Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

Structuring your Incident Response

Where to start when hit with a major Cyber Incident

What does a major cyber incident feel like?

A nice cliche ...

“No plan survives first contact with the enemy”

- Helmuth von Moltke

What does a major cyber incident feel like?

The reality....

“Everybody has a plan until they are punched in the mouth”

- Mike Tyson

Major incidents in general

What other industries deal with major incidents?

- Health care industry
  (Pre-hospital emergencies, emergency departments etc)
- Transport industry
  (Aviation incidents, mechanical failures, near misses)
- Military
  (Conflict, Peace Time duties)
- Policing
  (Traffic accidents, public order)

The nature of incidents

What are the common characteristics of major incidents

- Unexpected
- Badly timed (weekends, bank holidays, staff shortage)
- From a variety of causes (cyber incident, system outages)
- Human factors (emotional reactions, human adversary)
- Requiring rapid output of energy and resources from both people and systems

Irish Times,
Photograph: Damien Storan

Consider this

Questions for everyone in the room

- How many of you sitting here don’t have a fire marshall in your building?
- How many of you sitting here don’t have a designated first aider in your building?
- How many of you don’t know how to use a fire extinguisher?
- How many of you have never had a fire drill?

Cyber Incident Response

When is the last time you ....

- Restored your systems from backup or failed over to your DR site?
- Ran searches for malicious activity across your entire estate?
- Ran a table top exercise for incident response?
- Discussed incident response roles within your organisation?

Cyber Incident Response

Make it boring with 3 steps

Step 1: Identify (staff, assets, tools)

Step 2: Assess (situation, capabilities, gaps)

Step 3: Improve (resolve, resource, reflect)

The Roles

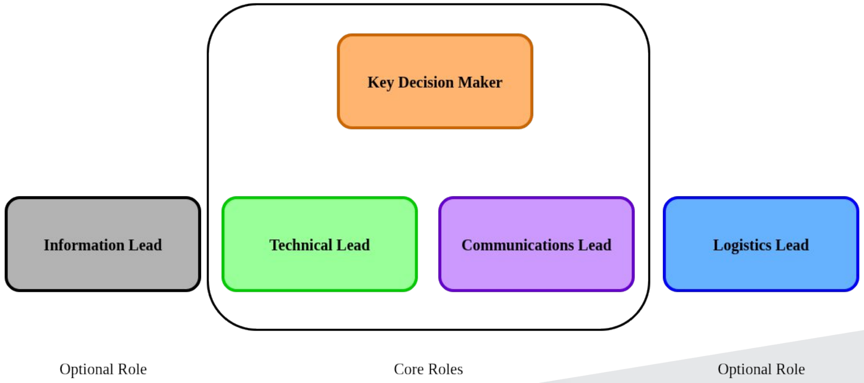
Who do you need to manage an incident?

- Key Decision Maker (CTO, CISO, Director)
- Technical Lead (Cyber lead, ICT Manager)
- Communications Lead (Sales, Marketing, HR, Legal)
- Information Lead (Accounting, Legal, Technical)
- Logistics Lead (Facilities, Site Manager)

The many hats of Incident Response

Just one head?

The Roles/Hats



Key Decision Maker

Information Lead

Technical Lead

Communications Lead

Logistics Lead

Optional Role

Core Roles

Optional Role

Key Decision Maker

Good characteristics to have

- Calm under pressure, keeps the response matter of fact
- Excellent communication style, clear messaging
- Good at keeping view of all aspects of the incident
- Has the respect and authority to gather resources
- Emotional Intelligence

Technical Lead

Good characteristics to have

- Good overall awareness of the infrastructure
- Capable of identifying key digital assets for prioritising analysis and recovery
- Capable of communicating how infrastructure relates to business functions
- Technical excellence is good but managing technical people is better

Communications Lead

Good characteristics to have

- Excellent at understanding stakeholder requirements
- Ideally has a pre-existing relationship with key stakeholders
- Emotionally intelligent and aware of sensitivities around messaging to public, media, clients & staff
- Resilient when faced with challenging requests from stakeholders

Information Lead (the sweeper)

Good characteristics to have

- Excellent attention to detail
- Excellent documentation and meeting management skills
- Good communication skills
- Good stamina for attending meetings and capturing information

Logistics Lead

Good characteristics to have

- Excellent knowledge of how the business works from a daily operations perspective
- Good organisation and anticipation of potential logistics hurdles
- Resourceful, creative and a self starter
- A peoples person who can beg, borrow or requisition logistics assets where required

Meeting Cadence

Objective, audience, actions

- Morning meeting - What we’re going to do
- Mid day meeting – What we’re doing and how it’s going
- Late afternoon meeting – What we’ve done and what’s next
- Stick to short meetings that are more regular (30 minutes or less)
- Tight agenda, assign someone to chair them (Information lead)
- Meeting momentum and discipline to keep visibility

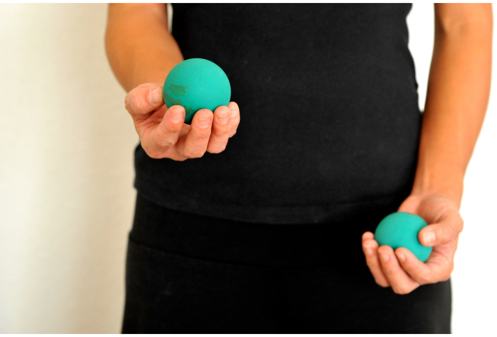
Common Incident Response questions

When you feel lost at the start

- “Where do I start?”
- “How bad is this really?”
- “How long will this continue?”
- “What are we missing?”
- “We’ve never done this before”

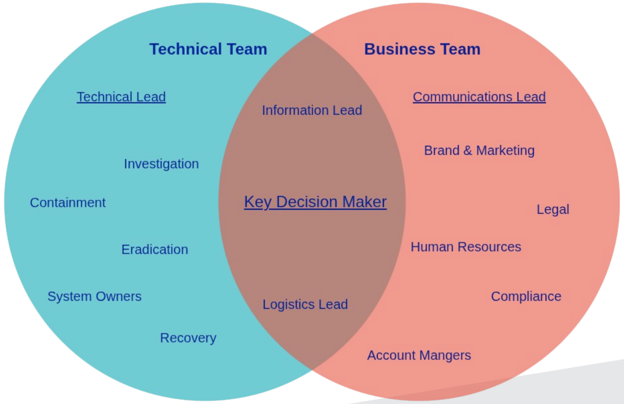
Business needs
vs
Response needs

A difficult juggling act



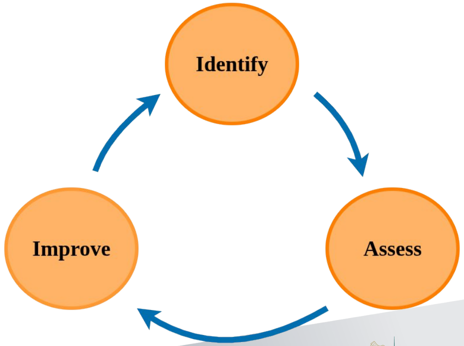
Business needs
vs
Response needs

A difficult juggling act



Common Incident Response

When you feel lost at the start



Incident Response Checklists

What to include within your checklists

1. Roles and their specific areas of responsibility
2. Initial actions for each role to consider
3. Continuous considerations for each role

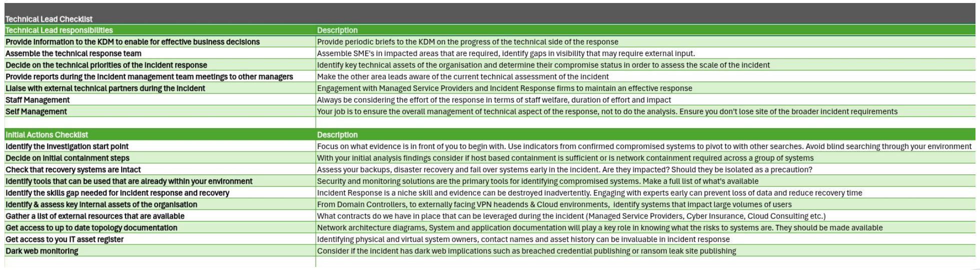
Checklists

In an emergency, don’t start with nothing

source: pilotinstitute.com

Start an incident response checklist

Have a panic proof checklist for your role



Technical Lead Checklist

Technical Lead responsibilities	Description
Provide information to the KDM to enable for effective business decisions	Provide periodic briefs to the KDM on the progress of the technical side of the response
Assemble the technical response team	Assemble SME's in impacted areas that are required, identify gaps in visibility that may require external input.
Decide on the technical priorities of the incident response	Identify key technical assets of the organisation and determine their compromise status in order to assess the scale of the incident
Provide reports during the incident management team meetings to other managers	Make the other area leads aware of the current technical assessment of the incident
Liaise with external technical partners during the incident	Engagement with Managed Service Providers and Incident Response firms to maintain an effective response
Staff Management	Always be considering the effort of the response in terms of staff welfare, duration of effort and impact
Self Management	Your job is to ensure the overall management of technical aspect of the response, not to do the analysis. Ensure you don't lose site of the broader incident requirements

Initial Actions Checklist	Description
Identify the investigation start point	Focus on what evidence is in front of you to begin with. Use indicators from confirmed compromised systems to pivot to with other searches. Avoid blind searching through your environment
Decide on initial containment steps	With your initial analysis findings consider if host based containment is sufficient or is network containment required across a group of systems
Check that recovery systems are intact	Assess your backups, disaster recovery and fail over systems early in the incident. Are they impacted? Should they be isolated as a precaution?
Identify tools that can be used that are already within your environment	Security and monitoring solutions are the primary tools for identifying compromised systems. Make a full list of what's available
Identify the skills gap needed for incident response and recovery	Incident Response is a niche skill and evidence can be destroyed inadvertently. Engaging with experts early can prevent loss of data and reduce recovery time
Identify & assess key internal assets of the organisation	From Domain Controllers, to externally facing VPN headends & Cloud environments, identify systems that impact large volumes of users
Gather a list of external resources that are available	What contracts do we have in place that can be leveraged during the incident (Managed Service Providers, Cyber Insurance, Cloud Consulting etc.)
Get access to up to date topology documentation	Network architecture diagrams, System and application documentation will play a key role in knowing what the risks to systems are. They should be made available
Get access to you IT asset register	Identifying physical and virtual system owners, contact names and asset history can be invaluable in incident response
Dark web monitoring	Consider if the incident has dark web implications such as breached credential publishing or ransom leak site publishing

https://www.ncsc.gov.ie/pdfs/Incident-Response-Management-Template.xlsx

Why use checklists?

Get organised, stay organised

- Excellent for quickly referencing requirements early in the response
- Assists with creating a structure for the teams responding
- It helps keep track of tasks, priorities & responsibilities
- Useful for documenting decisions and event timelines
- Excellent reference for use in retrospective assessments (lessons learned)

Cyber Security Incident Response Drills

Make it real for you and your staff

- Create a few scenarios for incidents based on your environment
  - Have the initial scenario description
  - Have follow up developments (extra context, media challenges etc)
  - Use a third party mediator if required (internal or external)
- Gather the senior management group who will respond in their roles
- Schedule a morning to discuss the scenario and work through the problems
- Develop tangible outputs & actions from the exercise

Example Scenario

Think about who would you have responding to this incident:

"SwiftTech Manufacturing Services are a company of 49 employees based in Cork with offices in Dublin. They manufacture electronic components such as printed circuit boards for programmable logic controllers used in the energy sector. It's Friday in June 2025 just before the bank holiday. Two members of the accounting department in Cork have contacted the IT servicedesk in Dublin stating they can't get access to some of their files and there is a text file on the Desktop claiming that their computers have been hacked and the note demands payment..."

What role would you most likely perform in this scenario?

First Steps

Decide on activities early

Initial considerations for the management team:

- Do we have enough information to make significant decisions?
- Does this incident meet the threshold to activate an incident response plan?
- Who is available that we can task with the Incident Management Team (IMT) roles?
- Do we have initial checklists for assessing the incident impact?

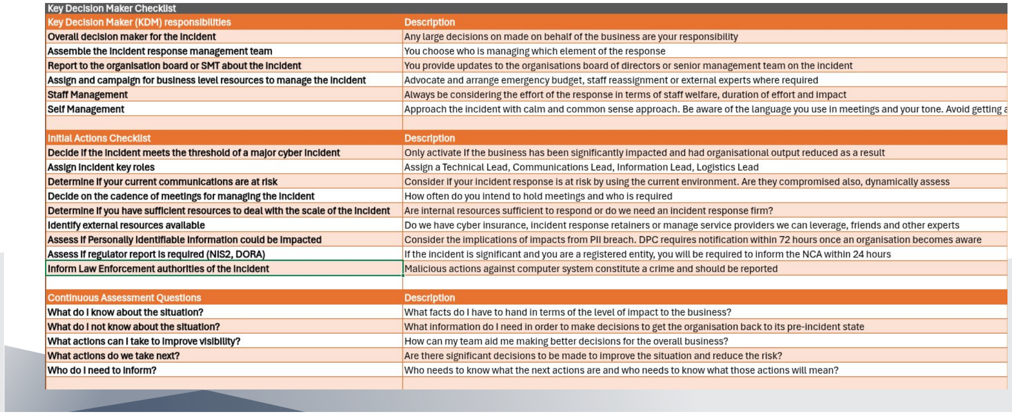
Example Scenario

Practice picking out the information for your area of responsibility

"SwiftTech Manufacturing Services are a company of 49 employees based in Cork with offices in Dublin. They manufacture electronic components such as printed circuit boards for programmable logic controllers used in the energy sector. It's Friday in June 2025 just before the bank holiday. Two members of the accounting department in Cork have contacted the IT servicedesk in Dublin stating they can't get access to some of their files and there is a text file on the Desktop claiming that their computers have been hacked and the note demands payment..."

Incident Response

Practice picking out the information for your area of responsibility



Key Decision Maker Checklist

Key Decision Maker (KDM) responsibilities	Description
Overall decision maker for the incident	Any large decisions on made on behalf of the business are your responsibility
Assemble the incident response management team	You choose who is managing which element of the response
Report to the organisation board or SMT about the incident	You provide updates to the organisations board of directors or senior management team on the incident
Assign and campaign for business level resources to manage the incident	Advocate and arrange emergency budget, staff reassignment or external experts where required
Staff Management	Always be considering the effort of the response in terms of staff welfare, duration of effort and impact
Self Management	Approach the incident with calm and common sense approach. Be aware of the language you use in meetings and your tone. Avoid getting a
Initial Actions Checklist	**Description**
Decide if the incident meets the threshold of a major cyber incident	Only activate if the business has been significantly impacted and had organisational output reduced as a result
Assign incident key roles	Assign a Technical Lead, Communications Lead, Information Lead, Logistics Lead
Determine if your current communications are at risk	Consider if your incident response is at risk by using the current environment. Are they compromised also, dynamically assess
Decide on the cadence of meetings for managing the incident	How often do you intend to hold meetings and who is required
Determine if you have sufficient resources to deal with the scale of the incident	Are internal resources sufficient to respond or do we need an incident response firm?
Identify external resources available	Do we have cyber insurance, incident response retainers or manage service providers we can leverage, friends and other experts
Assess if Personally Identifiable Information could be impacted	Consider the implications of impacts from PII breach. DPC requires notification within 72 hours once an organisation becomes aware
Assess if regulator report is required (NIS2, DORA)	If the incident is significant and you are a registered entity, you will be required to inform the NCA within 24 hours
Inform Law Enforcement authorities of the incident	Malicious actions against computer system constitute a crime and should be reported
Continuous Assessment Questions	**Description**
What do I know about the situation?	What facts do I have to hand in terms of the level of impact to the business?
What do I not know about the situation?	What information do I need in order to make decisions to get the organisation back to its pre-incident state
What actions can I take to improve visibility?	How can my team aid me making better decisions for the overall business?
What actions do we take next?	Are there significant decisions to be made to improve the situation and reduce the risk?
Who do I need to inform?	Who needs to know what the next actions are and who needs to know what those actions will mean?

Scenario update

Develop your scenarios with iteration and realism

“90 minutes pass. Upon further investigation, it becomes apparent that many workstations have been affected with more users calling the Dublin ICT helpdesk. Authentication is failing for external staff VPN services and the incident is impacting many users across departments in both locations. Some servers appear to be inaccessible through remote login services. A sales account manager has contacted to say he’s getting complaints from a large client about a customer portal not working. Staff in Dublin are now start reporting problems accessing internal ICT services.”

As the incident escalates ...

- Big incidents generate a lot of noise
- Protect the staff actioning the response
- Keep the communication flowing where it’s needed
- Continuous activity & assessment for senior leadership
- Always being asking questions
- Keep good notes, you’ll get tired and forget

Cadence of Incident Response

Large incidents

- Can go on longer than you would think
- Can have secondary incidents
  (threat actor returns or another campaign is detected)
- Managing staff energy for the duration of the incident (particularly key areas)
- Mistakes happen with fatigued decision making
- Recovery is often the most difficult part
- Lessons can often get lost
- Individuals or platforms taking the blame

Final thoughts ..

If you take nothing else away

If you are likely to be within a key role during an incident:

- Develop a checklist for your areas of responsibility
- Develop a tabletop exercise for your team & practice it
- Run through the exercise once every 6 months with the key roles (cyber security fire drill)
- Ask the hard questions of your organisation now

Contact Us

National Cyber Security Centre,
Department of Justice, Home Affairs and Migration,
Tom Johnson House, Beggar’s Bush, Dublin 4, D04 K7X4

E info@ncsc.gov.ie
T +353 (0)1 678 2333

ncsc.gov.ie

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre