Loss Prevention Standards – Cross Classes

Cyber - Incident Response Process

Version: 1.0
Date: 8th January 2025

A guide to developing an effective cyber incident response process.

AVIVA

Cyber - Incident Response Process

Introduction to Cyber Incident Response

Cyber Incident Response, also known as Incident Response, refers to the process of handling and responding to a cybersecurity incident. It involves a series of planned and coordinated actions that organisations undertake in response to a cybersecurity incident or breach. The goal of a Cyber Incident Response is to safeguard the organisation's digital assets and minimise the impact of the cyber incident, mitigate the damage, reduce potential financial losses, and restore normal operations as quickly as possible. An incident response plan ensures that organisations are well-prepared to handle cybersecurity incidents effectively. It provides a structured and documented approach, enabling teams to respond promptly and efficiently when an incident occurs. Without a plan, organisations may struggle to respond adequately, leading to delays in containment, increased damages, and longer recovery timelines.

What is a Security Incident?

A security incident refers to an occurrence that may signal a breach in an organisation's systems or data, or a failure in the security measures designed to protect them.

There is frequently a lack of clarity regarding the difference between a security incident and a security breach.

A security incident encompasses a broad spectrum of security violations, ranging from unauthorised access to computer systems, networks, and data, to occurrences such a malware, Denial of Service (DoS) attacks or even physical thefts. In contrast, a security breach specifically refers to incidents involving a data breach only. Hence, a security breach is a subset of security incident that focus solely on unauthorised data access or theft.

Some of the most common examples of cybersecurity incidents and security breaches include:

1. Social engineering attacks: Manipulating individuals into divulging confidential information or performing actions that compromise security, often through deception or psychological manipulation.

2. Malware infections: Software designed to disrupt, damage, or gain unauthorised access to computer systems, such as ransomware, viruses, spyware, and trojans.

3. Insider threats: Malicious or negligent actions by employees, contractors, or partners that pose a security risk to an organisation.

4. Denial of Service attacks: Overloading a network or system with excessive traffic to disrupt its availability and functionality, preventing legitimate users from accessing services.

5. Ransomware attack: Steals data and then demands for a ransom for its return.

6. Stealing a computer device or physical documents that contains sensitive data or personally identifiable information (PII).

7. Privilege escalation attacks entail a threat actor obtaining entry to a system with restricted privileges and subsequently leveraging vulnerabilities or utilising illicitly acquired credentials to elevate their access to higher level of authorisation. Such attacks pose a substantial threat to the overall security posture of a business.

Aviva: Public

A common misconception regarding cybercrime is the belief that some businesses are immune to being targeted and that cyber-attacks are exclusively orchestrated by organised crime groups against high-profile entities. However, the reality is that cybercrime is a pervasive threat that could affect any business, regardless of size or industry.

It is extremely crucial for businesses to remain vigilant, implement robust security measures, conduct regular risk assessments, and have a well-defined incident response plan to effectively mitigate the impact of such incidents. Incident response measures help to protect an organisations critical asset and ensure data confidentiality, integrity, and availability.

This guide is designed to help businesses develop an effective Cyber Incident Response Plan (CIRP) which can be tailored to best suit the organisation and their sector.

Plan: Your Cyber Incident Response Process

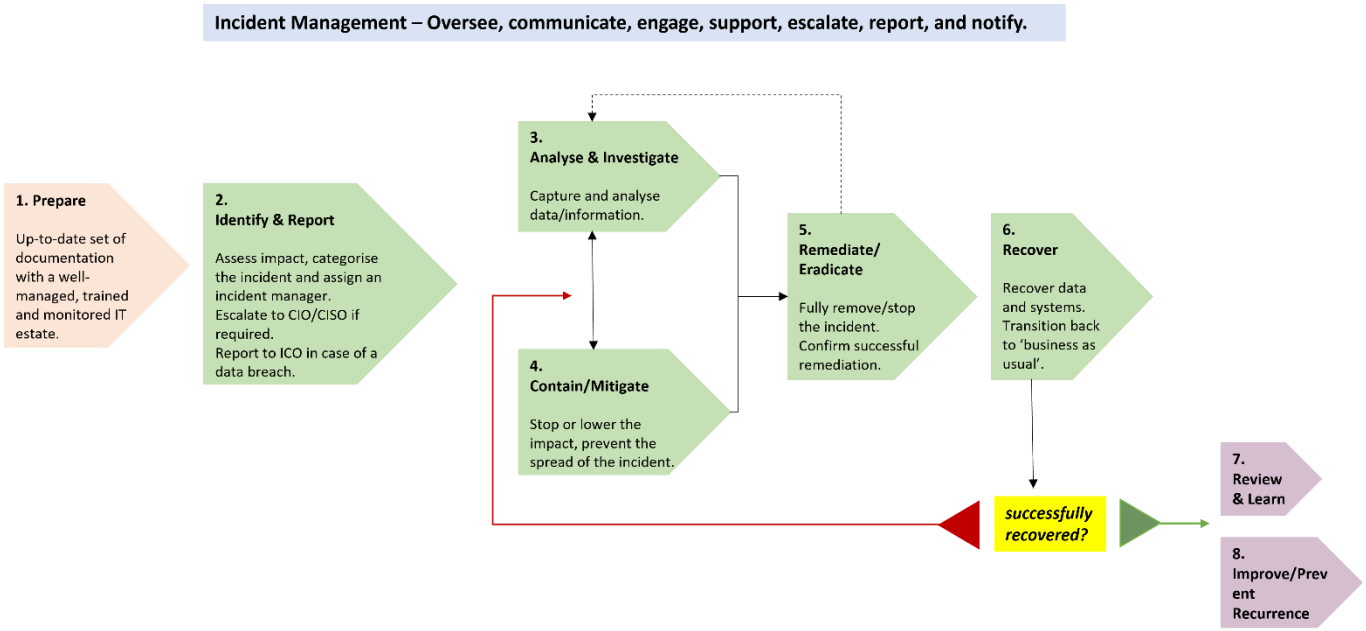
This section provides a comprehensive overview of the components of a core CIRP highlighting the specific steps involved in efficiently managing an event in context. Following this, an organisation will have the opportunity to create a strategy that is uniquely suited to their needs.

An essential component of an incident response strategy should encompass:

- Departmental primary contacts: Contact details of Senior Management, IT, Public Relations, HR, IR team, Legal, and Insurers. Provision should always be made for at least two contact methods and two separate key contacts per role to account for absences.
- Management roles and responsibilities: Cyber incidents are managed (triage, containment, eradication, lessons identified and reporting) by the Cyber Incident Response Team (CIRT). The CIRT team is responsible for analysing security breaches and taking any necessary responsive measures, along with advising the Senior Management Board of key breaches and the response developed. A Crisis Management Team (CMT) is a separate team, usually comprised of Senior Management Team, formed to deal with the strategic consequences and decisions that arise from the CIRT incident management. (See *Appendix A - Key Personnel that form CIRT & CMT*).
- 'RACI' matrix: The RACI matrix is a useful tool that assigns responsibility and maps out tasks, milestones or key decisions involved in completing a project such as managing an incident. It assigns which roles are: Responsible for each action item, which personnel are Accountable, and, where appropriate, defined who needs to be Consulted or Informed. *(See Appendix B outlines where key responsibilities in the incident handling process fall in the form of the RACI Matrix).*
- Notification / escalation criterion: With vital decision-making processes explained.
- Fundamental instructions about legal or regulatory obligations: Guidance on when legal and HR assistance should be sought.
- Process flow diagram: This should cover an entire event lifecycle.
- One or more conference dial-in options to always be accessible in case of an emergency.

Incident Response Process Flow Diagram

This section provides a high-level incident response lifecycle, which provides a structured approach for handling cybersecurity incidents. These phases are designed to be repeated for each incident that occurs to continually improve an organisation's incident response capabilities their overall security posture and readiness to respond to future threats.



Incident Management

Incident management supports the whole incident response process through:

1. Tracking, documenting, assigning, and correlating all findings, tasks, and communications.
2. Arranging regular update meetings or calls, and the involvement of relevant teams.
3. Ensuring resilient communications to key members of staff within the Core IT CIRT, and CMT can take place.
    a. Through the designated point of contacts, the core CIRT shall notify all confirmed CRITICAL or HIGH criticality cyber incidents to relevant senior management (business department managers, control owners, security management, regulatory authorities, policy owners, etc.) and the associated third parties.
    b. The CIRT will inform the HR personnel of those incidents which involves a major violation of security policies associated with a current or former employee so HR can take required steps such as providing customised cyber security training, disciplinary actions (if needed), and oversee any corporate press, social media, and PR responses.

Aviva: Public

c. All proven CRITICAL or HIGH criticality cyber incidents that compromise third party vendors information, such as PII or credit card details shall be communicated by the CIRT.

As needed, the CIRT will decide if and when to contact the National Cyber Security Centre (NCSC) or Police Scotland for incident support or carrying out a criminal investigation. This (along with any civil cases) may require careful handling of evidence.

The incident management ensures that the full incident lifecycle is covered from initial discovery through to closing of the incident.

*Consider options for secure or alternative communications in event of a sensitive incident, or where normal channels are unavailable due to network/email/phone system outage.

Preparation (Phase One)

The key to minimising the impact and quickly recovering from a cyber incident is in the planning and preparation. This is represented as step one on the flow chart above.

A well-trained team that has access to a comprehensive up-to-date set of documentation with a well-managed and monitored IT estate will greatly improve the response times to a cyber incident.

Key preparation considerations include:

1. Comprehensive documentation, easily accessible and stored in a centralised repository, such as Cyber Incident Response Plan, business continuity policies, inventory of digital assets, network diagrams, whitelisted or allowed services, protocols, ports information, backup and recovery processes, patch management plan, system configuration details, system logs, contact information of all core and external IT CIRT team members, etc.
2. Collect Cyber Threat Intelligence data to better understand the risks to the business and network infrastructure from various sources such as open-source intelligence feeds, security newsfeeds, National Cyber Security Centre threat reports.
3. Security awareness training should be given to all employees as part of the induction process along with annual refresher training. Annual training on cyber incident response plan actions should be given to all CIRT members. HR should maintain a record of all employee security training.
4. Conducting a testing programme is necessary to maintain and improve the organisation's capability to manage cyber incidents in line with the industry standards. This includes yearly penetration testing, annual incident response plan testing, internal testing of the playbooks for certain incident types, such as ransomware, denial of service (DoS), phishing, etc., business impact assessments and vulnerability management program.

Detection and Analysis (Phases Two – Three)

- Identify and Report (Phase Two)

  Any suspected or actual breach of information security policy or systems must be immediately reported to the organisation IT support. When reporting a cyber incident, it is important to collect as much information about the incident as possible to enable the service desk to give the incident an initial priority such as:

- Contact information of the person/group reporting the incident
- Details of suspected impacted systems
- Nature/type of incident
- The potential impact of the incident along with which business area is likely to be affected.
- Description of the activity and supporting evidence e.g., logs

Once the above information has been obtained, this will allow the Service/Helpdesk to assign a priority to the incident. Using their workflow process, this will then determine whether this is a security incident and needs to be referred to the CIRT.

The CIRT responsible person shall determine whether the incident amounts to a data breach which requires to be reported to the Information Commissioners Office (ICO). In line with the GDPR (Article 33), the ICO must be informed within 72 hours of the organisation becoming aware of an incident resulting in a "risk to the rights and freedoms of those involved".

- Analyse and Investigate (Phase Three)

This stage of the incident involves everything from technical analysis through to a review of social media reactions.

The core IT CIRT will perform an initial triage and classification of all suspected cyber incidents to confirm the validity and the potential impact of the incident. The goal of the triage is to acquire enough pertinent preliminary information to appropriately determine both the data classification involved and the estimated severity of the incident.

Severity is typically considered against the following:

1. Availability: Is the availability of data or systems impacted? (i.e., what is the impact on the business output?)
2. Confidentiality: Has sensitive data been accessed, leaked, or stolen?
3. Integrity: Could data or systems have been altered such that they cannot be trusted?

With all the above, consideration should be given to the scale of the problem, to what type of system or data is involved, and the practical consequences of the incident.

To aid the evaluation of incident severity, creating a matrix of example outcomes, rated for severity, help to inform how serious the response to the incident should be, who needs to be involved and whether the response needs to take priority over other activities.

Below is an example severity matrix. Think carefully about what matters most to the business and tailor the examples column to fit the organisation needs:

Aviva: Public

Severity Level	Impact Basis on Severity
CRITICAL	Highest severity level. Impacts are extraordinary and potentially catastrophic to the business, loss of public trust, and/or impact on operations or personnel. Examples of this degree of severity are: • Threat to life or physical safety of the public, customer, or employees. • Significant destruction of IT systems/applications. Over 80% of staff unable to work. • Critical systems offline with no known resolution • Massive loss of confidential information. Significant loss of public confidence. • Severe reputational damage. Risk of financial loss (generally more than £500,000).
HIGH	Impacts are substantial to the proper conduct of business, loss of public trust, and/or impact on operations or personnel. Examples of this degree of severity are: • Impactful destruction of some IT systems/applications. 50% of staff unable to work. • Risk of breach of confidential or personal information. • Substantial loss of public confidence. • Substantial reputational damage. Risk of financial loss (generally between £100,000 and £500,000).
MEDIUM	Impacts are moderate to the proper conduct of business, and/or impact on operations or personnel. Examples of this degree of severity are: • Multiple sites or multiple business units affected by the incident. 20% of staff unable to work. • Moderate loss or manipulation of restricted information. • Limited loss of public confidence. • Limited reputational damage.

LOW	Impacts are greatly limited to the proper conduct of business, and/or impact on operations or personnel. Examples of this degree of severity are: • Minimal, if any, impact • One or two sites or business units affected by the incident. • Limited or no unauthorised access to restricted information. • No impact to public confidence. • No impact to reputation.

The organisation should also determine what type of incident it is facing (*Please refer to the list of incident types and descriptions in the section above*). As with severity, it is very useful to create a matrix of the different categories.

The Core IT CIRT should appropriately note and/or close out incidents involving false-positives according to the incident-tracking procedures. Where a confirmed incident meets the severity score is determined as medium, high, and critical, it must be escalated to the CIRT. A low priority incident could most likely be handled by the Core IT security team itself.

Containment, Eradication and Recovery (Phases Four – Six)

- Contain / Mitigate (Phase Four)

The incident response team will implement measures to contain and isolate the incident from the corporate network in order to minimise the repercussions and avert further damage to the business. Typically, this phase entails identifying the systems and services that have been impacted, disconnecting them from the internet and internal network, revoking user access credentials and remote access, and executing protocols for collecting forensic evidence.

- Remediate / Eradicate (Phase Five)

Once you've contained the incident, the goal of this phase is to investigate the root cause and completely remove the threat from the affected network and systems. This means any malicious code or malware should be securely removed, unauthorised access points are closed off, all systems are hardened and patched with latest updates, a thorough review of network configurations is carried out, user permissions and access control lists are reviewed and corrected, and enhanced security protocols and additional safeguards are implemented to prevent the reoccurrence of the incident.

Aviva: Public

- Recover (Phase Six)

Following the confirmation of successful remediation actions by the incident response team, clean systems and data are put back online and systems are restored to their pre-incident state, transitioning back to 'business as usual'. It is imperative to conduct thorough monitoring of the estate to verify the closure of any vulnerabilities and continue to monitor the performance/activities of the affected systems.

Post Incident Activity (Phases Seven – Eight)

- Review and Learn (Phase Seven)

The goal of the 'lessons learned' phase is to provide a final report on the incident, which will be delivered to management. Feedback from this phase flows directly into continued preparation, where the lessons learned are applied to improve preparation for handling future incidents. Cyber incidents will be fully reported and reviewed within 5 days of the incident resolution.

After the incident, it's important to review what has happened, learn from any mistakes, and take action to try and reduce the likelihood of it happening again. Not only is it important to review the technical controls after the incident, but it is also a great opportunity to review and implement staff awareness or training measures to help develop security culture within the organisation. Collate and review the actions documented throughout the response to the incident, make a list of things that went well and things that could be improved from the response stage.

- Improve / Prevent Recurrence (Phase Eight)

Where necessary, make changes to the incident plan to reflect the lessons learnt. Reassess the risk and make any necessary changes to the policies and cyber strategy. For example, if the organisation was a victim of a password attack, then it may need to create a new password policy, provide new training, provide physical secure storage for passwords (or password manager apps) for your employees.

Conclusion

The risk of a cyber-attack is a real concern for every business especially those dealing with data and confidential information. By effectively responding to incidents, organisations can mitigate the risk of future incidents, protect sensitive information, and maintain the integrity and availability of their systems. Ultimately, developing a well-defined incident response plan is essential for helping organisations to remain secure in the face of cyber threats.

Aviva: Public

Appendix A – Cyber Incident Response Team Key Escalation Contacts

Cyber Incident Response Team Key Escalation Contacts
1. Senior / Executive Management
2. Head of IT
3. Head of Infrastructure & Security
4. Cyber Insurance Policy contact number
5. Department Unit Manager
6. HR personnel
7. Legal Counsel
8. Chief Finance Officer
9. IT Director
10. IT support team
11. Software developers
12. Cyber security analysts
13. Technical lead / Recovery Manager
14. Business continuity lead
15. Forensic Services
16. Press and PR
17. ICO
18. NCSC Incident Team

Aviva: Public

Appendix B – Example of a RACI Matrix

Task No.	Task	IT Managed Service Providers	Management Board	ORGANISATION ISM	Managed Service Provider	CIRT	Other ORGANISATION Personnel	Third Party Stakeholders	Impacted individuals	Law Enforcement and Regulators	Insurers
1	Identifying Incidents	R	-	A, R	R	-	R	R	-	-	
2	Reporting Incidents	R	-	A, R	R	-	R	R	-	-	
3	Assigning Incidents	-	-	A	R	-	-	-	-	-	
4	Analysis of Incidents	R	I	A	R	C	R	R, I	I	I	I
5	Containment of Incidents	R	I	A	R	C	R	R	I	I	I
6	Eradication of Incidents	R	I	A	R	C	R	R	-	I	I
7	Recovery from Incidents	R	I	A	R	R, C	R	R	I	I	I
8	Review & Learn from Incidents	R, C	I	A, R	R	R, C	C	C	-	I	I
9	Improve / Prevent Recurrence of Incidents	R, C	I	A, R	R	C	R	R	I	I	I

Reporting Incidents

In the UK, cyber security incidents can be reported to the National Cyber Security Centre (NCSC) by visiting here.

Action Fraud is the UK National Fraud & Cyber Crime Reporting Centre. Reporting the information to this website not only gives the Police key details in attempting to apprehend criminals, but it also raises awareness of the incident that could help other people/businesses avoid a similar attack.

Cyber Essentials Certification

Cyber Essentials Certification is a UK Government-backed scheme, which helps businesses achieve a satisfactory level of cyber protection.

The scheme will help businesses avoid, or at least minimise, the impact on their business of, phishing attacks, malware, ransomware, password guessing and network attacks.

Aviva: Public

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

For more information please visit:

Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- National Cyber Security Centre (NCSC)
- Action Fraud

Additional Information

Relevant Loss Prevention Standards include:

- Cyber - Cyber Essentials Accreditation
- Cyber - Ransomware
- Cyber - Respond and Recover
- Cyber - Social Engineering
- Cyber – 12 Top Tips to Protect Against a Cyber Attack
- Cyber - Homeworking
- Cyber - The Internet of Things

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to the circumstances.

8th January 2025

Version 1.0

ARMSGI2252024

LOSS PREVENTION STANDARDS

Aviva: Public