Abstract

This document is meant to help company employees in creating and maintaining incident response capabilities within the area of cyber security. The correct and efficient handling of incidents is pertinent to the security, safety, and privacy of company employees and customers. This document is to be used as a guide on how these incidents should be handled from start to finish, and contains important references and information when it comes to the different phases of an incident, along with guides surrounding before and after considerations and processes.

Table of Contents

Introduction

Authority

The security of company information is done by the current Chief Information Security Officer (CISO) who works in tandem with the other relevant members of the C-Suite. The CISO

ensures that all standards within their domain is upheld, along with regulations met, and compliance kept. The Information Technology (I.T.) Security Office is also granted to operate at a limited capacity concerning these items without approval of the CISO until an event that the integrity, confidentiality, and/or availability of company information or infrastructure is threatened, in which they may operate with full authority [1].

The I.T. department is responsible for maintaining an up-to-date incident response document that contains the proper procedures and information necessary, creating and training a computer incident response team that are able to fully perform the procedures described in the document, and manage a system that allows for reports to be submitted concerning I.T. security issues/exposures of company data or other potential cyber incidents [1].

The I.T. Security Office is in charge of managing and coordinating with other departments if necessary regarding different phases of the incident response process, and they directly coordinate with the I.T. department itself. The I.T. Security Officer is also able to determine at their own discretion if the risks being faced by the company are threats, and if so, they are able to activate the computer incident response team [1].

Purpose

This document is meant to outline and describe the standards and actions required for correct incident management by the I.T. Security Office [3]. This document also outlines proper response procedures in the case of a large-scale or major incident. Along with those items, the process and document are meant to continually change as practices, rules, regulations, and laws do.

Scope

The plans and procedures outlined here are to be the general guidelines for the company's response to an incident. Ensuring that standards and regulations are complied with in this process, this document is built with respect to the following ones:

- PCI Data Security Standards
- GDPR

An incident can mean many things. For examples, security breaches of computer systems, electronic items smuggled out by employees, contractors accessing systems that shouldn't have

access to, are all categorized as incidents. The response to these incidents includes but is not limited to the activities of detection, analysis, containment, and eradication [3].

This document's scope does not cover non-computerized security incidents, like paper documents. If this type of coverage is necessary, a separate incident response plan should be created specifically for the concerned items [3].

Utilization of this document is not meant to replace a Continuity or Disaster Recovery Plan, nor is it supposed to be an in-depth list that covers every detail or process in the incident response and handling process. It is meant to be used as a guiding framework in order to push efficiency, practice, strong communication across departments, maintain consistency throughout an incident, and ensure that the company and its employees have a way to prepare for incidents, handle them, and then reflect on them afterwards to improve the company's capabilities for handling them [1].

This document covers all company computer assets and infrastructure, along with all of the locations that the company maintains [1].

Audience

The audience that this document was primarily intended for is the I.T. Security Office, the I.T. Department, and the CISO. The other audiences that this document is applicable to is also the CIO, project managers, network administrators, and developers at the company [1].

Terms & Definitions

- Asset: Anything that has value to the company
- Control: A way to manage risk. This can be something like policies, procedures, guidelines, and more. These can then also be technical, administrative, legal, etc.
- Incident: A singular or series of information security events that are not wanted, or not expected. These events can cause harm, or they may also pose a large threat to information assets. They may need to be addressed through a form of preventative or corrective actions.
- Incident Response Plan: A document that acts as a type of framework or guide on how to handle an incident.

- Incident Response Procedures: A series of steps recorded on documents that are taken when handling an incident.
- Information: Any knowledge that can be communicated or documented, whether it is in a physical form or has physical characteristics. This means that verbal, paper, and electronic communication are all included.
- Information Security: The security of information, where confidentiality, integrity, and availability of information are the highest priorities to preserve and protect, and other things such as authenticity, accountability, reliability, and non-repudiation are important as well.
- Threat: This can potentially be the cause of an incident that is not wanted, and could potentially end up harming a system, company, etc.
- Data Steward: The specific department managers or the delegates that they have within the company who are responsible for the acquisition, development, and maintenance of databases which house company information.
- CIO: Chief Information Officer
- CIRT: Computer Incident Response Team
- CISO: Chief Information Security Officer
- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System
- IRM: Incident Response Manager
- ISO: Information Security Officer
- IT: Information Technology
- ITSO: IT Security Office or IT Security Officer
- NI&S: Network Infrastructure and Services
- PCI-DSS: Payment Card Industry Data Security Standard
- PII: Personally Identifiable Information
- PIRN: Personal Information requiring notification
- URL: Universal Resource Locator
- US-CERT: United States Computer Emergency Readiness Team

[1, 2, 3]

Incident Response Capabilities & Overview

Mission

The mission of the company's I.T. department is to provide our customers secure usage and access to well-maintained systems while accomplishing the overall goal of the company while every part of the CIA triad is upheld [1].

To accomplish these goals and uphold the mission of the company a Cyber Incident Response Team (CIRT) was created, which allows the company's I.T. infrastructure to be better protected, ensures the CIA triad is upheld in every part of I.T., collect necessary information, and generate proper documentation and investigations into incidents [1].

Goals

Being able to respond to an incident and the impacts it has on the company is essential, which means the response needs to be thorough and efficient [1]. The overall goal of this response is to mitigate the damage from the incident through means of proper decision making and actions that have been pre-reviewed and approved in the event of certain incidents.

Overall, the employees and customers at the company need to be protected, along with the data that is being held here. After an incident, the company needs to have that department back up and running with minimal downtime. The responding team to these incidents also needs to be consistent, which means that a proper framework of documentation, checklists, information, and more needs to be in place for them to utilize.

Communication is also an important goal, as it enables responders to have a more efficient channels, and to have more control over the knowledge surrounding a situation. If a third-party is impacted, there needs to be proper procedures in place to contact and communicate with them.

Strategy

In order to make sure the outlined goals are reached by the company and its employees, different incident response frameworks from approved authorities have been consulted in the creation of the company's incident response plan. This includes but is not limited to: NIST Special Publication 800-61 [1].

Outlined in later pages are the specific details surrounding the different phases of the incident response process. This includes preparation, identification, detection, analysis, containment, eradication, incident closure, and review. Other areas that are also covered later are those surrounding certain workflows, communication information, and more.

Company Authority

Certain members of the company are allowed to make decisions and requests when it comes to the incident response process at the company. Here is a list of them:

- CIO
- CTO
- CEO
- ITSO
- Legal Counsel
- I.T. Department Head
- Data Stewards

[1]

If some form of law enforcement makes contact with a member of the company, this does not mean that they have the right to any information of the company's at that point in time. Any request like this needs to be forwarded to the company's legal counsel. These can be requests like a warrant and subpoena [1].

Teams Involved

The teams involved in the incident response process are made up of I.T. Department and ITSO employees [1]. Additional members may join from general legal counsel. Along with these members, there may be employees from the Network Administration and Development Management teams joining at different times. The Public Relations department will be involved throughout the whole process to ensure that proper transparency is maintained, while at the same time not oversharing.

Approach Overview

When an incident occurs it needs to be reported as soon as it is noticed. There are multiple ways to report these incidents, but the first thing to do is ensure that any communication occurring about the incident is done through communication channels that are not affected by the current incident [1]. This is just to cover all of the bases, as the scope of the incident is unknown. From there a ticket or call to the I.T. Help Desk is the first step, and if a ticket is submitted, ensure the proper priority is marked on it ("Emergency" priority).

From there the I.T. Department will report to the ITSO right away, and the ITSO will have a member who is marked to be the IRM, who will then take control of the proceedings surrounding the incident [1]. The ITSO will then work with the I.T. Department and the reporting department to ensure all employees involved are aware of their roles in the incident response and to activate the beginning phases. Proper coordination throughout the company is essential here, which is why the ITSO designated IRM will be overseeing the process [1].

A few examples of incidents can be seen below:

- Ransomware
- Malware
- Stolen data
- Intrusion or damage to any company system

[1]

Education & Awareness

The company needs to make sure that incident response is properly addressed across the organization in programs that are meant to make employees more educated and aware about the potential threats and incidents, and the proper steps to take when an incident is potentially encountered [2].

From here training programs should be setup that are department and job specific. This enable each employee to receive the proper training, and to know what role they have when it comes to responding to an incident. Training programs need to be decided up, the elements contained within them, and the schedule that they will be arranged in. Each training program needs to be a apart of a cycle; like being annually for example [2].

Incident Response Process

The incident response process has different phrases that it moves through. It starts with preparation and then goes to identification, detection, and analysis. From there it moves to containment, then to eradication. For the final moves it jumps to recovery and then incident closure and review [1]. Specific steps needs to be taken in each of these phases to ensure that the incident is handled correctly, which is why there will be supplementary forms and checklists provided alongside this section [1].

Preparation

This is the first phase of the incident response process, and while each phase is extremely important, this is a foundational phase that could determine the outcome of the rest of the process [1]. There are many different things that can be done preemptively to prepare for an incident. From risk assessments to infrastructure audits, to external penetration tests and more. Putting the company's security to the test is extremely important, as everything that can be done and is recommended to do to prepare for an incident should be done.

For the company, the following list shows what preparation is done for these incidents:

- User Education and Awareness Programs
- Incident Response Practices
- Annual IT Risk Assessments
- Internal and External Network and Vulnerability Audits
- Penetration Tests

Identification & Detection

Near the beginning of the incident response process the entirety of the incident needs to be identified/detected, and analyzed. This helps to create a gameplan for the containment and eradication phases [1]. Identifying/detecting the incident can be anything from an IDS alert to a user reaching out to report suspicious activity, and from there it will be fully investigated and analyzed to determine what needs to be done. This is where the incident's scope, impact, and necessary response come into play. The overall goal of this phase is to find where the incident came from/occurred, and then to preserve the evidence of it [1].

The general outline of the steps for identifying an incident are to first check the audit guidelines for department personnel actions regarding things like unacceptable computer use, cyber security incidents, and more [1]. From there it can be decided if an incident has occurred or not.

Analysis

Every incident that occurs needs to be analyzed fully and correctly validated. As discussed in the last section, determining the scope of the incident, where it originated from, and how it is occurring is all very important. This analysis that is performed at the beginning will allow the team responding to the incident to prioritize the actions that come in the later sections. Once an incident has been fully identified, the ITSO will assign an employee to be the IRM. This employee will then be responsible for leading the response to the incident, becoming point of contact for the incident, and is in charge of managing things like investigation documentation, evidence gathering, and data documentation [1].

Containment & Eradication

The containment phase involves attempting to limit the "scope and magnitude of the attack" [1]. When in the containment phase evidence needs to be:

- Acquired
- Preserved
- Secured
- Documented

Data needs to be properly protected and kept from leaving the network over the machines that were affected in the incident. Along with that, whatever is causing the incident needs to be halted in its progress, so that the overall damage to assets and data can be stopped [1]. Specific information will be sought after if it is an attacker, such as exploit used, port, malware type, and more. After this information has been found, the ITSO will then order a firewall block or physical ethernet disconnect to be performed. This will cut the affected asset off from the network and internet. Even if this causes disruption it has to be done, as containment is a much higher priority than day-to-day business traffic [1].

In this phase all activities need to be properly coordinated with the local system administrator. Some activities that may occur are things like: Not allowing the system to be altered, making a forensic copy of the system, securing the physical site that the system is located at, and more. The next two steps are huge: Determining the risk of allowing operation to continue and backing up the system.

An attack could be mitigated or fully stopped by a simple action such as disabling a port. It has to be determined if it is worth it to allow the system involved to stay operational though. If the system is fully compromised, allowing it to remain online could potentially threaten the rest of the network. Other options might include things like changing the credentials for all of the users and systems on the affected machine [1]. Backing up the system could be a good option as well. A forensic image of the computer will allow the company's forensic team to analyze the affected machine more thoroughly, and it can be handed over to law enforcement if needed. The ITSO needs to be contacted if the forensic process needs to be initiated [1]. The systems being used to backup the affected system can also show what files were changed during the event by comparing their disk images.

Fully eradicating the issue is the next step. As stated before it can be many different things, not just the presence of malware on the computer. It can be unallowed access, malicious code, data that is against policy, and more [1]. During this stage it is also important to fix the issues that led to the incident occurring in the first place. This could be things like patching vulnerabilities, updating a system, and altering server code. When it comes to full-scale malware incidents, it is almost always best to just re-image the machine [1].

This phase has a series of steps that can be applied to any situation and modified as needed. Determining the benchmark for an eradication is one, which is where it needs to be defined what counts as fully eradicated for different types of incidents. The eradication of unallowed access is different to the eradication of ransomware. The next step is to find and mitigate the vulnerabilities present that were utilized [1]. From there, the unallowed permissions, malware, company data, and more can be removed. During this time, more systems might be found that were affected by the incident, so previous phases like detection and analysis might have to be repeated in order to find all of the impacted systems so that the incident can be fully taken care of [1].

Recovery

After the containment and eradication phases are finished is when the recovery phase begins. The main goals of this phase are to get the business fully-functional again, and to restore all previous operations, especially the ones that were impacted by the incident [1]. The general steps of this stage start by ensuring all sensitive data has been copied off of the system, then the operating system needs to be reinstalled and patched, along with the required applications for that employee.

Once this is done, if there are data backups of the system, one that has been evaluated to be free from the impact of the incident can be used and data can then be restored fully. At this point, the system then needs to be made ready for normal operations, and that it is functioning correctly. The ITSO can determine at this point if further monitoring is needed for the impacted system to keep an eye out for suspicious "Post-Incident Activity" [1].

Incident Closure & Review

Closure and review are extremely important phases because if done correctly, they will help make the organization much more secure in the future to the kind of incident that was handled. The incident response process up to this point should have been **fully documented**, which allows the company to improve on its incident response process, documentation, security controls, and more. Some incidents are different than others though, and require different depths of documentation, the ITSO will be able to provide further information on this if one occurs [1].

Follow-Up Report

The goal of a follow-up report is to properly document the incident, review the lessons that were learned throughout it, and how to utilize that new knowledge now and in the future [1]. A follow-up report can add a lot of great information to an ever-expanding knowledgebase that is maintained by the company, and lets the entire team fully learn from the experience. The default follow-up report for the company is known as an "**Incident Response Checklist**", and it can be found in **Appendix A**. It should also be used actively throughout the incident, but a "final copy" version can be utilized as a follow-up report.

This report will then be shared with the CTO and/or CIO, along with other people that could be potentially necessary to be there. Afterwards, a meeting will be held to go over the

lessons learned so that everyone that was involved with the incident and its handling/response so that they can learn, grow, and improve.

Communications

Communication is a vital part of the incident response process. Which is why is it important to know what role an employee has, who they communicate to, who they are managed by or are in charge of, and then to have access to ways to reach these other individuals in the case of an incident [2]. Due to the sensitive nature of the communications during an incident, all communications need to remain on secure channels.

The information channels during an incident need to be utilized fully and correctly, or else problems could occur. Certain employees may not need to know certain information regarding an incident, which is why it is important that this is laid out specifically for what department personnel are allowed to communicate certain types of information. Generally following the "need to know" rule is a good guideline [2]. Having a list of contacts is helpful as well as it allows the different departments to get in contact with each other, the upper management, customers, clients, and more if needed.

Throughout this process, transparency should be key unless stated otherwise. Most employees will not be in charge of speaking to the public, as this will be left to authorized employees listed within here, and what communication channels they are allowed to speak over [1]. Stakeholders will be identified as well in order to provide accurate information to them when necessary. Communication to the outside should be scheduled at intervals to keep our customers and others updated.

A communications plan will fully be developed tailored to the individual incident by the public relations team, the I.T. team, and the necessary stakeholders [1]. This is especially true if there has been a breach of PII. From there a communication flowchart can be developed. As a part of this communications flowchart, it should include things like the protocols for getting approval for a message, the internal and external communication channels available, communication scheduling and frequency, and notification procedures for third party organizations that were involved in the incident [1].

Authorized External Communicators		
Name	Communication Channel	Phone Number

Stakeholders	
Name	Phone Number

Communications Flow

An incident will normally start off with a call to the help desk. A normal hours call will come through to the employees in that department as a call, but an after-hours call will come through as an email. The steps to be taken by the **first-level service desk employee** who ends up fielding the initial incident will be to call the staff in order that are listed on the table below. The first cycle through the table, call all of the staff in order but **do not leave a voicemail on the first call if there is no answer** [3]. For the second cycle, call all of the staff in order again but make sure to leave a voicemail if there is no answer.

Name	Phone Number

If there are no answers from both cycles of the above list, one of the I.T. Managers or Security Officers needs to be contacted. Refer to the table below to do that.

Name	Position	Home	Mobile

If contact is not able to be made with individuals on the above table, please leave a voicemail for each manager and director. After leaving this voicemail, continue attempting to

reach I.T. staff from the first call list until an employee is able to be reached. Just leaving a message in this situation is **not acceptable** [3].

Once contact has successfully been made with a I.T. staff or a manager, let them know the details of the incident and inform them that they are now responsible for being apart of the effort to resolve this incident, and that they need to notify the other employees required in order to solve this issue [3].

Notifying External Organizations

If an external organizations data is involved in an incident, or investigations involving an incident show evidence that an external organization may either be affected or involved in some way, it becomes necessary to contact them. For contacting them, the technical and/or administrative contacts of the system need to be identified, along with the WHOIS contact information for the provider if there is one [1]. Next, see if there is a US-CERT or "abuse" email address if the system is in another country [1]. From there, it's best to send an email to the WHOIS contact and include information like the site's US-CERT, CC the ITSO and the affected department(s) head personnel, and then log the observed data in the text of the email [1]. No attachments or HTML should be sent.

Record of Changes

Version #	Date Revised	Author	Revision Description
1.0	2/28/2022	Evan Read	Created the document.
1.1	2/28/2022	Evan Read	Updated the table of contents and created section headers according to the outline.

Review Cycle

This document needs to be kept up to the ever-changing standards required to keep systems secure, so review of the document should be done every 6 months, and the resulting edits need to be fully audited and implemented within two months after the initial review. The ITSO will coordinate with other relevant offices and department leads to ensure that proper training and notes are distributed if necessary based on the changes as they occur.

Appendix A: Incident Response Checklist

Incident Response Checklist								
Incident Origin Information								
Incident #:		Date Reported:			Date of Event:			
Theft?	Yes No	Time Reported:		Time Zone	Time of Event:		Time Zone	
If Theft, Police Report ID:								
Reporting Party:	Name:		Department:		Title:			
	Cell Phone:		Email Address:					
Responding Party:	Name:		Department:		Title:			
	Cell Phone:		Email Address:					
Location:		Object:			Responsible Department:			
Inventory #:		Department Contact #:			Department Manager:			
Summary of incident:								
Compromised System Information								
Computer Name(s):		IP(s):			OS:			

Software Present:		Contain PII:	Yes No
Accessible Network Shares:		Computer Used Primarily By:	
Incident Type:	Malware DDoS Web-Application-Attack Phishing Policy-Violation Other		
If Web App Attack:	XSS Broken-Access-Control SQL-Injection Unpatched Other		
If Other, describe:			
Accounts Logged On to Computer:			

Web Attack Information			
Originating IP(s):		Affected IP(s):	
Originating Domain(s):		Affected Domain(s):	
Breach Detected:	Yes No	Attack Type:	
Information Regarding Attack:			

Malware Information			
Name of Malware:		Malware Family:	
AlienVault Link:		VirusTotal Link:	
Any.Run Link:		TrendMicro Link:	
MD5 Hash of File(s)			

IP(s) Associated w/ the Malware:		URL(s) Associated w/ the Malware:	
How was it Detected:			
Impact Characteristics:		Summary of Malware:	
Actions Taken:			
# Of Compromised Systems:			

Timeline of Incident Response Activities		
Date:	Time:	Event / Description:

Analysis			
Directly Impacted Systems:		Downtime of Direct Systems:	
Indirectly Impacted Systems:		Downtime of Indirect Systems:	
IT's Response to the Incident:		Future Impact on IT Services:	
Next Steps:			
Changes Made:			
Incident State:	Active Open Closed		

Chain of Custody		
From:	To:	Date:

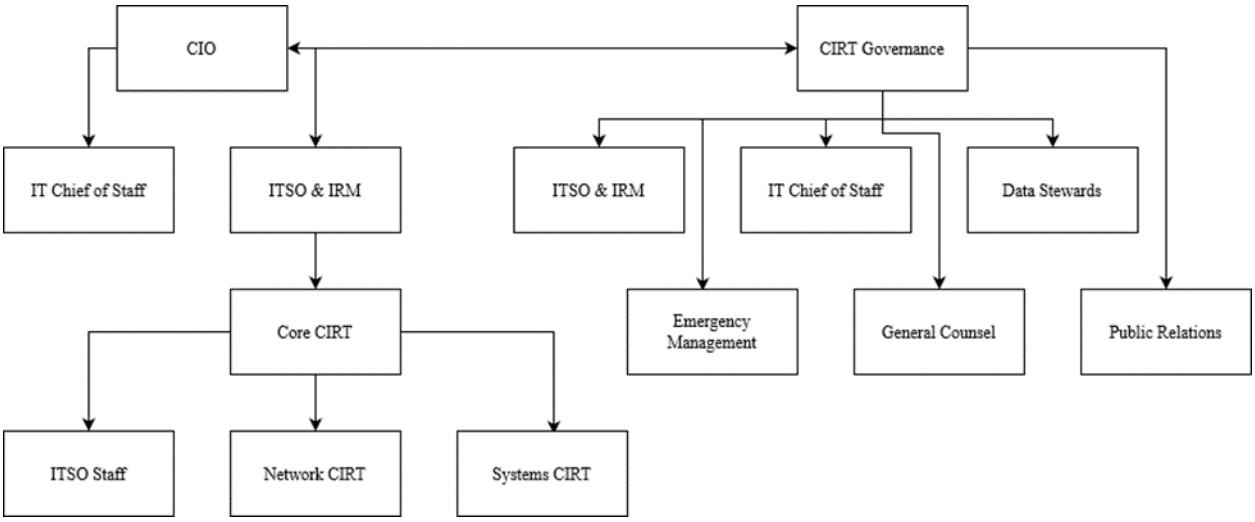
Communications Record					
Communication Type:	To:	From:	Date:	Time:	Description:

Lessons Learned				
Summary of Lessons Learned:				
Incident or Risk	Lessons Learned	Actionable Items	Owner of Item	Status

Revision Table		
Date Revised	Author	Revision Description

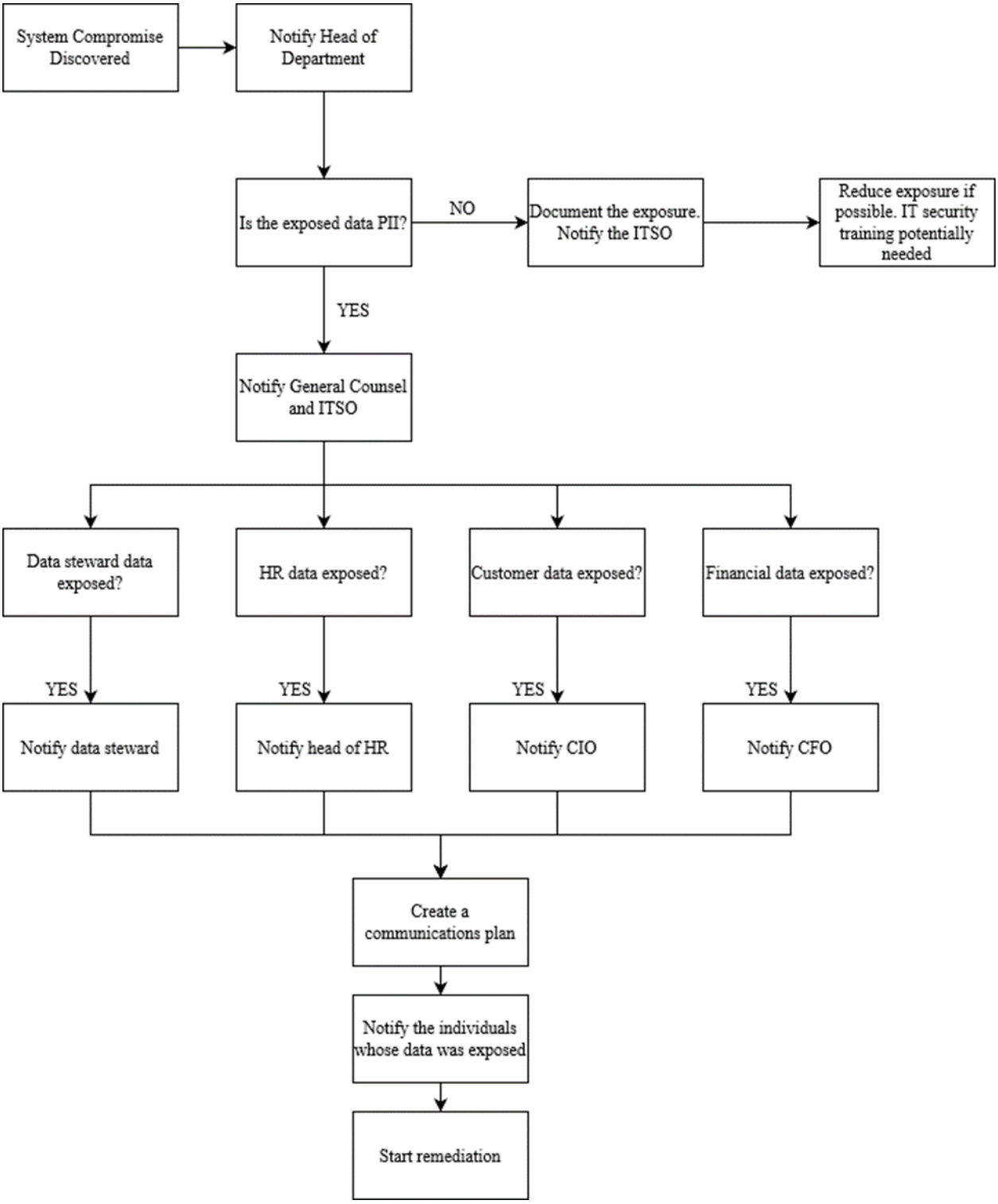
1/17/2022	Evan Read	Created the document
1/26/2022	Evan Read	Updated per Prof. Egeberg's recommendations

Appendix B: Incident Response Team Organizational Chart



[1]

Appendix C: Sensitive Data Exposure Response Chart



[1]

References

[1]
D. Raymond and Virginia Tech, “Virginia Tech Guide for Cyber Security Incident Response,” Jan. 2016. Accessed: Feb. 28, 2022. [Online]. Available: https://security.vt.edu/content/dam/security_vt_edu/downloads/incident_response.pdf.

[2]
A. Abimbola and Oregon Government, “Information security incident response,” Oregon Government, Dec. 2007. https://www.oregon.gov/das/OSCIO/Documents/incidentresponseplantemplate.pdf (accessed Feb. 28, 2022).

[3]
Information Technology Department, “Response and Incident Management Plan and Procedures,” Pierce County, Washington. https://www.piercecountywa.gov/DocumentCenter/View/75053/Incident-Response-Plan-Template (accessed Feb. 28, 2022).