Security Incident Response Guidelines & Procedures

Department: Information Security
Last Reviewed:
Created: 2/27/2023

OVERVIEW

The Information Security Response Procedures is intended to facilitate the effective implementation of the processes necessary to meet the Security Incident Response Plan as stipulated by COV ITRM Security Standard SEC501 and security best practices.

PURPOSE

The purpose of this procedure is to document the response procedures for potential information technology (IT) security incidents that threaten Christopher Newport University IT systems and services.

ACRONYMS

CL: Communications Lead
IRT: Incident Response Team
IRTL: Incident Response Team Lead
IST: Information Security Team
R: Reporter
SME: Subject Matter Expert

ROLES & RESPONSIBILITIES

This section provides a summary of the roles and responsibilities as described in APPENDIX J of the Security Incident Response Plan.

Name	**Description of Role**
Reporter (R)	End-User or technical staff person reporting the issue. Responsibilities: ● Provides information about the incident including dates, times, symptoms, problem scope, last known good state, and what changed since the last known good state.
Help Desk Technician/ITS Team Member	Members of Information Technology Services (ITS) in both desktop support and other system or infrastructure roles. ● Gather as much information as possible in detail ● Create a Help Desk Ticket and notify ITS Team Member with knowledge of particular issue i.e Subject Matter Expert (SME) ● Participate in After-Action Meetings
Subject Matter Expert (SME)	Responsibilities Provide expertise in subject area, systems, database operations, security etc. ● Investigate and document issue ● Act as Subject Matter Expert (SME) (will vary depending on system or issue) ● Recommend solutions ● Participate in After-Action Meetings and recommend changes
Incident Response Team Lead (IRTL)	The individual responsible for the overall management of the response. (This individual will vary based on the Incident) Responsibilities:

	• Confirm the occurrence of an Incident requiring the execution of this protocol
	• Ensure the Incident Response Log is created/updated. See APPENDIX Q
	• Manage and direct the appropriate response to an Incident
	  ○ Assess the situation
	  ○ Establish immediate priorities
	  ○ Identify and activate the necessary personnel
	• Participate in After-Action Meetings

Incident Response Team (IRT)	The IRT consists of: • The Information Security Officer (ISO) or designee • Information Technology Services staff and/or other SMEs as identified Responsibilities: • Contain the breach so it doesn't spread or cause further damage • Disconnect devices as necessary • Update event Log with actions taken by whom and when • Preserve evidence • Participate in After-Action Meetings Questions to address: • What's been done to contain the breach short term? • What's been done to contain the breach long term? • Has any discovered malware been quarantined from the rest of the environment? • What sort of backups are in place?
Communications Lead (CL)	• Act as the primary communications coordinator for Incident Response (IR) • Notify leadership on status updates according to the Communication Matrix in Appendix P • Participate in After-Action Meetings
Information Security Team (IST)	Responsibilities • Coordinate all aspects of the Incident Handling process • Determine whether or not to activate the Incident Response Plan • Verify forensic evidence has been securely stored and documented • Conduct an After-Action meeting with all Incident Response Team Members and Information Technology Services Team • Discuss and document lessons learned from the Incident • Draft and distribute an After-Action Report with assigned action items Questions to address

	• What went well, what went wrong? • What changes need to be made to the security? • How should employees be trained differently? • What weakness did the breach exploit? • How will you ensure a similar breach doesn't happen again?

PROCEDURES

Overview

There are seven (7) phases to the Incident Response Procedures. These procedures are the recommended steps and best practices that should be followed when investigating a suspected incident or data breach.

- **Preparation**—review and document an organizational security policy, perform a risk assessment, identify sensitive assets, define an Incident Response Plan.
- **Identification**—monitor IT systems and detect deviations from normal operations, and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything. The reporting phase is also included in this step.
- **Containment**—perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.
- **Eradication**—remove the issue(s) from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.
- **Recovery**—bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.
- **Lessons learned**—Perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.

FIGURE 1: Incident Response Procedures Summary

CHRISTOPHER NEWPORT UNIVERSITY

1. **Step 1: Reporting**

Role	Step	Action
Reporter (R)	1	Suspected incidents are reported to the Help Desk or member of ITS Team.
Help Desk Technician/ITS Team Member	2	Identify the request and gather as much detail as possible: - incident including dates, times, symptoms, problem scope, last known good state, and what changed since the last known good state. - Document the Who, What, Where, When, How and Why
Help Desk Technician/ ITS Team Member	3	Log the suspected incident with a Help Desk Ticket Request (if not yet logged) and route to the Information Security Team members in Help Spot.

2. **Step 2: Identification**

   This step involves detecting deviations from normal operations in the organization, understanding if a deviation represents a security incident, and determining how important the incident is.

Identification procedures include:

- **Ensuring monitoring** for all sensitive IT systems and infrastructure.
- **Analyzing events** from multiple sources including log files, error messages, and alerts from security tools.
- **Identifying an incident** by correlating data from multiple sources, and reporting it as soon as possible.
- **Notifying IRT members** and establishing communication protocols
- **Assigning roles**, one as the IRT Lead who assesses the incident and makes the decision, and the others to help investigate and gather evidence.
- **Documenting everything** that incident responders are doing as part of the attack—answering the Who, What, Where, Why, and How questions.

Role	Step	Action
Information Security Team (IST)	4	When notified by the Help Desk Ticket system, the Information Security Team (IST) will perform a preliminary analysis of the facts and assess the situation to determine the nature and scope of the suspected incident.

		- *If it is not confirmed as an incident, the information will be passed on to appropriate parties for resolution and communicated to IT Services.* - *If a confirmed incident, the appropriate parties will be contacted as stipulated in the Security Incident Response Plan* ***NOTE* Not all suspected incidents will end in incident response**
Information Security Team (IST)	4a	If a confirmed incident, Information Security (IST) or designee will notify IRT team members and establish communications channels within IT Services.
Information Security Team (IST)/Incident Response Team (IRT)	5	If a confirmed incident occurs, the IST and IRT will activate the Incident Response Protocol and begin to coordinate response activities according to the Incident Response Plan and Procedures.
Incident Response Team (IRT)	5a	The Incident Response Team (IRT) will assign an Incident Response Team Lead (IRTL)
Subject Matter Expert (SME)/Incident Response Team Lead (IRTL)	6	The IRTL assigns a Communications Lead.
Subject Matter Expert (SME)/Incident Response Team Lead (IRTL)	7	Create an ITS Incident Response Log under Issues and Outages Shared folder with the 20yy.mm.dd_Incident Log Template-Printout naming convention. - Refer to the "Incident Response Template" in APPENDIX R
Information Security Team (IST)/Incident Response Team Lead (IRTL)	8	Classify the Incident Based on the Incident Classification Level (See Figure A. below)
Communications Lead (CL)	10	Activate the Incident Communication Protocol. Utilize Standard Communication Messaging Components and notify leadership identified in APPENDIX Q .

FIGURE 2: Incident Categories and Severity

Category	Definition
CAT 0:	Used during cyber security exercises and approved activity testing of the internal/external network defenses or response capabilities.
CAT 1:	Used if an individual gains logical or physical access without permission to a BCG network, system, application, data, or other resource.
CAT 2:	Used if an attack successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources (i.e. DDoS).
CAT 3:	Used if an attacker successfully deploys malicious software that infects a BCG operating system or application.
CAT 4:	Used if an attacker/individual violates acceptable computing use policies.
CAT 5:	Includes any activity that seeks to access or identify a BCG computer, port(s), protocol(s), service, or any combination for later exploit.
CAT 6:	Includes unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Severity	Description
S1	• Potential for widespread impact. • Potential that sensitive data will be disclosed or stolen (privacy and/or proprietary). • Potential that client and/or data subjects and/or public notifications will be required. • Recovery from the incident is unpredictable and/or not possible.
S2	• Potential for widespread impact. • Potential that sensitive data will be disclosed or stolen (privacy and/or proprietary). • Unlikely that client and/or data subjects and/or public notifications will be required. • Will require additional resources to recover from the incident.
S3	• Likely to be limited to few affected systems. • Unlikely to lead to loss or theft of sensitive data. • Unlikely that client and/or data subjects and/or public notifications will be required. • Will require additional resources to recover from the incident.
S4	• Likely to be limited to few affected systems. • Unlikely to lead to loss or theft of sensitive data. • No impact to brand. • No additional resources needed for recovery.

3. Step 3: Containment

The goal of containment is to limit damage from the current security incident and prevent any further damage. Several steps are necessary to completely mitigate the incident, while also preventing destruction of evidence that may be needed for prosecution.

Containment process involves:

- **Short-term containment**—limiting damage before the incident gets worse, usually by isolating network segments, taking down hacked production servers and routing to failover.
- **System backup**—taking a forensic image of the affected, and only then wipe and reimage the systems. This will preserve evidence from the attack that can be used in court, and also for further investigation of the incident and lessons learned.
- **Long-term containmen**t—applying temporary fixes to make it possible to bring production systems back up. The primary focus is removing accounts or backdoors left by attackers on the systems, and addressing the root cause—for example, fixing a broken authentication mechanism or patching a vulnerability that led to the attack.

Role	Step	Action
Subject Matter Expert (SME) Incident Response Team (IRT)	11	Members of the IRT and SME(s) will take appropriate immediate actions to contain and control the incident. This may require removal of the infected machines or entire network segments from the larger university network. It may also require blocking university networks from access to the internet or other system resources. IRT members should also develop a plan of action for recovery of systems harmed in an incident. (Refer to APPENDIX L Incident Response Phases for more detail)
Subject Matter Expert (SME)/ Incident Response Team (IRT)/Information Security Team (IST)	12	Ensure that the forensic evidence has been secured and preserved for after the fact investigations (Refer to APPENDIX L Incident Response Phases for more detail) A member of the Information Security Team will verify that the evidence is collected and securely stored on the media identified in APPENDIX L
Subject Matter Expert (SME) Incident Response Team (IRT)	13	Ensure that the backups are valid and can be successfully restored (Refer to APPENDIX L Incident Response Phases for more detail)

Subject Matter Expert (SME) Incident Response Team (IRT)	14	Update actions in the Incident Tracking Log
Communications Lead (CL)	15	Notify leadership according to the Communications Matrix when the Incident has been contained and next steps in APPENDIX Q

4. Step 4: Eradication

Eradication is intended to actually remove the threat or other artifacts introduced or affected by the attacks, and fully restore all infected systems.

Eradication procedures involve:

- **Reimaging**—complete wipe and re-image of affected system hard drives to ensure any malicious content is removed.
- **Preventing the root cause**—understanding what caused the incident prevents future compromise, for example by patching a vulnerability exploited by the attacker.
- **Applying basic security best practices**—for example, upgrading old software versions and disabling unused services.
- **Scan for malware**—use anti-malware software, or vulnerability scan, to scan affected systems and ensure all malicious content is removed.

Role	Step	Action
Incident Response Team (IRT)/Incident Response Team Lead (IRTL)	16	Eradicate the threat (Refer to APPENDIX L Incident Response Phases for more detail)
Incident Response Team (IRT)/Incident Response Team Lead (IRTL)	17	Verify the forensic evidence has been preserved and stored in secure separate location (Refer to APPENDIX L Incident Response Phases for more detail)
Incident Response Team (IRT)/Incident Response Team Lead (IRTL)	18	Update Incident event log with actions taken
Communications Lead (CL)	19	Notify leadership according to the Communications Matrix when the Incident has been contained and next steps APPENDIX Q

5. Step 5: Recovery

The goal of recovery is to bring all systems back to full operation, after verifying they are clean and the threat is removed.

Recovery procedures involve:

- **Defining time and date to restore operations**—system owners should make the final decision on when to restore services, based on information from the IRT.
- **Test and verifying**—ensuring systems are clean and fully functional as they go live.
- **Monitoring**—ongoing monitoring for some time after the incident to observe operations and check for abnormal behaviors.
- **Do everything to prevent another incident**—considering what can be done on the restored systems to protect them from recurrence of the same incident.

Role	Step	Action
Incident Response Team (IRT)/Subject Matter Expert (SME)	20	Verify forensic evidence has been preserved in separate location
Incident Response Team (IRT)/Subject Matter Expert (SME)	21	Verify that backup data if needed is accessible and can successfully be restored
Incident Response Team (IRT)/Subject Matter Expert (SME)	22	Restore system(s) to pre-Incident state (Refer to APPENDIX L Incident Response Phases for more detail)
Incident Response Team (IRT)/Subject Matter Expert (SME)	23	Update and patch system(s) to most recent up to date security patch versions
Incident Response Team (IRT)/Subject Matter Expert (SME)	24	Update Incident Log with actions and updates
Communications Lead (CL)	25	Notify leadership according to the Communications Matrix when the system(s) restoration is complete and next steps APPENDIX Q
Information Security Team (IST)	26	Verify forensic evidence has been preserved and stored in a secure location.
Information Security Team (IST)	27	Run a post-Incident vulnerability scan on system(s) and save results in a secure location.

6. Step 6: Lessons Learned

No later than two weeks from the end of the incident, the CSIRT should compile all relevant information about the incident and extract lessons that can help with future incident response activity.

The lessons learned process includes:

- **Completing documentation**—it is never possible to document all aspects of an incident while it is going on, and achieving comprehensive documentation is very important to identify lessons for next time.
- **Publishing an After-Action report**—the report should provide a play-by-play review of the entire incident, and answer the Who, What, Where, Why, and How questions.
- **Identify ways to improve IRT performance**—extract items from the incident report that were not handled correctly and can be improved for next time.
- **Lessons learned meeting**—conduct a meeting with the IRT team and other stakeholders to discuss the incident and cement lessons learned that can be implemented immediately.

REFERENCES

- VITA ITRM Information Security Standard (SEC501)
- Security Incident Response Plan
- Incident Response Log Template

APPENDIX A - INCIDENT REPORTING GUIDELINES