Cybersecurity Incident Response Plan

A cybersecurity incident can put the organization, employees, systems, data, and CCDDR's ability to function at risk. It is impossible to develop a response plan for all types of cyberthreats, but the National Cyber Security Centre (NCSC) recommends developing responses to the most common attack vectors:

- External/Removable Media: An attack executed from removable media or a device, such as a USB stick
- Attrition: An attack that attempts to compromise, degrade, or destroy systems or services
- Web: An attack executed from a website or a web-based application
- Email: An attack executed through an email message or attachment (a.k.a. Phishing)
- Impersonation: An attack that replaces something benign with something malicious
- Improper Usage: Any incident resulting from a violation of an organization's acceptable usage policies
- Loss or Theft of Equipment: The loss or theft of a computing device or media used by the organization

The most important response to a cybersecurity incident is to be proactive, utilizing protective software, staff training, and safe data storage practices. Utilizing the cloud for data storage is safer than maintaining a physical server.

The NCSC defines a cyber incident as a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorized access or attempted access to a system or systems that may result in an actual or potential adverse effect.

Goals for Cyber Incident Response

When a cybersecurity incident occurs, timely and thorough action to manage the impact of the incident is critical to an effective response process. The response should limit the potential for damage by ensuring that actions are well known and coordinated. Specifically, the response goals are:

- Preserve and protect the confidentiality of the client and/or employee information and ensure the integrity and availability of CCDDR systems, networks, and related data
- Help CCDDR personnel recover their business processes after a computer or network security incident or other type of data breach
- Provide a consistent response strategy to system and network threats that put CCDDR data and systems at risk
- Develop and activate a communications plan including initial reporting of the incident as well as ongoing communications, as necessary
- Address cyber related legal issues
- Coordinate efforts with external Computer Incident Response Teams and law enforcement
- Minimize CCDDR's reputational risk

Purpose and Scope

This plan provides practical guidelines on responding to cybersecurity and data breach incidents in a consistent and effective manner. While this plan is primarily oriented around cyber-related incidents and breaches, it can also be utilized for data breaches that are not related to computer systems.

Detection

Detection of a cyber threat may be automated by an anti-malware program or may be noticed by an astute employee. The protective software and/or the firewall may send alerts, sever the internet connection, or shut down the computer.

The way an incident becomes known will have an impact on the response process and its urgency. Examples by which CCDDR becomes aware of an incident include, but are not limited to the following:

- CCDDR discovers through its internal monitoring that a cyber incident or data breach has occurred
- CCDDR is notified by one of its technology providers of an incident or becomes aware of the same
- CCDDR is made aware of a breach through a constituent or a third-party informant
- CCDDR and the public are made aware of the incident through the news media

Incident Response Team (IRT)

A team comprised of administrative staff, information technology (IT) personnel, and/or IT service providers shall be responsible for coordinating incident responses and be referred to as the Incident Response Team (IRT).

IRT members may take on additional roles during an incident, as needed. Contact information, including a primary and secondary email address, plus office and mobile telephone numbers shall be maintained and circulated to the team. The IRT will draw upon additional staff, consultants, or other resources, as needed, for the analysis, remediation, and recovery processes of an incident. The IT function plays a significant role in the technical details of incident detection and response.

Response

Any employee who suspects a dangerous file or program has been opened/initiated should:

- Immediately disconnect from the internet/network and shut down their computer/device
- Immediately contact the Executive Director and Compliance Manger
- Prepare a written description of the incident stating what happened

The Executive Director and/or Compliance Manager will:

- Disconnect the network from the internet
- Contact the IRT

The IRT will ascertain if any malware (virus, ransomware, phishing, etc.) has been downloaded on a CCDDR device. Data integrity will be evaluated immediately and at regular intervals until the threat has been isolated and resolved.

Incident Response Life Cycle Process

Cyber incident response management is an on-going process with a cyclical pattern. The specific incident response process elements that comprise the Cyber Incident Response Plan include:

1. **Preparation:** This is the on-going process of maintaining and improving incident response capabilities and preventing incidents by ensuring that systems, networks, applications, and data handling processes are sufficiently secure, and employee awareness training is in place.
2. **Identification:** This is the process of confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents.
3. **Notification:** This is alerting IRT members to the occurrence of an incident and communicating throughout the incident.
4. **Containment:** This is minimizing financial and/or reputational loss, theft of information, or service disruption. Initial communication with constituents and news media, as required.
5. **Eradication:** This is eliminating the threat.
6. **Recovery:** Restoring computing services to a normal state of operation and the resumption of business activities quickly and securely. Provide reputational repair measures and news media updates, if needed. Provide credit monitoring services to affected clients, or other remediation measures, as appropriate.
7. **Post-incident Activities:** This is assessing the overall response effectiveness and identifying opportunities for improvement through ‘lessons learned’. Incorporation of incident’s learnings into cyber fortification efforts and the response plan, as appropriate.

Process Phase & Approximate Timing	Process Detail Steps	Involved Parties
Identification (Hours)	1. Identify and confirm that the suspected or reported incident has happened and whether malicious activity is still underway. 2. Determine the type, impact, and severity of the incident. 3. Take basic and prudent containment steps.	IT and any monitoring service provider
Notification (Hours – 1 Day)	4. Inform or activate the IRT, based on the severity of the incident, as outlined in Appendix D, and provide the type, impact, and details of the incident to the extent that they are known. 5. Determine the need for Subject Matter Experts (SME) to be involved in the Containment, Eradication, and Recovery processes.	IT & IRT
Containment (Hours-2 Days)	6. Take immediate steps to curtail any on-going malicious activity or prevent repetition of past malicious activity. 7. Re-direct public facing websites, if needed. Provide initial public relations and legal responses as required.	IT & IRT
Eradication (Days -Weeks)	8. Provide full technical resolution of threat and related malicious activity. 9. Address public relations, notification, and legal issues.	IT & IRT
Recovery (Weeks -Months)	10. Recover any business process disruptions and re-gain normal operations. 11. Address longer term public relations or legal issues, if required, and apply any constituent remedies.	IRT
Post-incident (Months)	12. Formalize documentation of incident and summarize learnings. 13. Apply learnings to future preparedness.	IRT

Communication Methods

Company communication resources (email, phone system, etc.) may be compromised during a severe incident. Primary and alternate methods of communication using external infrastructure will be established and noted on the IRT member contact list to provide specific methods of communication during an incident. The IRT and any other individuals involved in an incident resolution will be directed as to which communication method will be used during the incident.

Information Recording

Information recording is very important during an incident, not only for effective containment and eradication efforts, but also for post-incident lessons learned, as well as any legal action that may ensue against the perpetrators. Each member of the IRT shall be responsible for recording information and chronological references about their actions and findings during an incident.

Summary

No perfect script can be written for the detailed activity encountered and decisions that will need to be made during an incident, as each incident will have its own uniqueness. This plan shall serve as a framework for managing cybersecurity and data breach incidents, allowing the details of confirmation, containment, eradication, and communication to be tailored to fit the specific situation.

Created: March 12th, 2024