National Communications Authority (NCA)

Somalia Computer Emergency Response Team (SOMCERT)

SOMCERT PROCEDURES

2021

1. General SOMCERT Procedures

During the initial stage of the event, process of decision making is already in progress. The information gathered and collected will provide a basis to evaluate and assess the relevancy of information to initiate series of responses to limit. This section covers the procedures for the three stages of computer emergency response plan of SOMCERT.

1.1. Detection and Reporting Procedure

Objectives:

1) Gathering and collecting of information should be identified and evaluated for relevancy of information and made available to the users who need them.
2) Documentation and appropriate logging of records and data shall be maintained for regular monitoring and update of the database.

Stage and Process

a. Receiving Calls or Reports

- All calls receive is filtered and directed to appropriate personnel with specific SOMCERT tasks and responsibilities.
- All reported calls received are immediately logged into the system after it has been filtered as relevant security information event that will prompt incident response team to initiate series of processes and responses.

b. Detection of Event through Human Means

1) Use Initial Assessment Form (IAF) to gather and collect data for analysis of relevancy of the information. Given the potentially time-critical nature of the process, it is not essential to complete all fields in the reporting form at this time.
2) Fill the Initial Assessment Form (IAF) with appropriate information and ensure approximate time is recorded when the event was initially detected.
3) Make sure that the name of the person reporting (if, applicable), the name of the person

gathering and collecting information and the person assigned to respond is clearly indicated in the IAF:

I. Initial assessment results with relevant information after initial evaluation of the SOMCERT Analyst are assigned with Case Number and prompted for Second Assessment.
II. Final assessment results considered to be relevant are forwarded to the appropriate personnel tasked and assigned with the roles to respond to a security incident or event.
III. Case Numbers with open or unresolved are reviewed and monitored closely to contain and control any other potential adverse impact.
IV. Case Numbers with close or resolved are logged into the system to update the record.
V. Summary of resolved and unresolved cases are reported on a daily and weekly basis.

c. Detection of Event through Automatic Means

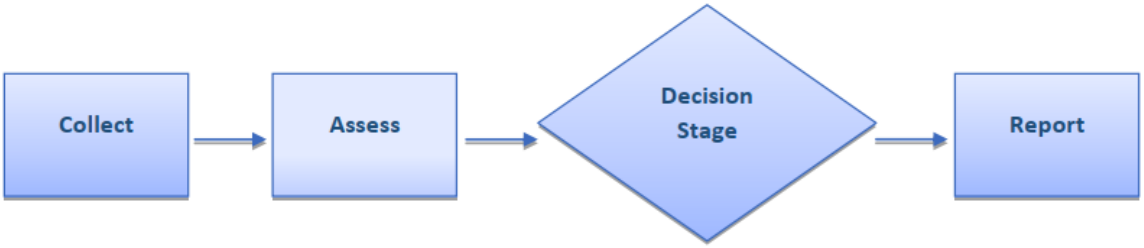
1) Use IAF to gather and collect data for analysis of relevancy of the information.
2) Fill the IAF with appropriate information and ensure approximate time is recorded when the event was initially detected.
3) System or network server clock is used as the official time when event was initially detected.
4) Use IAF to gather and collect information for evaluation by the SOMCERT Analyst.
5) Initial assessment results with relevant information after initial evaluation of the SOMCERT Analyst are assigned with Case Number and prompted for the Final Assessment Form (FAF).
6) Final assessment results considered to be relevant are forwarded to the appropriate personnel tasked and assigned with the roles to respond to a security incident or event.
7) Case Numbers with open or unresolved are reviewed and monitored closely to contain and control any other potential adverse impact.
8) Case Numbers with close or resolved are logged into the system to update the record.
9) Summary of resolved and unresolved cases are reported on a daily and weekly basis.

1.2. Assessment Decision procedure

Objectives

1) Determine the type of detected and reported incident from false alarm and relevant.
2) Classify assessment results according to the degree of loss and the adverse impact it may cause towards the organization.
3) Submit interim reports for reported incidents that require longer period of responses

Stages and Processes



a) Initial Assessment and Decision

1) All completed information security event reporting forms are acknowledged by the receiving person
2) All collected data and information are entered into the information security event/incident database;
3) All reports are reviewed after it has been logged into the system. Seek any clarification from the person reporting the information security event and collect any further information required and known to be available, whether from the reporting person or somewhere else.
4) Assessment is conducted to determine whether the information security event is determined to be a false alarm, a security incident or is in fact a false alarm:

I. If the information security event is determined to be a false alarm, the information security event reporting should be completed and communicated to SOMCERT for addition to the information security event/incident database and review, and copied to the reporting person and the manager under which the person is assigned to, with reference to the time zone difference as reference point:

a) If reported information security incident or event is identified as local source, response from the reporter should be within 24 hours after it was initially reported.

b) If reported information security incident or event is identified as international, response from the reporter should be within 48 hours after it was initially reported.

II. If the information security event is determined to be likely to be an information security incident, and if the person assessing it has the appropriate level of competence, further assessment must be conducted, otherwise, it should be forwarded to the person with appropriate set skills level to respond to the reported information security incident.

5) When considering the potential or actual adverse effect of an information security incident on the business of an organization, the first step will be to consider which of a number of consequences is relevant:

I. For information considered to be relevant, the related categories found under Classification of Security Incidents, should be used to establish the potential or actual impacts for entry into the information security incident report.

II. All reported information security incidents that are tagged as resolved include details of the safeguards that have been taken and any lessons learned (e.g. safeguards to be adopted to prevent reoccurrence or similar occurrences).

6) Reporting forms that have been completed are referred to the SOMCERT for entry into the information security event/incident database and review.

7) Interim reports are submitted for investigations likely to be longer than one week.

8) Analyst assigned to assess the information security incident report must know when it is necessary to escalate matters and to whom.

9) Documented change control procedures are applied in all activities conducted and must be followed.

b) Final Assessment and Incident Confirmation

1) SOMCERT is responsible for the confirmation or decision to categorize the information security event after the final assessment:

I. The information security incident reporting form must be acknowledged as soon has it has been received.

II. Enter the form into the information security even/incident database.

III. Seek clarification from the POC or operations support group to gain more information regarding the incident reporting form.

IV. Review the reporting form content.

V. Collect any further information required and known to be available, whether from the POC, the person who completed the information security event reporting form, the operations support group or elsewhere:

a) If there is still a degree of uncertainty to the authenticity of the information security incident or the completeness of the information, the SOMCERT should conduct an assessment to determine of the reported incident is real or is a false alarm.

b) If the reported information security event is determined to be a false alarm:

1. The information security report is completed and logged to update the database system for information security event/incident and communicated to the SOMCERT Team Leader.

2. Copies of the report should be sent to the POC, the SOMCERT Team Leader, the reporting person and the local manager of the reporting person.

c) If the reported information security incident is determined to be real then further assessment should be conducted, involving other colleagues with appropriate set skills and confirm the following:

1. How the information security incident was caused, its adverse effects, what has been affected, the impact or potential impact, indication of its significance.

2. Attacks done deliberately by human technical methods and techniques, determine the depth of the infiltration is into the ICT system, service and or

network and the level of control the attacker was able to obtain, the data that has been accessed, and the software that has been copied, altered or destroyed by the attacker.

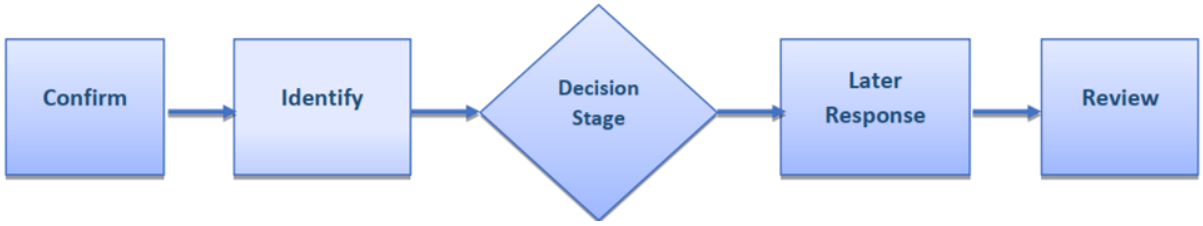
3. Attacks done deliberately through human physical attack on any of the ICT information system, service and/or network hardware and/or physical location, the physical damage whether indirect or direct must be examined and confirmed including the physical access into the facilities.
4. Information security incidents not directly caused by human actions, whether direct or indirect (e.g. physical access open because of fire), should be determined and confirmed.
5. Review state and progress of the information incident security incident has been dealt so far.
6. View being conducted on the potential or actual adverse effects of the information security incident on the operations should be confirmed to determine which of a number of consequences is relevant.

1.3. Response Procedure

Objectives

1. Confirmation of the assessment results on the relevant information to contain, minimize or control the effects of the report on information security incident
2. Identification and execution of immediate or later responses based on the situation
3. Review of the responses (immediate or later responses) including the procedures, processes and the management system for responding to information security incident

Stages and Processes



a. Response

1) Immediate response actions should be identified.
2) Record details on the information security incident form and within the information security event/incident database.
3) Notify required actions to appropriate persons or groups.
4) Initiation of emergency and permanent safeguards to control or minimize the damage and impact of the reported information security incident.
5) Determine the significance and severity of the information security incident report to SOMCERT.
6) Notify directly the appropriate senior management when information security incident is deemed to be sufficiently significant or has been elevated to a crisis stage.
7) Activation of a business continuity plan if "crisis situation" is evident and has been declared.

b. Actions

1) The critical applications and operations must be allowed to function correctly;
2) Collect as much information as possible about the attacker;
3) Appropriate authentication means are implemented to prevent unauthorized individuals into accessing and attacking the system when emergency safeguards are called into actions;
4) Prioritize prevention of re-occurrence, rectify the safeguard mechanisms through the exposed weaknesses of the attacker, and weigh the gains to justify the effort of tracking the attacker especially when it is non-malicious and has caused little or no damage at all;
5) Information security incident report caused other than by deliberate attack must be investigated to determine the cause;
6) Activation of surveillance techniques to counter the attacks of the hacker or attacker; and
7) Check information that may be corrupted by the information security incident report against backup records for any modification, insertions or deletions of information,
    I. Check integrity of the logs

c. Incident Information Update

1) Always update the information security incident report as much as is possible;
2) Record and add update into the information security event/incident database and notify the SOMCERT Team Leader and others, as necessary. Update includes:
    i. What the information security incident is?
    ii. How it was caused and by what and whom?
    iii. What it affects or could affect in the information system, operations, and critical missions of National Security?
    iv. The impact or potential impact of the information security incident on the business and operations of National Security
    v. Changes to the indication as to whether the information security incident is deemed significant or not.
    vi. Current state or progress of how the reported information security incident has been dealt so far.
3) If the reported information security incident has been resolved, the report include details of the safeguards that have been taken and any other lesson learned;
4) SOMCERT is responsible for ensuring the secure retention of all information pertaining to an information security incident for further analysis and potential legal evidential use,
    I. All volatile data are collected before the affected IT system, service or network is shut down for a complete forensic investigation which includes the following actions:
        1) Information to be collected includes contents of memories, cache and registers and details of any processes running.
        2) Full forensic duplication of the affected system, service and/or network, or a low level backup of logs and important files.
        3) Collect and review logs from neighboring systems, services and networks such as routers and firewalls.
        4) Store all information collected on read only media.
        5) At least two persons, while the forensic duplication is performed, must be present to assert and certify that all activities that have been carried out complies

with the relevant legislation and regulation.

6) Document the specifications and descriptions of the tools and commands used to perform the forensic duplication and must be stored together with the original media.
7) The SOMCERT member should facilitate the return of the affected facility to a secure operational state that is not susceptible to a compromise by the same attack.

d. Other Activities for Reports Assessed as Significant

1. Institute forensic analysis procedure;
2. Inform and coordinate with personnel responsible for internal and external communications of the facts and the proposals for what must be communicated in what form and to whom;
3. Any information security incident report that has been completed must be entered into the database system for information security event/incident to update records;
4. Interim reports must be instituted for investigations likely to have longer time to undertake;
5. SOMCERT members must observe and be made aware of the documentation requirements for the following:
    i. The manner of necessity to escalate matters and to whom
    ii. Change management
6. The information security incident report shall be reported in the first instance to relevant people in person, by telephone or text messaging as a contingency plan for communication:
    i. Establish a secure method of communication
    ii. Nominate backup advisors, deputies or representatives in the case of absence.

e. Incident Control

A review shall be conducted after immediate responses have been instigated to control the incident:

I. Consult with colleagues if necessary.
II. If the reported information security incident is confirmed to be under control, institute later responses, forensic analysis, and communications to close the reported incident and restore normal operations.
III. If reported information security incident is confirmed to be not under control,

institute “crisis activities” to activate the crisis management plan.

f. Later Responses

Identify the “if and what” further responses are required to deal with the information security incident, including:

I. Restoring the affected information systems, services and or networks back to normal operations;
II. Recording details on the information security incident reporting form;
III. Updating the details and information report into the information security incident/event database;
IV. Notifying the personnel responsible for completing related actions;
V. Contacting supplier immediately if Cyber Security relies on external vendors for hardware and software and other third party support services;
VI. Conducting additional monitoring activities after restoring to normal operations to detect other weaknesses or vulnerabilities; and
VII. Conducting recovery activities when incidents were caused by non-IT related cause.

g. Crisis Activities

1. Institute crisis activities leading to the activation of crisis management plan;
2. Activate fire suppression facilities and evacuation procedures for fire related incidents;
3. Activate flood prevention facilities and evacuation procedures for flood related incidents;
4. Activate bomb “handling” and related evacuation procedures for bomb threat and domestic terrorism related activities.
5. Activate procedures to put on board specialists such as information system fraud investigators and technical attack investigators for cyber-attacks and intrusion related incidents.

h. Forensic Analysis

1. Avoid having the target being rendered as unavailable, altered, or otherwise compromised by protecting the system, service and/or network during forensic analysis procedure:

i. Protect against new virus that may be introduced during the conduct of forensic analysis.
ii. Minimize or no effects will be made on normal operations.

2. Prioritize capture of evidence by proceeding from the most volatile to the least volatile;
3. Identify all relevant files on the subject systems, service, and/or network, including normal files, deleted files, password or password protected files, and encrypted files:
4. Recover discovered deleted files and other data:
    i. Uncover IP addresses, host names, network routes and website information;
    ii. Extract contents of hidden, temporary, and swap files used by both application and the operating system software;
    iii. Access the contents of protected or encrypted files unless it is a possible violation of a law.
    iv. Analyze all possible, relevant data found in special and typically inaccessible data and disc storage areas.
    v. Analyze file access, modification and creation times.
    vi. Analyze system, service, network, and application logs.
    vii. Determine the activity of users and/or applications on a system, service or network.
    viii. Analyze emails for source information and content.
    ix. Perform file integrity checks to detect Trojan horse files and files not originally from the system.
    x. If applicable, analyze physical evidence for possible fingerprints, property damage, video surveillance, alarm system logs, pass card access logs, biometric systems, and interview witnesses.
    xi. Handle and store the extracted potential evidence by securing and protecting it from being damaged or rendered unusable.

5. Make sure that sensitive information and material cannot be seen by those not authorized to view recovered potential evidence.
6. Evidence gathering must be with the accordance of the rules of the court or hearing, in which the evidence may be presented.
7. Make conclusions on the reasons for the information security incident and the actions

required including the timeframe. Provide list of the evidences of relevant files to be included as attachment to main reports.

8. When required, provide expert support to any disciplinary or legal action that Cyber Security Department will undertake.

i. Communications

1. Prepare certain information in advance that can be quickly adjusted to the circumstances of a particular information security incident issued to the Media such as:
    i. When security incident is confirmed as real;
    ii. When security incident is confirmed as under control;
    iii. When it is designated for "crisis" activities;
    iv. When it is resolved or closed; and
    v. When post incident review has been completed and conclusions reached.
2. Prepare the personnel who will be tasked and assigned to communicate with internal (outside of normal SOMCERT/management communication lines) and media.
3. Information that is to be released must be in accordance to Cyber Security Department's policy on information dissemination.
4. Information to be released must be reviewed by the relevant parties of Cyber Security Department.

j. Improve

1. Review the results of the forensic analysis that were further conducted after the information security incident report has been resolved and closure has been agreed;
2. Conduct further forensic analysis to identify evidence even after the information security incident report form has been completed and viewed as closed or resolved. Same toolsets and procedures must be used for further forensic analysis of evidences;
3. Identify the lessons to be learned once the information security incident has been concluded as closed or resolved, from the initial handling to quick identification up to the level when immediate or later responses were taken. Lessons may include:
    I. New or changed requirements for information security safeguards, either technical or non- technical safeguards which may include:

1. Rapid material updates.
2. Delivery of materials or support/shared services.
3. Security awareness briefings for end-users and personnel.
4. Rapid revision and issue of security guidelines and/or standards.

II. Changes to the SOMCERT and its processes, procedures, reporting forms, and information security event/incident database.

III. Look for patterns or trends beyond a single information security incident to help identify the need for safeguards or approach changes.

IV. Conduct information security testing and vulnerability assessment.

1.4. Responding to Information Security Report Procedure

As part of establishing the national security for information technology, all employees, contractors and third-party users will be made aware of the established procedures for reporting different types of events and weakness that might have an impact on the security of organizational assets. Early reporting upon detection will ensure that information security events and weaknesses associated with information systems of National Cyber Security are communicated in a manner that allows timely corrective actions to be taken by SOMCERT. The SOMCERT is tasked to respond to any reported information security event in a quick, effective, and orderly response to mitigate, prevent, minimize, control, or correct any vulnerability or threats that may create adverse impact to the organization. This section covers the response procedure of the SOMCERT. Control Objectives

1. Logging and recording of all activities undertaken when responding to the information security incident.
2. Established procedures must be reviewed to determine applicability and for continuous improvement of the processes, procedures and policies of Cyber Security Department for information security incident response.

a. Responding to Information Security Incident Report

1) Use Form IAF and FAF as reference when responding to reported incident or event associated with the information system.
2) Refer to the guidelines for handling incident response.

b. Procedures for Responding to Different Types of Information Security Incident

1. When responding to information system failures and loss of service:

i. Immediately halt attacks if caught while in progress;

ii. Follow back up procedures;

iii. Assess the extent of operational downtime and determine the earliest time possible to bring the system into a stable operating state;

iv. Check if data or information has been compromised or security breach has occurred during system failure or loss of service;

v. Check records of updates and regular maintenance being conducted such as version of the anti-virus software, installation or updates of patches to correct software vulnerabilities, firewall technology in place, etc.;

vi. Review and monitor systems and determine effectiveness of information security safeguards to detect and correct the breakdowns in security. Monitoring and review may include:

1. Sampling
2. System checks
3. Reports of access to systems
4. Review of Logs
5. Audit Reports

vii. Preserve and gather evidence that results from the incident that has occurred;

viii. In an urgent situation that requires immediate action please refer to the established escalation procedure:

1. SOMCERT member responding is authorized to secure the asset without the owner's consent when it is determined to be critical in nature:
    a) Appropriate logging and recording of artifacts must be conducted.
    b) Another member of the SOMCERT must be present or representative from the reporting party must be around to observe the secure removal of the item from the site.

2. When responding to malicious code attacks

i. Determine fully if a malicious code attack has occurred and this can be evaluated based from some of the examples below:
    1. Complaints on slow access to internet, exhaustion of system resources, slow disk access or slow system boots;
    2. Numerous alert reports have been generated by Host-based Intrusion Detection System (HID) or by anti-virus or malicious code detection software;
    3. Significance in increased network usage;
    4. Access violation entries are noticed and observed in perimeter router logs or firewall logs;
    5. A detected surge on out-bounced SMTP traffic originating from an internal IP address;
    6. Noticeable unusual deviation from typical network traffic flows observed by a system administrator;
    7. Security controls such as anti-virus software and personnel firewalls are disabled on many hosts.
    8. General system instability and crashes.

ii. Upon confirmation that there is a malicious code security breach, it is important to collect information about the malicious code.

iii. Identify characteristics of the malicious code to apply appropriate course of actions. Examples are given below:
    1. Type of malicious code: network mass, mass-mailing worm, virus, Trojan horse, etc.
    2. Vulnerability that is being exploited by the malicious code, services or ports being attacked, etc.

iv. Assess the scope, damage and impact of the outbreak to effectively deal with the incident;

v. Record all actions taken when dealing with the outbreak and any corresponding results,

(Please see General Procedures for Phase 2). Logging should be carried out throughout the whole security incident response process;

vi. Notify all appropriate parties and escalate the incident to the appropriate level following a predefined escalation procedure (Please see Escalation Procedure). The information provided during the escalation process should be clear, concise, accurate and factual. Inaccurate, misleading or incomplete information may hinder the response process or may even worsen the situation; and

vii. Carry out containment activities to prevent the malicious code from inflicting further damage through the following:

1. Identify infected systems;
2. Contain the outbreak;
3. Keep record of all actions taken;
4. Execute full eradication process as soon as possible or in parallel with the containment process to prevent files from being corrupted, destroyed or deleted on the infected system.
5. Notify all related parties before the resumption of suspended services. IT personnel must restore specific functions and servers stage by stage in a controlled manner and in the order of demand. Start with the most essential services or those servicing the majority.
6. Verify information that the restoration operation has been successful and that all services are back to normal after resuming the suspended services. Additional monitoring may be implemented to watch and observe for any suspicious activity in the network segments concerned.

3. When responding to Distributed Denial of Service (DDoS)

i. Immediately assess and determine the scope and impact to plan for the next course of action to be taken to address the incident.

ii. Determine the intent, capability and target of the attacker to deploy appropriate counter measures and install safeguard mechanisms.

iii. Additional components must be immediately available as replacement in the event of

component failure.

iv. Use load balancing mechanism to distribute the force of DDoS attacks between several components and geographic locations to prevent single component or network from receiving the full volume of traffic.

v. Immediately execute the escalation procedure.

vi. Ensure appropriate physical security measures are in place to detect unauthorized entry or access into the site.

vii. Immediately detect or remove reflectors or amplifiers from the network to minimize avenues of anonymity and large scale assault into the system as well as lower the risk for critical infrastructure of the organization,

4. When responding to breaches of confidentiality and integrity

i. Immediately assess the impact and the degree of security breach.

ii. Implement escalation procedure immediately.

iii. Review all logs and records on entry and exit of all personnel with access to critical information system and data processing facilities including data storage facilities.

iv. Change all passwords and entry codes immediately.

v. Record all activities taken for further analysis and improvement of the security systems being implemented,

5. When responding to misuse of information system

i. Trace logs and records of all transactions,

ii. Execute control measures immediately to further prevent any unauthorized access,

iii. Investigate and evaluate the intent and extent of the impact in the misuse of the information system,

iv. Change all passwords and entry codes immediately,

v. Review implementation of security password maintenance, security logs, and security access into the system,

vi. Immediately disconnect the equipment or remove from network connection when unauthorized use or access of the information system has been detected and confirmed,

vii. Record all activities taken for further analysis and improvement of the security systems

being implemented.

1.5. Reporting Procedure

When an information security event is detected whether by human and automated means and reported immediately, it increases the ability of the SOMCERT to verify the information and initiate immediate response when it has been determined to be relevant. It is important that the person tasked to receive all reported information security incidents is able to report and notify appropriate personnel. The process of reporting a security information incident is not only limited to reporting the initial report of the event but it is also important to know how to report an incident when it is deemed necessary to escalate the matter to the next level of decision makers. This section covers the reporting procedure upon the initial receipt of a report of an information security event or incident, interim reporting and escalated reporting.

Objectives

1. Acknowledgment receipt of the information security incident report
2. Recording of the official time stamp of the information security event upon initial report
3. Forms for the following: IAF and FAF

a. Initial Reporting of Information Security Incident Report

1. All calls are filtered by the POC to determine if the call is related to a report on an information security incident.
2. Initial incoming report on information security incident is logged into the system to record and log report into the database for information incident/event database.
3. Initial information from the incoming calls or report is recorded into the IAF.
4. The IAF with partial information is forwarded to the SOMCERT Analyst for data gathering and collection.
5. The Initial Report is forwarded to the concerned personnel for immediate response and the SOMCERT Team Leader is informed.
6. All reports must be updated when it has been closed or resolved to update the system.

1.6. Escalation Procedure

Escalation happens when there are circumstances where matters have to be escalated to the senior

management, another group or persons within the organization or groups outside the organization. However, it is also important that before the incident is escalated, it must exhaust all means to respond immediately to the incident or it qualifies as an urgent matter that can affect the national security. This section will cover procedures on escalation including when, what and who to notify a matter that is being escalated.

Objectives

1) Assessment reports to determine the relevance of the reported information security incident.
2) Impact and risk assessment reports that will initiate the decision to escalate matters.
3) Rating scale for vulnerability, threat and predisposing conditions to support and justify the action to escalate.
4) Escalation request form that will provide paper trail for auditing.

1. Factors to Consider for Escalation

1.1. When results of the evaluation is determined to have an impact to the national security:

i. When the results of the evaluation have severe or catastrophic adverse impact to the organization;
ii. When the results of the evaluation will is classified as critical and will severely affect the information system level of the organization;
iii. When major issues become evident at the early stages of reporting; and
iv. When information security incident report is a recurring incident after it has been previously resolved.

2. Escalation Procedure

1) Use the rating scale on vulnerabilities and threats to evaluate the degree or gravity of adverse impact to the organization.
2) The decision to escalate will be taken by the SOMCERT Leader after determining the results of the evaluation.
3) Escalation request must include the following:
    a. The type of event and when it happened
    b. The degree of severity or adverse impact to the national level, organizational level

or the information system level

c. The name of the person requesting for escalation and the official time stamp and date when escalation requests was made.
d. The case number assigned to the information security incident report.

4) The Analyst shall consult with the Team Leader when major issues are evident during the early stage of assessment;
5) Send an alert message notifying the appropriate personnel to respond to the escalated information security incident report;
6) The Analyst shall consult with the Team Leader when the reported information security incident is required for escalation;
7) The Analyst shall consult with the Team Leader to determine the next course of action whether it should be escalated or forwarded to another group to initiate immediate response or take series of actions.
8) Notification of escalation after assessment results are concluded and Escalation Request is forwarded and submitted to the Team Leader;
9) Escalating the information security incident report must have supporting documents that will justify and rationalize the escalation requests.
10) All escalated information security incident report must be monitored at regular intervals to ensure that it has been properly coordinated and forwarded to the personnel concerned.
11) Escalated information security incident report must be logged into the system to update the information security event/incident database.
12) A summary of escalated report on information security incident must be prepared and submitted to the SOMCERT Management for review and evaluation.

3. De-escalation Procedure

A. When the escalated information security incident report is addressed and its classification has been downgraded to manageable and controllable incident, a de-escalation notification is forwarded to:

i. The original source where the report has emanated
ii. The reporting Analyst

iii. The SOMCERT Team Leader
iv. The SOMCERT Supervisor
v. The SOMCERT

B. When the escalation request was reviewed and evaluated to determine the impact and severity and was concluded to be manageable, controllable and within the scope of and existing set skills of the SOMCERT Team, the escalation notification request will be downgraded and forwarded to the concerned personnel with the specific set skills to respond immediately or for later responses.

C. De-escalated information security incident report must be logged into the system to update the information security event/incident database.

1.7. Communication Procedure

When information security incident occurs, there are instances that the need to communicate and coordinate with other groups or third parties is very important. So whenever appropriate, such as contacting law enforcement agencies, responding to media inquiries or discussing and sharing information with ISPs and vendors of vulnerable software or other incident response team, the need to establish policies and procedures to ensure that sensitive information will not be disclosed to unauthorized party is required. This is to prevent potentially leading to additional disruption, reputation damage or financial loss. Any communication conducted with outside parties must be well documented for evidentiary and liability purposes. This section covers communication procedures with outside parties or external groups during incident response.

Objectives

1. Communication policies are developed to ensure that sensitive or critical information are not disclose when communicating and coordinating with parties and groups outside SOMCERT.
2. Record of communication activities are documented and must be stored and filed in a secure place.

A. Media Communications Procedure

All members of SOMCERT must be oriented and trained on how to interact with media regarding incidents. Included are as follows:

i. Emphasis on the importance of not revealing important information such as technical details of countermeasures that could assist other attackers.
ii. Discuss positive aspects of communicating and disclosing important information to the public fully and effectively.
iii. Hold mock interviews and press conferences to simulate media interaction during incident handling.
iv. A single POC person must be appointed tasked to respond to handle the media and inquiries.
v. Disclosure of information must have written approval from the Management to ensure protection of information security.
vi. All communication with outside parties must be documented accordingly.
vii. Media communications procedure must be reviewed at regular interval to determine its applicability, effectiveness and establish continuous improvement.

B. Contacting and Communicating with Law Enforcement Procedure

1. Whenever the situation requires contacting law enforcement agencies, this must be established immediately.
2. Communicating and sharing of information with law enforcement agency must be with written approval from the Cyber Security Departmetn.
3. Establish a single POC with the LEA or secure alternate contact persons to ensure availability when the need to communicate and coordinate with the agency arises.
4. All communication and coordination activities are recorded and documented accordingly.

C. Contacting Other Groups

1) Communicating and contacting other groups while responding to information security incident must be with written approval from SOMCERT or Cyber Security Department.
2) A single POC is assigned to have all communication directed and handled during incident response.

3) All contact details from external groups are updated and distributed to the SOMCERT member responding to the incident response.
4) The SOMCERT Supervisor must monitor all communication activities.
5) All communication with external groups or third parties are recorded and documented accordingly.
6) All records of communication are reviewed at regular intervals to evaluate the procedures and processes in conducting communication with other parties outside SOMCERT.

1.8. Review Procedure

The review stage is an important process to ensure that the established incident response system of SOMCERT is working efficiently and effectively. It is also a chance for SOMCERT to analyze and evaluate lessons that can be learned from the data gathered and collected including the related responses and associated decisions undertaken during initial and post incident activities. The review stage provides the avenue to also monitor all unresolved including resolved cases to evaluate the recommendations provided during incident response. This section will cover the review procedures that are conducted by the SOMCERT as part of the objective for continuous improvement.

Objectives

1. Post incident reviews are conducted to determine the efficiency of the processes and procedures established for the SOMCERT.
2. Outputs of the reviews and its corresponding results are used as an input for refining the processes and procedures of SOMCERT.
3. Review outputs are documented for evidentiary purposes.

A. Review Procedures

1. All records and documented activities for incident responses are reviewed at regular intervals.
2. A monthly meeting with the SOMCERT is scheduled to review all post incident reports that were resolved immediately during the initial response are summarized for discussion.
3. For incident reports requiring longer period of investigation, schedules for meeting are

conducted with more frequency to ensure that all response activities are monitored and reviewed.

4. All post incident reports that took longer time to be resolved are reviewed and evaluated further to gather lessons to be learned:
    i. Develop knowledge database of best practices from lessons learned.
    ii. Develop knowledge database for research and development.
    iii. Consolidate the knowledge database for latest techniques, approaches and methods for incident response.
    iv. All communication and coordination activities must be reviewed to improve the procedures and processes when communicating outside SOMCERT.
    v. Results of review meetings and discussions are reviewed during the next schedule of meeting.
    vi. All reviews are documented and records are submitted to SOMCERT.