether an insurance claim will be made or not, as this decides whether an insurance provider will need to be involved.

Crisis Management

Some organisations have crisis management teams, especially if they deal with human safety or are involved with national or local response services. In these cases, if an incident escalates it may be necessary to engage the crisis management teams to coordinate activities. If the contacts and methods of engagement have been defined beforehand it will make this process significantly easier in the event of a major incident.

Escalation Contacts

There should be clarity around escalation contacts if any of the designated response team members are not contactable. Incidents may occur after hours, or an incident could impact remote working or calling capabilities that make it impossible for the primary contacts to provide the right support. In these situations it must be clear who has the authority to act on behalf of the primary contacts and step into the appropriate roles.

External Support

If an incident escalates to a level where the organisation lacks the capability to manage it appropriately, it is important to have defined the escalation points for external support. This may be a government organisation such as the National Cyber Security Centre (NCSC) or the Computer Emergency Response Team (CERT NZ) but could also include non-government specialist incident response teams. Notably, if forensic analysis is required, specialist teams should be engaged as soon as possible.

> “The New Zealand Information Security Manual (NZISM) states: *Agencies MUST detail information security incident responsibilities and procedures for each system in the relevant Information Security Documents. (7.3.5.C.01).*”

STEP TWO:

IDENTIFY THREATS AND ASSETS

Understanding the threats to an organisation's assets and services is fundamental to effective incident management. When these are known, it's possible to plan and prioritise the most likely threat scenarios. Without this knowledge, an organisation's plan may be too broad and contain insufficient detail to be actionable.

Workshops are an effective way to determine what is important to the organisation and what might go wrong. Attendance at workshops should include those who understand the wider business, such as the leadership team and service owners, not just IT or security teams.

Focus first on understanding what is most important to the organisation and identifying its key assets and services, from the perspective of each participant. These assets need to be matched against a list of common threats to define the threat scenarios for which the organisation will prepare.

Unlike the process of identifying assets, defining common threats may require some preparation and research but there is no need to aim for perfection at first; rigour and structure can be built over time.

CONVERSATION STARTERS:

- What are the assets and services most critical to the ongoing operation of the business?
- What is the business impact of a disruption or compromise of these assets or services?
- How does our understanding of the assets and threats relate to our business continuity and disaster recovery planning?
- What are the biggest cyber security threats to the organisation and how is the organisation prepared to protect, detect and respond to these threats?
- Are the threats detailed in scenarios and prioritised in order of impact to the organisation?

Identify Your Assets

Start by understanding what business information or services a system holds, communicates or facilitates. A common way to capture this is in a service relationship model. After this is established, work out the relative priority of systems and identify who in the business is responsible for them. Finally, each asset's physical and logical location needs to be determined, including any cloud services or hosted environments.

These steps are necessary for good incident management because they enable:

- understanding of potential business impacts during an incident;
- prioritisation of response activities based on business need;
- a better awareness of dependencies between business services and information assets;
- a more detailed awareness of the sensitivity and availability requirements of data associated with certain assets;
- the definition of criticality levels to direct prioritisation during a response;
- identification of dependencies between assets, such as network connectivity, third parties, and cloud service providers.

> The PSR's INFOSEC1 states: *Identify the information and ICT systems that your organisation manages. Assess the security risks (threats and vulnerabilities) and the business impact of any security breaches.*

Know Your Threats

A vast amount of information is available on current cyber security threats. The difficulty is understanding which threats are the most important and how they would impact the organisation. A small organisation could rapidly exhaust its limited budget by attempting to protect itself against all potential threats.

To address this challenge, consider the threats most relevant to the organisation's assets. Significant threats could be established through workshops, but keep in mind a scale of likelihood and focus on those simple threats requiring a minimum number of steps necessary to be effective. These threats should be detailed in scenarios that describe the steps that are likely to occur for these to impact the organisation and its assets. Threat identification should be an ongoing activity to keep up with changes in technology and the organisation.

> “If a supplier was the source of an incident, what impact would this have on any response?”

STEP THREE:

HAVE A PLAN

At the core of effective incident management is a well-established plan for maintaining readiness and coordinating a response. This includes determining what resources will be required to achieve these tasks. Your plan should be the focus for building on your incident management readiness.

Key Elements of Incident Management Planning

The list of items in this section is not exhaustive but provides important considerations for establishing and maintaining a response capability.

Runbooks

These set out a pre-planned series of actions that are initiated when an incident occurs. The runbook draws on information gathered from the five steps set out in this document. A runbook is constructed according to likely threat scenarios and important assets. The runbook's actions are triggered by an alert that has been classified based on pre-existing instructions. All actions are performed by those assigned roles.

Technical Instructions

A runbook may be executed by someone who doesn't necessarily have a background or experience in all the relevant technologies. It is therefore vital to maintain up-to-date technical instructions for the technologies, and to ensure that appropriate access to systems is available when required.

Checklists

Checklists are an important part of incident management. Writing a checklist of actions to complete when an incident occurs helps to focus your efforts during a stressful situation. This ensures the right evidence is gathered, the appropriate staff are notified, and actions are clearly recorded.

Escalation Rules

Clear escalation rules should guide the runbooks and incident response plans. These rules can be aligned to the threat level framework covered in Step 5 and should have precise triggers for when potential incidents need to be escalated. In some situations, imposing time limits for each step may also help to prevent teams spending too long trying to restore a system and delaying the escalation process.

Notification Plan

In support of the runbooks, there should be a notification plan containing the contact details of all the relevant staff. This plan can include details such as an on-call roster and a call tree to notify the right staff, including who to call after hours.

Communications Bridge

Many incidents are managed using online communications technologies. It is important that these are defined and documented beforehand and are readily available for staff to connect to. It is vital to always have a backup communications system that runs outside of the organisation's IT infrastructure. This can be used as a fall-back should the primary IT system be unavailable or potentially compromised.

Equipment and Storage

Some types of incident may require that information or evidence is stored until it can be recovered and analysed by external specialists. It is important that appropriately secured storage facilities are available. Response teams may require laptops or specialist devices to carry out testing. This equipment should be readily available and configured prior to an incident occurring.

Regular Checks

Effective incident management is not just about responding to incidents as they occur, it should also involve regular and documented checks. These should include controls and systems checks, access reviews, alerts monitoring, and logs analysis. Proactive analysis will often reveal incidents that have gone unnoticed or systems that have stopped logging.

CONVERSATION STARTERS:

- What types of incidents are we prepared for?
- Who is available after hours if something goes wrong?
- Is someone carrying out regular checks to ensure no notifications are missed?
- If our systems are unavailable, do we still have a way to communicate and coordinate?
- Who can we call on if the situation becomes unmanageable?

STEP FOUR:

LOGGING, ALERTING AND INCIDENT AUTOMATION

It is important to draw a distinction between events, alerts and incidents. Incidents compel action because a suspected breach of policy has occurred. Events and alerts are potential indicators of some anomaly being detected, and these should be tuned to ensure that false positives are minimised while genuine incidents are reported.

Effective incident management requires the capability to manage logs, events, alerts and incidents in a systematic manner. Events and alerts may be indicative of required actions, while logs provide data for reactive analysis. Many organisations are challenged by a large quantity of alerts being generated, and face the risk that some are unattended. This situation is being exacerbated by the rapid move to cloud services and the use of multiple security technologies, each with distinct methods of logging and analysing events.

CONVERSATION STARTERS:

- How would our organisation detect an incident?
- Are we responding to all the alerts we are receiving?
- Are we receiving too many alerts because we aren’t tuning them correctly?
- If something happened, would we be able to go back and find the information in our logs?
- How far back can we go? Is it one week, one month, one year, or might we need longer?
- Have we produced reports for our security incidents?

Logging

Establish which systems produce log data. Once identified, determine if that logging needs to be captured and stored. This data could be used for investigative purposes, or it may be a longer-term compliance requirement. Define the most cost-effective method of storing this data: this could be on-site or in a cloud environment.

One of the most common problems to occur during a major incident is that insufficient logging data is available. Some investigations will need to go back months, and if detailed logs are not available the investigation may need to rely on guesswork and draw assumptions which could be incorrect and not identify the root cause of the incident.

Events and Alerts

Understand which systems are producing events and alerts, and where these are being directed. Tune all the events and alerts to ensure they are producing information relevant to the organisation and the defined threat scenarios. Capture these and, ideally, forward them into a dedicated tool or service management system.

> “If data doesn’t need to be retained, don’t store it unnecessarily.”

False Positives

Alerts can often prove to be indicators of routine activity that is not malicious. A challenge is that too many false positives will quickly overload even the largest security team and result in genuine incidents being missed. It is vital to establish a process that ensures false positives are rapidly tuned out and to focus on the alerts that indicate a likely incident. False positives should still be logged as they may be relevant to future investigations.

Incident Response Automation

The events and alerts that trigger an incident should be clearly defined and managed. They should be aligned to threats as defined in Step 2 and actioned in a timely fashion in accordance with the incident plan. Ideally, incident responses should be automated as much as possible and pushed to the relevant support teams with clear runbooks to follow and action.

STEP FIVE:

MAINTAIN AWARENESS, REPORT PROGRESS, CONTINUALLY IMPROVE

Effective incident management is a continuous practice and there is always scope for improvement.

A part of building cyber maturity is maintaining an active awareness of the current threat landscape. The organisation should ensure its security capabilities continually evolve to meet new threats. By considering these factors it is possible to ensure that ongoing investment is focussed on the right areas.

CONVERSATION STARTERS:

- What is our current threat level?
- Do we need to change our threat level in response to a vulnerability announcement?
- Have we tested our ability to restore from backups recently?
- Do we have methods of responding to specific threats?
- Are we improving our incident management capabilities?
- Have we produced reports for our security incidents?

Key Considerations for Step Five

Threat-Level Framework

A threat-level framework is composed of clearly defined levels of response and readiness within an organisation. The threat level is based on exposure to current threats, both internal and external, and could reflect unusual network behaviour, a new vulnerability, or even a restructure within the organisation. On a day-to-day basis an organisation may be at a guarded state, but if there is a targeted phishing campaign or an active incident the threat level will be elevated.

Each successive threat level should include clearly defined triggers, authority to move between levels, notifications, and pre-approved response actions. The actions will vary depending on the threat but could include blocking certain types of traffic or disconnecting systems and isolating them from the network. Establishing a framework like this is an iterative process but should be continually refined and updated based on lessons learned.

Testing and Validation

A plan is only as good as the last time it was tested. Building out response plans aligned to threats is useful but these need to be tried out in practice. Testing establishes whether:

- the defined roles and responsibilities are appropriate for the staff assigned to them;
- staff understand or remember what actions they need to take;
- the triage and escalation processes work in practice.

These factors will be vital when an incident does occur. By having practised, staff will be more confident and better able to manage a potentially stressful situation.

Testing could be as simple as running a workshop with key stakeholders and working through threat scenarios or simulating an outage. It could even involve contracting a third party to test threat scenarios. It’s important that testing and validation is aligned with the threats identified in Step 2, and that they leverage runbooks that are part of the incident management plan described in Step 3.

Metrics and Reporting

It is crucial that the effectiveness of the incident management capability is reported and measured against clear metrics. One way to begin this process is to create a dashboard. The measurable or quantifiable components of a dashboard should centre on events, alerts and incidents, and management of false positives. Eventually it will be possible to report on the mean time to detect incidents and the mean time to restore systems as key metrics.

Near-Miss Analysis

One particularly useful way of improving incident management is to carry out near-miss analyses. Like health and safety reviews, these analyses consider which controls were effective and which were not, even if the incident did not cause any impact. These analyses allow for targeted improvement in controls that did not effectively support the detection, protection, or response to a threat.

THE FIRST FIVE STEPS OF INCIDENT MANAGEMENT IN ACTION

The NCSC assists organisations in responding to cyber security incidents that may have high national impact. While many of these organisations believe their level of preparation is sufficient, the experience of a major incident is often a catalyst for increased investment in incident management. Suffering a poorly managed incident can be an expensive way to learn the value of the Five Steps.

The fictional scenario in this section has been designed to provide the same insight that a live incident might, but without the associated business impacts. The scenario describes a company's experience of two incidents: one before and one after an incident management uplift programme designed around the Five Steps.

SCENARIO:

BELLBIRD OPTICS

Introducing Bellbird Optics: a company that designs, manufactures and sells high-tech medical equipment. Bellbird Optics maintains a significant online presence, and their interaction with customers is mainly through an online sales and delivery portal.

Staff

Bellbird Optics has grown quickly over the past few years, and is now a thriving medium-size enterprise employing over 100 staff. The company is supported by a seven-person IT team consisting of one manager, two service desk analysts, two engineers, one developer, and one junior coordinator. The team supports most of the company's IT functions in-house. The IT manager is accountable for all security as part of his role and can leverage the help of a third-party networks company. The IT manager reports directly to the CEO.

The CFO manages risk and contracts a large consulting firm for one day per month to help run the registers and chair the audit and risk committee. The company also has a communications manager in the marketing team.

Technology

The company operates a manufacturing facility and head office, as well as three small regional offices. All its locations are equipped with Wi-Fi and print services. The company uses a fleet of mainly Windows 10 devices and a mix of mobile devices. The management of this network is outsourced to a third party, which also provides them with a managed firewall service.

The company uses Microsoft 365 for productivity, but still retains some on-premises capacity. The remaining services are hosted on infrastructure and platforms in Amazon Web Services, including the delivery of their online sales platform. They use software-as-a-service offerings for their human resources, customer relationship management, and project management.

INCIDENT ONE: RANSOMWARE STRIKES

Ransomware, a well-established cyber threat, infected one of Bellbird Optics' desktop computers. The malware spread quickly and staff were not quite sure what was happening at first, but they started to report access issues to the IT help desk. The IT team began to join the dots, and they realised something was badly wrong when a file server was encrypted. They then discovered a further 25 workstations had been affected.

It took Bellbird Optics almost a week to recover access to their systems. During this time they were unable to deliver many of their normal services to their customers. The customer support team, who were not aware of the details of the incident, sent out communications giving the impression that user data had been stolen. Incorrect news of stolen 'personally identifiable information' made it into the technology media.

The IT manager was quick to attempt system restoration and focused exclusively on getting systems back online. With this singular focus on restoration, the rest of the business was not aware of which systems were still usable. As a result, other teams were unable to assist with investigating non-IT workarounds for processes, or to help with managing customer expectations.

There was a significant delay before the company's senior leaders were updated on the incident. After they were made aware, the CEO and CFO attempted to contact the insurance company to file a claim. However, the claim was declined because the policy stipulated that the insurer must be contacted within a strict time frame after the incident was detected, and that time had elapsed.

The company's firewalls did detect the outbound ransomware traffic, but had not been configured to block that type of traffic. On review, the contract with Bellbird's third-party network provider only included basic maintenance support to ensure availability. Responsibility for correctly setting up the firewall rules sat with the IT team and had been overlooked.

A Catalyst for Change

Bellbird Optics' CEO asked the IT manager to review how the incident management capability for the company could be improved. If an event like this happened again, the CEO wanted the company to be able to manage and contain it more rapidly. The IT manager implemented a 90-day action plan to address the NCSC's Five Steps and improve the company's overall incident management capability.

INCIDENT TWO: CREDENTIAL THEFT

Credential theft is another common threat to which Bellbird Optics, as a user of software-as-a-service, is vulnerable. An example of credential theft is an unauthorised user illicitly obtaining a staff member's login details and then using these to conduct malicious activity.

Four months after the ransomware incident, Bellbird Optics became a victim of credential theft, and a cyber actor used the access these credentials provided to send phishing emails to Bellbird's customers.

Step 2 in action: The organisation has taken the time to identify key threats and the critical internal systems that are vulnerable to them. This groundwork has already identified credential theft as a threat and informs many of the following steps.

The first sign that Bellbird Optics could be a victim came from a customer querying the authenticity of an email they received. The sales representative receiving the question, John, did not recognise the email, which was purportedly sent by him and included a suspicious link. John immediately called the company's IT helpdesk.

Step 1 in action: Because cyber incident roles and responsibilities have been defined, everyone in the organisation was clear about whom suspicious activity should be reported to. This included the users' responsibility for identifying potential security incidents during their day-to-day work.

A helpdesk analyst examined the email and recognised it as being malicious by performing the documented steps from the company's incident runbook. Continuing to work through the steps, the analyst immediately disabled John's user account. The analyst then logged a ticket, assigned it to one of the engineers, and followed up with a call to the engineer.

Step 3 in action: The runbook is put into action. It reflected credential theft and enabled prompt identification of the malicious activity, as well as mitigation steps such as disabling the account.

The engineer reviewed the ticket and, after determining that the email was malicious, moved quickly to declare a security incident. Working through their checklist, the engineer raised the threat level of the organisation and informed the IT manager and other key staff of the potential need for incident response.

Step 3 in action: The engineer followed a checklist of actions defined in the incident response plan. When things start to happen quickly, it's easy to miss steps. Documenting each of the steps in writing helps to ensure they are carried out.

A review of the logs associated with John's account showed that it had been hijacked using stolen credentials. Based on the indicators of compromise found in the logs, the initial investigation showed a total of four other accounts had been compromised. All of these accounts sent phishing emails to their customers. There was also evidence of other suspicious activity in the logs that required further investigation.

Step 4 in action: Logging and alerting gave the incident team the exact locations and tools to investigate and obtain more detail. The team was able to quickly estimate the breadth of the incident and begin a containment process.

As the engineer and help desk worked to contain the incident, they set up a call with the IT manager, the remaining engineer, and the company's external network provider. The IT manager took on the role of the coordinator and passed on key details from the call to the CEO, the communications manager, and the legal counsel. Together they decided to advise potentially affected customers. With the aid of information on potential recipients of the phishing email provided by the IT team and an email drafted by the communications manager, customers were quickly advised to delete the email.

Step 2 in action: Recognised roles and responsibilities ensured that the right people gave advice at the right time. By quickly involving all the relevant people, an effective course action was decided upon.

Finally, the IT manager called a meeting to evaluate how the company performed during the credential theft incident. During the meeting they identified internal processes that would further enhance the effectiveness of their incident handling and response procedures. The manager then updated the relevant plans, runbooks, and checklists to ensure the improvements were made.

The evaluation determined that the incident management improvements had worked well. If the incident had not been resolved quickly, it could have impacted the company's reputation, financial transactions and customer security.

However, there were further lessons to be learned. The IT team found that the incident could have been prevented if the following measures were in place:

- Strong authentication (no multi-factor authentication was enabled);
- User awareness training (multiple users clicked on the email), and:
- Email filtration (an obvious phishing message was allowed in).

The IT manager initiated a series of actions to improve these control areas and follow up with testing to ensure the improvements are effective.

Step 5 in action: With the ongoing programme in place, it became possible to take the findings from the incident report, validate the effectiveness of the response plan, and track improvement actions.

CONCLUSION

The Bellbird Optics scenario, although fictional, is true to the NCSC's experience working on incidents with a range of nationally significant organisations.

> "The best opportunity to reduce the business impact of an incident happens before the incident occurs. Preparation is key."

The NCSC hopes the scenario enables organisations to learn from the mistakes of others. The beliefs that *'it'll never happen to us'* and *'we are as prepared as we need to be'* are common in New Zealand. The process of improving incident management begins with appreciating that this action is necessary. The experience of suffering a cyber incident should not be the impetus for better preparation.

Every organisation should be well-prepared to manage a cyber security incident. Although it is a technical field, effective cyber incident management is primarily a business activity that can be driven by management. The prevalence of cyber threats in the modern business environment makes it critical for boards of directors, business owners and senior executives to take an active interest in how their organisation will respond to and manage an incident. The conversation starters we have provided throughout this document will help in this area.

The five steps outlined in this guidance provide organisations with a starting point from which they can become prepared and resilient. We recommended that organisations develop and embed a comprehensive incident management plan. A full programme should focus on continuous improvement and be part of, or integrated with, a wider cyber security programme within the organisation.

For futher information visit: **www.ncsc.govt.nz**
or email: **info@ncsc.govt.nz**