CMSGu2012-02

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Incident Handling

CERT-MU

National Computer Board
Mauritius

March 2012

Issue No. 2

Version 1.1

Table of Contents

Tables and Figures

Tables

Figures

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to provide the basis for the creation of incident response policies, plans, procedures, and teams to handle incidents within an organisation. This document also includes an incident handler's checklist template that one can use to ensure that each of the incident response steps is being followed during an incident. This guide addresses only incidents that are computer security-related, not those caused by natural disasters, power failures, etc.

1.2 Audience

The target audience is focused towards IT professionals and managers who are responsible for incident handling and management within their organisations.

1.3 Document Structure

This document is organised into the following sections:

Section 1 includes the document's content, the targeted audience and the document's structure.

Section 2 presents a background on incidents and events

Section 3 describes incident response.

Section 4 discusses incident handling, including the incident handling lifecycle

Section 5 provides an incident handler's checklist

Section 6 concludes the document.

Section 7 comprises a list of references that have been used in this document.

Appendix A defines a set of acronyms used in this document.

2.0 Background

One of the greatest challenges facing today's IT professionals is the planning and preparation of unanticipated security incidents. An incident can be described as any violation of policy, law, or unacceptable act that involves information assets, such as computers, networks, smartphones.

2.1 Events

An **event** is any observable occurrence in a system or network. Events include a user connecting to a shared server, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.

Adverse events are events with a negative impact, such as system crashes, packet floods, unauthorised use of system privileges, unauthorised access to sensitive data, and execution of malware that destroys data.

2.2 Incidents

An **incident** is defined as an attempted or successful unauthorised access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy.

Examples of incidents are as follows:

- Unauthorised access of systems or data
- Inappropriate usage of systems or data
- Unauthorised change to computer or software
- Loss or theft of equipment used to store personal information or confidential data
- Unwanted disruption or denial of service
- Interference with the intended use of resources
- Compromised user account

While this definition covers numerous potential and actual incidents, the requirement for central incident reporting is aimed at serious incidents as defined below.

A **serious incident** is an incident that may pose a threat to an organisation's resources, stakeholders, and/or services. Specifically, an incident is designated as serious if it meets one or more of the following criteria:

- Involves potential unauthorised disclosure, modification or destruction of personal information
- Involves serious legal issues
- Causes severe disruption to critical services
- Involves active threats
- Is widespread, that is, extends beyond a single unit
- Is likely to raise public interest

3.0 Incident Response

Incident response has become an important component of IT programs. Security-related threats have become not only more frequent and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Defensive activities based on the results of risk assessments can reduce the number of incidents, but not all incidents can be avoided. The following sections explain why an incident response capability is therefore necessary.

3.1 Why do we require Incident Response?

Incident response is important because attacks frequently compromise personal and business data. It is vital to respond rapidly and proficiently when security breaches occur, so the concept of computer security incident response has become widely accepted and implemented. One of the benefits of having an incident response competence is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken.

Incident response helps personnel to minimize loss or theft of information and disruption of services caused by incidents. Another benefit of incident response is the ability to use information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data. An incident response capability also helps with dealing properly with legal issues that may turn up during incidents.

Apart from the business reasons to set up an incident response capability, organisations must comply with law, regulations, and policy directing a coordinated, effective defense against information security threats.

3.2 Incident Response Policies, Plans and Procedures

This section discusses policies, plans, and procedures related to incident response, with focus on interactions with third parties.

3.2.1 Incident Response Policy

Policy governing incident response is generally tailored to the organisation and depends to a large extent, on its nature. However, most policies include the same key components:

- Statement of management commitment

- Purpose and objectives of the policy
- Scope of the policy
- Definition of computer security incidents
- Organisational structure and definition of roles, responsibilities, and levels of authority
- Prioritisation or severity ratings of incidents
- Performance measures
- Reporting and contact forms

3.2.1 Incident Response Plan

Organisations should have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability. Each organisation needs a plan that meets its unique requirements, which relates to the organisation's mission, size, structure, and functions. The plan should outline the necessary resources and management support. The incident response plan should include the following elements:

- Mission
- Strategies and goals
- Senior management approval
- Organisational approach to incident response
- How the incident response team will communicate with other departments of the organisation and with external organisations
- Metrics for measuring the incident response capability
- Roadmap for maturing the incident response capability
- How the program fits into the overall organisation.

The organisation's mission, strategies, and goals for incident response should help in determining the structure of its incident response capability. The incident response program structure should also be discussed within the plan.

Once an organisation develops a plan and obtains management approval, the organisation should implement the plan and review it at least on an annual basis to ensure the organisation is following the roadmap for optimising the capability and meeting their targets for incident response.

3.2.3 Standard Operating Procedures

Procedures should be based on the incident response policy and plan. Standard operating procedures (SOPs) are an explanation of the specific technical processes and technique as well as checklists and forms used by the incident response team. SOPs should be comprehensive and detailed to ensure that incidents are responded to according to their priorities and severity. Moreover, standardized responses should be in place to reduce potential errors that can be caused by pressure, stress or other factors.

SOPs should be tested to validate their accuracy and usefulness, and then distributed to all team members. Training should also be provided for SOP users.

3.2.4 Sharing of Incident Information with Third Parties

Very often, organisations need to communicate with third parties about an incident, and they should do so whenever appropriate, such as contacting law enforcement agencies and responding to media inquiries. Another example is discussing incidents with other involved parties, such as Internet service providers (ISPs), the vendor of vulnerable software, or other incident response teams. The incident response team should eventually discuss information sharing with the organisation's public relations department, legal department, and management before an incident occurs in order to establish policies and procedures regarding incident information sharing. Otherwise, sensitive information may be disclosed to unauthorised parties, potentially leading to additional disruption, reputation damage and financial loss. The team should document all contacts and communications with outside parties for liability and evidentiary purposes.

The following sections provide guidelines on communicating with several types of third parties, as depicted in Figure 1. The double-headed arrows indicate that either party may initiate communications.

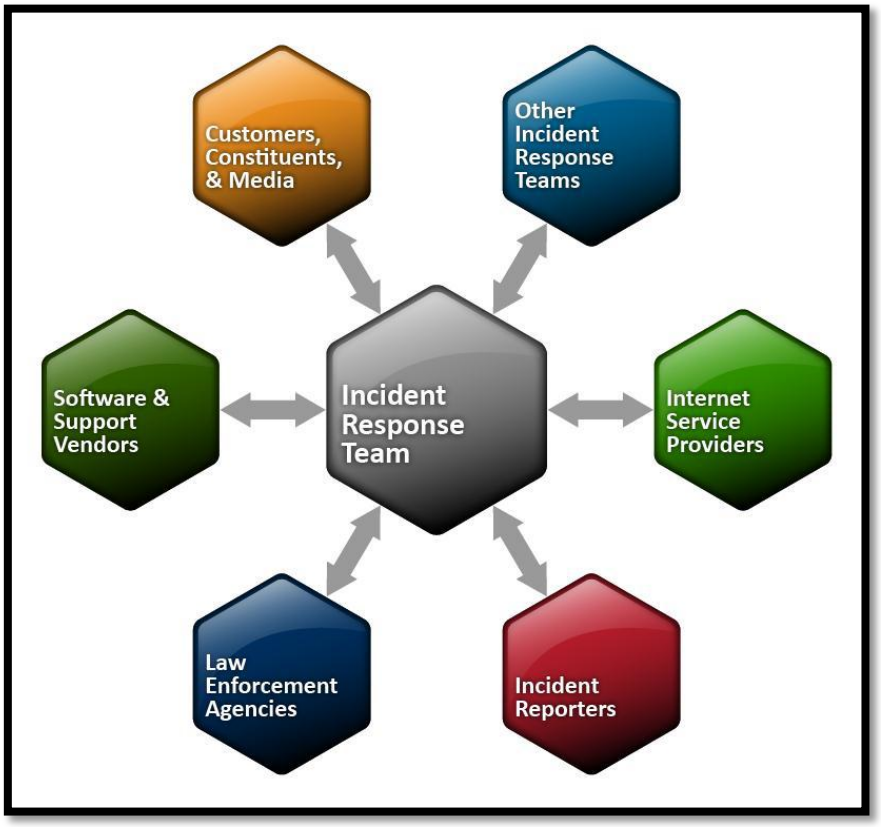


Figure 1 Communications with Third Parties

3.2.4.1 The Media

The incident handling team should establish media communications procedures that comply with the organisation's policies on media interaction and information disclosure. For discussing incidents with the media, organisations often find it beneficial to designate a single point of contact (POC) and at least one backup contact. The following actions are recommended for preparing these designated contacts and should also be considered for preparing others who may be communicating with the media:

- Conduct training sessions on interacting with the media regarding incidents, which should include the importance of not revealing sensitive information, such as technical details of countermeasures that could assist other attackers, and the positive aspects of communicating important information to the public fully and effectively.
- Establish procedures to brief media contacts on the issues and sensitivities regarding a particular incident before discussing it with the media.
- Hold mock interviews and press conferences during incident handling exercises. The following are examples of questions to ask the media contact:
  - Who attacked you? Why?

- When did it happen? How did it happen? Did this happen because you have poor security practices?
- How widespread is this incident? What steps are you taking to determine what happened and to prevent future occurrences?
- What is the impact of this incident? Was any personally identifiable information exposed? What is the estimated cost of this incident?

3.2.4.2 Law Enforcement

One of the reasons why many security-related incidents do not result in convictions is that some organisations do not properly contact law enforcement. The following levels of law enforcement are available to investigate incidents in Mauritius: The Cybercrime Unit, Mauritius Police Force and the State Law Office. In addition, the Computer Emergency Response Team of Mauritius (CERT-MU) is in place to analyse and handle incidents for throughout the country.

The incident response team should become familiar with its various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them, how the reporting should be performed, what evidence should be collected, and how it should be collected.

Law enforcement should be contacted through designated individuals in a manner consistent with the requirements of the law and the organisation's procedures. Many organisations prefer to appoint one incident response team member as the primary POC with law enforcement. This person should be familiar with the reporting procedures for all relevant law enforcement agencies and well prepared to recommend which agency, if any, should be contacted. The organisation typically should not contact multiple agencies because doing so might result in jurisdictional conflicts. The incident response team should also understand what the potential legal issues are.

3.2.4.3 Incident Reporting Organisations

International CERTs and other reporting organisations do not replace existing incident response teams, for example, CERT-MU; rather, they boost the efforts of CERT-MU by serving as a focal point for dealing with incidents. The reporting organisations analyse the team-provided information to identify trends and indicators of attacks; these are easier to

discern when reviewing data from many organisations than when reviewing the data of a single organisation. Organisations should create a policy that states who is designated to report incidents and how the incidents should be reported.

All organisations are encouraged to report incidents to their appropriate CSIRTs. If an organisation does not have its own CSIRT to contact, it can report incidents to other organisations, as appropriate. One of the functions of these industry-specific private sector groups is to share important computer security-related information among their members.

3.2.4.4 Other Third Parties

An organisation may want to discuss incidents with other groups, including those listed below.

- **The Organisation's ISP**

  An organisation may need assistance from its ISP in blocking a major network-based attack or tracing its origin.

- **Owners of Attacking Addresses**

  If attacks are originating from an external organisation's IP address space, incident handlers may want to talk to the designated security contacts for the organisation to alert them to the activity or to ask them to collect evidence. It is highly recommended to coordinate such communications with CERT-MU for local incidents.

3.3 Incident Response Team Services

The main focus of an incident response team is performing incident response, but it is fairly rare for a team to perform incident response only. The following are examples of additional services a team might offer:

- **Intrusion Detection**

  The first level of an incident response team often assumes responsibility for intrusion detection. The team generally benefits because it should be in a position to analyse incidents more quickly and accurately, based on the knowledge it gains of intrusion detection technologies.

- **Advisory Distribution**

A team may issue advisories within or outside the organisation regarding new vulnerabilities and threats. Automated methods, such as RSS Feeds should be used whenever appropriate to disseminate information. Advisories are often most necessary when new threats emerge, such as a high-profile social or political event (e.g., celebrity weddings) that attackers are likely to influence in their social engineering process. Only one group within the organisation should distribute computer security advisories to avoid duplicated effort and conflicting information.

- **Education and Awareness**

  Education and awareness are resource multipliers - the more the users and technical staff know about detecting, reporting, and responding to incidents, the less drain there should be on the incident response team. This information can be communicated through many means: workshops, websites, newsletters, guidelines and posters.

4.0 Incident Handling

The incident handling process has several phases. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, the organisation also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, residual risk will inevitably persist after controls are implemented.

Detection of security breaches is thus necessary to alert the organisation whenever incidents occur. In keeping with the severity of the incident, the organisation can mitigate the impact of the incident by containing it and ultimately recovering from it. During this phase, activity often cycles back to detection and analysis, for example, to see if additional hosts are infected by malware while eradicating a malware incident.

After the incident is adequately handled, the organisation issues a report that details the cause and cost of the incident and the steps the organisation should take to prevent future incidents.

This section describes the major phases of the incident response process: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity in detail. Figure 2 illustrates the incident handling life cycle.

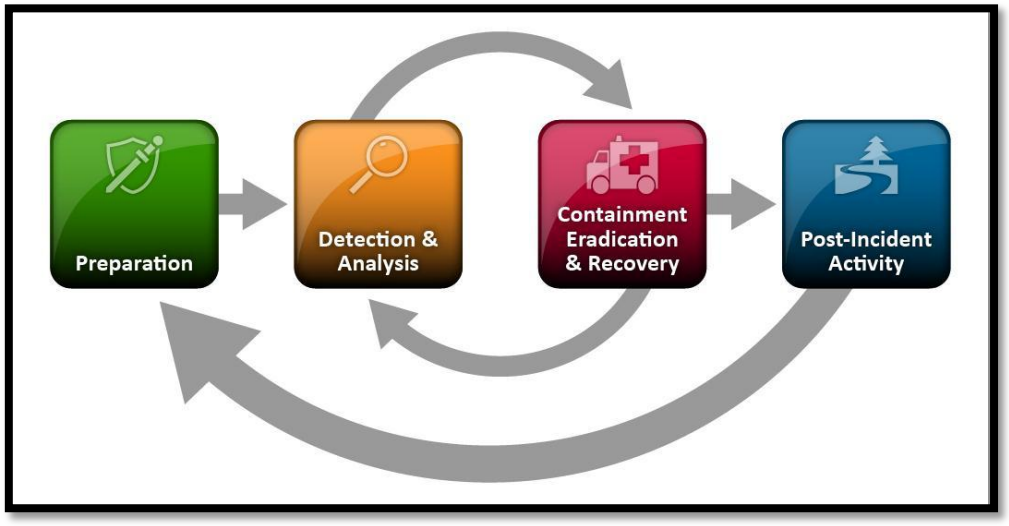


Figure 2 Incident Handling Lifecycle

4.1 Preparation

This phase as its name implies, deals with the preparation of a team to be ready to handle an unforeseen incident. An incident can range from anything such as a power outage or hardware failure to the most extreme incidents such as a violation of organisational policy by disgruntled employees or being hacked by state sponsored hackers. Regardless of the cause of the incident, preparation is the most crucial phase compared to all of the others, as it will determine how well your team will be able to respond in the event of a crisis.

4.1.1 Preparing to Handle Incidents

Table 1 below lists tools and resources available that may be of value during incident handling.

Acquired	Tool / Resource
Incident Handler Communications and Facilities	
	Contact information for team members and others within and outside the organisation (primary and backup contacts), such as law enforcement and other incident response teams; information may include phone numbers, email addresses, public encryption keys
	On-call information for other teams within the organisation, including escalation information
	Incident reporting mechanisms, such as phone numbers, email addresses, online forms, and secure instant messaging systems that users can use to report suspected incidents; at least one mechanism should permit people to report incidents anonymously
	Issue tracking system for tracking incident information, status, etc.
	Smartphones to be carried by team members for off-hour support, onsite communications
	Encryption software to be used for communications among team members, within the organisation and with external parties; software must use a valid and legal encryption algorithm
Incident Analysis Hardware and Software	
	Digital forensic workstations and/or backup devices to create disk images, preserve log files, and save other relevant incident data
	Laptops for activities such as analyzing data, sniffing packets, and writing reports (see discussion below table)
	Spare workstations, servers, and networking equipment, or the virtualized equivalents, which may be used for many purposes, such as restoring backups and trying out malware
	Blank removable media
	Portable printer to print copies of log files and other evidence from non-networked systems
	Packet sniffers and protocol analysers to capture and analyse network traffic

	Digital forensic software to analyse disk images
	Removable media with trusted versions of programs to be used to gather evidence from systems
	Evidence gathering accessories, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions
Incident Analysis Resources	
	Port lists, including commonly used ports and Trojan horse ports
	Documentation for OSs, applications, protocols, and intrusion detection and antivirus products
	Network diagrams and lists of critical assets, such as database servers
	Current baselines of expected network, system, and application activity
	Cryptographic hashes of critical files to speed incident analysis, verification, and eradication
Incident Mitigation Software	
	Access to images of clean OS and application installations for restoration and recovery purposes

Table 1 Tools and Resources for Incident Handling

Many incident response teams create a "jump kit", which is a portable case that contains materials that may be needed during an investigation. The jump kit should be ready to go at all times. Jump kits contain many of the same items listed in Table 1. For example, each jump kit typically includes a laptop, loaded with appropriate software (e.g., packet sniffers, digital forensics). Other important materials include backup devices, blank media, and basic networking equipment and cables. Because the purpose of having a jump kit is to facilitate faster responses, the team should avoid borrowing items from the jump kit.

Each incident handler should have access to at least two computing devices (e.g., laptops). One, such as the one from the jump kit, should be used to perform packet sniffing, malware analysis, and all other actions that risk contaminating the laptop that performs them. This laptop should be scrubbed and all software reinstalled before it is used for another incident. Note that because this laptop is special purpose, it is likely to use software other than the standard enterprise tools and configurations, and whenever possible the incident handlers should be allowed to specify basic technical requirements for these special-purpose investigative laptops. In addition to an investigative laptop, each incident handler should also have a standard laptop, smart phone, or other computing device for writing reports, reading email, and performing other duties unrelated to the hands-on incident analysis.

4.1.2 Preventing Incidents

Keeping the number of incidents reasonably low is very important to protect the business processes of the organisation. If security controls are insufficient, higher volumes of incidents may occur, overwhelming the incident response team. This can lead to slow and incomplete responses, which translate to a larger negative business impact (e.g., more extensive damage, longer periods of service and data unavailability).

It is outside the scope of this document to provide specific advice on securing networks, systems, and applications. Although incident response teams are generally not responsible for securing resources, they can be advocates of sound security practices. Other documents already provide advice on general security concepts and operating system and application-specific guidelines. The following, however, provides a brief overview of some of the main recommended practices for securing networks, systems, and applications:

- **Risk Assessments**

  Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities. Each risk should be prioritized, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasize monitoring and response activities for those resources.

- **Host Security**

  All hosts should be hardened appropriately. In addition to keeping each host properly patched, hosts should be configured to follow the principle of least privilege. Hosts should have auditing enabled and should log significant security-related events. The security of hosts and their configurations should be continuously monitored. Many organisations use Security Content Automation Protocol (SCAP) expressed operating system and application configuration checklists to assist in securing hosts consistently and effectively.

- **Network Security**

The network perimeter should be configured to deny all activity that is not expressly permitted. This includes securing all connection points, such as virtual private networks (VPNs) and dedicated connections to other organisations.

- **Malware Prevention**

  Software to detect and stop malware should be deployed throughout the organisation. Malware protection should be deployed at the host level (e.g., server and workstation operating systems), the application server level (e.g., email server, web proxies), and the application client level (e.g., email clients, instant messaging clients).

- **User Awareness and Training**

  Users should be made aware of policies and procedures regarding appropriate use of networks, systems, and applications. Applicable lessons learned from previous incidents should also be shared with users so they can see how their actions could affect the organisation. Improving user awareness regarding incidents should reduce the frequency of incidents. IT staff should be trained so that they can maintain their networks, systems, and applications in accordance with the organisation's security standards.

4.2 Detection and Analysis

This phase deals with the detection and determination of whether an abnormal operation within an organisation is an incident, and its scope assuming that the abnormal behaviour is indeed an incident. This particular step requires one to gather events from various sources such as log files, error messages, and other resources, such intrusion detection systems and firewalls, that may produce evidence as to determine whether an event is an incident. If a particular event is determine to be an incident, and then it should be reported as soon as possible in order to allow the CSIRT enough time to collect evidence and prepare for the preceding steps.

At this stage of an incident CSIRT members should be notified and communication should be coordinated between members along with designated command center staff (e.g. management and/or systems administrators). It is recommended that at least two incident handlers be available to handle an incident so that one can be the primary handler who can identify and assess the incident and the other to help gather evidence. Communication and coordination

between members of the CSIRT (and management) is critical, especially if the scope of the incident can have a significant impact on business operations. This is also the phase where incident responders should be documenting everything that they are doing, as stated earlier these documents should be able to answer the Who, What, Where, Why, and How questions in case the documentation is to be used to prosecute the perpetrator(s) in. After determining the scope of the event and documenting the evidence, then the CSIRT team can move forward with the next phase. A good example of the detection and analysis phase is a user contacting the help desk and reporting that their system is acting strangely or intrusion detection systems report unusual network traffic from certain hosts. It could come from something hostile as usual activity in system logs that have never appeared before a specific date. It is extremely beneficial to keep an open mind the number of possibilities that an incident could be identified. Two other examples worth mentioning are a missing USB drive or other storage media, and a user finding a USB drive somewhere that has public access and plugs into their computer kicking off an auto-run script that steals data or infects systems.

4.3 Containment, Eradication and Recovery

The primary purpose of this phase is to limit the damage and prevent any further damage from happening. There are several steps to this phase; however, each one is necessary in order to completely mitigate the incident and prevent the destruction of any evidence that may be needed later for prosecution.

4.3.1 Short-term Containment

The first step is Short-term Containment; basically the focus of this step is to limit the damage as soon as possible. Short-term containment can be as straightforward as isolating a network segment of infected workstations to taking down production servers that were hacked and having all traffic routed to failover servers. Short-term containment is not intended to be a long term solution to the problem; it is only intended to limit the incident before it gets worse.

4.3.2 System Backup

The second step is System Backup; it is necessary before wiping and reimaging any system to take a forensic image of the affected system(s) with tools that are well known in the computer forensics community such as Forensic Tool Kit (FTK). The reason behind this is that the forensic software will capture the affected system(s) as they were during the incident and

thereby preserving evidence in the event that the incident resulted from a criminal act or to be used for observing how the system(s) were compromised during the lessons learned phase.

4.3.3 Long-term Containment

The last step before the next phase is Long-term containment, which is essentially the step where the affected systems can be temporarily fix in order to allow them to continue to be used in production, if necessary, while rebuilding clean systems in the next phase. Basically the primary focus would remove accounts and/or backdoors left by attackers on affected systems, installing security patches on both affected and neighboring systems, and doing other work to limit any further escalation of the incident while allowing normal business operations to continue. A good example of containment is disconnecting affected systems by either disconnect the affected system's network cable or powering down switches and/or routers to entire portions of the network to isolate compromised systems from those that have not been compromised. This will in turn isolate the problem from the rest of the production network and limit the spread of any malware or reduce the risk of further systems being compromised.

Eradication means the actual removal and restoration of affected systems. As with each of the prior phases of incident response, continued documentation of all actions taken will be necessary to determine the cost of man hours and other resources as a means of determining the overall impact to the organisation. It is also necessary to ensure that proper steps were taken to remove malicious and other illicit content off of the affected systems, and ensuring that they are thoroughly clean. In general that would mean a complete reimaging of a system's hard drive(s) to ensure that any malicious content was removed and prevent re-infection. This phase is also the point where defenses should be improved after learning what caused the incident and ensure that the system cannot be compromised again (e.g. installing patches to fix vulnerabilities that were exploited by the attacker, etc).

A good example of actions performed during the eradication process would be using the original disk images that were created prior to a system being deployed into production to restore the system and then installing patches and disabling unused services to harden the system against further attacks (e.g. disk images created with "Clonezilla" or "Symantec Ghost"). One would also scan affected systems and/or files with anti-malware software to ensure any malware that is latent is removed (i.e. using an anti-virus program like

"Kaspersky" combined with "CCleaner" to disinfect systems and scan the Windows registry for keys that may initiate any latent malware).

The purpose of the recovery process is to bring affected systems back into the production environment carefully, as to insure that it will not lead another incident. It is essential to test, monitor, and validate the systems that are being put back into production to verify that they are not being re-infected by malware or compromised by some other means. Some of the important decisions to make during this phase are:

- Time and date to restore operations – it is vital to have the system operators/owners make the final decision based upon the advice of the CSIRT.
- How to test and verify that the compromised systems are clean and fully functional.
- The duration of monitoring to observe for abnormal behaviors.
- The tools to test, monitor, and validate system behavior.
- There are many more beneficial decisions that could be listed; however, the above information should provide a few ideas as what is entailed. The primary goal overall, as stated earlier, is to prevent another incident from happening that was due to the same problems that cause the one that was just resolved.

4.4 Post Incident Activity (Lessons learned)

The most critical phase after all of the others is Lessons Learned. The purpose of this phase is to complete any documentation that was not done during the incident, as well as any additional documentation that may be beneficial in future incidents. The document should also be written in a form of a report to provide a detailed review of the entire incident. This report should be able to answer the: Who, What, Where, Why, and How questions that may come up during the lessons learned meeting. The overall goal is to learn from the incidents that occurred within an organisation to improve the team's performance and provide reference materials in the event of a similar incident. The documentation can also be used as training materials for new team members or as a benchmark to be used in comparison in future crisis. The lessons learned meeting should be performed as soon as possible. A good rule of thumb is within two weeks after the incident has happened. The meeting should go through the incident response report with finalization in an executive summary format. It should be kept short, as to not lose the audience's attention and remain professional.

A good example of performing lessons learned is to have a power point that summarizes the following information:

- When was the problem was first detected and by whom.
- The scope of the incident.
- How it was contained and eradicated.
- Worked performed during recovery.
- Areas where the CSIRT teams were effective.
- Areas that need improvement.

It should also include time for suggestions and discussion between members of how to improve the overall team. This phase is extremely beneficial to have members share ideas and information in order to improve team effectiveness in future incidents.

5.0 Incident Handler's Checklist

1. Preparation

a) Are all members aware of the security policies of the organisation?
b) Do all members of the Computer Security Incident Response Team know whom to contact?
c) Do all incident responders have access to journals and access to incident response toolkits to perform the actual incident response process?
d) Have all members participated in incident response drills to practice the incident response process and to improve overall proficiency on a regularly established basis?

2. Detection and Analysis

a) Where did the incident occur?
b) Who reported or discovered the incident?
c) How was it discovered?
d) Are there any other areas that have been compromised by the incident? If so what are they and when were they discovered?
e) What is the scope of the impact?
f) What is the business impact?
g) Have the source(s) of the incident been located? If so, where, when, and what are they?

3. Containment

a) Short-term containment
    i. Can the problem be isolated?
        1. If so, then proceed to isolate the affected systems.
        2. If not, then work with system owners and/or managers to determine further action necessary to contain the problem.
    ii. Are all affected systems isolated from non-affected systems?
        1. If so, then continue to the next step.
        2. If not, then continue to isolate affected systems until short-term containment has been accomplished to prevent the incident from escalating any further.
b) System-backup

i. Have forensic copies of affected systems been created for further analysis?
ii. Have all commands and other documentation since the incident has occurred been kept up to date so far?
    1. If not, document all actions taken as soon as possible to ensure all evidence are retained for either prosecution and/or lessons learned.
    2. Are the forensic copies stored in a secure location?
        a. If so, then continue onto the next step.
        b. If not, then place the forensic images into a secure location to prevent accidental damage and/or tampering.

c) Long-term containment
    i. If the system can be taken offline, then proceed to the Eradication phase.
    ii. If the system must remain in production proceed with long-term containment by removing all malware and other artifacts from affected systems, and harden the affected systems from further attacks until an ideal circumstance will allow the affected systems to be reimaged.

4. Eradication

a) If possible can the system be reimaged and then hardened with patches and/or other countermeasures to prevent or reduce the risk of attacks?
    i. If not, then please state why?
b) Have all malware and other artifacts left behind by the attackers been removed and the affected systems hardened against further attacks?
    i. If not, then please explain why?

5. Recovery

a) Has the affected system(s) been patched and hardened against the recent attack, as well as possible future ones?
b) What day and time would be feasible to restore the affected systems back into production?
c) What tools are you going to use to test, monitor, and verify that the systems being restored to productions are not compromised by the same methods that cause the original incident?
d) How long are you planning to monitor the restored systems and what are you going to look for?

e) Are there any prior benchmarks that can be used as a baseline to compare monitoring results of the restored systems against those of the baseline?

6. Post-Incident Activity/Lessons Learned

a) Has all necessary documentation from the incident been written?
    i. If so, then generate the incident response report for the lessons learned meeting.
    ii. If not, then have documentation written as soon as possible before anything is forgotten and left out of the report.
b) Assuming the incident response report has been completed, does it document and answer the following questions of each phase of the incident response process: (Who? What? Where? Why? And How?)?
c) Can a lessons learned meeting be scheduled within two weeks after the incident has been resolved?
    i. If not, then please explain why and when is the next convenient time to hold it?
d) Lessons Learned Meeting
    i. Review the incident response process of the incident that had occurred with all CSIRT members.
    ii. Did the meeting discuss any mistake or areas where the response process could have been handled better?
        1. If no such conversations occurred, then please explain why?

6.0 Conclusion

Organisations should always be concerned about "when", and not "if" an incident will occur. Incidents can sometimes have serious impact or very low effect on organisations. In any case, it is imperative that we have realistic incident response policies, plans and procedures in place to ensure that each of the incident handling steps are being followed during an incident to prevent further disruption to an organisation's operations. Thus, a dedicated incident response team should be trained to deal with incidents as and when they occur and proper documentation should be in place for any interactions with third parties.

7.0 References

- SANS, The Incident Handler's Handbook
- The University of Arizona, Incident Response Standard
- NIST, Computer Security Incident Handling Guide

Appendix A

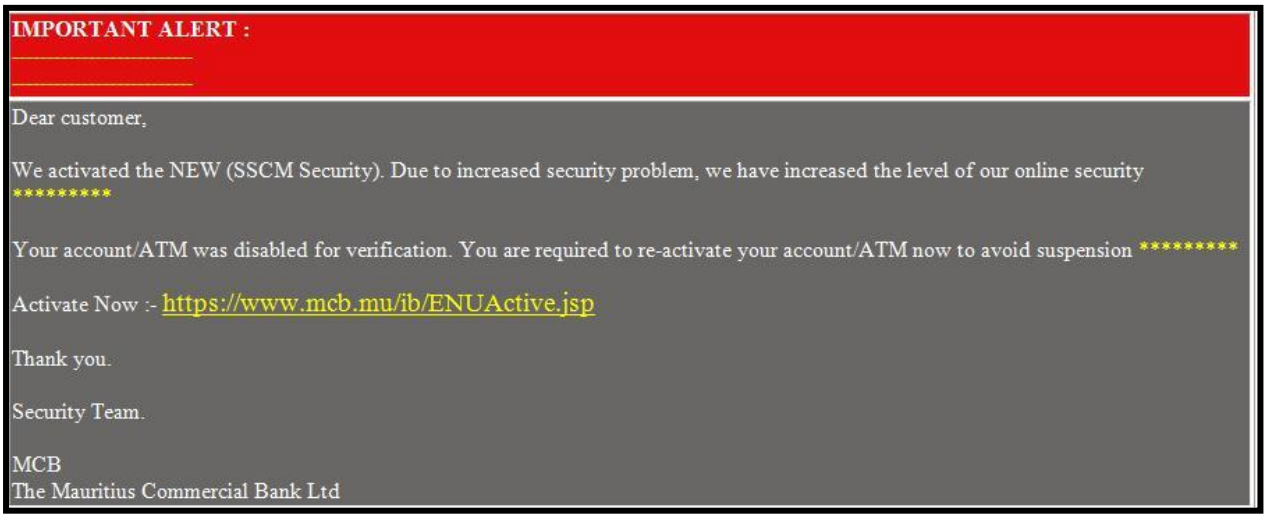
List of Acronyms

CERT	Computer Emergency Response Team
CERT-MU	Computer Emergency Response Team of Mauritius
CSIRT	Computer Security Incident Response Team
FTK	Forensic Tool Kit
ISP	Internet Service Provider
OS	Operating System
POC	Point of Contact
SCAP	Security Content Automation Protocol
SOP	Standard Operating Procedure
USB	Universal Serial Bus

Appendix B

A real-life incident scenario - The case of Mauritius Commercial Bank (MCB) Phishing Attack

The customers of one of the most prestigious bank in Mauritius, The Mauritius Commercial Bank (MCB) have been victim of phishing. The customers were tricked through an e-mail that seemed to be originated from the bank stating that their accounts have been blocked due to some reasons. The email is shown below:



IMPORTANT ALERT :

Dear customer,

We activated the NEW (SSCM Security). Due to increased security problem, we have increased the level of our online security **********

Your account/ATM was disabled for verification. You are required to re-activate your account/ATM now to avoid suspension **********

Activate Now :- https://www.mcb.mu/ib/ENUActive.jsp

Thank you.

Security Team.

MCB
The Mauritius Commercial Bank Ltd

In order to activate their accounts, the customers had to click on a link that was provided in the email. On clicking on the link, the customers were redirected to a phishing website that looked like the original website of the bank. They were then asked to enter their banking details such as their user ID and password. By entering their details on the web page allowed the phishers to get into the bank account of the customers and steal their money. The first incident was detected in October 2011 where a customer reported the loss of Rs150, 000 from her account. From October 2011 to February 2012, 5 customers of the MCB became victim and lost their money. According to L'Express newspapers dated 03rd March 2012, around 1 million rupees has been stolen from the customers' account. After the investigations made by the Police with the help of the Interpol, the phishing attack originated from Africa and was conducted by a Nigerian. The criminal set up phishing websites to trick customers of major banking institutions in Mauritius who use Internet Banking service. It was also discovered that the stolen money was transferred to an African country via MoneyGram.

Proposed Solution – A Phishing Incident Response Plan

Phishing scams are constantly evolving and are becoming more sophisticated. With the wide adoption of Internet banking, financial institutions should be more careful about targeted attacks. Therefore, the bank should develop a proper approach to deal with such situation. No bank would be able to operate without a plan of escape in the case of a fire. These situations place the bank in a precarious position as it could quickly escalate to a major emergency. Similarly, if bank do not has an incident response plan, a successful phishing attack could quickly lead to a catastrophe. When phishing attacks occur, a quick response is important to limit the resulting damage. Thus, it is vital for the financial institution to include an appropriate phishing incident response plan to facilitate prompt actions to minimize the threat and cost of the breach. By adopting an incident response plan, the organisation will be able to respond and mitigate the impact by containing and ultimately recovering from it. The phishing incident response plan shall consist of the following phases of the incident:

1. Preparation

The preparation phase usually takes place before the phishing incident occurs. Since time is critical in such situation, it is very important for the bank to be prepared to react to the phishing incident as quickly as possible to minimize the risks it can has on the business. The bank can create an internal centralized Computer Security Incident Response Team (CSIRT) - a team located in one physical or geographical location that has responsibilities for the entire organization and is dedicated to CSIRT works. In addition, the team should have the necessary resources, infrastructure and tools to better respond to the incident. However, even if all necessary precautions are taken, a successful phishing attack could still happen and there is a need to be prepared to respond to it.

2. Detection and Analysis

In most phishing cases targeting banks, the incident is detected through e-mails sent to customers of the bank. Upon the detection of any phishing attack, the bank should

immediately gather all necessary data that can be helpful to bring the phishing website down. The details include the original phishing e-mail, TCP-IP and ISP information, URLs, and screen shots of the illegal web site.

In addition, the employees of the bank should be alerted of the incident. They should watch out for and report unusual activity such as unusual address change requests, account transactions, or new account activity.

3. Containment Eradication and Recovery

When a phishing attack has been detected and analyzed, it is important for the bank to contain it before the damage increases. Therefore, the process of containment eradication shall consist of the measures taken by the bank to the respond to the phishing attack and avoid damages. These can include the following steps:

- **Bringing Down or blocking access to the phishing site**

  Necessary measures should be taken by the bank to bring the phishing website down. If the bank cannot bring down the site, the next action can be to block access to the phishing site. However, this depends on the location where the phishing site is hosted. If the site is hosted in a foreign country, it is possible to block the phishing site by name or IP at the gateway routers of the home country. The bank should contact the concerned authorities so that prompt actions can be taken.

- **Feeding the wrong data**

  The bank can also access the phishing site and supply wrong user ID or passwords. This could be a useful mechanism to confuse the phisher and reduce chances of the attacker of being able to identify the correct user ID or passwords from the pile of data.

- **Introducing additional authentication or multi-factor authentication**

  Introducing additional authentication layer at the original website in addition to the normal procedure is another measure that the bank can take to prevent the hacker from using the data collected at the phishing site. The challenge here is to ask for a parameter that is already known to the user and the Bank but not to the phisher. For example, the bank can ask the customer for one or more of the following:

- Enter the branch name
- Enter date of birth
- Enter last four digits of the account number

Multifactor authentication adds an additional level of security to the logon procedure. While multifactor authentication is still subject to phishing attacks, it makes phishing more difficult. For example, if the phishing site tricks a customer into providing a username and password, and the bank site also required a hardware token, it would be more difficult to gain access since the phisher cannot obtain the token from the consumer through a phishing e-mail.

- **Tracking weblogs for attacker connections**

  The attacker will surely try to use the user name and passwords collected at the phishing site against the original site. By tracking the weblogs will allow the bank to detect whether login attempts for multiple user IDs are coming from a single source-IP. Although, it will not be appropriate to conclude that a particular IP would be that of the attacker, suspicious IP can be detected. If the source points to a country where the chances of valid customer being present are remote, then the bank can restrict access from that block of IP address.

- **Customer Education**

  Customer education is one of the most important measures and is a key component of building the trust necessary to overcome phishing fears. The goal of phishing attacks is to trick the customer to willingly provide information that can be used for identity theft or to access his or her bank account. Thus, a key defensive measure is to educate customers so that they will be on guard for these attacks, recognize them when they occur, and not provide the information that these attacks seek to obtain. This can be done by teaching them how to recognize the signs of a phishing attempt such as misspellings, general greetings instead of being personalized, urgent calls-to-action, account status threats, requests for personal information, and fake domain names or links. Other examples include teaching them how to recognize a valid and secure web site before providing any information by looking for the green bar or making sure that the URL is HTTPS.

4. Post Incident Activity

After the incident, the bank should create a report whereby all relevant information about the incident, the chronology of events, the actions taken by the bank and the damage caused by the incident such monetary cost are included. This report should be submitted to the Management for further actions.

The report will also provide a reference to assist in handling similar incidents in the future. After the incident, the bank can consider whether to compensate the customers for the stolen money. This is done to ensure that the trust of customers in the bank and for business continuity.

Additional measures that can also be implemented in the bank in order to avoid or minimize the damages in case such attack occur in the future. For example:

- **Sender Policy Framework**

  Phishing emails often forge the sending domain of the targeted institution. Sender Policy Framework (SPF) is an email validation system designed to prevent email spam by detecting email spoofing and common vulnerabilities, by verifying the sender IP addresses. SPF allows administrators to specify which hosts are allowed to send mail from a given domain by creating a specific SPF record in the Domain Name System (DNS). Mail exchangers will use the DNS to check that mail from a given domain is being sent by a host sanctioned by that domain's administrators.

- **Digitally Signed Email**

  Customers lack means for verifying the authenticity of important messages from legitimate institutions. Hence, the bank can establish a policy whereby all high-value e-mail communications to customers are digitally signed with an authorized private key. Upon receipt of the e-mail, the customer would verify the authenticity of the e-mail using the bank’s public key. In such situations, there is a low probability that a phisher could create a valid signature on a fraudulent e-mail.