

Assignment Guidance and Front Sheet

This front sheet for assignments is designed to contain the brief, the submission instructions, and the actual student submission for any WMG assignment. As a result the sheet is completed by several people over time, and is therefore split up into sections explaining who completes what information and when. Yellow highlighted text indicates examples or further explanation of what is requested, and the highlight and instructions should be removed as you populate 'your' section.

This sheet is only to be used for components of assessment worth more than 3 CATS (e.g. for a 15 credit module, weighted more than 20%; or for a 10 credit module, weighted more than 30%).

To be completed by the student(s) prior to final submission:

Your actual submission should be written at the end of this cover sheet file, or attached with the cover sheet at the front if drafted in a separate file, program or application.

Student ID or IDs for group work	U2136249
----------------------------------	----------

To be completed (highlighted parts only) by the programme administration after approval and prior to issuing of the assessment; to be consulted by the student(s) so that you know how and when to submit:

Date set	25 th October 2023
Submission date (excluding extensions)	09 th February 2024
Submission guidance	via Tabula, please also see 'Special instructions'
Marks return date (excluding extensions)	20 working days from the date of the submission
Late submission policy	If work is submitted late, penalties will be applied at the rate of 5 marks per University working day after the due date, up to a maximum of 10 working days late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means after the submission deadline time as well as the date – work submitted after the given time even on the same day is counted as 1 day late.
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

To be completed by the module owner/tutor prior to approval and issuing of the assessment; to be consulted by the student(s) so that you understand the assignment brief, its context within the module, and any specific criteria and advice from the tutor:

Module title & code	WM3A6 – Cyber Security Incident Management
Module owner	Dr Olga Angelopoulou
Module tutor	Dr Olga Angelopoulou
Assessment type	Written report – Proposal of a cyber incident plan
Weighting of mark	60%

Word count	2000 words You will not be penalised for producing under length work, provided quality is not sacrificed to brevity. Learning to write to a limit is one of the skills the degree is designed to encourage you to cultivate.		
Does the word count allow +10%? Select ONE	Does the word count include tables? Select ONE	Does the word count include references? Select ONE	Does the word count include appendices? Select ONE
Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>
If appendices are included, will they be marked? Yes <input type="checkbox"/> No <input type="checkbox"/> NA <input type="checkbox"/>			

Submission format	Word <input type="checkbox"/> PDF <input type="checkbox"/> Other _____
--------------------------	---

Module learning outcomes (numbered)	<ol style="list-style-type: none"> 1. Critically evaluate the operation of a cyber-incident response plan. 2. Investigate digital artefacts against a realistic brief, preserving, analysing, interpreting and reporting significant material. 3. Critically evaluate the significant characteristics of relevant tools and techniques.
Learning outcomes assessed in this assessment (numbered)	1, 2, 3
Marking guidelines	<p>You will be marked based on the following criteria:</p> <ol style="list-style-type: none"> 1. Critical discussion and comparison of Incident Response Methodologies 2. Development of the SOP based on a given scenario – validity, applicability and appropriateness 3. Evaluation of relevant tools and techniques 4. Report structure and formatting <p>Please also see marking scale.</p>
Academic guidance resources	<p>You will have an opportunity to ask questions and get support on the assessment after it has been handed to you. You will be supported in this assessment through:</p> <ol style="list-style-type: none"> 1. The Teams Channel. 2. Through emails directed to the module tutor. 3. Specialist assessment support session. 4. One to one sessions (please arrange meetings with the module leader). <p>Notes to students: If support is provided on a Teams Channel or a Moodle forum, please ensure you check previous questions posted on the channel. The Teams/Moodle channel will typically be closed one week before the submission date and no new questions will be addressed, please organise your time accordingly. Please be patient with module tutors. Please turn on your Teams Channel/Moodle notifications. If a tutor has not responded to a query within 5 working days, please email the module leader.</p>
Special instructions	<p>Do not include the Assignment Guidance and Front Sheet in the submission.</p> <p>Spelling/grammar. Ensure that you spell check the submission, use a grammar checker and ensure that you proofread your work prior to submission. Spell/grammar checkers must be set to UK English, do not use ‘Americanised’ spellings.</p> <p>References. References are to be included at the end of the report using the Harvard referencing system. You may also include a bibliography.</p>

	<p>Each reference must be connected to a citation within the main body of the report.</p> <p>Do not attempt to hide text within JPEGs, this will be construed as an attempt to mislead the assessor.</p> <p>Coherence. A poorly worded report will hide excellent content. The narrative should be easy to read, and arguments should be presented coherently and convincingly.</p> <p>Presentation. At this stage in your studies, there is no excuse for poor presentation. You will not receive marks for presentation; however, your submission will be penalised for poor presentation.</p> <p>Formatting. All figures and tables must be properly labelled and captioned. All pages must be numbered. Formatting must be consistently applied throughout the submission. Submissions that stray from this guidance may be penalised.</p>
--	---

Table of Contents

Part A: Discussion.....	5
Part B: Standard Operating Procedure	7
1. Purpose.....	7
2. Scope.....	7
3. Roles & Responsibilities.....	8
4. Procedure	10
4.2 Triage Phase - Pre Breach	10
4.3 Core Response – The Incident Response Cycle.....	11
4.3.1 Scenario 1 – Phishing.....	11
4.3.2 Scenario 2 – Hacktivism	11
4.3.3 Scenario 3 – Ransomware.....	12
4.3.4 Process for all incidents.	12
4.4 Key Contacts	13
5 Glossary	13
Appendix A – Description of IR Methodologies Phases.....	14
Appendix B – Severity Matrix.....	16
Appendix C – Common Types of Information Security Incidents.....	17
References.....	18
Figure 1 - ABC's Organisational Structure	8
Figure 2 - ABC's Incident Response Life Cycle	10
Figure 3 - NIST Incident Response Life Cycle - (Cichonski et al., 2012).....	14
Figure 4 - SANS Incident Response Life Cycle (Kral, 2012).....	15
Figure 5 - NCSC Incident Response Life Cycle (NCSC, 2019a)	15
Figure 6 - Severity Matrix.....	16

Part A: Discussion

According to the NIST standard a computer incident, without lawful authority is a violation or imminent threat to the confidentiality, integrity or availability of information or an information system (Cichonski et al.). An incident response is a process that enables organisations respond to cybersecurity incidents methodically (Kral, 2012), its objective is to prevent similar attacks before they happen, minimise the cost and business disruption resulting from the incident (Souppaya and Scarfone, 2013). An organisation's incident response efforts are guided by an incident response plan (IRP), these are created and executed by a computer security incident response team (CISRT).


According to Accenture's (2023) cybersecurity resilience report, organisations develop custom IRPs based on general incident response methodologies developed by established institutions and governmental bodies such as the SANS Institute, the National Institute of Standards and Technology (NIST) and the National Cyber Security Centre (NCSC), enabling them to respond and prevent cyber threats including DDoS attacks, malware, ransomware, and phishing. Table 1 discusses and compares the most widely used methodologies. See appendix A for a detailed description of each methodology phases.

Criteria	SANS	NIST SP 800-61	NCSC
Framework Overview	Offers a set-by-step guide to incident respond with six phases: preparation, identification, detection, containment, eradication, recovery and lessons learned. (Kral, 2012)	Provides a comprehensive guide with four phases: preparation and prevention, Detection and analysis, containment, eradication, and recovery, post-incident activity. (Cichonski et al., 2012)	Offers a structured approach with four stages; analyse, contain, remediate, recover. NCSC (2019)
Scope and Applicability	Applicable to specific industries and organisations of different sizes	Designed to be flexible and adaptable to different organisational structures and sizes	Tailored for UK government entities but can be adopted to organisation globally
Strengths	<ul style="list-style-type: none"> Detailed incidents respond steps. Offers specific and detail guidance for various types of threats. 	<ul style="list-style-type: none"> Well-documented and widely adopted. Provides detailed technical guidance 	<ul style="list-style-type: none"> Focuses on practical application. Offers a clear guidance for incident prioritisation.
Weaknesses	<ul style="list-style-type: none"> It can be overwhelming for organisations with limited resources. Lack specificity for certain industries 	<ul style="list-style-type: none"> Too detailed and technical for Small to Medium Enterprises Implementation may require significant resources 	<ul style="list-style-type: none"> Lacks in-depth technical aspects. Too prescriptive for larger organisations
Integration with Standards	Integrates well with other security frameworks such as ISO 27001 and NIST Cybersecurity Framework.	Aligns with other NIST guidance such as SP 800-53 and the Cybersecurity Framework	Complies with UK government cybersecurity guidance and integrates easily with other industry frameworks such as NIST-800-61.

Adoption and Recognition	Widely recognised and used across industries globally	Adopted by US government agencies and large private sector organisations	Recognised within the UK government and adopted by SMEs.
---------------------------------	---	--	--

Table 1 - Industry Standard & Academic Incident Response Framework

Part B: Standard Operating Procedure

	Information Technology Standard Operating Procedure		Published Date: 01/01/2024	
	Information Security Incident Response Procedures		<table><tr><td>SOP #: 10-01-001</td><td>Revision #: Version 1.0</td></tr></table>	SOP #: 10-01-001
SOP #: 10-01-001	Revision #: Version 1.0			

1. Purpose

- 1.1 This Standard Operating Procedure (SOP) sets written guidelines containing both operational and technical components for incident response (CISA, 2023). It outlines in a systematic way, approaches to cyber incidents against ABC's infrastructure for prompt action.
- 1.2 This SOP aligns with UK data protection regulations such as the General Data Protection Regulation (GDPR) and Data Protection Act 2018 to protect ABC's customer and employee personal identifiable information (PII) data.
- 1.3 The SOP follows the National Cyber Security Centre's (NCSC) guidelines for incident response to enable ABC mitigate risks of significant operational, financial, or reputational damages by meeting industry standards and best practices.

2. Scope

- 2.1 This SOP details the necessary procedural to be taken to handle adverse events that attempts to breaches ABC's system security policy to affect its integrity or availability and the unauthorised access of ABC's digital assets; in line with the computer Misuse Act (1990).
- 2.2 This SOP focuses on three prevalent cybersecurity incidents within the media industry relevant to ABC's business:
 - 2.2.1 **Phishing Attacks:** Attempts to acquire sensitive information (login credentials, financial data) via deceptive emails, links, or websites.
 - 2.2.2 **Hacktivism:** Acts of disruption or data leaks against ABC driven by ideological or political motivations.
 - 2.2.3 **Ransomware:** Malicious software that encrypts, deletes data and systems and demanding a ransom for decryption or recovery.

3. Roles & Responsibilities

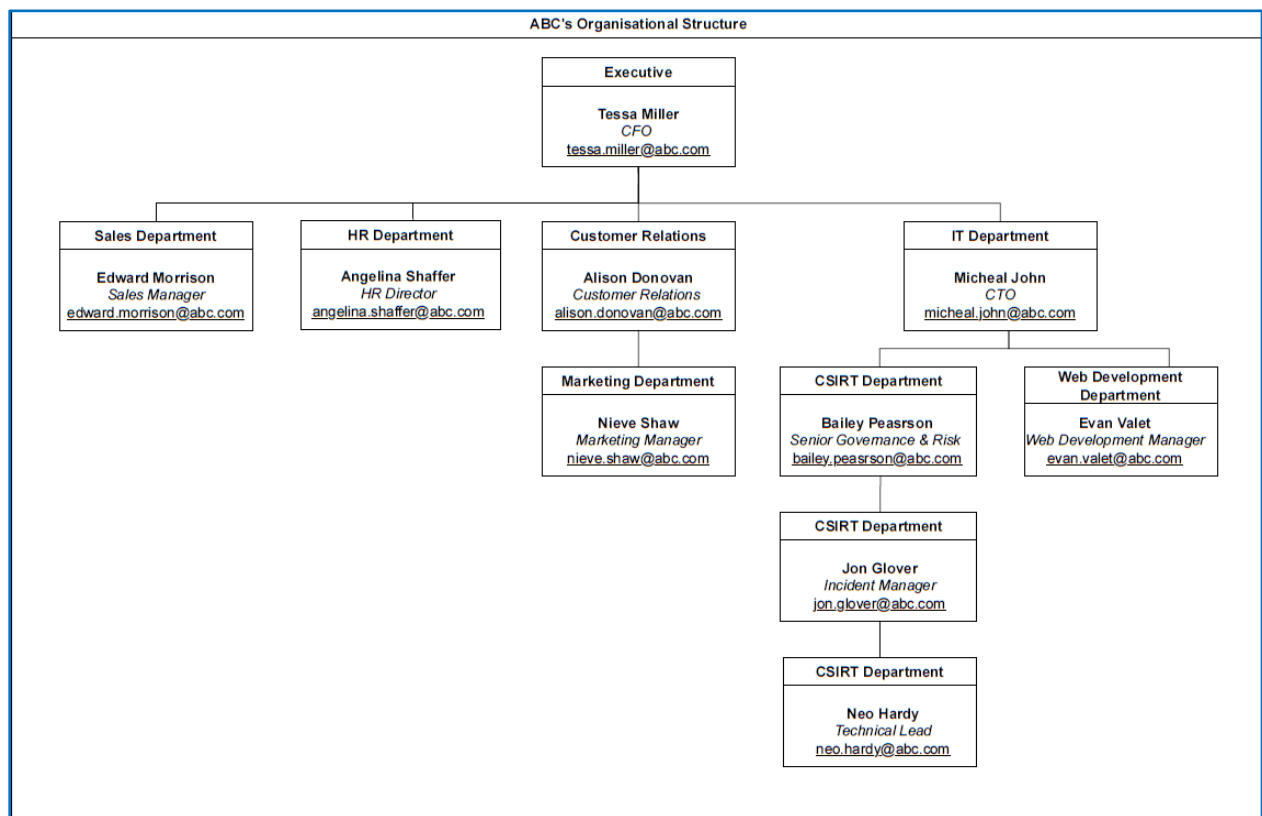


Figure 1 - ABC's Organisational Structure

3.1 The following outlines the key incident response responsibilities for each ABC's departmental personnel illustrated in Figure 1.

3.2 Chief Technology Officer (CTO):

- 3.2.1 Handles the leadership and accountability for incident response, legal, regulatory compliance.
- 3.2.2 Ensures that ABC incident response process to protect computer systems and data resources is followed.
- 3.2.3 Reviews incidents that attempt to breach ABC's CIA triad with the CSIRT.
- 3.2.4 Prepares a written report containing recommendations to ABC's management staff for addressing the causes of the incident.

3.3 Incident Manager:

- 3.3.1 Directs technical team in investigation, containment, and remediation tasks.
- 3.3.2 Coordinates the execution of IT-related aspects of the incident response SOP.
- 3.3.3 Implements temporary access restrictions and system shutdowns as needed.

3.4 Technical Lead:

- 3.4.1 Perform detail analysis of logs, network traffic, and compromised systems.
- 3.4.2 Identify the scope and nature of the attack.

- 3.4.3 Assists in remediation efforts. E.g. password resets and patching fixes.

3.5 Web Development:

- 3.5.1 Assist the IT Team to identify compromised websites or / and web applications.
- 3.5.2 Implements technical fixes for identified vulnerabilities.
- 3.5.3 Works with communications on public-facing messages around website disruptions.

3.6 Marketing Manager:

- 3.6.1 Manages all internal communications on the incident.
- 3.6.2 Handles external communications and press inquiries in coordination with the CTO.
- 3.6.3 Develops holding statements and talking points for media inquiries.

3.7 Senior Governance & Risk:

- 3.7.1 Ensures compliance during incident response and advises CTO on potential liabilities and regulatory requirements.
- 3.7.2 Guides potential reporting obligations under UK GDPR or other relevant regulations.
- 3.7.3 Evaluates and prepares document on ABC's liabilities and contractual consequences of the incidents.

3.8 Human Resources (HR):

- 3.8.1 Supports staff involved or affected by the incident.
- 3.8.2 Coordinates any potential disciplinary actions if an insider threat is found.

3.9 Customer Relations Team:

- 3.9.1 Handles customer inquiries and potential fallout from data breaches.
- 3.9.2 Follows communication scripts prepared by the communications team.
- 3.9.3 Provides a feedback loop to inform further decision-making.

4. Procedure

4.1 To manage incident response against the potential threats for ABC, a simplified model from the NIST's Computer Security Handling Guide (2012) developed by the NCSC, which divides incident response life cycle into four stages: analyse, contain, remediate, and recover, is applied, and illustrated in Figure 2.

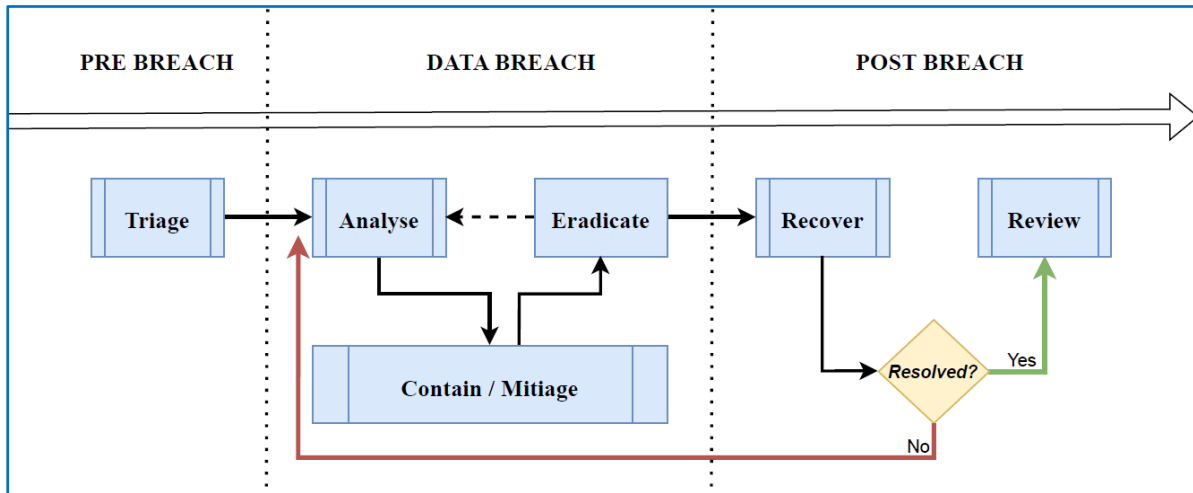


Figure 2 - ABC's Incident Response Life Cycle

4.2 Triage Phase - Pre Breach

- 4.2.1 It is essential to understand the type and severity of the potential / current incident to determine its urgency to act, the response approach and the correct people involved.
- 4.2.2 There are two types of aspects when addressing any incident: **Severity** and **Category**.
- 4.2.3 The Incident Manager must consider severity against the following:
- **Availability**: is the availability of ABC's digital assets impacted? What is the impact on ABC's business operations? (i.e. business continuity)
 - **Confidentiality**: has sensitive (e.g. customer PII data) been accessed, leaked, or stolen?
 - **Integrity**: could data or systems have been altered such that they cannot be trusted?
- 4.2.4 With all the above criteria, consideration should be given to the scale of the incident. To what type of system or data is involved, and the practical consequences of the incident.
- 4.2.5 Documentation detailing all critical assets and data impacted due to the incident must be carried out.
- 4.2.6 See appendix B for a severity matrix to aid the evaluation of incident severity.
- 4.2.7 The Incident Manager must also determine the type of incident ABC faces. Below are the most prevalent types of threats for ABC:
- Phishing.
 - Hacktivism.
 - Malware – Ransomware.
- 4.2.8 See appendix C for a list of other common types of incidents relevant to ABC.

4.3 Core Response – The Incident Response Cycle

4.3.1 See appendix A for a description of each of the Incident Response Cycles stages.

4.3.2 This SOP details below the key steps that ABC must take when encountering the most prevalent incidents following the NCSC incident response life cycle:

4.3.1 Scenario 1 – Phishing

Phase	Key Steps to Conduct
Analyse	<ol style="list-style-type: none">1. Identify the initial point of compromise (email, link, attachment)2. Collect and analyse email headers, URLs to uncover sender identities and malicious infrastructure.3. Determine the attack scope – Which users clicked, opened attachments,4. Contact the affected parties and maintain up-to-date communication
Contain / Mitigate	<ol style="list-style-type: none">1. Quarantine affected user accounts and machines.2. Temporarily block suspicious domains or IP addresses at firewall level.3. Change the credentials (e.g. passwords) of affected parties.4. Issue communication to all staff empathising heightened awareness and caution.
Remediate / Eradicate	<ol style="list-style-type: none">1. Perform deep scans for malware or unusual activity across affected systems.2. Enforce password resets for potential affected accounts.3. Recover affected systems from clean backups.4. Seek third-party assistance if required.
Recover	<ol style="list-style-type: none">1. Create an incident report and list actions that had been taken.2. Conduct evaluation & review session: “Were the defences in place adequate?” “Are there user training gaps?”.3. Determine if customer PII was leaked, ensure necessary reports are made within legal timeframes.4. Contact law enforcement if further actions are required (e.g. report of financial loss due to incident)5. Conduct user awareness training.

4.3.2 Scenario 2 – Hacktivism

Phase	Key Steps to conduct
Analyse	<ol style="list-style-type: none">1. Assess the type of attack (e.g. DDoS)2. Evaluate threat actor demands or messages if provided.3. Identify possible hacktivist groups likely to target ABC (e.g. TTPs)
Contain / Mitigate	<ol style="list-style-type: none">1. Coordinate with third party providers to mitigate effects if needed.2. Consider alternative communication channels if main websites are compromised.3. Work with the Communications teams to craft talking points for external response.
Remediate / Eradicate	<ol style="list-style-type: none">1. Restore disrupted or defaced websites from clean backups.2. Address technical vulnerabilities used in the attack and apply critical security patches.3. Heighten overall network monitoring and security posture against further attack.

Recover	<ol style="list-style-type: none"> 1. Conduct a through risk assessment to identify weak / vulnerable digital assets exposed. 2. Proactive media engagement is crucial to counter hacktivist narratives. 3. Assess if incident reporting to law enforcement agencies is needed.
----------------	--

4.3.3 Scenario 3 – Ransomware

Phase	Key Steps to conduct
Analyse	<ol style="list-style-type: none"> 1. Verify ransomware variant through IOCs. 2. Determine systems impacted and isolate infected systems as soon as possible and keep it within powered state for further analysis. 3. Analyse the attack scope (i.e. files or databases encrypted). 4. Communicate with affected parties and maintain up-to-date communication.
Contain / Mitigate	<ol style="list-style-type: none"> 1. Quarantine malware and ensure complete removal before resuming to normal system opinations. 2. Check the network, system, and memory logs for malicious activity and identify injection vectors (e.g. remote protocols, malicious attachments, or removable drives). 3. Block network communication with suspected threat actor's C2 server. 4. Work with the Communications teams to craft talking points for external response.
Remediate / Eradicate	<ol style="list-style-type: none"> 1. Prioritise recovery of the most critical systems & data first. 2. Determine if decryptor is available from a trusted source. If not, identify possible offline backups and recover data from affected systems. 3. Seek third-party assistance, if required 4. Consult law enforcement or forensics specialists if ransom payment is being considered. 5. Proceed to data recovery once the malware has been contained.
Recover	<ol style="list-style-type: none"> 1. Review the security of the affected systems (e.g. firewall configuration) 2. Create an incident report and list all the actions that have been taken during the incident. 3. Hold discussion session for improvements. 4. Determine if customer PII was leaked, ensure necessary reports are made within legal timeframes. 5. Contact law enforcement if further actions are required (e.g. report of financial loss due to incident)

4.3.4 Process for all incidents.

4.3.5 All information security incidents must be recorded and investigated in a timely manner.

4.3.6 Establish a clear reporting channel: all employees must know hoe and to whom they should report suspicious activity.

4.3.7 Technical lead should perform a preliminary analysis of the incident, to determine incident cause and potential risks for ABC. Collection of evidence, remediation activities,

and recommendations must be documented.

- 4.3.8 Establish clear rules for escalating incident to full response team.
- 4.3.9 Examine the affected computer systems and databases.
- 4.3.10 Coordinate external assistance to remove incident if necessary.
- 4.3.11 Notify or alert legal entities if required.
- 4.3.12 A final report on the findings, root of cause, future steps and countermeasures must be completed upon high and medium level incidents.
- 4.3.13 Restore data, remediate vulnerabilities, and implement new safeguards as required.

4.4 Key Contacts

- 4.4.1 Security incidents communication must be treated on a 'need-to-know' basis. Individuals who are not directly involved in the handling of the incident must be given information about the existence of the incident or methods used to contain or remediate the incident (e.g. external parties). The following list of the appropriate channels of communication.
- 4.4.2 Internal:
 - See Figure 1 for all the ABC internal personnel.
- 4.4.3 External:
 - Microsoft - <https://msrc.microsoft.com/create-report>
 - Apple - product-security@apple.com
 - Oracle - <https://support.oracle.com/portal/>
 - Cisco - csirt-notify@cisco.com
- 4.4.4 Legal:
 - NCSC – Report Incident - <https://report.ncsc.gov.uk/>
 - Data Protection Authority - <https://ico.org.uk/>

5 Glossary

- 5.1 CIA Triad – model to protect the Confidentiality, Integrity, and Availability of data.
- 5.2 IOC – Indicators of Compromise
- 5.3 TTPs – Tactics, Techniques and Procedures
- 5.4 DDoS – Distributed Denial-of-Service
- 5.5 C2 – Command & Control

Appendix A – Description of IR Methodologies Phases

Phase	Description
Preparation	In the preparation phase, the focus is on proactive measures for prevention. Including conducting risk assessments to understand potential threats and their impact, having a well-defined incident response plan that outlines roles and procedures, training staff to identify and report suspicious activity, and implementing the technical safeguards such as firewalls, intrusion detection systems, and data backup strategies.
Detection & Analysis	The objective of the Detection & Analysis phase is to identify and understand the nature of a security incident. This requires establishing a robust monitoring system that look for unusual activity, triaging the incident to assess its severity, preserving crucial evidence like logs and system states, and carefully analysing the attack methodology, attack vectors, and potential effects on the business.
Containment Eradication & Recovery	The Containment, Eradication & Recovery face Is where immediate action is taken to limit the damage caused by the incident and return affected systems to their normal state. This involves isolating infected systems, or compromised network segments to limit further spread, removing the root cause of the attack (e.g. malware), restoring from clean backups, patching any vulnerabilities that may have been exploited. This phase also includes implementing additional safeguards to harden defences against similar attacks.
Post- incident Activity.	The post-Incident Activity phase emphasises learning from the incident to avoid future recurrence. This includes performing a thorough analysis to understand how the breach initially occurred, using lessons learned to update the incident response plan and procedures, and implementing new security measures to address any weaknesses that were exposed by the incident. This phase also requires the communication with affected stakeholders (e.g. customers) or any regulatory reporting obligations.

Figure 3 - NIST Incident Response Life Cycle - (Cichonski et al., 2012)

Phase	Description
Preparation	The Preparation phase establishes the foundation for effective incident response. Key activities include developing a clear incident response plan, defining roles and responsibilities, providing necessary training for staff, acquiring the tools and resources required for response, and managing communications plans in case an incident were to occur.
Identification	The identification phase focuses on recognizing the occurrence of a potential security incident. This requires monitoring systems for anomalies, analysing suspicious activity, and determining if there is a legitimate security incident.
Containment	The Containment phases prioritises limiting the scope and impact of the incident. This includes isolating affected systems or network segments, preventing the attacker from escalating privileges or spreading laterally, and implementing short-term tactical measures to contain the threat.
Eradication	The eradication phase involves actions to remove any threats found within the environment. This involves removing malware, malicious code, reversing unauthorised system changes, disabling attacker tools, and addressing root causes that enabled the incident to occur.
Recovery	With the threat contained and eradicated, the recovery phase restores the affected system and operations to their normal state. This includes rebuilding systems, restoring from clean backups, implementing patches and any needed

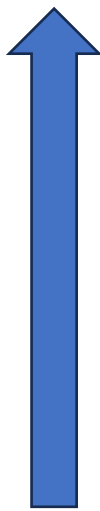
	configuration changes, and conducting testing to ensure functionality and security before returning systems to production.
Lessons Learned	The lessons learned phase is a critical review process conducted after an incident. This includes analysing the incident timeline, assessing response efficiency, reviewing root causes, and making recommendations for improving the incident response plan, policies, procedures, and security defences to mitigate future risks.

Figure 4 - SANS Incident Response Life Cycle (Kral, 2012)

Phase	Description
Analyse	The analyse phase involves gathering and interpreting information to understand the nature, scope and impact of the incident. This involves analysing log files, network traffic, and affected systems to determine the attack methods, identify compromised assets and accounts, and assess the potential damage and the risk of further compromise.
Contain / Mitigate	This phase focuses on limiting the effects of the incident to prevent further damage. This involves isolating affected systems, temporarily block malicious traffic, disabling compromised accounts, and implementing any tactical measures necessary to prevent the threat actor from gaining additional access.
Remediate / Eradicate	The remediate and eradication phase focuses on removing the threat from the environment and restoring systems to their secure, operational state. It involves activities such as removing malware and attacker tools, rebuilding systems from clean backups, implementing patches and updates to address exploited vulnerabilities, and enhancing security configurations to mitigate future risks.
Recover	In the recovery phase, the focus is on returning the systems and operations to their normal state and improving defences to prevent similar incidents. This includes extensive testing of restored systems to ensure they are secure and functional, documenting the incident and response actions, and conducting a post-mortem analysis to identify lessons learned to implement specific measures to strengthen the organisation's security posture.

Figure 5 - NCSC Incident Response Life Cycle (NCSC, 2019a)

Appendix B – Severity Matrix



Severity	Criteria
<i>Critical</i>	<ul style="list-style-type: none"> • Over 80% of critical personnel / departments unable to work. • Critical systems offline with no known resolution • High risk to breach of customer / client PII data • Potential financial impact of 45-75% of company's value
<i>High</i>	<ul style="list-style-type: none"> • 50% of personnel unable to work. • Risk of breach of customer / client PII data • Potential financial impact of 25-35% of company's value
<i>Medium</i>	<ul style="list-style-type: none"> • 20% of personnel unable to work. • Possible breach of small amounts of non-sensitive data • Low risk to reputation • Small number of non-critical systems • Affected with known resolutions
<i>Low</i>	<ul style="list-style-type: none"> • Minimal, if any, impact • One or two non-sensitive / critical systems affected. • <10% of non-critical personnel affected temporarily.

Figure 6 - Severity Matrix

Appendix C – Common Types of Information Security Incidents

- **Malicious Code:** Malware injection on the organisation's network, including ransomware attacks.
- **Distributed Denial of Service (DDoS):** Flood of network traffic taking down company's critical websites, phone lines, or other web facing systems e.g. databases, or internal systems e.g. payroll software.
- **Unauthorised Access:** Illegal access to systems, accounts, data by a threat actor (internal / external) – for example an attacker access a staff's email or account due to phishing attack.
- **Insider Threat:** Malicious or accidental actions by an employee causing a security incident.
- **Data Breach:** Lost / Stolen devices or hard copy documents, unauthorised access, or extraction of data from the organisation's network.

References

- Accenture (2023). *State of Cybersecurity Report 2023* | Accenture. [online] [www.accenture.com](https://www.accenture.com/us-en/insights/security/state-cybersecurity). Available at: <https://www.accenture.com/us-en/insights/security/state-cybersecurity>.
- Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. *Computer Security Incident Handling Guide*, [online] 2(2). doi:<https://doi.org/10.6028/nist.sp.800-61r2>.
- CISA (2020). *Standard Operating Procedures (SOPs)* | CISA. [online] www.cisa.gov. Available at: [https://www.cisa.gov/safecom/sops#:~:text=Standard%20Operating%20Procedures%20\(SOPs\)%20are](https://www.cisa.gov/safecom/sops#:~:text=Standard%20Operating%20Procedures%20(SOPs)%20are).
- Kral, P. (2012). *Incident Handler's Handbook* | SANS Institute. [online] www.sans.org. Available at: <https://www.sans.org/white-papers/33901/>.
- legislation.gov.uk (1990). *Computer Misuse Act 1990*. [online] Legislation.gov.uk. Available at: <https://www.legislation.gov.uk/ukpga/1990/18/contents>.
- NCSC (2019a). *Develop: Technical Response Capabilities*. [online] www.ncsc.gov.uk. Available at: <https://www.ncsc.gov.uk/collection/incident-management/technical-response-capabilities>.
- NCSC (2019b). *Plan: Your Cyber Incident Response Processes*. [online] Ncsc.gov.uk. Available at: <https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes>.
- Souppaya, M. and Scarfone, K. (2013). Guide to Malware Incident Prevention and Handling for Desktops and Laptops. *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*. [online] doi:<https://doi.org/10.6028/nist.sp.800-83r1>.