CMSGu2014-06

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Incidents and Digital Evidence

CERT-MU

National Computer Board
Mauritius

Version 1.0

November 2014

Issue No. 6

Table of Contents

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

This guideline has been formulated to assist staff in dealing with allegations of crime which involve a high-tech element and to ensure they collect all relevant evidence in a timely and appropriate manner.

1.2 Audience

The target audience for this guideline includes cybercrime investigators, information security consultants, incident handlers, system administrators and network administrators.

1.3 Document Structure

This document is organised into the following sections:

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

Section 2 gives a background on digital evidence.

Section 3 illustrated the lifecycle of incidents and investigations.

Section 4 elaborated on the treatment of data and investigations.

Section 5 concludes the document.

Section 6 contains a list of references that have been used in this document.

2.0 Background on Digital Evidence

Information Technology is ever developing and each new development finds a greater role in our lives. The recovery of evidence from electronic devices is now firmly part of investigative activity in both public and private sector domains.

Electronic evidence is valuable evidence and it should be treated in the same manner as traditional forensic evidence - with respect and care. The methods of recovering electronic evidence, whilst maintaining evidential continuity and integrity may seem complex and costly, but experience has shown that, if dealt with correctly, it will produce evidence that is both compelling and cost effective.

It cannot be overemphasized that the rules of evidence apply equally to computer-based electronic evidence as much as they do to material obtained from other sources. It is always the responsibility of the case officer to ensure compliance with legislation and, in particular, to be sure that the procedures adopted in the seizure of any property are performed in accordance with statute and current case law.

This good practice guide is intended for use in the recovery of computer-based electronic evidence; it is not a comprehensive guide to the examination of that evidence.

3.0 Lifecycle of Incidents and Investigations

No two computer investigations are identical. However, the timeline shown below gives an indication of the number, complexity and duration of typical corporate tasks that may occur, and for which a management framework is essential. The actual details may vary considerably.

The table concentrates on what happens in an "incident". Note that many of the tasks shown here will operate concurrently.

Task	Description
Detection:	Detection may be prompted by a dramatic event, such as the arrival of an extortion demand or the failure of major services or by no more than a suspicion triggered by anomalous behaviour.
Reporting:	All organisations need a designated point to which reports can be made, whether corporate security, computer security, audit, the company secretary, human resources or a legal adviser. In practice the full extent of an incident may take some time to evolve, so there could be several reports. In addition, some reports will turn out to be false.
Diagnosis - initial:	Whoever receives the report should have the skill, experience, resources to make an assessment of what may have happened and to provide initial guidance about how the organisation should tackle the problem.
Management actions based on initial diagnosis:	At this point, the relevant executives will be informed and staff detailed to carry out specific tasks. This will usually involve setting up a special "taskforce".
Evidence collection:	This is one of the most important early stages. It includes identifying likely sources of evidence, collection under controlled conditions and preservation.
Diagnosis – mature:	Initial diagnoses are likely to be wrong. Evidence collection soon moves into evidence assessment, with a consequential effect on how the problems are perceived. Few crises are so purely computer-based that the only kind of evidence is obtained from computers. The ongoing process of diagnosis will take in evidence from and about individuals and businesses and paper based documents.
Management actions based on mature diagnosis:	As the nature of the problem becomes clearer, the organisation is able to define its objectives with greater clarity and certainty. Once the immediate risks to the integrity of information systems have been resolved, corporate aims will have a more long-term focus.
Business/asset recovery activity:	If computer systems have been compromised, there has been some interruption to business, assets have been lost or some aspect of the

	crisis has become public, there will need to be a business recovery phase, similar to that after premises have been affected by fire or flood., Experience from the established disaster recovery/business contingency planning industry suggests that full recovery always takes much longer than expected. Typical tasks include: restarting computer systems; recovering lost assets; and public relations.
Remedial activity:	This includes learning lessons, preventing repetition, introducing new management and audit procedures, and new security engineering facilities. These lessons may extend beyond the immediate events to problems with corporate culture and management structure.
Civil legal activity:	This covers, for example, insurance claims, asset recovery, claims for damages, negligence, breach of confidence, etc.
Law enforcement agency activity:	There may be several phases of law enforcement activity: initial enquiries; collection of statements and evidence; return visits for further interviews and search for evidence; preparation for trial; and attention to defense requests for disclosure.
Criminal and regulatory proceedings:	A complex criminal trial may go through several phases, including committal and the substantive trial. Further information may be requested during the trial process.

4.0 Treatment Of Data During Investigations

4.1 Evidence Preservation Following An Incident

It is critical that as much evidence (and other information) as possible is gathered at this stage as there may not be an opportunity to gather it at a later time. It should be noted that the quality of the outcome of an investigation will be highly dependent on the quality of the information that is provided as a result of the incident response.

Preservation of evidence (for subsequent presentation in court in the event of a prosecution) is a critical factor in any criminal investigation. The appropriate action to take to preserve the evidence will depend on the circumstances but may involve actions ranging from copying unmodified computer logs to CD/DVD through to forensic copying of computer hard drives. Forensic copying of computer hard drives by appropriately trained personnel is the most effective means of preserving ALL of the evidence; however, it is also the most intensive and time consuming.

Sources of evidence may include any or all of the following:

- Systems that have been compromised;
- Hard drives of systems that have been compromised;
- Web, mail, ftp or any other relevant server logs;
- Proxy logs;
- RADIUS logs;
- Intrusion Detection System (IDS) logs;
- Firewall logs;
- Router logs.

4.2 Digital Evidence

The International Organisation on Computer Evidence (IOCE) has developed a set of principles when establishing procedures for the collection, preservation and use of digital evidence, according to its national law and standards bodies, and to be aware of potential differences when collecting evidence at the request of other States.

These principles are:

- When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
- All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review
- An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.

Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

4.3 Computer Based Electronic Evidence

Shown below are brief recommendations for the collection of computer based electronic evidence, derived from the UK Metropolitan Police Computer Crime Unit.

- Keep a written log of all action taken during the investigation of an incident
- Put a single individual in charge of any investigation
- Preserve system logs by archiving off the target system
- Record any discrepancies in the system clock and do not adjust it during an investigation
- Do not rely on the integrity of the target machine's operating system or other utilities (so examine it from a remote machine if possible)
- Where an attack is still in progress, adopt a clear policy on whether to continue monitoring or to attempt to exclude the intruder – this is entirely up to the organisation being targeted
- Once it has been secured, conduct a thorough investigation of the means used to access the system; do not exclude the possibility of internal collusion
- Pay particular attention to gathering network address information originating from the attacker (Source and destination IP addresses, MAC address, packet length and type, open ports etc.)
- Identify and preserve previous system backups, which can be used to establish modifications to the system made by the intruder
- Notify the police as soon as possible

5.0 Conclusion

Computers can be used to commit cybercrime. They can contain evidence of crime and can even be targets of crime. Understanding the role and nature of electronic evidence that might be found, how to process a crime scene containing potential electronic evidence and how an agency might respond to such situations is crucial.

5.0 References

- **http://www.7safe.com**
- **http://www.europeanpaymentscouncil.eu**
- **en.wikipedia.org**