LOYOLA
UNIVERSITY CHICAGO

Preparing people to lead extraordinary lives

Information Technology Services Procedure
Title: Incident Response Plan - Appendix
Approved: June 7, 2012
Author: Information Security Advisory Council (ISAC)
Version: 1.10

Introduction

The Loyola University Chicago Information Security Incident Response Team (LISIRT) is a collection of designated security contacts the various administrative and academic departments who manage Loyola's IT resources. This handbook provides guidelines for these personnel so that IT Incidents can be handled in a repeatable and documented way, as well as provide for clear communication between response team members and the Coordinator of Incident Response.

Because the realm of IT security is always evolving, this handbook should be considered a living document. As new response techniques are discovered, and as our procedures and processes evolve, this handbook will be updated to reflect these changes.

Before you read

Coordination of incident response for Loyola University Chicago is performed by the University Information Security Office (UISO). The UISO is responsible for publishing and providing updates to the Incident Response Plan and associated documentation. For consistency purposes, when the term "incident" stands by itself, it is assumed to be "IT Incident" unless otherwise stated.

Table of Contents

Chain Email Senders

This document provides an overview of the procedure for handling chain emails sent by a member of the Loyola community.

Procedure

Whenever chain emails are reported to have originated within Loyola’s network, the following steps will be taken:

1. Identify affected resources - Based on supplied headers and IP addresses, confirm that the headers do not appear to be spoofed. If the IP address appears to be spoofed, respond to the sender and close the incident as a non-issue.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or the on-call LISIRT member will assign the incident a severity level. Chain email senders will typically be classified as level 2 (minor) if it is not affecting the integrity of the network or level 5 (critical) if it is.
4. Assign responsible LISIRT members - LISIRT members with experience parsing email headers and locating network devices will be assigned.
5. Contain the incident - When the network device that is sending the spam is located, it may have its network connection terminated. This decision is left with the LISIRT member leading the investigation, based on the amount of chain emails being sent and the likelihood of the user disappearing if their connection is terminated.
6. Collect evidence - Any spam email messages sent to LISIRT are treated as evidence. If the reported emails do not contain email headers, ask the sender to re-send the messages with the email headers. If the headers point to the need to gather local logs, the LISIRT will gather those logs. Each piece of evidence will be assigned an evidence number consisting of the case number plus a four digit counter. All collected digital evidence will be documented.
7. Determine vulnerability - There are typically no vulnerabilities associated with chain email.
8. Determine malicious actions taken - There are typically no malicious actions associated with chain email.
9. Provide recovery steps / Take recovery actions - There are typically no recovery steps required for chain email.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month. Student Development or an appropriate Dean may also be informed of the incident.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will also work to identify any elements of the Chain Email Senders Incident Handling process that require improvement.

Forged Email

This document provides an overview of the procedure for handling email containing forged headers. The primary content of the email (spam, chain email, etc) will be handled by the appropriate procedure. This document only deals with handling the forged header aspect of the email.

Procedure

Whenever an incident involving email contains an email with forged headers, the following additional steps will be taken:

1. Identify affected resources - There are four possible versions of forged headers. One is an IP address outside of Loyola is forged to appear as a different IP outside of Loyola (O-O). The second is an IP address outside of Loyola forged to appear as a Loyola IP address (O-L). The third is a Loyola IP address forged to appear as an IP address outside of Loyola (L-O). The fourth is a Loyola IP address forged to appear as another Loyola IP address (L-L).
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or the on-call LISIRT member will assign the incident a severity level. O-O forgeries will typically be level 1 (non-issue) as they most likely do not involve any Loyolans. O-L forgeries will typically be level 2 (minor) as they may impact the reputation of a Loyolan. L-O forgeries will typically be assigned a level 2 (minor) as they are typically associated with a Loyolan sending spam. L-L forgeries will typically be level 3 (medium), as one Loyolan is impersonating another.
4. Assign responsible - LISIRT members LISIRT members with experience parsing email headers and locating network devices will be assigned.
5. Contain the incident - If a Loyola network device is being used in the forgery, it may have its network connection terminated. This decision is left with the LISIRT member leading the investigation, based on the circumstances of the incident.
6. Collect evidence - Any email messages with forged headers sent to LISIRT are treated as evidence. If the reported emails do not contain email headers, ask the sender to re-send the messages with the email headers. If the headers point to the need to gather local logs, the LISIRT will gather those logs. Each piece of evidence will be assigned an evidence number consisting of the case number plus a four digit counter. All collected digital evidence will be documented.
7. Determine vulnerability - If a vulnerability was exploited to allow the forgery, identify and mitigate the vulnerability. Depending on the nature of the exploit, server compromise or account compromise procedures may be invoked.
8. Determine malicious actions taken - The LISIRT will examine the forgery to extrapolate why the headers were forged. Based on the content, email incident response procedures may be invoked.
9. Provide recovery steps / Take recovery actions - The LISIRT will assist in closing any vulnerability that was used to assist with the forgery.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month. Depending on the circumstances of the forged email sent, Student Development or an appropriate Dean may also be informed of the incident
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.

12. Process improvement - The LISIRT will also work to identify any elements of the Forged Email Incident Handling process that require improvement.

Harassing Email

This document provides an overview of the procedure for handling harassing emails received by a member of the Loyola community.

Procedure

Whenever email harassment is reported, the following steps will be taken:

1. Identify affected resources - Initial affected resources will only be the recipient of the harassing email.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or the on-call LISIRT member will assign the incident a severity level. Harassing email will typically be classified as level 1 (nonissue), level 3 (medium), or level 5 (critical).

   An example non-issue would be if the user received an automatically generated harassing message from a virus.

   A harassing message will otherwise be classified at critical if it contains a threat, and as medium otherwise. In either case, the recipient will be advised to contact Loyola's Department of Public Safety (8-6039 non-emergency / 44911 emergency only) or Chicago Police (311 non-emergency / 911 emergency) if they feel threatened.

4. Assign responsible LISIRT members - LISIRT members with experience parsing email headers and good interpersonal skills will be assigned. Based on the content, LISIRT may involve Student Development or Human Resources to serve as a liaison with the recipient of the harassing email.
5. Contain the incident Containment is not necessary for harassing email.
6. Collect evidence Ask the recipient for copies of the offensive emails containing email header information. If the headers point to the need to gather local logs, the LISIRT will gather those logs. Each piece of evidence will be assigned an evidence number consisting of the case number plus a four digit counter. All collected digital evidence will be documented.
7. Determine vulnerability There are typically no vulnerabilities for harassing email.
8. Determine malicious actions taken - The LISIRT will examine mail logs to determine if the sender has communicated with any other members of the Loyola community.
9. Provide recovery steps / Take recovery actions - The LISIRT will cooperate with any law enforcement agencies that become involved. Steps to automatically move emails from the harassing sender to a specified folder will be provided to the recipient.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within three business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Depending on the circumstances of the

spam sent, Student Development or an appropriate Dean may also be informed of the incident. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.

11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will also work to identify any elements of the Harassing Email Incident Handling process that require improvement.

Spam Received

This document provides an overview of the procedure for handling spam emails received by a member of the Loyola community.

Procedure

Whenever spam is reported by a member of the Loyola community, the following steps will be taken:

1. Identify affected resources - The only affected resource should be the recipient’s mailbox.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or the on-call LISIRT member will assign the incident a severity level. Spam recipients will typically be classified as level 1 (nonissue) if the spam does not contain illegal content or level 2 (minor) if it does.
4. Assign responsible LISIRT members - LISIRT members with experience parsing email headers will be assigned.
5. Contain the incident - Typically no containment is necessary.
6. Collect evidence - Obtain a copy of each reported spam message along with full headers for each. If the headers point to the need to gather local logs, the LISIRT will gather those logs. Each piece of evidence will be assigned an evidence number consisting of the case number plus a four digit counter. All collected digital evidence will be documented.
7. Determine vulnerability - Typically there will be no vulnerabilities associated with a spam report. This is an opportunity to discuss configuring rules with the recipient.
8. Determine malicious actions taken - Ask recipient if they clicked on any links contained in the email. If they did, determine if this created any vulnerabilities on their machine. Also go over phishing scams with the recipient.
9. Provide recovery steps / Take recovery actions - If the recipient may have provided personal information, advise them to follow up with their banks / credit card providers and to monitor their credit reports. Assist the recipient with configuring rules to delete spam if they request it.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month. Depending on

the circumstances of the spam sent, Student Development or an appropriate Dean may also be informed of the incident.

11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will also work to identify any elements of the Spam Recipient Incident Handling process that require improvement.

Spam Senders

This document provides an overview of the procedure for handling spam emails sent by a member of the Loyola community.

Procedure

Whenever spam is reported to have originated within Loyola’s network, the following steps will be taken:

1. Identify affected resources - Based on supplied headers and IP addresses, confirm that the headers do not appear to be spoofed. If the IP address appears to be spoofed, respond to the sender and close the incident as a non-issue.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or the on-call LISIRT member will assign the incident a severity level. Spam senders will typically be classified as level 2 (minor) if it is not affecting the integrity of the network or level 5 (critical) if it is.
4. Assign responsible LISIRT members - LISIRT members with experience parsing email headers and locating network devices will be assigned.
5. Contain the incident - When the network device that is sending the spam is located, it may have its network connection terminated. This decision is left with the LISIRT member leading the investigation, based on the amount of spam being sent and the likelihood of the user disappearing if their connection is terminated.
6. Collect evidence - Any spam email messages sent to LISIRT are treated as evidence. If the reported emails do not contain email headers, ask the sender to re-send the messages with the email headers. If the headers point to the need to gather local logs, the LISIRT will gather those logs. Each piece of evidence will be assigned an evidence number consisting of the case number plus a four digit counter. All collected digital evidence will be documented.
7. Determine vulnerability - If any vulnerability was exploited to allow relaying of spam, identify and mitigate the vulnerability. Depending on the nature of the exploit, server compromise or account compromise procedures may be invoked.
8. Determine malicious actions taken - The LISIRT will determine the nature of the spam that was sent, and whether or not the sender intentionally sent the spam.
9. Provide recovery steps / Take recovery actions - The LISIRT will assist in closing any vulnerability that was used to create a spam relay. The LISIRT will close any spam relays that are found.

10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month. Depending on the circumstances of the spam sent, Student Development or an appropriate Dean may also be informed of the incident.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will also work to identify any elements of the Spam Senders Incident Handling process that require improvement.

Malware – Target

This document provides an overview of the procedure for handling malware (viruses, spyware, etc) found on a computer in the Loyola network.

Procedure

Whenever malware is found on a computer in Loyola's network, the following steps will be taken:

1. Identify affected resources - Determine what computers are affected by the malware.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or the on-call LISIRT member will assign the incident a severity level. Malware severity is assigned based on the infected system and the effects of the malware.
4. Assign responsible LISIRT members - LISIRT members with experience in removing malware from the affected operating systems will be assigned.
5. Contain the incident - The malware will be removed, if possible. It may be necessary to wipe the machine and install a fresh image, depending on the type of malware installed.
6. Collect evidence - Any identified malware binaries will be collected as evidence. If there are any logs to indicate when the infection began, they will also be collected.
7. Determine vulnerability - If any vulnerability was exploited to install the malware, identify the vulnerability.
8. Determine malicious actions taken - Determine if the malware was designed to perform any malicious actions.
9. Provide recovery steps / Take recovery actions - The LISIRT will assist in closing any vulnerability that was used to install the malware. If the vulnerability exists in the standard Loyola image, remediation steps will be provided to the team responsible for that image.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to

the ITS Leadership Team as part of a summary report at the end of the month. Depending on the circumstances of the spam sent, Student Development or an appropriate Dean may also be informed of the incident.

11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will also work to identify any elements of the Malware – Target Incident Handling process that require improvement.

Malware – Sender

This document provides an overview of the procedure for handling malware (viruses, spyware, etc) found on a computer in the Loyola network affecting a computer outside or inside of the Loyola network.

Procedure

Whenever malware is found on a computer in Loyola's network and is affecting a computer outside or inside of the Loyola network, the following steps will be taken:

1. Identify affected resources - Determine what computers are affected by the malware.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or the on-call LISIRT member will assign the incident a severity level. Malware severity is assigned based on the infected system and the effects of the malware.
4. Assign responsible LISIRT members - LISIRT members with experience in removing malware from the affected operating systems will be assigned.
5. Contain the incident - The malware will be prevented from sending traffic to other devices on the Loyola network and will then be removed, if possible. It may be necessary to wipe the machine and install a fresh image, depending on the type of malware installed.
6. Collect evidence - Any identified malware binaries will be collected as evidence. If there are any logs to indicate when the infection began, they will also be collected.
7. Determine vulnerability - If any vulnerability was exploited to install the malware, identify the vulnerability.
8. Determine malicious actions taken - Determine if the malware was designed to perform any malicious actions.
9. Provide recovery steps / Take recovery actions - The LISIRT will assist in closing any vulnerability that was used to install the malware. If the vulnerability exists in the standard Loyola image, remediation steps will be provided to the team responsible for that image.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month. Depending on

the circumstances of the malware, Student Development or an appropriate Dean may also be informed of the incident.

11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will also work to identify any elements of the Malware – Target Incident Handling process that require improvement.

Denial of Service – Target

This document provides an overview of the procedure for handling denial of service attacks directed at Loyola resources.

Procedure

Whenever a denial of service attack against Loyola resources is detected, the following steps will be taken:

1. Identify affected resources - The LISIRT will work to identify what resources might be affected, how many resources are affected, and if any services are unavailable as a result of the incident.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or the on-call LISIRT member will assign an the incident a severity level. The severity level will be based on the resources that are affected and the effectiveness of the attack. Denial of service attacks frequently have significant a negative impact on the entire network, so they will often be classified as 4 (major) or 5 (critical).
4. Assign responsible LISIRT members - LISIRT members with experience with firewalls, routers, and packet shapers will be assigned.
5. Contain the incident - To stop the initial attack, certain IP ranges, protocols, or ports may be blocked. This may cause a disruption of services for Loyola. The only traffic that will not be blocked is email, but specific senders or domains may be blocked. The decision to block traffic will be left to the LISIRT lead.
6. Collect evidence - The LISIRT will collect any logs that point back to the attacker. Each piece of evidence will be assigned an evidence number consisting of the case number plus a four digit counter. All collected digital evidence will be documented.
7. Determine vulnerability - If the denial of service occurred due to a vulnerability with a Loyola resource, the vulnerability will be identified and mitigated.
8. Determine malicious actions taken - The LISIRT will attempt work with the attacker to determine if the denial of service was caused by accidentally through a misconfiguration or intentionally. If the attack was intentional, the LISIRT will work with the Office of the General Counsel to determine if outside law enforcement should be involved in the investigation.
9. Provide recovery steps / Take recovery actions - If a vulnerability was identified, close the vulnerability. Identify possible architecture changes to better handle denial of service attacks.

10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will work to ensure that the same vulnerability is not present on other Loyola systems. The LISIRT will also work to identify any elements of the Denial of Service -Target process that require improvement.

Denial of Service – Attacker

This document provides an overview of the procedure for handling denial of service attacks from Loyola resources.

Procedure

Whenever a denial of service attack against Loyola resources is detected, the following steps will be taken:

1. Identify affected resources - The LISIRT will work to identify where the attack originates from, how many systems are involved in the attack, and what system is being targeted.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or the on-call LISIRT member will assign an the incident a severity level. The severity level will be based on the target of the attack and the impact on the network. Denial of service attacks frequently have significant a negative impact on the entire network, so they will often be classified as 4 (major) or 5 (critical).
4. Assign responsible LISIRT members - LISIRT members with experience with firewalls, routers, and packet shapers will be assigned.
5. Contain the incident - To stop the initial attack, certain IP ranges, protocols, or ports may be blocked. This may cause a disruption of services for Loyola. The only traffic that will not be blocked is email, but specific senders or domains may be blocked. The decision to block traffic will be left to the LISIRT lead.
6. Collect evidence - The LISIRT will collect any logs that point back to the attacker. Each piece of evidence will be assigned an evidence number consisting of the case number plus a four digit counter. All collected digital evidence will be documented.
7. Determine vulnerability - If the denial of service occurred due to a vulnerability with a Loyola resource, the vulnerability will be identified and mitigated.
8. Determine malicious actions - taken The LISIRT will attempt work with the attacker to determine if the denial of service was caused by through a compromised machine or intentionally. If the

attack was intentional, the LISIRT will work with the Office of the General Counsel and the appropriate internal disciplinary body.

9. Provide recovery steps / Take recovery actions - If a vulnerability was identified, close the vulnerability. Identify possible architecture changes to better handle denial of service attacks.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will work to ensure that the same vulnerability is not present on other Loyola systems. The LISIRT will also work to identify any elements of the Denial of Service -Attacker process that require improvement.

Monitoring Network Communications

This document provides an overview of the procedure for handling unauthorized monitoring of network communications by a member of the Loyola community.

Procedure

Whenever unauthorized monitoring of network communications is reported, the following steps will be taken:

1. Identify affected resources - Determine what traffic may have been monitored, and what sort of information may have been contained in that traffic.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or on-call LISIRT member will assign the incident a severity level based on the type of information that may have been accessed. If the information includes information classified as Loyola Protected data, the incident will automatically be classified as a 5 (critical).
4. Assign responsible LISIRT members - LISIRT members with experience with network infrastructure and network sniffing programs will be assigned.
5. Contain the incident - If specific steps are available to contain the incident and the traffic is believed to contain Loyola Protected data, the LISIRT will take the necessary steps to protect that resource. If the traffic does not contain Loyola Protected data, the access may be allowed to continue to gather evidence.
6. Collect evidence - Most evidence in this case will be log files showing the access. If the source of the access is identified, a forensic examination of the source machine should be performed.
7. Determine vulnerability - If the monitoring was allowed through a vulnerability or improper access control, the LISIRT will research appropriate fixes.

8. Determine malicious actions taken - The LISIRT will determine if any malicious actions were taken.
9. Provide recovery steps / Take recovery actions - If future monitoring can be prevented by modifying access control lists or applying a patch, the LISIRT will make that recommendation. If information from the network monitoring has been distributed, the LISIRT will work to identify any recipients of the traffic.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month. Depending on the circumstances of the spam sent, Student Development or an appropriate Dean may also be informed of the incident.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will also work to identify any elements of the Monitoring Network Communications Incident Handling process that require improvement.

Commercial use of the network

This document provides an overview of the procedure for handling commercial use of the network at Loyola.

Procedure

Whenever an incident is detected, the following steps will be taken:

1. Identify affected resources - The LISIRT will work to identify any commercial uses of the network.
2. Begin documentation of the incident - The LISIRT assigns each incident a unique incident number.
3. Assess incident - Commercial use of the network is typically classified as either 2 (minor) or 3 (medium), depending on whether or not any of Loyola’s trademarks are being used.
4. Assign responsible LISIRT members - Commercial use of the network typically involves either a website or email, so an appropriate LISIRT member will be assigned.
5. Contain the incident - As commercial use of the network is a violation of policy without approval of the CIO, the website or email will be blocked if the CIO did not grant approval.
6. Collect evidence - The LISIRT will collect evidence of the commercial use of the network.
7. Determine vulnerability If a vulnerability permitted the commercial use of the network, the LISIRT will research fixes for the vulnerability.
8. Determine malicious actions taken - The LISIRT will work to determine if any malicious actions were taken.

9. Provide recovery steps / Take recovery actions - If a vulnerability was used, the LISIRT will offer assistance in patching it.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will work to ensure that the same vulnerability is not present on other Loyola systems. The LISIRT will also work to identify any elements of the Commercial Use of the Network Incident Handling process that require improvement.

Disclosure of Loyola Protected Data

This document provides an overview of the procedure for handling disclosure of Loyola Protected data.

Procedure

Whenever an incident is detected, the following steps will be taken:

1. Identify affected resources - Determine what resources were disclosed.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or on-call LISIRT member will assign the incident a severity level. All incidents involving the release of Loyola Protected data will automatically be classified as a 5 (critical).
4. Assign responsible LISIRT members - Based on how the information was released, LISIRT members with the appropriate knowledge will be assigned to the incident.
5. Contain the incident - If the release of information is in progress, the LISIRT will take the necessary steps to block the release.
6. Collect evidence - The LISIRT will gather any evidence relating to the disclosure. If the source of the disclosure is identified, a forensic examination should be performed.
7. Determine vulnerability - If the disclosure was allowed through a vulnerability or improper access control, the LISIRT will research appropriate fixes.
8. Determine malicious actions taken - The LISIRT will work to determine what malicious actions were taken.
9. Provide recovery steps / Take recovery actions - If future disclosures can be prevented by modifying access control lists or applying a patch, the LISIRT will make that recommendation.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be

provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.

11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will work to ensure that the same vulnerability is not present on other Loyola systems. The LISIRT will also work to identify any elements of the Disclosure of Loyola Protected Data Incident Handling process that require improvement.

DMCA Violation Reports

This document provides an overview of the procedure for handling reports of DMCA violations by a member of the Loyola community.

Procedure

Whenever a DMCA violation is reported to the LISIRT, the following steps will be taken:

1. Begin documentation of the incident - Assign an incident number to the case.
2. Send incident to DMCA agent - Loyola has an appointed DMCA agent who handles all reported DMCA violations. Any reports of DMCA violations should be forwarded to dmcaagent@luc.edu.
3. Assign responsible LISIRT members - If the DMCA agent requests assistance, LISIRT members with experience locating network devices will be assigned to assist.
4. Collect evidence - Any information gathered by the LISIRT during the course of the DMCA investigation is treated as evidence. Each piece of evidence will be assigned an evidence number consisting of the case number plus a four digit counter. All collected digital evidence will be documented. A copy of all collected digital evidence will be provided to the DMCA agent.
5. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #4. Reports of assisting with DMCA investigations will be provided to the ITS Leadership Team and the DMCA agent as part of a summary report at the end of the month.
6. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
7. Process improvement - The LISIRT will also work to identify any elements of the DMCA Violation Report Incident Handling process that require improvement.

Non-DMCA Copyright Violations

This document provides an overview of the procedure for handling copyright violations by members of the Loyola community that are not DMCA violations.

Procedure

Whenever a non-DMCA copyright violation is reported within Loyola's network, the following steps will be taken:

1. Identify affected resources - The LISIRT will identify what resources house the alleged copyright violations, and what user IDs were used to access those files.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident The LISIRT lead or the on-call LISIRT member will assign the incident a severity level. Non-DMCA violations are typically assigned a 2 (minor), but the severity will increase if a subpoena has been issued regarding the copyright violation.
4. Assign responsible LISIRT members - LISIRT members with experience correlating user access with specific machines will be assigned to the incident.
5. Contain the incident - If a user is identified, they should be provided with any Loyola policies concerning copyright violations. If the alleged copyright violation is being transmitted across the Loyola network, that transmission will be severed.
6. Collect evidence - A copy of the alleged copyright violation should be obtained and secured.
7. Determine vulnerability - If any vulnerability was used, the LISIRT will research fixing the vulnerability.
8. Determine malicious actions taken - The LISIRT will determine if any malicious actions were taken.
9. Provide recovery steps / Take recovery actions - If any vulnerability was used, the LISIRT will provide instruction on closing the vulnerability.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month. Depending on the circumstances of the spam sent, Student Development or an appropriate Dean may also be informed of the incident.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will also work to identify any elements of the Non-DMCA Copyright Violations Incident Handling process that require improvement.

Policy Violation

This document provides an overview of handling a violation of ITS policy or of a Loyola policy listed in the Student Handbook, Staff Handbook, or Faculty Handbook.

Procedure

Whenever an incident is detected, the following steps will be taken:

1. Identify affected resources - LISIRT will work to determine what resources may have been affected by this violation of policy.
2. Begin documentation of the incident - Assign an incident number to the case. If appropriate, work with Human Resources, the Office of the General Counsel, and/or Student Development to ensure that they have a copy of anything documented by the LISIRT.
3. Assess incident - The LISIRT lead or the on-call LISIRT member will assign the incident a severity level. The severity will be based on the resources that have been affected by the policy violation. The incident severity may be changed by Human Resources, the Office of the General Counsel, and/or Student Development.
4. Assign responsible LISIRT members - Based on the affected resources and the classification level, LISIRT members with the appropriate knowledge will be assigned to the incident.
5. Contain the incident Depending on the affected resources; steps may be taken to contain the incident. Any actions will first be discussed with Human Resources or Student Development.
6. Collect evidence - LISIRT will collect, document, and store any digital evidence. Copies of all collected evidence will be provided to Human Resources, the Office of the General Counsel, and/or Student Development.
7. Determine vulnerability - The LISIRT will work to determine how the incident occurred. If any vulnerability is found on the resource, the LISIRT will determine if a patch or workaround is available.
8. Determine malicious actions taken - The LISIRT will work to determine what malicious actions may have been performed on the resource. Determining what actions might have been taken will influence the recommended recovery steps. Depending on the incident, forensic analysis may be required to determine what actions were taken on the resource.
9. Provide recovery steps / Take recovery actions - Any recovery steps will need to be approved by Human Resources or Student Development before proceeding.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker. Copies will be provided to Human Resources, the Office of the General Counsel, and/or Student Development as requested.
12. Process improvement - The LISIRT will work to ensure that the same vulnerability is no present on other Loyola systems. The LISIRT will also work to identify any elements of the Policy Violation Incident Handling process that require improvement.

Unauthorized Account Access – External

This document provides an overview of the procedure for handling someone outside of the Loyola community using the account of another member of the Loyola community.

Procedure

Whenever an incident is detected, the following steps will be taken:

1. Identify affected resources - Determine what resources were accessed, and by what user ID.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident The LISIRT lead or on-call LISIRT member will assign the incident a severity level based on the type of information accessed. If the information includes Loyola Protected data, the incident will automatically be classified as a 5 (critical).
4. Assign responsible LISIRT members - Based on the type of resources accessed, LISIRT members with the appropriate knowledge will be assigned to the incident.
5. Contain the incident - If specific steps are available to contain the incident and the resource is believed to contain Loyola Protected data, the LISIRT will take the necessary steps to protect that resource. If the resource does not contain Loyola Protected data, the access may be allowed to continue to gather evidence. But in most cases, the connection will be severed. Once the connection is severed, the account being used to access the resource should be disabled and have its password changed. The account owner should be contacted to inform them of the password change.
6. Collect evidence - Most evidence in this case will be log files showing the access. A forensic analysis of the target machine should be performed.
7. Determine vulnerability - If the access was allowed through a vulnerability or improper access control, the LISIRT will research appropriate fixes.
8. Determine malicious actions taken - The LISIRT will work to determine what actions were taken while accessing another individual’s account.
9. Provide recovery steps / Take recovery actions - If future access can be prevented by modifying access control lists or applying a patch, the LISIRT will make that recommendation. The LISIRT will attempt to remediate any malicious actions taken.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will work to ensure that the same vulnerability is not present on other Loyola systems. The LISIRT will also work to identify any elements of the Unauthorized Account Access – External Incident Handling process that require improvement.

Unauthorized Account Access – Internal

This document provides an overview of the procedure for handling one member of the Loyola community using the account of another member of the Loyola community.

Procedure

Whenever an incident is detected, the following steps will be taken:

1. Identify affected resources - Determine what resources were accessed, and by what user ID.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident The LISIRT lead or on-call LISIRT member will assign the incident a severity level based on the type of information accessed. If the information includes Loyola Protected data, the incident will automatically be classified as a 5 (critical).
4. Assign responsible LISIRT members - Based on the type of resources accessed, LISIRT members with the appropriate knowledge will be assigned to the incident.
5. Contain the incident - If specific steps are available to contain the incident and the resource is believed to contain Loyola Protected data, the LISIRT will take the necessary steps to protect that resource. If the resource does not contain Loyola Protected data, the access may be allowed to continue to gather evidence. Once the connection is severed, the account being used to access the resource should be disabled and have its password changed. The account owner should be contacted to inform them of the password change.
6. Collect evidence - Most evidence in this case will be log files showing the access. If the source of the access is identified, a forensic examination of the source machine should be performed.
7. Determine vulnerability - If the access was allowed through a vulnerability or improper access control, the LISIRT will research appropriate fixes.
8. Determine malicious actions taken - The LISIRT will work to determine what actions were taken while accessing another individual's account.
9. Provide recovery steps / Take recovery actions - If future access can be prevented by modifying access control lists or applying a patch, the LISIRT will make that recommendation. The LISIRT will attempt to remediate any malicious actions taken.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will work to ensure that the same vulnerability is not present on other Loyola systems. The LISIRT will also work to identify any elements of the Unauthorized Account Access – Internal Incident Handling process that require improvement.

Unauthorized Resource Access – External

This document provides an overview of the procedure for handling someone outside of the Loyola community accessing Loyola resources.

Procedure

Whenever an incident is detected, the following steps will be taken:

1. Identify affected resources - Determine what resources were accessed, and by what user ID.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or on-call LISIRT member will assign the incident a severity level based on the type of information accessed. If the information includes Loyola Protected data, the incident will automatically be classified as a 5 (critical).
4. Assign responsible LISIRT members - Based on the type of resources accessed, LISIRT members with the appropriate knowledge will be assigned to the incident.
5. Contain the incident - If specific steps are available to contain the incident and the resource is believed to contain Loyola Protected data, the LISIRT will take the necessary steps to protect that resource. If the resource does not contain Loyola Protected data, the access may be allowed to continue to gather evidence. But in most cases, the connection will be severed.
6. Collect evidence - Most evidence in this case will be log files showing the access. A forensic analysis of the target machine should be performed.
7. Determine vulnerability - If the access was allowed through a vulnerability or improper access control, the LISIRT will research appropriate fixes.
8. Determine malicious actions taken - The LISIRT will work to determine what was done to the resources. Possible actions to be investigated include reading, modifying, deleting, copying, and distributing the resources.
9. Provide recovery steps / Take recovery actions - If future access can be prevented by modifying access control lists or applying a patch, the LISIRT will make that recommendation. If the resources have been modified or deleted, the LISIRT will provide assistance in restoring the resources. If the resources have been distributed, the LISIRT will work to identify any recipients of a copy of the resources.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will work to ensure that the same vulnerability is not present on other Loyola systems. The LISIRT will also work to identify any elements of the Unauthorized Resource Access – External Incident Handling process that require improvement.

Unauthorized Resource Access – Internal

This document provides an overview of the procedure for handling a member of the Loyola community improperly accessing Loyola resources.

Procedure

Whenever an incident is detected, the following steps will be taken:

1. Identify affected resources - Determine what resources were accessed, and by what user ID.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or on-call LISIRT member will assign the incident a severity level based on the type of information accessed. If the information includes Loyola Protected data, the incident will automatically be classified as a 5 (critical).
4. Assign responsible LISIRT members - Based on the type of resources accessed, LISIRT members with the appropriate knowledge will be assigned to the incident.
5. Contain the incident - If specific steps are available to contain the incident and the resource is believed to contain Loyola Protected data, the LISIRT will take the necessary steps to protect that resource. If the resource does not contain Loyola Protected data, the access may be allowed to continue to gather evidence.
6. Collect evidence - Most evidence in this case will be log files showing the access. If the source of the access is identified, a forensic examination of the source machine should be performed.
7. Determine vulnerability - If the access was allowed through a vulnerability or improper access control, the LISIRT will research appropriate fixes.
8. Determine malicious actions taken - The LISIRT will work to determine what was done to the resources. Possible actions to be investigated include reading, modifying, deleting, copying, and distributing the resources.
9. Provide recovery steps / Take recovery actions - If future access can be prevented by modifying access control lists or applying a patch, the LISIRT will make that recommendation. If the resources have been modified or deleted, the LISIRT will provide assistance in restoring the resources. If the resources have been distributed, the LISIRT will work to identify any recipients of a copy of the resources.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will work to ensure that the same vulnerability is not present on other Loyola systems. The LISIRT will also work to identify any elements of the Unauthorized Resource Access – Internal Incident Handling process that require improvement.

Server Compromise

This document provides an overview of the procedure for handling the compromise of a server at Loyola.

Procedure

Whenever the server compromise is detected, the following steps will be taken:

1. Identify affected resources - Identify the affected servers.
2. Begin documentation of the incident - The LISIRT assigns each incident a unique incident number. Documentation includes a brief description of any actions taken, along with the time that action was taken.
3. Assess incident - The LISIRT lead or on-call LISIRT member will assign the incident a severity level. A server compromise will either be a 4 (high) or a 5 (critical), depending on the type of information housed on the server.
4. Assign responsible LISIRT members - LISIRT members with experience in forensics and in administering the affected operating system will be assigned.
5. Contain the incident - Initial forensic information will be gathered from the server. The server will then be disconnected from the network and downed.
6. Collect evidence - A forensic image of the server will be taken and examined.
7. Determine vulnerability - The LISIRT will work to determine how the incident occurred. If the compromise occurred because of a vulnerability, the LISIRT will determine if a patch or workaround is available.
8. Determine malicious actions taken - The LISIRT will work to determine what malicious actions may have been performed on the resource. Determining what actions might have been taken will influence the recommended recovery steps.
9. Provide recovery steps / Take recovery actions - If the time of the exploit can be determined, the server may be restored from an older backup and properly patched. Backup procedures for server will be followed in accordance within the Server Security Standard. If the time of the exploit cannot be determined, then the server should be rebuilt from the scratch.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will work to ensure that the same vulnerability is not present on other Loyola systems. The LISIRT will also work to identify any elements of the Server Compromise Incident Handling process that require improvement.

Webserver Defacement

This document provides an overview of the procedure for handling the defacement of a webserver at Loyola.

Procedure

Whenever the server compromise is detected, the following steps will be taken:

1. Identify affected resources - Identify the affected servers.
2. Begin documentation of the incident - The LISIRT assigns each incident a unique incident number. Documentation includes a brief description of any actions taken, along with the time that action was taken.
3. Assess incident - The LISIRT lead or on-call LISIRT member will assign the incident a severity level. A server compromise will either be a 4 (high) or a 5 (critical), depending on the public visibility of the server.
4. Assign responsible LISIRT members - LISIRT members with experience in forensics and in configuring the affected webserver will be assigned.
5. Contain the incident - Initial forensic information will be gathered from the server. The server will then be disconnected from the network and downed.
6. Collect evidence - A forensic image of the server will be taken and examined.
7. Determine vulnerability - The LISIRT will work to determine how the incident occurred. If the compromise occurred because of a vulnerability, the LISIRT will determine if a patch or workaround is available.
8. Determine malicious actions taken - The LISIRT will work to determine what malicious actions may have been performed on the server.
9. Provide recovery steps / Take recovery actions - If the time of the exploit can be determined, the server may be restored from an older backup. Backup procedures for server will be followed in accordance within the Server Security Standard. If the time of the exploit cannot be determined, then the server should be rebuilt from the scratch.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will work to ensure that the same vulnerability is not present on other Loyola systems. The LISIRT will also work to identify any elements of the Webserver Defacement Incident Handling process that require improvement.

Criminal Acts

This document provides an overview of the procedure for handling criminal activities performed on the Loyola network.

Procedure

Whenever possible criminal activity is reported to within Loyola's network, the following steps will be taken:

1. Identify affected resources - Identify any possible resources that were affected.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - Based on the criminal act in question, highly likely that the incident response will be driven by either Campus Safety or the Office of the General Counsel. If so, the LISIRT will provide whatever assistance is requested. If this is not the case, the LISIRT will assign a severity level based on the alleged crime. Special care will be taken in determining the appropriate time to contact law enforcement, as that will cause Loyola to operate under "color of law".
4. Assign responsible LISIRT members - The appropriate LISIRT members will be assigned.
5. Contain the incident - Depending on the incident, it will either be stopped or allowed to continue so that further evidence may be collected.
6. Collect evidence - Any evidence of the alleged crime will be collected and stored by the LISIRT. As with all incidents, the evidence will be collected under the assumption that it may be used in a court of law.
7. Determine vulnerability - If a vulnerability was exploited to allow the criminal act, the LISIRT will research fixes for the vulnerability.
8. Determine malicious actions taken - The LISIRT will work to determine the extent of the criminal attacks performed by the attacker.
9. Provide recovery steps / Take recovery actions - The LISIRT will assist in closing any vulnerabilities that were used to allow the criminal act.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month. Depending on the circumstances of the spam sent, Student Development or an appropriate Dean may also be informed of the incident.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will also work to identify any elements of the Criminal Acts Incident Handling process that require improvement.

Failures of Hardware, Software and Critical Security Controls (CSC)

This document provides an overview of the procedure for handling hardware, software or critical security control (CSC) failures on the Loyola network.

Whenever critical hardware, software or critical security control (CSC) failures are reported to within Loyola's network, the following steps will be taken:

Procedure

The following procedure has been documented as a guideline for determining how to best recover the system. The procedure includes a list of possible participants in the recovery process. Once the scope of the problem has been identified, a determination can be made as to which staff resources will participate in the recovery process.

1. Identify affected resources - Identify any possible resources that were affected.
2. Begin documentation of the incident - The LISIRT assigns each incident a unique incident number. Documentation includes a brief description of any actions taken, along with the time that action was taken.
3. Assess incident - The LISIRT lead or on-call LISIRT member will assign the incident a severity level. A hardware, software, or critical security control failure in the CDE will either be a 4 (high) or a 5 (critical), depending on the type of information that the failure contains.
4. Assign responsible LISIRT members - LISIRT members with experience in forensics and in administering the affected operating system will be assigned.
5. Determine the extent of the problem (hardware/software/CSC-related, which components).
6. If the problem is determined to be hardware-related, it may be necessary to contact the vendor via Server Operations or Networking. Server Operations and Networking maintain lists of vendor contact information.
7. If the problem involves server-side or networking issues, the proper representatives of ITS should be contacted to trouble-shoot and assist in resolving the problem.
8. If the problem and its resolution will require an extended downtime to apply, the Server Operations Manager will contact the ITS Leadership Team with an estimate of the length of the downtime. At their discretion, they may ask a designee to do the contacting. Use the call list/procedures detailed in LUC Disaster Recovery Plan to make these contacts.
9. If the problem resolution requires the restoration of software/data from backups, Server Operations will retrieve the appropriate backup media locally or from Offsite Storage. Backup procedures will be followed in accordance within the Server Security Standard.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will work to identify any elements of the Incident Handling process that require improvement.

Rogue Access Points (CDE)

This document provides an overview of the procedure for handling rogue access points connected to the Cardholder Data Environment (CDE) on the Loyola network.

Procedure

Whenever a possible rogue access point connected to the Cardholder Data Environment (CDE) is reported to within Loyola's network, the following steps will be taken:

1. Identify affected resources - Identify any possible resources that were affected.
2. Begin documentation of the incident - The LISIRT assigns each incident a unique incident number. Documentation includes a brief description of any actions taken, along with the time that action was taken.
3. Assess incident - The LISIRT lead or on-call LISIRT member will assign the incident a severity level. A rogue access point in the CDE will either be a 4 (high) or a 5 (critical), depending on the type of information that can be accessed by the rogue.
4. Assign responsible LISIRT members - LISIRT members with experience in forensics and in administering the affected operating system will be assigned.
5. Contain the incident - Initial connectivity information will be gathered from the rogue. The rogue will then be disconnected from the network and confiscated.
6. Collect evidence – Determine if other devices are broadcasting or connected to the rogue SSID.
7. Determine ownership - The LISIRT will work to determine ownership of the rogue. If ownership can be determined, Campus Safety will be contacted along with an attempt to contact the owner. It is preferred that the owner be contacted by Campus Safety.
8. Determine malicious actions taken - The LISIRT will work to determine what malicious actions may have been performed on the resource. Determining what actions might have been taken will influence the recommended breach notification steps.
9. Provide breach notification steps / Take breach notification actions – Establish contacts with Risk Management, Treasury, and Finance along with the Sr VP Admin Services & CHRO and the Chief Information Officer. Determination will be made by the breach notification team regarding reporting of the breach.
10. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.
11. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
12. Process improvement - The LISIRT will work to identify any elements of the Rogue Access Point Incident Handling process that require improvement.

Payment Card Data Incidents

This document provides an overview of the procedure for handling a breach of Payment Card Data on the Loyola network.

Procedure

1. Identify affected resources - Determine what resources were disclosed.
2. Begin documentation of the incident - Assign an incident number to the case.
3. Assess incident - The LISIRT lead or on-call LISIRT member will assign the incident a severity level. All incidents involving the release of Payment Card data will automatically be classified as a 5 (critical).
4. Assign responsible LISIRT members - Based on how the information was released, LISIRT members with the appropriate knowledge will be assigned to the incident.
5. Perform appropriate steps to notify the payment brands within 24 hours of incident notification.
6. Contain the incident - If the release of information is in progress, the LISIRT will take the necessary steps to block the release.
7. Collect evidence - The LISIRT will gather any evidence relating to the disclosure. If the source of the disclosure is identified, a forensic examination should be performed.
8. Determine vulnerability - If the disclosure was allowed through a vulnerability or improper access control, the LISIRT will research appropriate fixes.
9. Determine malicious actions taken - The LISIRT will work to determine what malicious actions were taken.
10. Provide recovery steps / Take recovery actions - If future disclosures can be prevented by modifying access control lists or applying a patch, the LISIRT will make that recommendation.
11. Create final report - The LISIRT lead will create a report detailing the incident and all steps taken. All reports will be available within 3 business days after the completion of item #9. Reports for major incidents will be provided to the ITS Leadership Team. Reports for critical incidents will be provided to the ITS Leadership Team and the CIO. Minor and medium reports will be provided to the ITS Leadership Team as part of a summary report at the end of the month.
12. Archive evidence and report - The LISIRT will archive all evidence obtained during the course of the investigation, along with a copy of the final report. Digital evidence will be stored on removable media. If the digital evidence does not have a built-in hash, an MD5 hash of the file will be created and stored as a text file with the evidence. All evidence will be stored in the LISIRT evidence locker.
13. Process improvement - The LISIRT will work to ensure that the same vulnerability is not present on other Loyola systems. The LISIRT will also work to identify any elements of the Disclosure of Loyola Protected Data Incident Handling process that require improvement.

Steps for Payment Brands

- MasterCard Specific Steps:
    1. Within 24 hours of an account compromise event, notify the MasterCard compromised Account Team via phone at 1-636-722-4100.
    2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
    3. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers

    4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evalutation).
    5. Provide a weekly written status to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
    6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
    7. Provide finding of all audits and investigation to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.
- VISA Specific Steps:
    1. Refer to documentation online at http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf
- Discover Card Specific Steps
    1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at 1-800-347-3102.
    2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
    3. Prepare a list of all known compromised account numbers.
    4. Obtain addition specific requirements form Discover Card.
- American Express Specific Steps
    1. Within 24 hours of an account compromise event, notify American Express Merchant Services at 1-800-528-5200.
    2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
    3. Prepare a list of all known compromised account numbers.
    4. Obtain addition specific requirements form American Express. If the entity being assessed is a service provider
- General Steps
    1. Restore security functions
    2. Identify and document the duration (date and time start to end) of the security failure
    3. Identify and document cause(s) of failure, including root cause
    4. Document remediation required to address root cause
    5. Identify and address any security issues that arose during the failure
    6. Perform a risk assessment to determine whether further actions are required as a result of the security failure
    7. Implement controls to prevent cause of failure from reoccurring
    8. Resume monitoring of security controls

Assessment of Incidents Involving HIPAA PHI

Refer to the most recent version of the document entitled Information Breach Decision Tree for HIPAA. The LISIRT must perform and document a risk assessment (in accordance with that document) to determine whether there is a significant risk of harm to the individual whose PHI (protected health information) was inappropriately released or disclosed into the wrong hands. Ensure compliance with any required notifications.

Procedure

The complete evidence collection and subsequent analysis process should be documented thoroughly and in detail.

Complete and submit the Incident Report required by the Incident Response Plan, ensuring that the following information is included:

1. Define the incident – what happened? When did it happen? Who was involved? When was it discovered?
2. Stop the incident – if a smartphone is lost take the steps to disable the access, if a breach is found take the steps to prevent further access, etc.
3. Document the incident – fill in all the details of what occurred from step 1 (define the incident) and step 2 (steps taken to stop the incident). Clearly document all aspects of the incident.
4. Determine who has been affected by the incident – which patient records have been affected?
5. Notify appropriate individuals / agencies –the amount of patient records affected will determine what notification steps are needed. Individual patients and Health and Human Services (HHS) will need to be notified.

Create a Technical Report that includes:

1. Detailed information about the event, including actions taken and personnel involved
2. Detailed information about the investigation
3. System Information
4. System Interconnections
5. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
6. The unauthorized person who used the PHI or to whom the disclosure was made;
7. Whether the PHI was actually acquired or viewed; and
8. The extent to which the risk to the PHI has been mitigated.
9. Recommendations for further action.

Document other information such as:

1. Number and size of sectors, operating systems, significant software, anti-virus software, etc.
2. All conclusions reached
3. How and when the evidence was returned or the manner in which it was disposed

Note: data used in this report should reference collected evidence and be verifiable.

Note on the EU General Data Protection Regulation (GDPR)

1. In the case of a personal data breach involving data covered under the GDPR, there are specific compliance tasks that must be performed within very specific timeframes. The LISIRT lead acting as the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, send a notification of the personal data breach to the EU supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and

freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The LISIRT should follow continue following the process appropriate for the type of breach contained in this document while maintaining compliance with the GDPR.

3. The notification referred to in section uses the form located at: https://www.luc.edu/gdpr/policies/noticeofpersonaldatabreachform/

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

6. All documentation will be sent to the supervisory authority to verify compliance with GDPR regulations.

7. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, then if no GDPR exceptions apply, the LISIRT shall communicate the personal data breach to the data subject, without delay. Such communication shall be in clear and plain language and contain, at a minimum, the information and measures summarized in Sections 3.b, 3.c, and 3.d above.

8. In addition to the GDPR-required actions specified above, other applicable measures specified herein shall also be complied with.

Questions about this document
If you have questions about this document, please contact the Information Security team at datasecurity@luc.edu.

Definitions

ITS Leadership Team – CIO and direct reports

References

Server Security Standard

History

June 23, 2008: V 1.0, Initial document
January 24, 2011: V 1.1, Minor grammatical corrections
August 25, 2014: V 1.3, Added Cardholder Data Environment

June 24, 2015: V 1.3, Review for PCI Compliance
April 20, 2016: V 1.3, Annual Review for PCI Compliance
May 17, 2017: V 1.3, Annual Review for PCI Compliance
June 1, 2017: V 1.4, Renamed and modified Cardholder Data Environment to read Payment Card Data section
June 14, 2017: V 1.5, Added Section to cover hardware/software failure per PCI Audit
July 21, 2017 V 1.6, Modified HIPAA section to reflect HHS IR Planning.
September 7, 2017 V 1.7, Modified Hardware/Software failure section to cover failure of critical security controls for PCI-DSS V3.2
Sep 21, 2017: V1.7, added backup procedure reference
May 17, 2018: V1.8 Added GDPR section, annual review for PCI compliance
September 17, 2018: V1.9 modifications to reflect ITS structure changes and to correct department names
October 5, 2018: V1.10 modifications to the GDPR response plan
August 27, 2019: V1.10 Annual Review for PCI Compliance
September 1, 2020: V1.10 Annual Review for PCI Compliance
May 27, 2021: V1.10 Annual Review for PCI Compliance