UCT CSIRT

INFORMATION AND CYBER SECURITY RESPONSE PLAN

Document Name:	CSIRT Plan
Prepared by:	Bruce Fielies
Date:	28 September 2016
Document Number:	1
Version:	4.0

DOCUMENT INFORMATION

DOCUMENT TITLE	CSIRT Plan
DOCUMENT NUMBER	1
DOCUMENT CATEGORY	Draft Proposal
DOCUMENT VERSION NUMBER	4.0
EFFECTIVE DATE	8 September 2016
REVISION DATE	

DOCUMENT APPROVAL

NAME	ROLE	DATE	SIGNATURE
AUTHOR:			
Bruce Fielies	TCS,TSS, ICTS, University of Cape Town	26 July 2016	
Philemon	TCS,TSS, ICTS, University of Cape Town	26 July 2016	
REVIEWER(S):			
Andre Le Roux	TSS, ICTS, University of Cape Town	18 August 2016	
Bruce Fielies	TCS, TSS, ICTS, University of Cape Town	18 August 2016	
Bruce Fielies	TCS, TSS, ICTS, University of Cape Town	28 September 2016	
APPROVER(S):			
Andre Le Roux	TSS, ICTS, University of Cape Town	22 August 2016	
CLIENT SIGNATURE:			

DOCUMENT CONTROL

REVISION HISTORY:

VERSION NO	AUTHOR	DATE	DESCRIPTION
1.0	Bruce Fielies	July 2016	CSIRT Plan Draft
2.0	Bruce Fielies	August 2016	CSIRT Plan Draft
3.0	Bruce Fielies	August 2016	CSIRT Plan
4.0	Bruce Fielies	September 2016	CSIRT Plan

Table of Contents

1. Introduction

An information technology (IT) security incident at UCT, is an event involving an IT resource at University of Cape Town that has the potential of having an adverse effect on the confidentiality, integrity, or availability of that resource or connected resources. Resources include individual computers, servers, storage devices and media, and mobile devices, as well as the information, messages, files, and/or data stored on them. Prompt detection and appropriate handling of these security incidents is necessary to protect UCT's information and communication technology assets.

2. Incident Handling and Response

The Cybersecurity Incident Response Process has several phases; and 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.

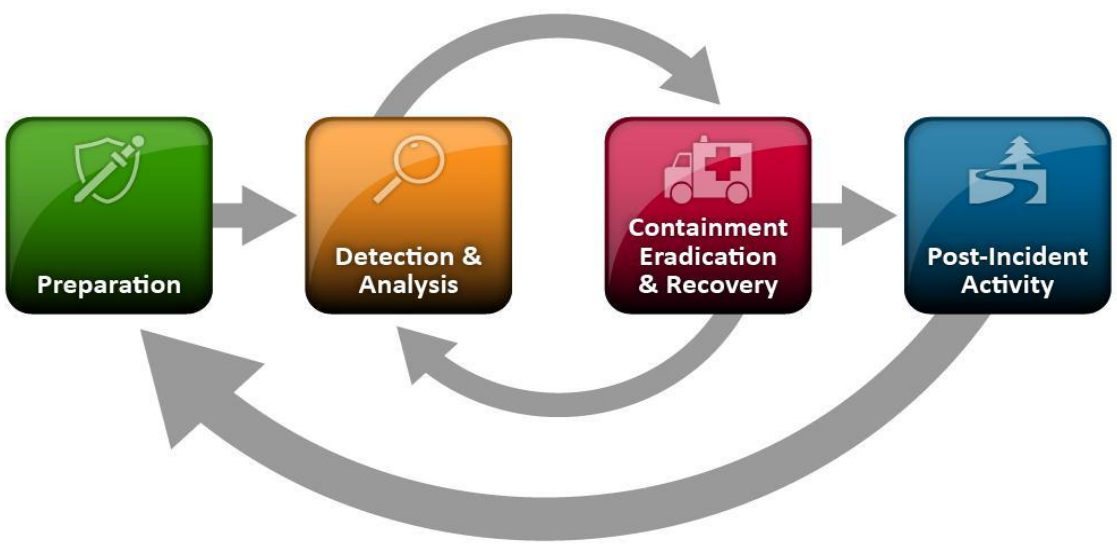

Figure 1 illustrates the incident response life cycle.

The sections below describe:

1) How to notify the appropriate persons upon identification of an incident;
2) How to handle the incident, and recover from an incident in a manner appropriate to the type of incident;
3) Establish a reporting format and evidence retention procedures.

The initial approach involves establishing and training an incident response team, and acquiring the necessary tools and resources.

The **Preparation Phase** as implied by the name, deals with preparing a Cyber Security Incident Response Team to be ready to handle the Incident at the moment of incident notice. A security incident can range from anything such as a power outage or Hardware failure to the most extreme incidents such as a violation of organizational policy.

Detection and Analysis Phase attempts to deal with the security breaches and is thus necessary to alert the organization whenever incidents occur.

During the **Containment, Eradication and Recovery Phase** the organization in keeping with the severity of the incident, 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 organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents.

2.1. Cyber Security Incident Response Process Overview

The purpose of this *Cyber Security Incident Response Process* is to provide general guidance to UCT staff who manage ICT resources to enable a quick and efficient recovery from security incidents; a quick response in a systematic manner to incidents and carry out all necessary steps to correctly handle the incident; preventing or minimizing the disruption of critical computing services. The process aims to provide guidance in order to minimize loss or theft of sensitive or mission critical information.

Security incident response will be typically handled through several Phases: Preparation, Analysis and Detection, Containment, Eradication and Recovery, and Post Incident Review.

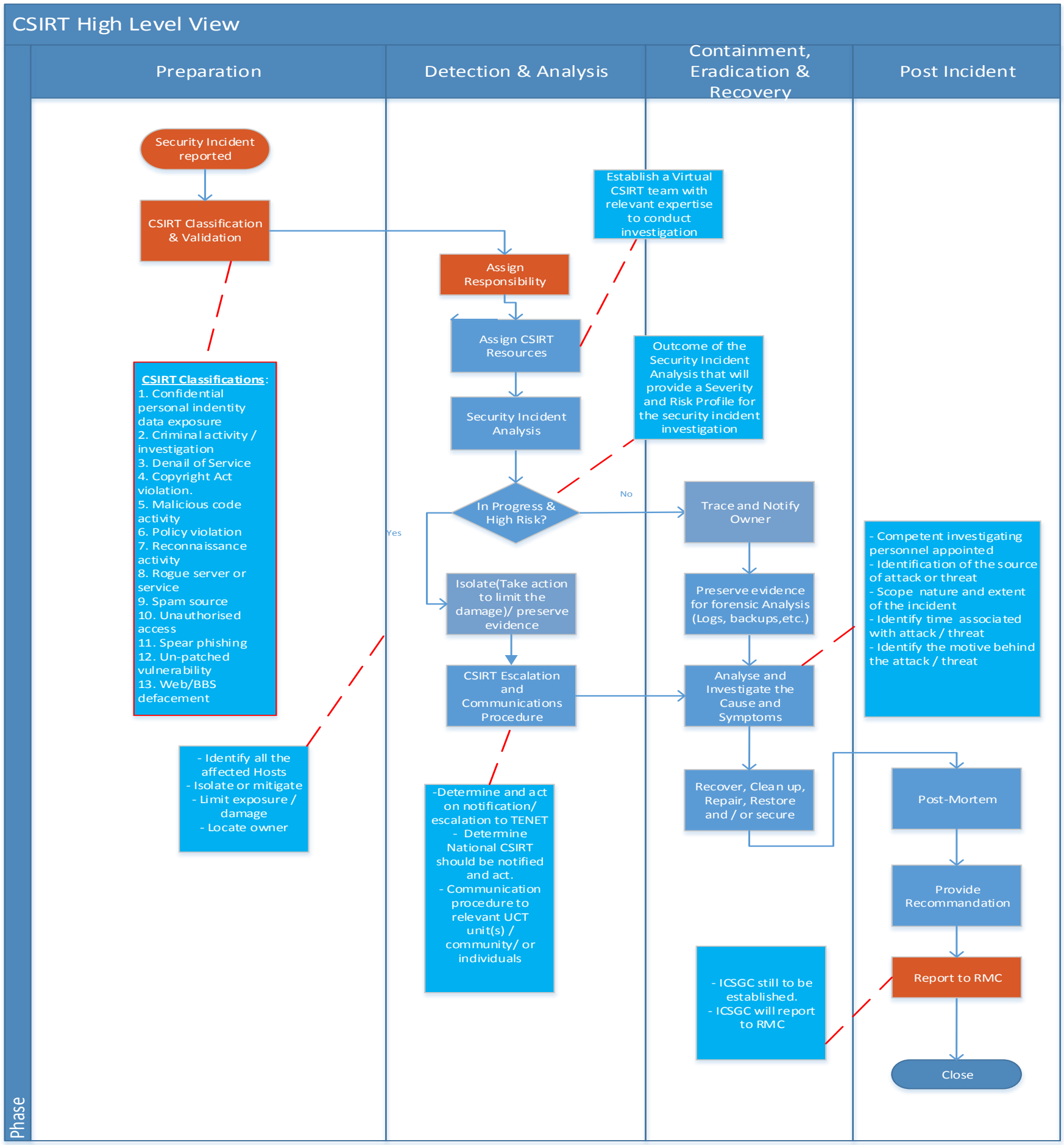

Figure 2: CSIRT High Level Process Overview

3. CSIRT Preparation Phase

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs. This section provides basic advice on preparing to handle incidents and on preventing incidents.

Regardless of the cause of the incident, the preparation phase is a crucial phase in the incident life cycle. It will determine how well your team will be able to effectively respond in the event of a crisis.

3.1. Security Incident Reporting and Detection

In addition to reports from the University community of suspected or confirmed security incidents, anomalous events may be detected that indicate potential security incidents. Having mechanisms to detect anomalous events early and reliably helps minimize their impact. Detection can be very challenging since there are potentially so many different types of incidents and vectors for attack on a huge number and variety of systems and networks. Thus no one person, unit, or technology can possible monitor it all. Detection is therefore a collaborative effort among University and departmental IT and security personnel

3.1.1. Security Incident Reporting

1. All members of the University community must be responsible for promptly reporting suspected or known security incidents, including observed or suspected security weaknesses in systems or services, in accordance with University of Cape Town's IT Security Policy.

2. All suspected high severity incidents, including those involving possible breaches of personal identity information, must be reported directly to the Cybersecurity and Incident Response Team as quickly as possible by phone ext 4500 or by email csirt@uct.ac.za

3. **Warning:** If reporting a suspected security weakness or system vulnerability, do not attempt to confirm it by testing the weakness since that could be interpreted as a potential misuse of the system or cause damage to it.

4. When receiving a report of a suspected or confirmed security incident, the CSIRT or designee will gather as much of the following information as possible:

   a. Name, affiliation, e-mail address, and phone number of person reporting the incident

   b. Description of the suspected security incident

   c. Information to help identify the source of the suspicious activity, like an IP address or an e-mail message with full headers.

   d. Date(s) and time(s) of the suspicious activity, noting the time zone.

   e. Evidence of suspicious activity (for example, full headers of an e-mail message suspected to be spam originating at K-State, appropriate log records, etc.)

5. In addition to documenting the initial report, the CSIRT or designee will:

   a. Create an entry in the University security incident tracking system

   b. Initiate appropriate incident handling procedures

   c. As appropriate, communicate with and provide feedback about the results to those reporting the incident once the incident has been handled and closed

3.1.2. Security Incident Detection

1. Channels for detecting possible security incidents include:

   a. E-mail sent to csirt@uct.ac.za

   b. Network performance monitoring (e.g., noticing a congested network segment)

   c. Reports from external entities (CSIRTS, ISP's), including BITSight.

   d. Notification from a copyright owner or representative sent to University of Cape Town designated copyright agent

   e. Court orders (for example, a subpoena or search warrant). All IT-related court orders should be directed to the Office of General Counsel.

   f. A customer contacts the IT Help Desk ext 4500

   g. Monitoring security mailing lists and web sites for threat alerts (for example, the SANS Internet Storm Center — isc.sans.org)

   h. Monitoring external sources of information about new vulnerabilities and exploits and about incidents occurring at other organizations

   i. Employing passive detection techniques such as network flow analysis (top talkers, traffic volume thresholds, communication with known malicious sites, etc.); log file analysis (operating system, system services, databases, applications, network devices, etc.); intrusion detection/prevention systems, and monitoring alerts from security systems (firewalls, anti-virus protection, intrusion detection/prevention systems, wireless network management systems that detect rogue wireless access points, etc.)

   j. Employing active detection techniques such as port scans looking for unusual services, vulnerability scans, manual monitoring of radio frequencies to detect unauthorized wireless access points, and file integrity verification that detects changes to important files

3.2. Security Incident Classification System

Security incidents will be classified according to incident categories and severity of incident in order to determine the appropriate response to the reported incident. A security incident classification scheme will be maintained by the Chief Information Security Officer to describe security events and support incident tracking over time.

3.2.1. *Incident Categories*

The following categories will be used to describe IT security incidents at University of Cape Town. Several categories may apply to a single incident. The examples listed in each category are not meant to be exhaustive.

3.2.1.1. Identity data exposure

A personal identity information is defined as any information that directly or indirectly identifies an individual (the information can be in digital format or on paper). This should be handled in accordance with the Protection of Personal Information Act in the RSA (Act, 2013) / Protection of personal information Bill, and the privacy and the protection of individuals' and organisation's data should be taken seriously.

- Personal identification information
- Identity theft and Identity Fraud
  - The main point of the definition for both identity theft and identity fraud, are that the identity was wrongfully obtained and used in ways that involved deceit.
- Destruction / exposure of the university data
- Disclosure of the University sensitive information
- Misuse (bad handling) of the university intellectual property

3.2.1.2. Criminal activity/investigation

On this category of incidents, an external legal/criminal process needs to be invoked by UCT Campus Protection Services.

- Subpoena, search warrant, or other court order
- Litigation hold request (aka e-Discovery)
- Online theft, fraud
- Threatening communication
- Child pornography
- Physical theft, break-in

3.2.1.3. Denial of Service

The denial of service attack is the attack of threat that deprives legitimate users or organisation access to resources expected to be had. It can be targeted to a single user or service as it can target a number of interconnected systems/ services. Whether it is in or outbound attack, if it is determined that outside parties involved, the interaction with the university ISP will be required and the National CSIRT will be called upon according to the nature and extent of the incident. The handling of these types of incidents will be kept to the internal CSIRT handling processes and depending on the nature of the incident resources to be assigned will be decided upon;

- Single or distributed (DoS or DDoS)
- Inbound or outbound

3.2.1.4. Copyright Act violation

Copyright is to be understood in the sense of intellectual property. The Act stipulates that someone's creative work, ideas, invention written works, program… should not be copied by anybody else without the consent of the owner. Some violations of this Act includes following acts:

- Copyright Act violation (Ref. to ICTS - Copyright Guidelines)
- Official notification from copyright owner or legal representative
- Illegal distribution of copyrighted or licensed material (movies, music, software, games)

3.2.1.5. Malicious code activity / Malware

A malware is an umbrella term that stands for a variety of malicious software, including Trojans, spyware, worms, adware, ransomware, and viruses (all viruses are malwares but all malware are not viruses).

NB: Anti-virus normally deals with the more established threats, such as Trojans, viruses and worms. However anti malware, focus on the newer stuff (i.e. polymorphic malware, zero-day-exploit)

These types of threats are the maliciously exploit of the systems, with the intention of getting hold of people's information/ system, and in the worst case scenario destroy/ cause damages to the system:

- **Worm** (a computer worm is a self-replicating program that penetrates the system with the intention to spread malicious code. Worms use networks to send copies of the original code t other computers causing harm by consuming bandwidth or possibly deleting files or sending documents via email. They can also install back door on the computers.

  The difference between a worm and a virus is that they self-spread out the network, exploring vulnerabilities found on the system automatically, no need of cybercriminals action required to spread as opposed to a virus which requires a human intervention; causing a significant threat to the network.

- **Virus** (a virus is a piece of code that is capable of copying itself in order to do damage to your computer, including corrupting your system or destroying data. It is a specific type of malware). A virus spread requires a human action(ex. opening an executable file)

- **Trojan**: A Trojan horse presents itself as a useful software hiding the built in capabilities of destroying/ damaging the systems once installed. Trojans can be simply dormant software designed to annoy rather than malicious (changing icon on desktop, adding active icons desktops..); other are designed to sleep quietly on the computers installed on and open back doors for malicious access to the system.

- **Botnet(Zombie army**):
  A bot net is a network of machines interconnected without owners being aware of it, that have been set up to send transmissions to other computers on the network / internet. Each of those is referred to as a bot (robot) or zombie. Normally the attacker targets the less guarded machines and create a network of them. They normally connect to an external entity which controls them called a command and control server or C2 or C&C server.

- **Key logger**: A key logger is a keyboard capturing software maliciously installed on the computer. It is a surveillance software whose purpose is to record the key stroke of your key board and send them to a log file (encrypted generally). The file created can be sent to the specified recipient maliciously can record emails, email addresses, web addresses,… depending on the cybercriminal's plan. It can be of type hardware or software.

- **Rootkit:** A rootkit is a collection of tools that enable administrator level access to a computer or computer network. The cracker accesses the computer as a user and installs a rootkit generally by exploiting known vulnerabilities or via other means. Once installed, the rootkit allows the attacker to gain admin privileges on the computer and ale to control the computer in question and or network.

- **Ransomware:** type of malware that prevents or limits access the system from users (screen or file/folders), until a ransom is paid. Generally selected files (based on a specific type) are encrypted and users are forced to do online payment in order to get the decrypt key and access their files. Ransomware are installed on machines from downloads from/ or visit to malicious or compromised websites.

3.2.1.6. Policy violation

- UCT Security policy violation
- Violation of student code of conduct
- Personnel action/investigation

3.2.1.7. Spam source

SPAM are unsolicited emails which can be categorised as inbound or outbound Spams.
An **Inbound Spam** is an unsolicited email destined to the UCT addresses.
An Outbound Spam is an unsolicited email sent from a host within the UCT network; typically where a machine is compromised and being used to send out many copies of the same message.

3.2.1.8. Phishing

The following known types of phishing events are possible;

- Spear Phishing
  - Scam e-mail specifically targeting a UCT e-mail addresses that tries to trick people into divulging private information.
- Clone Phishing
  - Previous legitimate sent email has the content or recipient address taken and used to create identical emails.
- Whaling Phishing
  - Phishing targeting executives of the organisations, or individuals in managerial positions of a given organisation.
- Phishing scam web server

3.2.1.9. Unauthorized access

- Abuse of access privileges
- Unauthorized access to data
- Unauthorized login attempts
- Brute force password cracking attempts
- Stolen password(s)

3.2.1.10. Un-patched vulnerability

Unpatched vulnerability denotes the risk of potential threat that can lead to a system(s) vulnerability exploit which can be an entry point for malicious actors to gain access into the system. Note that these malicious actors do not stop conducting their reconnaissance activities, via systems scanning and monitoring, trying to identify parts of the system susceptible for exploit.

Below are a few of the main types of probable candidate for vulnerability exploits:

- Vulnerable operating system
- Vulnerable application
- Vulnerable web site/service
- Weak or no password on an account

3.2.1.11. Reconnaissance activity

- Port scanning
- Other vulnerability scanning
- Unauthorized monitoring

3.2.1.12. Web/BBS defacement

- Defacement of web site
- Inappropriate post to BBS, wiki, blog, etc.
- Redirected web site

3.2.1.13. Other

This classification will be used for any new unclassified security incidents that has not yet been categorised.

4. CSIRT Detection and Analysis Phase

In this phase, responsibilities are assigned based on the classification of the security incident. Once a potential security incident is reported or anomalous activity detected, analysis must be conducted to determine and understand the nature and extent of the security incident.

During this initial analysis activity, it would be important if possible, to identify who is the attacker, scope and the extent of the attack, time frame of the attack and what might be the motivation for the attack.

4.1. Goals

a. Understand the nature and scope of the incident
b. Collect enough information about the incident so the response team can prioritize the next steps in handling the incident, which is normally containment
c. Determine if confidential data is involved in the incident

4.2. Components of security incident analysis

a. Responsibility will be assigned to the designated CSIRT member who will take the full responsibility of coordinating the relevant security investigation activities.

b. The Virtual CSIRT team must be activated, which will comprise of various professionals (for example, a security analyst, network analyst, system administrator, and application manager) which will assist in the follow-on investigations that will be required.

c. CSIRT will also consult with other external sources like TENET, SA National CSIRT and CPS to work together with the investigation team.

d. Understanding normal system and network behaviour so anomalous activity can be identified

e. Analysis and correlation of as many indicators as possible, such as monitoring network traffic to/from the host suspected of being compromised, network packet captures for more in-depth analysis, log file analysis, interviews with users and/or system administrators, etc.

f. Initial determination of the appropriate incident's scope:

1. Who has attacked us?
2. What is the scope and extent of the attack?
3. When did the attack occur?
4. What did the attackers take from us?
5. Why did they do it?

g. Research of the specific malware or type of attack

h. Collection of additional data which may require permission from the CIO.

4.3. Procedures for Analysis

a. Detect security event (see section above - Security Incident Detection)

b. Analyse event data to determine the extent of a security incident and get an initial impression of the nature and scope of the incident.

c. If there's a need to access personal data, like an individual's e-mail or files, in order to gather more information about the incident, first get approval from the Vice Chancellor or CIO in accordance with Policy and Rules on Internet and Email Use.

d. Determine what type of security data breach was or might have been affected. Refer to the draft UCT Data Classification Policy.

e. The security incident Severity and Risk Profile will determine the appropriate cause of action to be taken; (see section below – Incident Severity)

1. High severity incidents are the incidents that have a high impact on the University's operations; and require an immediate response and focused, dedicated attention by the CSIRT and other appropriate University officials and IT security staff until remediated.

2. Medium severity incidents have in nature a moderate impact on the university's operations, no critical system is affected by this type of incidents. This type incidents requires a quick response by appropriate personnel (usually from the affected unit) who have primary responsibility for handling the incident. A Post-Incident Report is not required unless requested by the Chief Information Officer or other appropriate administrator.

3. Low severity incidents would require a response as quickly as possible as, no later as the next business day.

f. If there is a need to perform additional forensics sufficient to characterize the incident then the procedural approach outlined below needs to be engaged upon;

The performance of computer forensics, aims for a structured investigative and analysis procedures, at the same time maintain a documented chain of evidence that can indicate what happened on a given computing device at a certain point in time. It provides the indication of who should be given account of the identified activities. The outcome of the forensics investigation should be in a form suitable for presentation in a court of law. The point of departure is to set up / build the systems having in mind the forensic readiness need for probable digital investigations.

1. Analyse net flow data (only if there is network transactions involved in the incident).

2. Forensically, Image the hard drive, memory, and any other relevant media before performing analysis that might alter evidence. For hard drives, bit-by-bit copies are required in case deleted files need to be recovered. This is especially important for cases that involve confidential data, possible criminal investigation, or sensitive personnel actions. Before the imaging can take place, a number of forensic steps need to be taken:

- The entire forensics process must be documented
- If forensics process is invoked as a result of a criminal procedure, then it must be handed to SAPS who may request access to certain artefacts (e.g. proxy logs, net flow logs, email logs, hard drives)
- Chain of custody to be maintained at all times from the moment a hard drive due to be imaged and investigated is obtained. Chain of custody forms to be used
- If hard drives are removed from laptops/desktops, they should be placed in evidence bags which have dates, serial numbers, signatures of individuals signing over the drives and taking ownership of the drives
- Imaging process must include a verification hash to ensure the copy is an exact bit-for-bit copy of the original
- Imaging software and hardware tools must, where applicable, be licensed and relevant serial numbers of software and hardware tools should be added to the documentation being kept
- Imaging, indexing, analysis and reporting should preferably be taking place in a secured location to which access must be controlled
- Findings should be documented (including the query terms used during the analysis phase). Where possible it is preferable to provide the findings in the form of an affidavit

3. Preserve the original media in a secure location and perform analysis on a copy of the data.

4. Take notes on all actions taken.

4.4. Incident Severity

The severity of incident is a subjective measure of its impact on or threat to the operation or integrity of the institution and its information. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response.

The following factors are considered in determining the severity of an incident:

6. Scope of impact – how many people, departments, or systems does it affect?
7. Criticality of the system or service – how important is it to the continuing operation of the institution? What would be the impact on the business, either functional or financial, if this system or service were unavailable or corrupted?
8. Sensitivity of the information stored on or accessed through the system or service as stipulated in the draft Data Classification Policy.
9. Probability of propagation – how likely is it that the malware or negative impact will spread or propagate to other systems, especially to other systems off campus?

4.5. Prioritisation (Security Incident Risk Profile)

It is to be understood that a security incident is to be treated of high level of criticality, as compared to the normal operational incidents. This does not take away the fact that a classification process that is optimally consistent needs to be followed in resolving them. The following considerations needs to be taken into account in order to effectively prioritise a security incident response and handling.

1. *High*
The severity of a security incident will be considered "high" if any of the following conditions exist:

- Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire institution is affected)

- Poses a potential large financial or reputational risk or legal liability to the University.
- Threatens confidential data (for example, the compromise of a server that contains or names with social security numbers or credit card information)
- Adversely impacts an enterprise system or service critical to the operation of a major portion of the university (for example, e-mail, student information system, financial information system, human resources information system, learning management system, Internet service, or a major portion of the campus network)
- Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.
- Has a high probability of propagating to many other systems on campus and/or off campus and causing significant damage or disruption

2. *Medium*
   The severity of a security incident will be considered "medium" if any of the following conditions exist:
   - Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building
   - Adversely impacts a non-critical enterprise system or service
   - Adversely impacts a departmental system or service, such as a departmental file server
   - Disrupts a building or departmental network
   - Has a moderate probability of propagating to other systems on campus and/or off campus and causing moderate damage or disruption
3. *Low*
   Low severity incidents have the following characteristics:
   - Adversely impacts a very small number of systems or individuals
   - Disrupts a very small number of network devices or segments
   - Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate
4. *NA ("Not Applicable")*
   This is used for events reported as a suspected IT security incident but upon investigation, no evidence of a security incident is found. This usually corresponds to the incident category, "No Incident."

5. CSIRT Escalation and Communication Procedure

Based on the incident classification the appropriate communication processes will need to be engaged with. For a High Risk security incident the required ICTS Communications Procedures will be invoked to ensure that the relevant stakeholders at UCT are well informed. In all cases, the ICTS EDICT and TSS Director will be informed of the envisaged action, and their approval is a mandatory requirement before the communication can be sent out.

If the security incident involves parties beyond the control of the University of Cape Town (external entities), the Service provider (TENET) will be notified and might be required to invoke additional escalation and communication procedures with the National CSIRT depending on the nature of incident.

In cases where a security incident is requiring some sort of investigation of criminal nature, the ICTS CSIRT will be required to escalate the case to the Campus Protection Services (CPS) for further investigation.

5.1. External Experts and Resources

The UCT CSIRT will also be collaborating with security experts and will maintain a List of Security Experts that will contain contact information of professional and knowledgeable security experts within the industry that will be able to be called upon to assist with security investigations at UCT.

6. CSIRT Containment, Eradication and Recovery Phase

The primary purpose of this phase is to limit the damage and prevent any further damage from happening; the actual removal and restoration of affected systems and to bring affected systems back into the production environment carefully, as to insure that it will not lead another incident.

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.

6.1. Containment

The first step is Short-term Containment; basically the focus of this step is to limit the damage as soon as possible. Depending of the nature of the incident, containment can be simply 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.

Next step is systems back-up if required; and an appropriately backup of the system/ or snapshot is required to be safely kept.

The third step is Long-term containment, which is essentially the step where the affected systems can be temporarily fixed in order to allow them to continue to be used in Production, while rebuilding the clean systems for a permanent solution

6.1.1. *Goals*

a. Stop the impact of the security incident on the university assets identified in prior investigations.

b. Protect other computers and information on the campus network and Internet (for example, keep the malware from spreading to other computers on or off campus)

c. Prevent further damage to the compromised system and/or information

d. Identify the location and owner of the computer(s) so they can be engaged in containment, eradication, and recovery

61.2. Delayed containment

In some cases, containment may need to be delayed in order to monitor the attacker's activity, usually to collect more evidence. This should be decided on

carefully after considering the risk impact associated with the incident. There will be a requirement for ICTS directorate to consult the Registrar and legal representatives as needed before deciding to delay the containment.

6.1.3. Procedures for Containment

a. Identify the location and/or owner of the system(s) involved in the incident by checking any of the following:

i. Cisco Prime Infrastructure for connected user computers, Mac Address, IP Address and user credentials.

ii. Men and Mice can be used to interrogate the DHCP information to trace the associated IP linked to a MAC Address, reserved IP address, Subnet, Building, switch, etc.

iii. Search for related information within Elastic Search, i.e. IP address, time of event, Mac Address, etc.

b. Isolate the affected computer(s) either by unplugging the network cable (preferred) or shutting down the computer. Unplugging the network cable and leaving it running is best since shutdown can alter or destroy evidence, like with memory-resident malware. For wireless computers, the wireless interface can be disabled while leaving the computer running.

c. Determine if the computer needs to have its network access blocked. If so, this can be accomplished in several ways:

iv. At the switch port, router interface, campus border

v. To block user access on the wireless network.

vi. Disable VPN access.

vii. If the offending device is an unauthorized wireless access point, its connection to universities data network must be blocked or removed. This can be done either via the network switch port to which it is connected, or by physically locating the device and unplugging it.

e. There may be cases when a specific protocol or UDP/TCP port needs to be blocked at the campus border or some other network interface in order to prevent propagation of the malware or to protect the campus from further attacks.

6.2. Eradication and Recovery

In Eradication and Recovery Stage, the affected systems are removed from the normal operations, properly cleaned and restored to the optimal working standard. Before reintroducing the system into operation, a thorough test must be conducted ensuring no further harm can be experienced from the system in question.

6.2.1. **Goals**

a. Preserve evidence if it has not already done

b. Perform additional analysis as needed to complete the investigation

c. Remove the components of the incident impacting the affected systems, such as deleting the malicious code or disabling a compromised user account.

d. Mitigate the attack vector so a similar incident does not occur (for example, patch the vulnerability used to compromise the system, apply standard system hardening procedures, adjust firewall rulesets, etc.)

e. Restore systems to normal operation

6.2.2. **Procedure for Eradication and Recovery**

f. Determine the full scope of the incident – how many systems did it affect and therefore need to be repaired?

g. Determine if any additional analysis is needed:

i. Determine if any of the affected systems still need to have memory, hard drive(s), or other media imaged to preserve evidence; make an image copy of the media, preserve the original and perform analysis on the copy.

ii. Perform additional analysis, which may include:

- Searching for malware by running an anti-virus scan and/or rootkit detection software, or looking for specific files known to be associated with current threats
- Recover deleted files and file fragments
- Perform a vulnerability scan
- Check for unusual running processes and suspicious registry entries, especially ones that run on start-up
- Determine open network ports and processes listening to those ports
- Take a network packet capture and analyze the network traffic
- Analyze network flow data
- Analyse log files for unusual activity
- Search for confidential data that may have been missed in the initial analysis

h. If eradication and recovery keeps the system or service out of operation beyond the length of time that can be tolerated by the institution, invoke business recovery and continuity procedures to restore the service until normal operations can be resumed.

i. The CSIRT will determine when a specific type of compromise requires reformat/reinstall;

   i. Reformatting the hard drive and re-installing from a backup tape prior to the compromise is acceptable, as is restoring from a clean image for those systems that use disk imaging technology.

   ii. Note that reinstalling must occur without exposing the vulnerable system to the campus network and the Internet

j. If infected with malware and a reformat/reinstall is not required, remove the malware from the system. Running an anti-virus scan after updating virus definition/pattern file may suffice. Specific instructions for removing certain types of malware may also be found by searching the Internet.

k. If the incident involves an unauthorized wireless access point, locate the device and contact the person responsible for it to ensure that it ceases operation.

l. Mitigate the attack vector to prevent further instances. This may include:

   i. Patching vulnerabilities in the operating system and all applications software

   ii. Changing passwords

   iii. Placing the system behind a firewall

   iv. Adjusting firewall rules

   v. Updating or installing new security software (for example, anti-virus software or a host-based personal firewall)

   vi. Applying standard system security hardening techniques

   vii. Passing a security assessment

   viii. User training

m. Restore network access if the system was blocked during the containment stage.

n. Return the system to normal operations.

7. Post Incident Review

The Post Incident Review Phase is critical in the security incident life cycle, as it is the opportunity to complete any documentation that was not done during the incident, as well as any additional documentation that may be of good use in future incidents.

During this phase, the CSIRT assess the way the incident was handled, what was done, what should have been done differently, or what should be avoided in the future.

One of the most important parts of incident response process and most often omitted, is learning and improving from previous experience. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned.

Holding a “lessons learned” meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself. Multiple incidents can be covered in a single lessons learned meeting.

This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident.

8.1. Incident Response Review check list

1. Exactly what happened, and at what times?
2. How well did staff and management perform in dealing with the incident?
3. Were the documented procedures followed?
4. Were they adequate?
5. What information was needed sooner?
6. Were any steps or actions taken that might have inhibited the recovery?
7. What would the staff and management do differently the next time a similar incident occurs?
8. How could information sharing with other organizations have been improved?
9. What corrective actions can prevent similar incidents in the future?
10. What precursors or indicators should be watched for in the future to detect similar incidents?
11. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?
12. Have we missed anything?

Acknowledgement

NIST, 2012, “*Computer Incident Handling Guide*”, viewed 1 May 2016, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
http://dx.doi.org/10.6028/NIST.SP.800-61r2

Kansas State University, “IT Security Management” viewed 1 May 2016
http://www.k-state.edu/its/security/procedures/incidentmgt.html#analysis

Related Documents

Policy and Rules on Internet and Email Use
ICTS - Crisis communication procedures
Draft Electronic Communications Policy
Draft UCT Information and Cybersecurity Policy
Draft UCT Information and Data Classification Policy