



**Suruhanjaya Sekuriti**  
Securities Commission  
Malaysia

# **GUIDANCE NOTE ON MANAGEMENT OF CYBER INCIDENTS**

**SC-GN/ (2-2022)**

1<sup>st</sup> Issued: 17 November 2022

## GUIDANCE NOTE ON MANAGEMENT OF CYBER INCIDENTS

Effective Date upon 1 <sup>st</sup> Issuance	17 November 2022
--	------------------

<b>Revision Series</b>	<b>Revision Date</b>	<b>Effective Date of Revision</b>	<b>Series Number</b>
-	-	-	-

## CONTENT

	Page
Chapter 1 <b>INTRODUCTION</b>	1
Chapter 2 <b>CYBER INCIDENT RESPONSE PLAN PROCESS OVERVIEW</b>	2
Chapter 3 <b>COMMUNICATION TO STAKEHOLDERS</b>	4
Chapter 4 <b>INCIDENT RESPONSE SCENARIOS</b>	5
<b>Part a: Preparation and Post Incident Phase</b>	5
<b>Part b: General Incident Scenario</b>	10
<b>Part c: Malware/Ransomware</b>	15
<b>Part d: Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)</b>	19
<b>Part e: Phishing</b>	22
<b>Part f: Unauthorised Access</b>	25
<b>Part g: Data Breach</b>	28
<b>Part h: Web Defacement</b>	33
<b>Part i: Successful Attacks from SQL Injection</b>	36
<b>Part j: Detection of Advance Persistent Threat</b>	38
<b>Part k: Successful Attacks from Zero-day Exploit</b>	41
<b>APPENDICES</b>	
<b>APPENDIX I</b>	45
<b>APPENDIX II</b>	53
<b>Definitions and Interpretation</b>	55

## Chapter 1

### INTRODUCTION

- 1.01 The Securities Commission Malaysia (SC) has set out requirements under the *Guidelines on Management of Cyber Risk* for capital market entities to have in place clear and comprehensive cyber policies and procedures, which commensurate with its risk profile and include the requirements to report <sup>1</sup>cyber incidents to the SC.
- 1.02 As part of efforts to manage cyber risks, all capital market entities are encouraged to establish its own cyber incident response process to enable timely, effective identification of cyber incidents, to manage and minimise damage from cyber incidents, and to recover and learn from such incidents.
- 1.03 A cyber incident is an observable occurrence indicating a possible breach in the systems, network and operating environment of a capital market entity.
- 1.04 This *Guidance Note on Management of Cyber Incidents* (Guidance Note) serves as a **guide** for all capital market entities in establishing their own cyber incident response process. As such, a capital market entity may adopt the processes and procedures in this Guidance Note to the extent that is appropriate and commensurate with the nature, scale and complexity of its business activities and risk profile.
- 1.05 The adoption of the practices in this Guidance Note does not necessarily denote compliance with the SC's requirements relating to the management of cyber risk by a capital market entity but will be taken into consideration by the SC in determining whether such requirements are complied with.
- 1.06 The information provided in this Guidance Note is not exhaustive and capital market entities are reminded to ensure that all aspects of managing cyber incidents risks have been taken into consideration in establishing its own processes.
- 1.07 A capital market entity should not reproduce and use this Guidance Note as its own. Instead, a capital market entity is expected to customise and establish its own cyber incident response process and may use this Guidance Note as reference.
- 1.08 This Guidance Note also includes sample cyber incident scenarios for capital market entities to consider for adoption when customising its own cyber incident response process.

---

<sup>1</sup> Capital market entities are required to report cyber incidents to SC via SC's Vault platform  
<<https://vault.seccom.com.my/>>

## CHAPTER 2

### CYBER INCIDENT RESPONSE PLAN PROCESS OVERVIEW

2.01 The following are phases in a cyber incident response process.

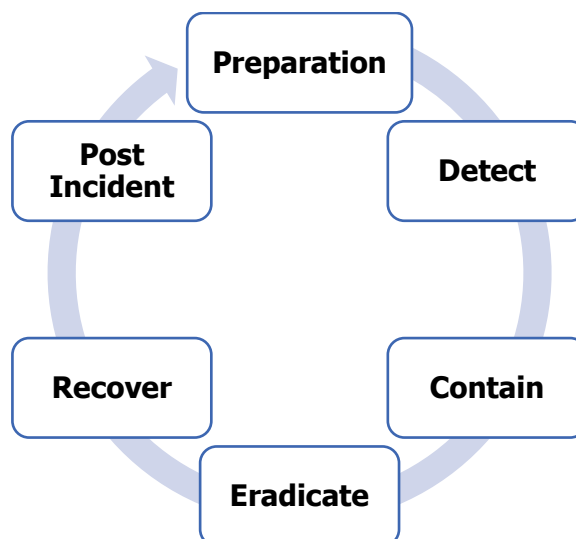


Figure 1: Cyber Incident Response Process<sup>2</sup>

2.02 **Preparation Phase:** The purpose of this phase is to ensure the capital market entity's policies and procedures; human resources and technology has the capability in dealing with cyber security incident. A capital market entity's security goals as well as policy and procedures for protecting critical information assets, should be aligned with its technology and business needs during this phase.

2.03 A capital market entity should consider establishing the following prior to adoption of the practices in this Guidance Note:

- i. Develop a written guidelines for prioritisation of incidents based on the criticality of the affected resources and current or potential technical effects.
- ii. Establish logging standards and procedures to ensure good quality data that is collected for detection and analysis.
- iii. Implement effective security controls and review these controls periodically to reduce the frequency of incidents.

*Computer Security Incident Handling Guide, Special Publication* Cichonski, P. , Millar, T. , Grance, T. and Scarfone, K. (2012), National Institute of Standards and Technology (NIST SP), Gaithersburg, MD, [online], <https://doi.org/10.6028/NIST.SP.800-61r2> (Accessed October 21, 2022).

- iv. Establish a Computer Security Incident Response Team (CSIRT) to coordinate incident response escalation within the capital market entity internally and communication to external parties.

- 2.04 **Detection Phase:** In the detection phase, it is integral to quickly detect the incident and have the incident response team to respond to the breaches. Once an incident is detected, the scope of impact should be determined, and a fresh incident report should be created to record the identified precursors<sup>3</sup> and indicators<sup>4</sup> including the chronological events.
- 2.05 **Containment Phase:** The focus of the containment phase is to limit damages, avoid further losses, and keep data for subsequent evaluation or legal reasons. Decision-making is an important aspect of confinement (e.g., shut down a system, disconnect it from a network, disable certain functions). Capital market entities should identify acceptable risks and establish appropriate short-term and long-term strategy in dealing with incidents. If containment steps are not viable or could not prevent recurrence of the incident, it is recommended that the system is rebuilt from a clean image.
- 2.06 **Eradication Phase:** The eradication phase entails removing the tactics or components used by a perpetrator to obtain or maintain a foothold in the impacted systems. During this phase, unwanted changes to systems are restored and exploited vulnerabilities are removed.
- 2.07 **Recovery Phase:** In the recovery phase, affected systems should be restored into operation. Recovery tasks include restoring systems from a clean backup, rebuilding systems from scratch, replacing corrupted files, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists). During this phase, affected systems which have been restored should be tested and monitored.
- 2.08 **Post Incident Phase:** The goal of this phase is to identify and address the gaps within the capital market entity, including its policies and procedures, human resources (i.e., skills required) and technology. A capital market entity should also identify the lesson learned and consider adopting long-term plans to reduce the risk of exposure to similar threat and strategise the communications to stakeholders.

---

<sup>3</sup> Signs or information that shows an attacker is preparing to cause an incident. For example, vulnerability scanning from unknown source and threatening email to attack the capital market entity.

<sup>4</sup> Signs or information that shows that an incident has occurred or is happening. For example, IPS alerts, antivirus alerts, or file integrity alerts.

## Chapter 3

### COMMUNICATION TO STAKEHOLDERS

3.01 A capital market entity is highly recommended to have in place an effective communication plan to its stakeholders, including prepare a guide with up-to-date contact details of the relevant parties. This is to limit the impact of cyber incidents while providing timely, factual, relevant and concise information to its stakeholders.

For the purpose of communication to stakeholders, including external parties, the following personnel and departments are recommended to be included in the communication plan:

- Chief Executive Officer (CEO);
- Chief Information Security Officer (CISO) or Head of IT, Information Security Manager or ISO;
- Head of Information Governance;
- Service Desk;
- Legal and Human Resource;
- Corporate Communications; and
- Business Continuity Leader.

In addition, a capital market entity may include effective instruction to the relevant stakeholders such as global reset of login credential requirement, as part of the operations restoration activities. A capital market entity should also consider the right timing in communicating with its stakeholders to ensure an effective and efficient implementation of the communication plan.

Note: Depending on the incident, a capital market entity may wish to engage with other interested parties including the capital market entity's Internet Service Provider (ISP), owners of the attacked IP address, third-party service provider including software vendor, affected external parties and law enforcement.

## CHAPTER 4

### INCIDENT RESPONSE SCENARIOS

4.01 In this section, examples of cyber incidents scenarios are set out below together with the recommended mitigation steps in each of the incident response phase. The steps should be further tailored according to the respective capital market entity's landscape, strategy, business continuity or disaster recovery plan and communication plan.

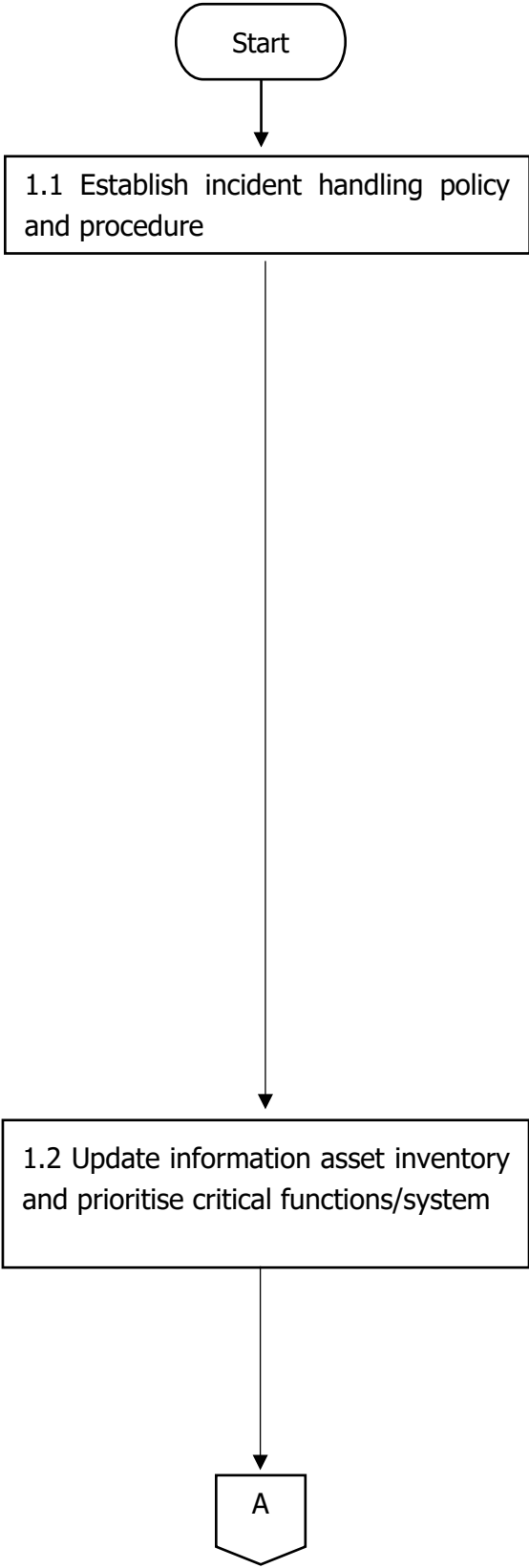
#### **a. Preparation and Post Incident Phase**

The Preparation and Post Incident phase in a cyber incident response plan is the general standard approach that would be applicable in every cyber incident scenario.

#### **i. Preparation phase**

- i.i. This phase is crucial for a capital market entity to successfully manage cyber risks and cyber incidents. It mainly covers the area of policies and procedures, human resources and technology (e.g., tools, communication plan, critical information assets, risk management, awareness training program, etc).
- i.ii. Capital market entities are encouraged to establish a clearly defined escalation and decision-making processes to ensure that any adverse effect of a cyber incident is properly managed and initiate recovery action quickly.
- i.iii. Capital market entities are encouraged to involve their key personnel responsible for the management of cyber risks when establishing their cyber incident response process and ensure all relevant employees in their organisation understand the cyber incident response process including their roles and responsibilities.
- i.iv. Capital market entities are encouraged to regularly review and update their cyber incident response process to ensure it remains relevant, comprehensive and effective.



Phase	Steps	Remarks
Preparation	 <pre> graph TD     Start([Start]) --&gt; S1[1.1 Establish incident handling policy and procedure]     S1 --&gt; S2[1.2 Update information asset inventory and prioritise critical functions/system]     S2 --&gt; A{{A}}             </pre>	<p>1.1 Establish policy which entails the incident handling procedures, including:</p> <ul style="list-style-type: none"> <li>• Personnel who has the authority to conduct interviews, make requests, review sensitive data, and co-ordinate communications.</li> <li>• Define incident and threats to guard against and respond to.</li> <li>• Identify core incident response team and stakeholders*.</li> <li>• Describe actions allow to be taken and when to take such actions.</li> <li>• Establish crisis communication plan which includes the contact details of interested parties, communication method and frequency.</li> </ul> <p>*Note: Refer to Appendix II for a sample of Responsible, Accountable, Consulted and Informed (RACI) chart to describe the roles and responsibilities of various parties in operating the cyber incident response process.</p> <p>1.2 Update asset inventory and perform regular identification of critical information asset, to ensure assets are protected. This includes, but not limited to the following:</p> <ul style="list-style-type: none"> <li>• Update the inventory of trusted IP which contains prioritised traffic.</li> <li>• Create data classification scheme and obtain approval.</li> <li>• Classifying data according to business criticality and sensitivity level.</li> <li>• Label data based on the classification.</li> </ul>

Phase	Steps	Remarks
	<pre> graph TD     A{{A}} --&gt; S13[1.3 Implement and review compliance of the preventative security practice]     S13 --&gt; S14[1.4 Review network architecture diagram]     S14 --&gt; S15[1.5 Regular monitoring of security log/alert]     S15 --&gt; S16[1.6 Provide training and awareness]     S16 --&gt; S17[1.7 Perform backup and recovery testing]     S17 --&gt; N21{{Next step 2.1}}                     </pre>	<p>1.3 Ensure layered preventative security practice are followed and assessed regularly. This includes firewalls, endpoint protection, IPS, IDS etc.</p> <p>1.4 Ensure logical and physical network architecture diagram is available and up to date. Where feasible, data flow diagram is to be established and maintained.</p> <p>1.5 Regular monitoring of security report to understand normal behavior and allow team to recognise abnormal behavior, when it happens.</p> <p>1.6 Necessary training to be provided to (i) key member to maintain the skillset and (ii) end user to promote awareness on IT hygiene.</p> <p>1.7 Ensure backup policy is met and disaster strategy is tested periodically. Suggest to also conduct tabletop exercise among the relevant parties.</p>

The following is the sample checklist for the preparation phase:

Action		Completed
<b>1.0</b>	<b>Identify stakeholder</b>	
1.1	Identify internal and external parties to be involved in incident response process	
1.2	Reach consensus with stakeholders on the planning and revision of incident response policy	
<b>2.0</b>	<b>Document Incident Response Plan and Policy</b>	
2.1	Incident response process and procedure	
2.2	Handling of liability issues including legal team action for external parties or customers and Human Resource action for internal stakeholders	
2.3	Communication plan/strategy	
2.4	Inventory of critical information assets and impact severity matrix	
2.5	Authorisation to conduct interview, invoke incident response team, access sensitive data, and co-ordinate communications	
<b>3.0</b>	<b>Develop RACI Matrix</b>	
3.1	Identify key response team member	
3.2	Define roles and responsibilities	
<b>4.0</b>	<b>Asset Inventory list</b>	
4.1	Classify data with approved data classification scheme (by business criticality and sensitivity of data)	
4.2	Critical information assets list (of which handles critical or sensitive data)	
4.3	Network architecture diagram (logical and physical)	
4.4	Data flow diagram (collate with network diagram)	
<b>5.0</b>	<b>Network security posture review</b>	
5.1	Set up of security solutions	
5.2	Regularly assess and review security posture	
5.3	Review by reputable third-party security vendor	
5.4	Risk assessment on the result of review	
5.5	Vulnerability assessment and penetration testing	
<b>6.0</b>	<b>Training and Awareness</b>	
6.1	Primary team or incident response team (e.g., incident handling skillset training, incident response tools training etc.)	
6.2	User awareness training	
<b>7.0</b>	<b>Testing and simulation</b>	
7.1	Testing of the recovery plan, backups recoverability, full-scale exercise, functional exercise, tabletop exercise and unannounced exercise	

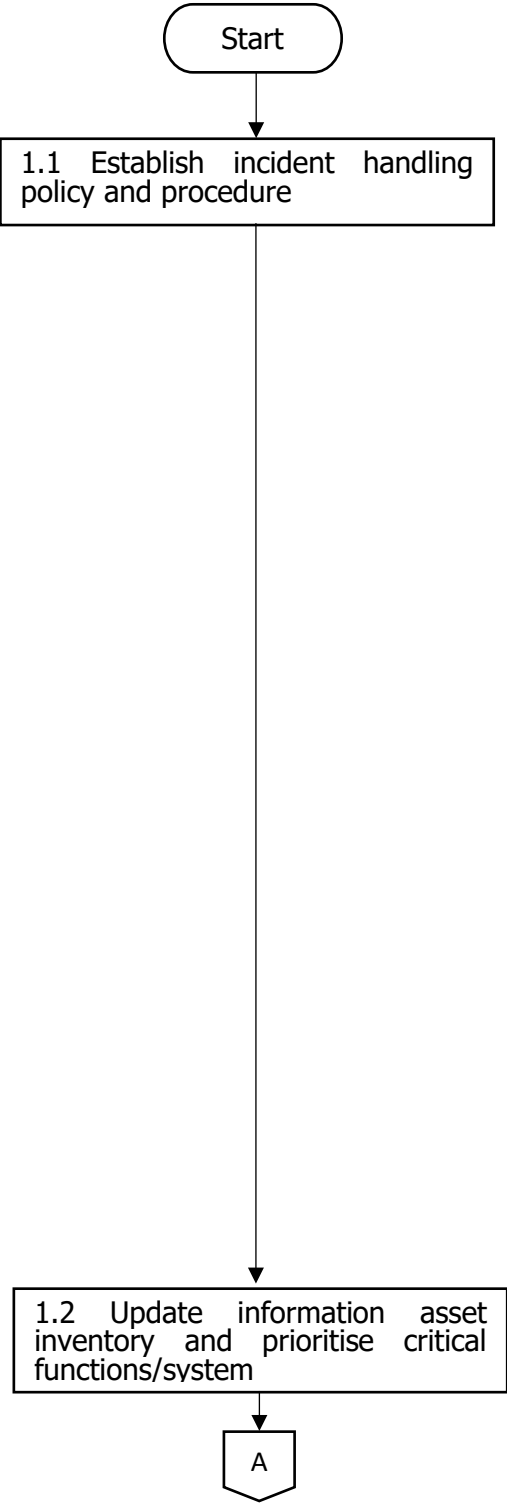
**ii. Post Incident Phase (Post Recovery Phase)**

In this phase, the personnel responsible for handling the incident response (Incident Response Handler) should gather feedback from those involved in the incident handling event and further review the policies and procedures, human resources (e.g., skills and awareness), and technology (e.g., tools for the purposes of strategy improvement) to reduce the likelihood of reoccurrence of similar incidents.

Phase	Steps	Remarks
Post Incident Activity	<pre> graph TD     A[Previous step] --&gt; B[6.1 Gather feedback]     B --&gt; C[6.2 Review the incident report]     C --&gt; D[6.3 Discuss improvement strategy]     D --&gt; E[6.4 Communication to stakeholders]     E --&gt; F([End])             </pre>	<p>6.1 On-scene Incident Response Handler to immediately gather feedbacks from all affected parties after recovery phase.</p> <p>6.2 Incident report to be reviewed and consensus to be reached with the relevant stakeholders prior to finalisation and preparation of executive summary.</p> <p>*Note: Please refer Appendix II for more elaboration on how to report and review an incident.</p> <p>6.3 From lesson learned, plan opportunities to reduce the risk, update policies and procedures and improve its cyber incident management process.</p> <p>6.4 Follow through incident escalation process and provide update of the situation to pre-identified parties i.e., enforcement regulatory agency (e.g., police and National Cyber Security Agency (NACSA)) and the SC.*</p> <p>*Note: Capital market entities are strongly advised to follow internal processes and procedures relating to incident escalation and management.</p>

**b. General Incident Scenario**

This general guide contains a general incident response plan covering from the initial incident preparation until post incident. This general guide may be used together with the capital market entity’s own guidelines for Business Continuity Plan (BCP) and Disaster Recovery (DR).

Phase	Steps	Remarks
Preparation	 <pre> graph TD     Start([Start]) --&gt; Step1[1.1 Establish incident handling policy and procedure]     Step1 --&gt; Step2[1.2 Update information asset inventory and prioritise critical functions/system]     Step2 --&gt; A{{A}}             </pre>	<p>1.1 Establish policy which entails the incident handling procedures, including:</p> <ul style="list-style-type: none"> <li>• Personnel who has the authority to conduct interviews, make requests, review sensitive data, and co-ordinate communications.</li> <li>• Define incident and threats to guard againsts and respond to.</li> <li>• Identify core incident response team and stakeholders*.</li> <li>• Describe actions that allow to be taken and when to take such actions.</li> <li>• Establish crisis communication plan which includes the contact details of interested parties, communication method and frequency.</li> </ul> <p>*Note: Refer to Appendix I for a sample of Responsible, Accountable, Consulted and Informed (RACI) chart to describe the roles and responsibilities of various parties in operating the cyber incident response process.</p> <p>1.2 Update asset inventory and perform regular identification of critical information asset, to ensure assets are protected. This includes, but not limited to the following:</p> <ul style="list-style-type: none"> <li>• Update the inventory of trusted IP which contains prioritised traffic.</li> </ul>

Phase	Steps	Remarks
	<pre> graph TD     A{{A}} --&gt; S13[1.3 Implement and review compliance of the preventative security practice]     S13 --&gt; S14[1.4 Review network architecture diagram]     S14 --&gt; S15[1.5 Regular monitoring of security log/alert]     S15 --&gt; S16[1.6 Provide training and awareness]     S16 --&gt; S17[1.7 Perform backup and recovery testing]     S17 --&gt; Next{{Next 2.1}}                     </pre>	<ul style="list-style-type: none"> <li>• Create data classification scheme and obtain approval.</li> <li>• Classifying data according to business criticality and sensitivity level.</li> <li>• Label data based on the classification.</li> </ul> <p>1.3 Ensure layered preventative security practice are followed and assessed regularly. This includes firewalls, endpoint protection, IPS, IDS etc.</p> <p>1.4 Ensure logical and physical network architecture diagram is available and up to date. Where feasible, data flow diagram is to be established and maintained.</p> <p>1.5 Regular monitoring of security report to understand normal behavior and allow team to recognise abnormal behavior, when it happens.</p> <p>1.6 Necessary training to be provided to (i) key member to maintain the skillset and (ii) end user to promote awareness on IT hygiene.</p> <p>1.7 Ensure backup policy is met and disaster strategy is tested periodically. Suggest to also conduct tabletop exercise among the relevant parties.</p>

Phase	Steps	Remarks
Detection	<pre> graph TD     A[Previous steps 1.7] --&gt; B[2.1 Initiate incident]     B --&gt; C[2.2 Restrict/disconnect the infected equipment]     C --&gt; D[2.3 Identify any blackmail notes]     D --&gt; E[2.4 Identify the sources]     E --&gt; F[2.5 Peruse incident severity matrix established in 'Preparation' phase to decide on the business impact]     F --&gt; G[2.6 Communication to stakeholder]     G --&gt; H[Next 3.1] </pre>	<p>2.1 Initiate incident report ticket to trigger the incident report process.</p> <p>2.2 Disconnect / restrict the infected equipment from any network e.g., physically / logically disconnect the device from network immediately, including any mirrors or DR versions.</p> <p>2.3 Identify if the capital market entity has received threat or blackmail from competitor or there is any internal feud.</p> <p>2.4 Identify the attack sources.</p> <p>2.5 Peruse incident <i>impact severity matrix</i> established in 'Preparation' phase to decide the preliminary business impact. This may also include performing triage on the affected host to determine the source host, criticality of users (i.e. administrative or power users) and determine impact.</p> <p>2.6 Follow through incident escalation process and provide update of the situation to pre-identified parties i.e., enforcement regulatory agency (e.g., police and National Cyber Security Agency (NACSA)) and the SC.*</p> <p>*Note: Capital market entities are strongly advised to follow internal processes and procedures on any part relating to incident escalation and management.</p>

Phase	Steps	Remarks
Containment	<pre> graph TD     A[Previous step 2.6] --&gt; B[3.1 Isolate network/ isolate system/ disable compromised ID]     B --&gt; C[3.2 Stop unwanted/ low priority services and identify compromised system or network]     C --&gt; D[3.3 Block sources]     D --&gt; E{3.4 Threat contained?}     E -- No --&gt; F[Go to 3.1]     E -- Yes --&gt; G[Next 4.1]             </pre>	<p>3.1 Isolate network/ system from the attack; or disable compromised ID</p> <p>3.2 Stop unwanted / low priority services and identify compromised system or network to avoid disruption to other services or operation.</p> <p>3.3 Block incoming sources (i.e., malicious domain using Domain Name System (DNS), firewall or proxies, block messages, isolate incoming traffic etc.)</p> <p>3.4 Identify the threat status, repeat the steps from 3.1 if the threat still exists.</p>
Eradication	<pre> graph TD     A[Previous step 3.4] --&gt; B[4.1 Perform vulnerabilities testing to identify gaps in the environment]     B --&gt; C[4.2 Develop remediation plan and apply accordingly]     C --&gt; D[Next 5.1]             </pre>	<p>4.1 Perform vulnerabilities testing on network and other infrastructure to identify other security gaps.</p> <p>4.2 Develop remediation (countermeasure) plan including tools and process e.g., antivirus signature update, external support/ vendor fixes, malware removal tool, implement</p>



Phase	Steps	Remarks
		<p>rules to block the suspicious traffic, disable compromised account.</p>
Recovery	<pre> graph TD     A[Previous step] --&gt; B{5.1 Threat contained?}     B -- No --&gt; C[Go to 2.2]     B -- Yes --&gt; D[5.2 Restore Services]     D --&gt; E[/Next 6.1/]             </pre>	<p>5.1 Verify the threat has been mitigated successfully. Repeat the steps from 2.2 if the threat still exists.</p> <p>5.2 Resume the services which stopped during incident and ensure all impacted services are running.</p>
Post Incident Activity	<pre> graph TD     A[Previous step] --&gt; B[6.1 Gather feedback]     B --&gt; C[6.2 Review the incident report]     C --&gt; D[6.3 Discuss improvement strategy]     D --&gt; E([End])             </pre>	<p>6.1 On-scene Incident Response Handler to immediately gather feedbacks from all affected parties after recovery phase.</p> <p>6.2 Incident report to be reviewed and consensus to be reached with the relevant stakeholders prior to finalisation and preparation of executive summary.</p> <p>*Note: Please refer Appendix II for more elaboration on how to report and review an incident.</p> <p>6.3 Following the incident, plan opportunities to reduce the risk, update policies and procedures and improve its cyber incident management process.</p>

Phase	Steps	Remarks
Post Incident	Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.	

### c. Malware/Ransomware

Malware is malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware. Additionally, ransomware is a type of malware that encrypts a user's or an organisation's critical data, making it impossible to access files, databases, or programs. It is frequently intended to propagate over a network and target database and file servers, paralysing a whole enterprise in the process. The attacker then demands a ransom from the victim in exchange for restoring access to the data.

Phase	Steps	Remarks
Preparation	Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.	
Detection	<pre> graph TD     A1[Previous step 1.7] --&gt; B[2.1 Initiate incident report]     B --&gt; C["2.2 Peruse incident severity matrix established in 'Preparation' phase to decide on the business impact"]     C --&gt; D[2.3 Collate initial incident data]     D --&gt; E{A}           </pre>	<p>2.1 Initiate incident report ticket to trigger the incident report process.</p> <p>2.2 Peruse incident <i>impact severity matrix</i> established in 'Preparation' phase to decide the preliminary business impact. This may also include performing triage on the affected host to determine the source host, criticality of users (i.e., administrative or power users) and determine impact.</p> <p>2.3 Collate initial incident data including:</p> <ul style="list-style-type: none"> <li>• Timeline of malware detection</li> <li>• Source of alert</li> <li>• Location (physical and logical) of detection</li> <li>• Number of affected machines, if possible</li> </ul>

	<pre> graph TD     A{{A}} --&gt; B[2.4 Communication to stakeholders]     B --&gt; C{{Next 3.1}}             </pre>	<ul style="list-style-type: none"> <li>Perform sandboxed execution of malware to determine the behavior</li> </ul> <p>2.4 Follow through incident escalation process and provide update of the situation to pre-identified parties i.e., enforcement regulatory agency (e.g., police and National Cyber Security Agency (NACSA)) and the SC.*</p> <p>*Note: Capital market entities are strongly advised to follow internal processes and procedures relating to incident escalation and management.</p>
<b>Phase                      Steps    Remarks</b>		
<p>Containment</p>	<pre> graph TD     A{{Previous step 2.4}} --&gt; B[3.1 Restrict the infected equipment from network]     B --&gt; C[3.2 Collect evidence]     C --&gt; D[3.3 Run scan and prevent spread]     D --&gt; E{{A}}             </pre>	<p>3.1 Disconnect / restrict the infected equipment from any network e.g., physically or logically disconnect the device immediately, including to any mirrors or DR site.</p> <p>3.2 Forensic image is best to be collected prior to any mitigation effort. This includes snapshot of virtual systems and clone of physical drives. Also collect evidence from other sources (e.g., system logs, network device logs etc.).</p> <p>3.3 Run a scan across entire system and search for indicators. Apply countermeasure to stop malware/ransomware spreading, including but not limited to:</p> <ul style="list-style-type: none"> <li>Block identified Command and Control (C&amp;C) communication with firewall and DNS server</li> <li>If required, block email messages, sender, sender IP, any attached links and send global</li> </ul>

	<pre> graph TD     A{{A}} --&gt; D{3.4 Attack contained?}     D -- No --&gt; N31{{Next 3.1}}     D -- Yes --&gt; N41{{Next 4.1}}             </pre>	<p>notification to inform users and remind users to stay vigilant</p> <ul style="list-style-type: none"> <li>• Suspend suspected compromised accounts</li> <li>• Disable suspected compromised component</li> <li>• Update Anti-Virus (AV) signatures</li> <li>• Update security patches</li> <li>• Update firewall and Security Information and Event Management (SIEM) rules</li> </ul> <p>3.4 Use analysis tool to observe malware if infection is contained. Repeat steps from 3.1 until malware stops spreading.</p>
<p>Eradication</p>	<pre> graph TD     Start{{Previous step 3.4}} --&gt; 41[4.1 Perform thorough review to identify root cause]     41 --&gt; 42[4.2 Finalise incident chronology]     42 --&gt; 43[4.3 Develop and apply remediation]     43 --&gt; A{{A}}             </pre>	<p>4.1 Analyse evidence to identify malware/ransomware execution time, features utilised to execute the malware, and plan appropriate mitigation steps to close the gaps.</p> <p>4.2 Draw incident chronology with as many details as possible. These may include, but not limited to:</p> <ul style="list-style-type: none"> <li>• Who accessed;</li> <li>• What changed, code installed/used, data affected/accessed/exfiltrated, file extension being encrypted;</li> <li>• When it occurred, and how long; and</li> <li>• How it happened/ vulnerability/exploitation which has been used.</li> </ul> <p>4.3 Thorough identification of affected machine, develop remediation (countermeasure) plan including tools and processes (e.g., antivirus signature update, external support/ vendor fixes, malware removal tool).</p>

	<pre> graph TD     A[A] --&gt; D{4.4 Attack contained?}     D -- No --&gt; B[Go to step 3.1]     B --&gt; D     D -- Yes --&gt; C[Next step 5.1]             </pre>	<p>4.4 Run a scan across entire organisation and monitor threat using analysis tool. Repeat the steps from 3.1 if the threat is not contained.</p>
<p>Recovery</p>	<pre> graph TD     D[Previous step 4.4] --&gt; E[5.1 Rebuild and repair systems]     E --&gt; F[5.2 Reconnect to the network]     F --&gt; G[Next 6.1]             </pre>	<p>5.1 Rebuild and repair systems. This may include the following steps:</p> <ul style="list-style-type: none"> <li>• Fully patch all deployed systems prior to redeployment</li> <li>• Hardened systems based on industry-standard i.e. refer to Center for Internet Security (CIS) benchmark</li> <li>• Scan systems for vulnerabilities</li> <li>• Risk review process to be performed for systems with entirely new applications</li> <li>• Close/mitigate gaps in endpoint protection</li> <li>• Recover affected files</li> <li>• Improve backup process to include ransomware resistance</li> </ul> <p>5.2 Reconnect to the production environment and restore the services which stopped during the incident. Ensure all impacted services are running.</p>
<p>Post Incident</p>	<p>Note: Please refer to the general 'Preparation' and 'Post Incident' phase in paragraph (a) of Chapter 4.</p>	

#### d. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)

DoS and DDoS attack is a type of cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to a network. The results of DDoS may prevent genuine traffic from being able to get through. Recent trends show that attackers attempt to extort money from organisations by threatening them with DDoS, also known as Ransom DDoS (RDDoS).

Phase	Steps	Remarks
Preparation	Note: Please refer to the general 'Preparation' and 'Post Incident' phase in paragraph (a) of Chapter 4.	
Detection	<pre> graph TD     A[Previous step 1.7] --&gt; B[2.1 Initiate incident report]     B --&gt; C[2.2 Identify type of DDoS attack, targeted service, and sources]     C --&gt; D[2.3 Peruse incident severity matrix established in 'Preparation' phase to decide on the business impact]     D --&gt; E{A}           </pre>	<p>2.1 Initiate incident report ticket to trigger the incident report process.</p> <p>2.2 Based on network monitoring activities sourcing from multiple resources/tools (e.g., SIEM, IDS, firewall, scanners etc.), identify type of attack, attack symptoms, scope of attack, affected service, service accessibility (internal &amp; external). The capital market entity to consider the following:</p> <ul style="list-style-type: none"> <li>• Identify if the capital market entity has received threat or blackmail from a competitor or there is any internal feud.</li> <li>• Analyse incoming packets to identify attack pattern</li> <li>• Create attack timeline</li> <li>• Look out for signs of other ongoing attack</li> </ul> <p>2.3 Peruse incident <i>impact severity matrix</i> established in 'Preparation' phase to decide the preliminary business impact. This may also include performing triage on the affected host to determine the source host, criticality of users (administrative or power users) and determine impact.</p>

	<pre> graph TD     A{{A}} --&gt; B[2.4 Communication to stakeholder]     B --&gt; C{{Next step 3.1}}             </pre>	<p>2.4 Follow through incident escalation process and provide update of the situation to pre-identified parties i.e., enforcement regulatory agency (e.g., police and National Cyber Security Agency (NACSA)) and the SC.*</p> <p>*Note: Capital market entities are strongly advised to follow internal processes and procedures relating to incident escalation and management.</p>
--	---	---

Phase	Steps	Remarks
-------	-------	---------

<p>Containment and Eradication</p>	<pre> graph TD     Prev{{Previous step 2.4}} --&gt; S31[3.1 Isolate the internal traffic from external connection]     S31 --&gt; S32[3.2 Stop unwanted services to servers and routers]     S32 --&gt; S33[3.3 Disrupt/filter DDoS traffic]     S33 --&gt; D34{3.4 Attack contained}     D34 -- No --&gt; S32     D34 -- Yes --&gt; Next{{Next step 4.1}}             </pre>	<p>3.1 Isolate the network service between internal and external usage.</p> <p>3.2 Stop unwanted or low priority services that contributes to the high utilization.</p> <p>3.3 Based on the traffic analysis result, block DDoS traffic via load balancer, firewall or router and configure device to not respond for the incoming DDoS traffic.* And further request assistance from ISP to activate secondary line for mitigation e.g., perform filtration for Tier 1 and Tier 2 / traffic scrubbing.</p> <p>*Note: Filtering is usually only effective against attack targeting computer resource and not viable for volumetric attack.</p> <p>3.4 Verify the attack status. If not contained, repeat the steps start from 3.2.</p>
------------------------------------	---	--

<p>Recovery</p>	<pre> graph TD     A[Previous steps 3.4] --&gt; B[4.1 Restore services]     B --&gt; C[4.2 Restore operation]     C --&gt; D[Next step 6.1]             </pre>	<p>4.1 Restore the services which stopped during DDoS attack and ensure all impacted services are running.</p> <p>4.2 Rollback to working state and apply Intrusion Detection System (IDS)/IPS and firewall updates.</p>
<p>Post Incident</p>	<p>Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.</p>	



**e. Phishing**

Phishing is a type of social engineering where an attacker sends a fraudulent message (using deceptive email messages, websites etc.) designed to trick Internet users into revealing personal or confidential information which can then be used illicitly.

Phase	Steps	Remarks
Preparation	Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.	
Detection	<pre> graph TD     A1[Previous step 1.7] --&gt; B[2.1 Initiate incident report]     B --&gt; C[2.2 Identify type of phishing activity, target, and source]     C --&gt; D[2.3 Peruse incident severity matrix established in 'Preparation' phase to decide on the business impact]     D --&gt; E[A]             </pre>	<p>2.1 Initiate incident report ticket to trigger the incident report process.</p> <p>2.2 Identify type of attack*, email, spear, whaling, smishing and vishing and angler. And identify compromised data* and if the phishing is targeted at a certain individual or group.</p> <p>Note:</p> <ul style="list-style-type: none"> <li>• This may include mass mailing, spear phishing, spoofing, impersonation attack, compromise of business email or email infrastructure.</li> <li>• If malicious link or attachment found in phishing email, suggest to run the malware/ransomware scenario guide.</li> </ul> <p>2.3 Peruse incident <i>impact severity matrix</i> established in 'Preparation' phase to decide the preliminary business impact. This may also include performing triage on the affected host to determine the source host, criticality of users (e.g., administrative or</p>

	<pre> graph TD     A{{A}} --&gt; B[2.4 Communication to stakeholders]     B --&gt; C{{Next step 3.1}}             </pre>	<p>power users) and determine impact.</p> <p>2.4 Follow through incident escalation process and provide update of the situation to pre-identified parties i.e., enforcement regulatory agency (e.g., police and National Cyber Security Agency (NACSA)) and the SC. If necessary, send global notification to inform users together with instruction to be followed.</p> <p>*Note: Capital market entities are strongly advised to follow internal processes and procedures relating to incident escalation and management.</p>
<div style="display: flex; justify-content: space-between; padding: 5px;"> <span><b>Phase</b></span> <span><b>Steps</b></span> <span><b>Remarks</b></span> </div>		
<p>Containment</p>	<pre> graph TD     D{{Previous step 2.4}} --&gt; E[3.1 Block sources]     E --&gt; F[3.2 Suspend compromised credentials]     F --&gt; G{{Next step 4.1}}             </pre>	<p>3.1 As result of initial analysis (2.2), block (i) malicious domain using DNS, firewall, proxies, and (ii) sender (including email subject/body/attachment etc.)</p> <p>3.2 Proceed to suspend compromised or at-risk credentials and disable vulnerable technical component.</p>

<p>Eradication</p>	<pre> graph TD     A[Previous step 3.2] --&gt; B[4.1 Remove the phishing email and content]     B --&gt; C[Next step 5.1]             </pre>	<p>4.1 Purge related messages from user inbox or make the messages not accessible. Suggest applying the following controls:</p> <ul style="list-style-type: none"> <li>• Implement antispam, anti-impersonation, email authentication, email encryption or IP based restriction.</li> <li>• Reset password to the compromised accounts.</li> </ul>
<p>Recovery</p>	<pre> graph TD     A[Previous step 4.1] --&gt; B{5.1 Attack contained?}     B -- No --&gt; C[Go to step 3.1]     B -- Yes --&gt; D[5.2 Increase detection]     D --&gt; E[Next step 6.1]             </pre>	<p>5.1 Verify the phishing has been mitigated successfully. Repeat the steps from 3.1 if the threat still exists.</p> <p>5.2 Increase the alert detection level with improved monitoring, mainly related to account, IP address or domains.</p>
<p>Post Incident</p>	<p>Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.</p>	

**f. Unauthorised Access**

Unauthorised access is a type of attack used to gain unauthorised access to systems within a security perimeter. Attackers start by finding weak points in a capital market entity’s defences and gaining access to a system.

Phase	Steps	Remarks
Preparation	<p>Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.</p>	
Detection	<pre> graph TD     A1[Previous steps 1.7] --&gt; B[2.1 Identify type of attack and Initiate incident report]     B --&gt; C[2.2 Identify compromised access, system and services]     C --&gt; D[2.3 Peruse incident severity matrix established in 'Preparation' phase to decide on the business impact]     D --&gt; E[A]             </pre>	<p>2.1 Identify type of attack: (i) horizontal (e.g. credential exploitation, privileged vulnerabilities and exploit, misconfigurations, malware and social engineering); or (ii) vertical (e.g. security question, brute force, credential stuffing, password change and reset). Initiate incident report ticket to trigger the incident report process.</p> <p>2.2 Identify the compromised access by reviewing logs, database query, generating report etc. Identify compromised systems (e.g. servers, desktop, laptop, mobile or Virtual Machine (VM)) and services (e.g., web, financial system).</p> <p>2.3 Peruse incident impact severity matrix established in 'Preparation' phase to decide the preliminary business impact. This may also include performing triage on the affected host to determine the source host, criticality of users (e.g., administrative or power users) and determine impact.</p>

	<pre> graph TD     A{{A}} --&gt; B[2.4 Communication to stakeholders]     B --&gt; C{{Next 3.1}}             </pre>	<p>2.4 Follow through incident escalation process and provide update of the situation to pre-identified parties i.e., enforcement regulatory agency (e.g., police and National Cyber Security Agency (NACSA)) and the SC*.</p> <p>Note: Capital market entities are strongly advised to follow internal processes and procedures relating to incident escalation and management.</p>
Phase	Steps	Remarks
Containment	<pre> graph TD     D{{Previous step 2.4}} --&gt; E[3.1 Disconnect compromised system or network]     E --&gt; F[3.2 Disable compromised account]     F --&gt; G{{Next 4.1}}             </pre>	<p>3.1 Disconnect the compromised server, desktop, VM or system from the network and perform integrity check</p> <p>3.2 Identify compromised account and disable it to prevent it from further manipulation.</p>

<p>Eradication</p>	<pre> graph TD     A[Previous step 3.2] --&gt; B[4.1 Perform patching and assessment to implement stronger control]     B --&gt; C[4.2 Remove affected system]     C --&gt; D[Next 5.1]             </pre>	<p>4.1 Request for system patch for the affected systems, perform vulnerabilities and security posture assessment, and enforce strong authentication method.</p> <p>4.2 Remove/replace affected systems, perform data forensics, and determine level of access to identified system.</p>
<p>Recovery</p>	<pre> graph TD     A[Previous step 4.2] --&gt; B{5.1 Perform scan and verify whether attack is contained?}     B -- No --&gt; C[Go to 3.1]     B -- Yes --&gt; D[5.2 Recover System]     D --&gt; E[Next 6.1]             </pre>	<p>5.1 Scan system and host with the updated signature. Clear vulnerabilities and update routers. Repeat the steps from 3.1 if the threat still exists.</p> <p>5.2 Reimage operating system, restore IDS/IPS and update firewall.</p>
<p>Post Incident</p>	<p>Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.</p>	

**g. Data Breach**

A data breach incident involves confidential, sensitive, and restricted information being exposed or stolen, copied, or used by a malicious insider (an insider may also purposefully or inadvertently cause loss of data or information) or an external perpetrator.

Phase	Steps	Remarks
Preparation	Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.	
Detection	<pre> graph TD     A1[Previous steps 1.7] --&gt; B[2.1 Initiate incident report]     B --&gt; C[2.2 Conduct initial investigation]     C --&gt; D[2.3 Peruse incident severity matrix established in 'Preparation' phase to decide on the business impact]     D --&gt; E[A]             </pre>	<p>2.1 Initiate incident report ticket to trigger the incident report process.</p> <p>2.2 Initial investigation on the incident to include: cause of the incident, (e.g., hacker; loss of device; likelihood of employee involvement; malware)</p> <ul style="list-style-type: none"> <li>• location of data (physical and logical)</li> <li>• quantity/size of data (e.g., number of accounts, unique numbers, client names)</li> <li>• type of data (e.g., financial/customer)</li> <li>• data format (e.g., encrypted, layout, length)</li> <li>• encryption, if any,</li> <li>• possible data source or owner.</li> </ul> <p>2.3 Peruse incident impact severity matrix established in 'Preparation' phase to decide the preliminary business impact. This may also include performing triage on the affected host to determine the source host, criticality of users (e.g., administrative or power users) and determine impact.</p>

	<pre> graph TD     A{{A}} --&gt; B[2.4 Communication to stakeholders]     B --&gt; C{{Next 3.1}}         </pre>	<p>2.4 Follow through incident escalation process and provide update of the situation to pre-identified parties i.e., enforcement regulatory agency (e.g., police and National Cyber Security Agency (NACSA)) and the SC.*</p> <p>*Note: Capital market entities are strongly advised to follow internal processes and procedures relating to incident escalation and management.</p>
<p>Containment</p>	<pre> graph TD     D{{Previous step 2.4}} --&gt; E[3.1 Perform detailed investigation]     E --&gt; F{{A}}         </pre>	<p>3.1 Based on technical investigation, confirm the data involved is from the organisation, legitimate, connected to their stakeholders, and other relevant considerations. Capital market entities may consider conducting full forensic investigation. The scope of investigation may include the following, but is not limited to:</p> <ul style="list-style-type: none"> <li>• Analysis of suspicious network activity.</li> <li>• Review of AV logs and events.</li> <li>• Identification of the data source and the data set.</li> <li>• Review the vulnerability scan report.</li> <li>• Correlation of security events or indicators of compromise with suspicious activity on the network.</li> </ul>



	<pre>graph TD; A{{A}} --&gt; B[3.2 Analyse the extent of compromised]; B --&gt; C[3.3 Develop remediation plan and disconnect compromise system or network]; C --&gt; D{{B}}</pre>	<p>3.2 Engage data owners and senior management for detailed understanding of the impact of compromised data, this include determining the attack methodology and timeline, type of data (e.g. personal data, business strategy document, credit card details), quantity of data, source of data (e.g. only found in organisation environment or shared on third party system) and also potential breach of regulatory compliance.</p> <p>3.3 Develop remediation (countermeasure) plan and disconnect or restrict the infected equipment from any network (e.g., shut down a system), and monitor suspicious activity. This includes implementing rules to block suspicious traffic, and disabling the compromised account. Depending on the analysis, consider the following:</p> <ul style="list-style-type: none"><li>• Secure copies of infected system or malware, if not already completed.</li><li>• Reverse engineer malware to identify the indicators of compromise.</li><li>• Engage experts to take down stolen data from online markets.</li></ul>
--	--	--

	<pre> graph TD     B{{B}} --&gt; S34[3.4 Safeguard critical information assets]     S34 --&gt; Next41{{Next step 4.1}}             </pre>	<p>3.4 To avoid further harm, reset passwords for legitimate users and reduce permissions, or consider remotely erasing stolen data and further isolate unauthorised users.</p>
--	---	---

Phase	Steps	Remarks
-------	-------	---------

<p>Eradication</p>	<pre> graph TD     Prev34{{Previous step 3.4}} --&gt; S41[4.1 Perform eradication to evict the adversary from environment]     S41 --&gt; A{{A}}             </pre>	<p>4.1 Perform actions to eradicate the adversary, including but not limited to:</p> <ul style="list-style-type: none"> <li>• Identify common removal methods and remove any malware identified.</li> <li>• Remove any identified artifacts used to facilitate the breach, (e.g., scripts, code, and binaries)</li> <li>• Disable systems and user accounts that have been used.</li> <li>• Perform testing on fixes, apply an update to the endpoint protection, and implement other protection capabilities such as encryption, Data Loss Prevention (DLP) or other alternatives.</li> </ul>
--------------------	---	--

	<pre> graph TD     A[A] --&gt; B[4.2 Reset compromised access credentials]     B --&gt; C{4.3 Attack contained?}     C -- No --&gt; D[Go to step 3.1]     C -- Yes --&gt; E[Next 5.1]         </pre>	<p>4.2 Reset credentials of compromised account and enforce stronger authentication.</p> <p>4.3 Run a scan across the entire organisation and monitor threats using the analysis tool. Repeat the steps from 3.1 if the threat is not contained.</p>
<p>Recovery</p>	<pre> graph TD     F[Previous step 4.3] --&gt; G[5.1 Recover Service]     G --&gt; H[5.2 Restore suspended services]     H --&gt; I[Next 6.1]         </pre>	<p>5.1 Perform restoration from trusted backup.</p> <p>5.2 Continue restoring any suspended services and reintegrate the compromised system.</p>
<p>Post Incident</p>	<p>Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.</p>	

## h. Web Defacement

Web defacement is a type of attack in which malicious attackers get access to a website and alter the files and content with their own messages. The impact of such attack may result in long-term damage to brand and reputation during and after the incident. The motives for defacement attack may include hacktivism, political reason, ransom demands for restoring website, or revenge.

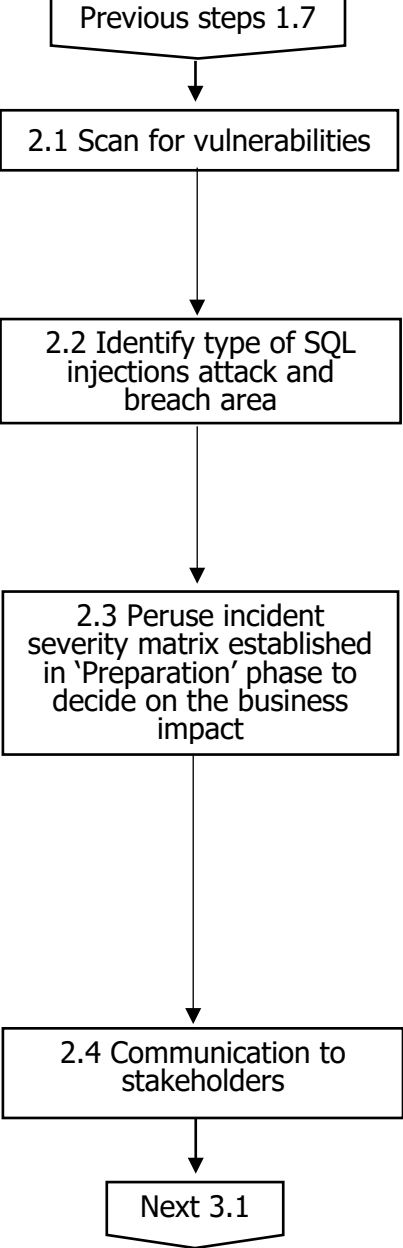
Phase	Steps	Remarks
Preparation	Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.	
Detection	<pre> graph TD     A[Previous step 1.7] --&gt; B[2.1 Initiate incident report]     B --&gt; C[2.2 Conduct initial investigation]     C --&gt; D[2.3 Identify origin and vulnerabilities]     D --&gt; E[2.4 Communication to stakeholder]     E --&gt; F[Next 3.1]           </pre>	<p>2.1 Initiate incident report ticket to trigger the incident report process. This may include means of detection (e.g. notification from employee or security check result).</p> <p>2.2 Initial investigation on the incident to include verification on the ownership of the web server and verify defacement via modification date and hash signature.</p> <p>2.3 Identify the defacement origin* and vulnerability including analyse present links, log files and scan database for malicious content, running services, etc.</p> <p>*Note:</p> <ul style="list-style-type: none"> <li>• Depends on the analysis result and likelihood of internal threat, consideration to be given to run 'Unauthorised access' guide.</li> <li>• Close any exploited vulnerability or backdoors and apply patches.</li> </ul> <p>2.4 Follow through incident escalation process and provide update of the situation to pre-identified parties i.e., enforcement regulatory agency (e.g., police and National Cyber Security Agency (NACSA)) and the SC.*</p>

		<p>*Note: Capital market entities are strongly advised to follow internal processes and procedures relating to incident escalation and management.</p>
<p>Containment</p>	<pre> graph TD     A[Previous step 2.4] --&gt; B[3.1 Disconnect compromised system or network and minimise]     B --&gt; C[3.2 Collect forensic image]     C --&gt; D[Next 4.1]             </pre>	<p>3.1 Isolate the website or redirect web traffic to predetermined temporary websites following defacement incident.</p> <p>3.2 Forensic image is best to be collected prior to any mitigation effort. This includes snapshot of virtual systems and clone of physical drives. Also collect evidence from other sources (e.g., system logs, network device logs, etc.)</p>
<p>Eradication</p>	<pre> graph TD     A[Previous steps 3.2] --&gt; B[4.1 Perform clean up]     B --&gt; C[4.2 Perform monitoring]     C --&gt; D[4.3 Update and enforce components and patches]     D --&gt; E{4.4 Attack contained?}     E -- No --&gt; F[Go to step 3.1]     E -- Yes --&gt; G[Next 5.1]             </pre>	<p>4.1 Perform clean up on the infected machines and restore from earlier backup which is free from vulnerabilities.</p> <p>4.2 Determine any suspicious movement between systems in network.</p> <p>4.3 Update vulnerable components, apply security patches (if applicable), enforce strong authentication and reset credentials for breached accounts.</p> <p>4.4 Verify the threat status, repeat the steps from 3.1 if the threat still exists.</p>

<p>Recovery</p>	<pre> graph TD     A[Previous step 5.1] --&gt; B[5.1 Restore service]     B --&gt; C[5.2 Restore operation]     C --&gt; D[Next 6.1]             </pre>	<p>5.1 Continue restoring any suspended services and reintegrate the compromised system.</p> <p>5.2 Restore web to business-as-usual (BAU) state</p>
<p>Post Incident</p>	<p>Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.</p>	

### i Successful Attacks SQL Injection

Structured Query Language (SQL) injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.

Phase	Steps	Remarks
Preparation	Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.	
Detection	 <pre> graph TD     A[Previous steps 1.7] --&gt; B[2.1 Scan for vulnerabilities]     B --&gt; C[2.2 Identify type of SQL injections attack and breach area]     C --&gt; D[2.3 Peruse incident severity matrix established in 'Preparation' phase to decide on the business impact]     D --&gt; E[2.4 Communication to stakeholders]     E --&gt; F[Next 3.1]           </pre>	<p>2.1 Detect SQL injections attack using vulnerability scanner as well as database query and examine any unexpected behaviour.</p> <p>2.2 Identify type of attack (e.g., unsanitised input, blind SQL, out of band). Identify the breach area (e.g., data breach, data exfiltration, modifying or corrupting data, deleting data).</p> <p>2.3 Peruse incident <b>impact severity matrix</b> established in 'Preparation' phase to decide the preliminary business impact. This may also include performing triage on the affected host to determine the source host, criticality of users (e.g., administrative or power users) and determine impact.</p> <p>2.4 Follow through incident escalation process and provide update of the situation to pre-identified parties i.e., enforcement regulatory agency (e.g., police and National Cyber Security Agency (NACSA)) and the SC.*</p> <p>*Note: Capital market entities are strongly advised to follow internal processes and procedures</p>

		relating to incident escalation and management.
Containment and Eradication	<pre> graph TD     A{{Previous steps 2.4}} --&gt; B[3.1 Disconnect compromised system and constrain user]     B --&gt; C[3.2 Perform input validation]     C --&gt; D[3.3 Perform Vulnerability Assessment (VA) and patching]     D --&gt; E{{Next 4.1}}         </pre>	<p>3.1 Disconnect or restrict the infected equipment from any network e.g., shut down a system, and monitor suspicious activity. This includes implementing rules to block the suspicious traffic. Constraint users to small set of well-define functionality on the server side and all application to run in the least privileged mode.</p> <p>3.2 Validate the size and values of input parameter request to database and sanitise all user input to remove all unwanted characters before going to SQL engine.</p> <p>3.3 Perform vulnerabilities testing to identify the existence of other potential threat.</p>
Phase                      Steps                      Remarks		
Recovery	<pre> graph TD     A{{Previous steps 3.3}} --&gt; B{4.1 Attack contained?}     B -- No --&gt; C{{Go to step 3.1}}     B -- Yes --&gt; D[4.2 Resume Services]     D --&gt; E{{Next 6.1}}         </pre>	<p>4.1 Verify the attack has been mitigated successfully. Repeat the steps from 3.1 if the threat still exists.</p> <p>4.2 Resume the web and database operation.</p>
Post Incident	Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.	

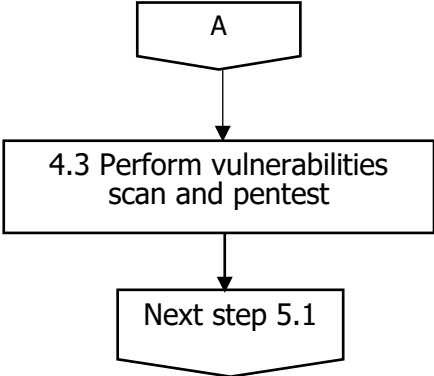
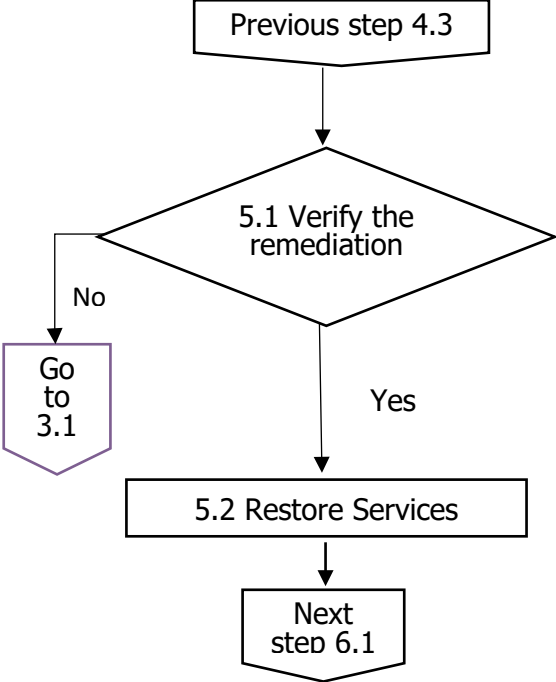


**j. Detection of Advance Persistent Threat**

An advanced persistent threat (APT) is a sophisticated and sustained cyber-attack in which an intruder establishes an undetected presence in a network.

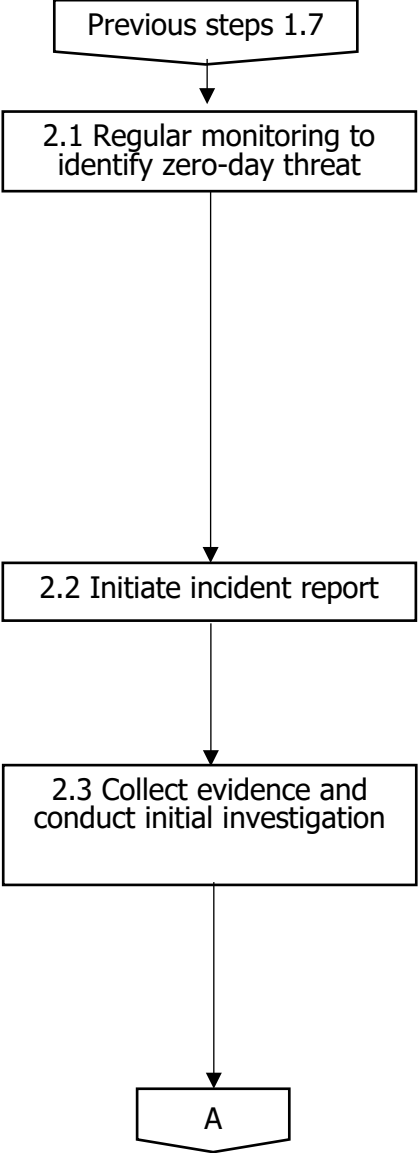
Phase	Steps	Remarks
Preparation	<p>Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.</p>	
Detection	<pre> graph TD     A[Previous step 1.7] --&gt; B[2.1 Initiate incident report]     B --&gt; C[2.2 Identify breach]     C --&gt; D[2.3 Peruse incident severity matrix established in 'Preparation' phase to decide on the business impact]     D --&gt; E[2.4 Communication to stakeholders]     E --&gt; F[Next step 3.1]             </pre>	<p>2.1 Initiate incident report ticket to trigger the incident report process.</p> <p>2.2 Identify breach (e.g., Data extraction, network infiltration, unusual user account activities).</p> <p>2.3 Peruse incident <b>impact severity matrix</b> established in 'Preparation' phase to decide the preliminary business impact. This may also include performing triage on the affected host to determine the source host, criticality of users (i.e., administrative or power users) and determine impact.</p> <p>2.4 Follow through incident escalation process and provide update of the situation to pre-identified parties i.e., enforcement regulatory agency (e.g., police and National Cyber Security Agency (NACSA)) and the SC.*</p> <p>*Note: Capital market entities are strongly advised to follow internal processes and</p>

Phase	Steps	Remarks
Containment	<pre> graph TD     A[Previous step 2.4] --&gt; B[3.1 Isolate the compromised network, account, or system]     B --&gt; C[3.2 Update securities patches for network]     C --&gt; D[3.3 Filter incoming network packets]     D --&gt; E{3.4 Threat contained?}     E -- No --&gt; F[Go to 3.1]     F --&gt; B     E -- Yes --&gt; G[Next step 4.1]             </pre>	<p>procedures relating to incident escalation and management.</p> <p>3.1 Isolate compromised network, disable account, or compromised system from the infrastructure.</p> <p>3.2 Update security patches, group policy, firewall and whitelist.</p> <p>3.3 Filter network packets and block suspicious activities.</p> <p>3.4 Identify the threat status, repeat the steps from 3.1 if the threat still exists.</p>
Eradication	<pre> graph TD     A[Previous step 3.4] --&gt; B[4.1 Create image for forensic investigation]     B --&gt; C[4.2 Reset password and reimage OS, AD]     C --&gt; D[A]             </pre>	<p>4.1 Create image as a method to collect evidence for forensic investigation (if required).</p> <p>4.2 Reset password for compromised account, reimage operating system (OS), Lightweight Directory Access Protocol (LDAP)/Active Directory (AD) (if required).</p>

Phase	Steps	Remarks
	 <pre> graph TD     A{{A}} --&gt; B[4.3 Perform vulnerabilities scan and pentest]     B --&gt; C{{Next step 5.1}}             </pre>	<p>4.3 Run vulnerabilities scan and pentest to identify gaps in security.</p>
Recovery	 <pre> graph TD     D1{{Previous step 4.3}} --&gt; D2{5.1 Verify the remediation}     D2 -- No --&gt; D3{{Go to 3.1}}     D2 -- Yes --&gt; R1[5.2 Restore Services]     R1 --&gt; D4{{Next step 6.1}}             </pre>	<p>5.1 Verify the attack has been mitigated successfully. Repeat the steps from 3.1 if the threat still exists.</p> <p>5.2 Enable user account and remove the isolation.</p>
Post Incident	<p>Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.</p>	

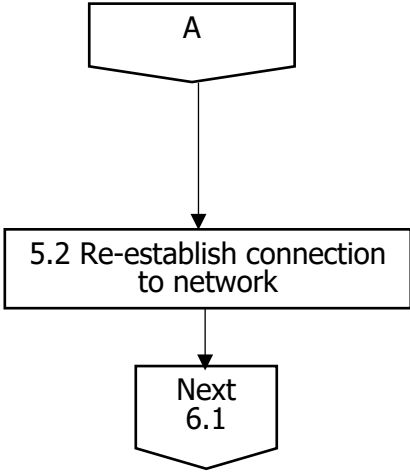
**k. Successful Attacks Zero-day Exploit**

A zero-day attack occurs when attackers exploit software vulnerabilities that are unknown to the software vendor, users, or antivirus vendors. In the event of a zero-day attack, the impacted system may lose data encryption and authorisation, or cause algorithm failure, password security issues, etc. Since zero-day attacks are difficult to prevent, a capital market entity’s ability to survive one is dependent on its ability to monitor, recognise and respond to an incident after it has occurred.

Phase	Steps	Remarks
Preparation	Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.	
Detection	 <pre> graph TD     A[Previous steps 1.7] --&gt; B[2.1 Regular monitoring to identify zero-day threat]     B --&gt; C[2.2 Initiate incident report]     C --&gt; D[2.3 Collect evidence and conduct initial investigation]     D --&gt; E[A]             </pre>	<p>2.1 Ongoing engagement with third party security service provider to identify zero-day threats. This may also be detected from unusual user/network behavior, unauthorized changes or other indicator of compromise.</p> <p>2.2 Initiate incident report ticket to trigger the incident report process.</p> <p>2.3 Forensic image is best to be collected prior to any mitigation effort. This may comprise snapshot of virtual systems and clone of physical drives. Also collect evidence from other sources (e.g., system logs, network device logs etc.). Subsequently, conduct initial investigation on the incident together with solution provider, including identifying the attack vector.</p>



<p>Eradication</p>	<pre> graph TD     A[Previous steps 3.1] --&gt; B[4.1 Connect with vendor]     B --&gt; C[4.2 Perform further monitoring]     C --&gt; D[4.3 Remove vulnerability]     D --&gt; E{4.4 Attack contained?}     E -- No --&gt; F[Go to 3.1]     E -- Yes --&gt; G[Next 5.1]             </pre>	<p>4.1 Communicate with software vendor to understand their mitigation timeline and strategy.</p> <p>4.2 Determine any suspicious movement between systems in network.</p> <p>4.3 Upon receiving patch / update from vendor, perform testing on fixes and apply update on the endpoint protection.</p> <p>4.4 Verify the threat status, repeat the steps from 3.1 if the threat still exists.</p>
<p>Recovery</p>	<pre> graph TD     A[Previous steps 4.4] --&gt; B[5.1 Rebuild and restore system]     B --&gt; C[A]             </pre>	<p>5.1 Rebuild and restore systems. This may include the following steps, but not limited to:</p> <ul style="list-style-type: none"> <li>• Fully patch all deployed systems prior to redeployment.</li> <li>• Hardened systems based on industry-standard i.e., refer to CIS benchmark</li> <li>• Scan systems for vulnerabilities</li> <li>• Risk review process to be performed for systems with entirely new applications</li> </ul>

	 <pre> graph TD     A[A] --&gt; B[5.2 Re-establish connection to network]     B --&gt; C[Next 6.1]             </pre>	<ul style="list-style-type: none"> <li>• Close/mitigate gaps in endpoint protection</li> <li>• Recover affected files</li> <li>• Improve backup process to include ransomware resistance</li> </ul> <p>5.2 Reconnect to the production environment and restore the services which stopped during the incident.</p>
<p>Post Incident</p>	<p>Note: Please refer to the general 'Preparation' and 'Post Incident' phase discussed in paragraph (a) of Chapter 4.</p>	

## APPENDICES

### APPENDIX I General Incident Response Checklist

The following are cyber incident response checklists containing recommended actions to be taken in pre-incident phase and other phases of incident response in various types of incidents. A capital market entity should not reproduce and use the sample checklists as its own. Instead, a capital market entity is expected to customise and establish its own incident response strategy and may use the sample checklists as reference.

#### General Pre-incident Response Checklist

The checklist below describes a guide of recommended steps to be taken by a capital market entity upon discovery of a potential incident during 'Pre-Incident' phase. This phase involves identification of an incident, determining whether an incident has occurred and classifying the type of incident.

No	Action	Completed
<b>Detect</b>		
1.	Determine whether an incident has occurred	
a.	Analyse the precursors and indicators	
b.	Search for correlating information	
c.	Perform research (e.g., search engine, knowledge base)	
d.	Once an incident is identified, begin documenting the incident response flow, and consider collecting evidence for future use.	
2.	Classify the incident using categories stated in paragraphs (a) to (k) of Chapter 4. Note: An incident may consist of more than one component and hence, more than one scenario incident response checklist may be applicable.	

The following are scenario incident response checklists which may be used as reference by a capital market entity in different types of incidents as set out below. For each specific type of incident, the checklist may vary based on individual incidents and the strategies adopted by the capital market entity.



For example:

i. Denial-of-Service / Distributed Denial-of-service

No	Action	Completed
<b>Detect</b>		
3.	A denial-of-service incident has occurred. Start logbook/report on:	
a.	Report time and report personnel	
b.	Affected system (hostname, operating system, IP address, location)	
c.	DoS/DDoS symptoms	
d.	Status and scope of attack (Stopped, Confined, Spreading, Spreading to Internal)	
e.	Identify the impact: <ul style="list-style-type: none"> <li>List of affected services</li> <li>Services accessibility from internal and external</li> </ul>	
4.	Analyse the precursors and indicators	
a.	Capture and analyse incoming packets to identify common elements: <ul style="list-style-type: none"> <li>Sending IP addresses</li> <li>Port</li> <li>Protocol</li> <li>User agent</li> <li>Payload</li> <li>Packet flags</li> </ul>	
5.	Search for correlating information	
a.	DoS/DDoS attack type	
b.	Ransom email	
c.	Timeline of events starting from detection of first attack	
d.	Signs of other ongoing attack whilst DoS/DDoS could be used as distraction	
6.	Report the incident according to communication plan	
<b>Contain</b>		
7.	Consideration to be given to whether:	
a.	Filter traffic with the identified attack pattern	
b.	Request ISP to initiate DoS/DDoS mitigation	
c.	Separating Internet web and email traffic from product and services	
d.	Request ISP to completely stop all traffics toward affected systems	

No	Action	Completed
e.	Implement Business Continuity Plan	
<b>Eradicate</b>		
8.	Consideration to be given to whether:	
a.	Patching affected systems to protect against exploited vulnerabilities	
b.	Implementation of network segmentation	
c.	Blacklist attackers' IP addresses	
d.	Removal of vulnerable systems or services	
<b>Recover</b>		
9.	Restore all affected systems and stopped services to an operationally ready state	
10.	Confirm that the affected services are functioning normally	
11.	Consideration to be given as to whether to implement additional monitoring to look out for future related activity	
<b>Post-Incident Activity</b>		
12.	Create a lesson-learned report with minimum details below: <ul style="list-style-type: none"> <li>• Details of the identified and remediated cyber incident to include timing, type, and location of incident as well as the effect on users</li> <li>• Activities that were undertaken by relevant working groups, service providers and business stakeholders that enabled normal business operations to be resumed</li> <li>• Recommendations where any aspects of policies and procedures, human resources or technology could be improved across the capital market entity to help prevent a similar cyber incident from reoccurring, as part of a formalised lessons identified process</li> </ul>	
13.	Complete the formalised lessons identified process to provide feedbacks for future preparation activities	

## ii. Malicious code

No	Action	Completed
<b>Detect</b>		
1.	A malicious code incident has occurred. Start logbook:	
a.	Report time and report personnel	

No	Action	Completed
b.	Affected system (hostname, operating system, IP address, location)	
c.	Malicious code symptoms	
d.	Scope of attack (user endpoint, server endpoint, spreading in local network, spreading in domain connected network, spreading in entire network)	
e.	Identify the impact: <ul style="list-style-type: none"> <li>• List of affected systems</li> <li>• Data loss (if can be determined at this phase)</li> </ul>	
2.	Analyse the precursors and indicators	
a.	Record and collate the initial incident data including but not limited to: <ul style="list-style-type: none"> <li>• Timeline of malware starting from first detection and other identified indicators (if can be determined at this phase)</li> <li>• Source of alert</li> <li>• Sandboxed execution of malware to determine its behaviour</li> <li>• The probable scope of effect besides the identified machine</li> <li>• Action and result of anti-malware solution on the malware</li> </ul>	
3.	Search for correlating information	
a.	Malware name and family	
b.	Ransom email	
c.	Research threat intelligence sources and consider security vendor assistance to gain further intelligence and supported mitigations	
d.	Sign of theft or misuse of privileged credential	
4.	Secure artifacts, include forensically sound copies of suspected malicious code and copies of affected system. Preserve all evidence to support attribution or anticipated legal action	
5.	Report the incident according to communication plan	
<b>Contain</b>		
6.	Consideration to be given to whether:	
a.	Monitor any new infections which may indicate that the malware has started spreading	
b.	Ensure that anti-malware solution has the latest definitions and patch deployed	
c.	Initiate an anti-malware scan for all live computer systems	

No	Action	Completed
d.	Determine if infected machines are communicating with external parties – block or sinkhole such communication	
e.	Suspend login of suspected compromised accounts	
f.	Physically or logically isolate infected machines from network	
g.	Implement corporate disaster recovery process	
<b>Eradicate</b>		
7.	Consideration to be given to whether:	
a.	Identify removal methods based on the result of malicious code analysis or trusted sources	
b.	Create a malware removal process to eradicate malware using appropriate tool	
c.	Restore affected system from trusted back up	
d.	Change password of suspected compromised accounts	
e.	Rebuild affected system from clean image and update with trusted backup of data	
f.	Apply all available security patching before restoring any system back to network	
<b>Recover</b>		
8.	Restore all affected systems and stopped services to an operationally ready state	
9.	Confirm that the affected services are functioning normally	
10.	Monitor indicators of compromise which might be a sign of re-emerging malware attack	
11.	Restore any suspended services or accounts	
12.	Consideration to be given as to whether to implement additional monitoring to look out for future related activity	

## iii. Unauthorised access

No	Action	Completed
<b>Detect</b>		
1.	An unauthorised access incident has occurred. Start logbook:	
a.	Report time and report personnel	
b.	Affected system/application/data	
c.	Identify the current and potential impact on: <ul style="list-style-type: none"> <li>Personal data</li> </ul>	

No	Action	Completed
	<ul style="list-style-type: none"> <li>• Sensitive organisation data</li> <li>• Privileged access</li> <li>• Privileged operation</li> </ul>	
2.	Analyse the precursors and indicators	
a.	Record and collate the initial incident data including but not limited to: <ul style="list-style-type: none"> <li>• Access logs of compromised system, if available</li> <li>• Recorded footage, if available</li> <li>• Details of attacker</li> <li>• Affected system</li> <li>• Affected user</li> <li>• Technology components of affected system</li> <li>• Entry point of foothold (if can be determined at this phase)</li> </ul>	
3.	Look for correlating information including:	
a.	Threat intelligence or cybersecurity news on recently disclosed arbitrary access to vulnerabilities or ongoing hacktivism that has been announced	
b.	Patching status of affected system	
c.	Technical details of access control (IP based restriction, password policy, MFA, least privilege, etc.)	
d.	Flow of authentication (i.e. from public to Azure AD, then federated authentication to on-premises AD)	
4.	Report the incident according to communication plan	
<b>Contain</b>		
5.	Consideration to be given to whether:	
a.	Determine if affected systems are communicating with external parties – block or sinkhole such communication	
b.	Physically or logically isolate affected systems from network	
c.	Suspend login of suspected compromised accounts	
d.	Initiate system integrity check to detect any unwanted change	
e.	Patch all technical components of affected systems	
<b>Eradicate</b>		
6.	Consideration to be given to whether:	
a.	Patching affected systems to protect against vulnerabilities exploited	
b.	Risk and vulnerability assessment and remediation	
c.	Network security posture assessment and remediation	
d.	Removal/upgrade of vulnerable technology components	

No	Action	Completed
e.	Enforce strong authentication method	
<b>Recover</b>		
7.	Restore all affected systems and stopped services to an operationally ready state	
8.	Confirm that the affected services are functioning normally	
9.	Monitor indicators of compromise which might be a sign of re-emerging attack	
10.	Restore any suspended services or accounts	
11.	Consideration to be given as to whether to implement additional monitoring to look out for future related activity	

## iv. Inappropriate usage

No	Action	Completed
<b>Detect</b>		
1.	An inappropriate usage incident has occurred. Start logbook:	
a.	Report time and report personnel	
b.	Affected system (hostname, operating system, IP address, location)	
c.	Inappropriate action (unauthorised service usage, access to inappropriate materials, launching attack against external without clearance)	
d.	Identify the impact of: <ul style="list-style-type: none"> <li>• Damage to capital market entity's reputation</li> <li>• Criminal activity</li> </ul>	
2.	Analyse the precursors and indicators	
a.	Record and collate the initial incident data including but not limited to: <ul style="list-style-type: none"> <li>• Network/security appliance alert</li> <li>• Running of new software/service</li> <li>• Abnormal usage of network or computing resources</li> <li>• Application logs on servers (email, File Transfer Protocol (FTP), proxies, etc)</li> <li>• Inappropriate file content detected on endpoint solution</li> <li>• Internal/external report</li> </ul>	
3.	Look for correlating information including:	
a.	Recent occurrence of security incident, especially in the nature of unauthorised access type	

No	Action	Completed
b.	Sign of compromised accounts/servers	
c.	Ransom mail	
4.	Report the incident according to communication plan	
<b>Contain</b>		
5.	Consideration to be given to whether:	
a.	Suspend misused credentials or resources	
b.	Removal of inappropriate materials	
c.	Preserve all evidence to support attribution or anticipated legal action	
<b>Eradicate</b>		
6.	Consideration to be given to whether:	
a.	Privilege control on abused resources	
b.	Human resource or legal team action (the handling procedures for internal employees should incorporate elements of discretion and confidentiality)	
c.	Implement/apply filter to inappropriate content on both inbound and outbound	
d.	Removal of vulnerable systems/services	
<b>Recover</b>		
7.	Restore any suspended accounts or services	
8.	Consideration to be given as to whether to implement additional monitoring to look out for future related activity	

## **APPENDIX II Reporting an Incident**

For the purpose of incident reporting, Root Cause Analysis (RCA) is typically used to identify root cause, track incidents, and resolve the cause of an incident.

The objectives of the incident report analysis are to:

- Prevent problems or incidents from occurring
- Eliminate recurring incidents
- Minimise the impact of inevitable incidents

A capital market entity is recommended to establish a general guide to assist in making the incident reporting discussion informative and focused.

Below are some techniques that can be used in conducting an incident reporting discussion:

1. Identify the correct teams to engage in discussion and this should include the subject matter experts (SME) or technical teams; senior managers and those that assisted in resolving the incident.
2. It is important to ensure that the SME focuses on the root cause in the discussion.
3. Collect and analyse forensic data.
4. Always request for elaboration from SME to get more detailed response.
5. Monitor the meeting to ensure it is in line with the overall purpose and understanding of the problem by the SMEs. It is crucial to ensure that SMEs are in agreement with the statements made by each party.
6. Identify the Root Cause Factor: Once a root cause is agreed, move on to the potential contributing factors or remediating the gaps identified by the team during the incident. This may include action items detection and prevention methods.
  - Detect: monitoring mechanism that can help in detecting the issue before it becomes an incident
  - Prevent: steps that can be taken to address the gaps identified during the RCA discussion.
  - This may include corrective actions as well.
7. Root cause statements to consider: "What happened", "Why it happened" and "What is the impact".
8. Document the incident report and associated action items to formalise the remediation timeline. It is important to ensure that remediation tasks are being performed by the respective teams according to the timeline.



9. An incident report typically includes the following:
  - Personnel reported;
  - Personnel in charge, including position, department, contact number;
  - Reported date and time of incident;
  - Type of incident;
  - Description of incident;
  - Actions taken;
  - Root Cause Analysis;
  - Lesson learned;
  - Short-term / Long-term action plan;
  - Financial impact from the incident;
  - Implication to the business / client;
  - Incident status; and
  - Closed date and time.

### Responsible, Accountable, Consulted, and Informed (RACI) Chart

A capital market entity is recommended to prepare a Responsible, Accountable, Consulted, and Informed (RACI) chart to describe the roles and responsibilities of various parties in operating its own cyber incident management process. The sample chart below is made available as a reference for capital market entities to create its own incident handling RACI chart.

Stage	Activity	<EXAMPLE ROLE>	<EXAMPLE ROLE>	<EXAMPLE ROLE>	<EXAMPLE ROLE>	<EXAMPLE ROLE>
Identification	Incident Logging and Categorisation	A	I		R	
Identification	Incident Assignment and Escalation	A/I	I	I	R	
Identification	Identification and Analysis of Incident	A	C/I	R		C/I
Containment	Stop the Bleed	A	C/I	R		C/I
Containment	Preservation of Evident	A	C/I	R		C/I
Eradication	Prevent attack from recurring	A	C/I	R		C/I
Recovery	Restore to BAU	A	C/I	R	I	I
Recovery	Incident Review and Closure	A	C/I	R	I	I
Lessons learned	Long term action plan	A	C/I	R	I	I
Recovery	SLA Monitoring	A/I	R	I		
Recovery	Complaint Handling	A/I			R	C/I

R – Responsible, A – Accountable, C – Communicated, I – Informed

Figure 3: Sample of RACI Chart

## DEFINITIONS AND INTERPRETATION

Unless otherwise defined, all words or terms used in this Guidance Note have the following meanings–

Active Directory or AD	means a directory to manage access and permission to access resources in capital market entity;
Business Continuity Plan or BCP	means a plan to ensure a capital market entity continues operating when facing major disruptions to its business;
CIS	means the Center of Internet Security;
Forensic image	means a clone or copy or replication of the source of device, operating system, file, application which is used to ensure the evidence is retained for investigation;
Intrusion Detection System or IDS	means a monitoring system that detects suspicious activities and then generates a system alert when intrusion is detected;
Information assets	means information or data that is of value to the capital market entities, including such information as company records, intellectual property, client information, networks, hardware, software, device, or other component of the environment that supports information-related activities;
Integrity check	means an assessment which is used to check if any unauthorised modifications have been made to the files or systems;
Intrusion Prevention System or IPS	means a system with the function of identifying and blocking any suspicious activity and keeping logs of its activities for analysis or further action;
ISP	means Internet Service Provider;
Multi-Factor Authentication or MFA	means a method that requires users to enter two or more verification before accessing any system or services;
Production environment	means the live environment where software, hardware, data, processes, and programs are made available to users, as opposed to any testing, training, and other non-production, non-live environments;
Penetration testing or pentest	means a simulation of cyber-attack to the capital market entity's IT security system to identify any potential for exploitation using tools or techniques;
Security posture	means the overall status and capabilities of a capital market entity with respect to cybersecurity defence;

Severity matrix means a tool that depicts the potential risk level affecting a business based on probability and likelihood; and

SLA means service level agreement.