Nebraska State Treasurer's Office

Incident Response Plan

About This Document

This document contains the incident response plan for Nebraska State agencies Computer Incident Response Team (CIRT). This document is for internal use only and is not to be distributed.

Table 1 - Revision History

Version	Date	Author	Description of Change
1.0	June 2, 2017	Treasury Staff	Document created

Contents

Scope

The purpose of this document is to create and implement an incident response plan to be prepared to respond swiftly in the event of a system breach.

The scope includes any incidents or suspected incidents associated with the security of the cardholder data network or cardholder data itself, as these must be responded to quickly and in a controlled, coordinated and specific manner. The purpose of the Incident Response Plan is to assist Nebraska State Agency's Computer Incident Response Team (CIRT) members to identify, respond to and report a data security breach. These procedures also describe the way OCIO or Agency technical staff will aid in the eradication, recovery and permanent remediation of the root cause of the incident. This is important to preserve as much evidence as practical while keeping in mind that prevention of damage is of the highest priority.

The Nebraska State Treasurer's Incident response plan is based on industry standard incident response framework consisting of these seven phases:

- Preparation
  - Formation of Computer Incident Response Team
  - Incident response training of CIRT members
  - Technical incident handling training for IT and security staff
  - Contact list for CIRT members, law enforcement, payment card brands and acquiring bank
  - Annual incident response testing
- Identification
  - Observation of anomalous event
- Assessment
  - Determine scope of incident
  - Assign severity to incident
- Containment
  - System isolation
  - Forensically sound system backups
- Eradication
  - Removing unauthorized code
  - Applying patches
  - Installing Security Software
  - Removing unnecessary services
- Recovery
  - Rebuilding of systems
  - Operating system and application hardening
  - Clean backup restoration
- Follow-up/Lessons Learned
  - Forensic review report
  - Re-evaluation of security infrastructure

Card brands and acquiring banks must be notified upon discovery of a data security breach involving cardholder data. Visa and many acquiring banks may require a forensic review of a cardholder data security breach by a PCI Forensic Investigator (PFI). The list of approved PFIs can be found at: https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators.

Preparation

Computer Incident Response Team Requirements

The Computer Incident Response Team is comprised of employees from the agency, Office of the Chief Information Officer, and Nebraska State Treasurer employees with the required skills to identify and control system compromises or other intrusion incidents (See Appendix A).

1. List the members and the roles and responsibilities of the Computer Incident Response Team. (Ref. Nebraska State Treasurer's Office Information Security Policy sec. 12.10.1a)
2. Train the members of the Computer Incident Response Team to deal with security breach incidents. (Ref. Nebraska State Treasurer's Office Information Security Policy sec. 12.10.4)
3. Ensure availability of team members at all times (24/7) to respond to alerts, intrusion detection, or other incidents. (Ref. Nebraska State Treasurer's Office Information Security Policy sec. 12.10.3)
4. Train members of the Computer Incident Response Team to keep current with technical developments in the industry.
5. Notify the Computer Incident Response Team Leader of any unauthorized activity, critical Intrusion Detection System (IDS) alerts, or reports of unauthorized critical system or content file changes and determine the need to activate the full Incident Response Plan.

Recommended CIRT Members

CIRT Members	CIRT Role
Agency Director/Manager	Provide authority to operate and has authority to make business-related decisions based on information garnered from the other team members.
State Information Security Officer	Assess security incidents, perform containment, eradication and basic forensics. Assist information technology in recovery role.
Agency Information Security Officer	Minimize the impact to system end users. Assist the Information Security team with technical issues and recovery roles.
Chief Information Officer	Understand the root cause of the incident and any failures of compliance, which may have contributed to the incident.
Network Services Administrator	Assess any physical damage and investigate any physical theft of data. Document chain of custody for any physical evidence.
Agency Legal	Ensure that evidence collected is usable in a criminal investigation. Act as legal counsel to senior management.
Agency Human Relations Representative	Provide advice to senior management if an employee caused the incident.
Public Relations – State Treasurer's Office Staff	Work with all members of the CIRT to understand the incident. Coordinate with senior management, acquirers, card brands and law enforcement to develop a disclosure plan (if any).

Incident Response Plan – Annual Review and Testing

Regular review and testing of the Nebraska State Treasurer's Office Incident Response Plan is essential to maintain compliance with the Payment Card Industry Data Security Standard.

The following must be completed at least annually to maintain compliance with the PCI Data Security Standard. Documentation of completion is required. (See Appendix B).

1. Review the Incident Response Plan annually and modify as necessary to ensure it is up to date according to lessons learned and industry developments. (Ref. Nebraska State Treasurer's Office Information Security Policy sec. 12.10.6)
2. Test the Incident Response Plan annually. (Ref. Nebraska State Treasurer's Office Information Security Policy sec. 12.10.2)

Identification and Assessment

The Incident Response Plan includes continuous monitoring with the ability to send real time alerts to appropriate personnel from intrusion detection, intrusion prevention, and file integrity monitoring systems for all critical systems components. (Ref. Nebraska State Treasurer's Office Information Security Policy sec. 12.10.1b and 12.10.5)

A detailed process or procedure for monitoring critical security breach indicators (event logs, IDS logs, File Integrity report, wireless scans or wireless IDS logs, wireless access point ID, etc.) must be defined and documented in the IRP. (PCI-DSS Requirement 12.10.5)

Nebraska State agency's use the following process for monitoring its cardholder environment:

[Need to detail procedure/process for monitoring and alerting of IDS/IPS, FIM, SIM/SIEM, system logs, firewall logs, wireless logs, rouge wireless access point detection, etc. here.]

Use the incident response form to help assigned personnel with the identification and initial assessment of security incidents. The form helps incident responders gather information necessary to confirm the existence of an incident. Information gathered allows CIRT members to determine the scope and potential impact of an incident. Any incident involving the compromise or suspected compromise of cardholder information must be reported to impacted card brands, the acquiring bank and any other entities as required by contract or law, this function will be done by State Treasurer Staff.

(See Appendix C – Incident Response Form)

(See Appendix D – Incident contact list)

(See Appendix E – Legal requirements)

Containment

The containment phase allows Nebraska State Treasurer's Office incident handlers to regain control of the situation and to minimize the amount of impact caused by an incident. Incident handlers will work closely with the State Information Security Officer, Department Management and the OCIO to take careful steps to contain systems storing, transmitting or processing cardholder information. The following general guidelines should be followed to protect evidence and limit the exposure of cardholder information.

- Perform system backup (backups must be forensically sound to preserve the machine state)
- Remove system from network
- Change administrative, application and system passwords

- Create additional firewall restrictions

Business impact must be evaluated before removing a system from a production environment.

Eradication and Recovery

During the eradication and recovery phases of an incident, the root cause of an incident must be determined. Qualified personnel must perform eradication and recovery phase incident response reports. Forensic analysis of system memory, disk storage and logs must be analyzed to determine the cause of the incident. Administrative tools found on the compromised system should not be used in the event the perpetrator has modified system tools.

Re-installing the operating system and restoring a known clean system backup should perform recovery. The applicable NITC 8-103 System Hardening and Configuration Standards procedure must be followed prior to placing the system back into production. Once the system is placed back into production, increased monitoring and testing should be performed to validate that the eradication has been successful and that the root cause of the compromise has not persisted.

Card Association members may require Nebraska State Treasurer's Office to contract with a PCI Forensic Investigator (PFI). For a list of approved PFIs, go to https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators. Forensic work performed by a PFI will be coordinated with the card brands and the acquiring bank.

Follow-up and Lessons Learned

Incident response plan tests and live incidents provide valuable insight into the effectiveness of the incident response plan. At the end of the incident response process, there is often a tendency to return to "business as usual" without updating Nebraska State Treasurer's Office policies, procedures and guidelines. A post-mortem examination of the incident should be conducted to validate that Nebraska State Treasurer's Office policies, procedures and guidelines are up to date and being followed. Any changes need to be documented and communicated to relevant personnel.

Appendix A: Assignment of CIRT Member Roles and Responsibilities

As required by policy in section 12.6 of the Nebraska State Treasurer security policy, the following table contains the assignment of management roles for security incident response.

CIRT Member Roles and Responsibilities

Each agency will complete the contact information and make available to all employee that handle credit card data. A copy will be emailed to NST.TMStaff@nebraska.gov and will be updated at least every June or when staff changes.

Name	Title	Date Assigned	Date Training Received	Email Contact Information	Telephone Contact Information	Description of Role and Responsibility	24/7
	Agency Information Security Officer					Minimize the impact to system end users. Assist the Information Security team with technical issues and recovery roles.	
	Agency Director					Provide authority to operate and has authority to make business-related decisions based on information garnered from the other team members.	
Chris Hobbs	State Information Security Officer	5/31/2017	5/31/2017	chris.hobbs@nebraska.gov	402-471-3677 C402-471-1099	Assess security incidents; perform containment, eradication and basic forensics. Assist information technology in recovery role.	

Name	Title	Date Assigned	Date Training Received	Email Contact Information	Telephone Contact Information	Description of Role and Responsibility	24/7
Ed Toner	Chief Information Officer	5/31/2017	5/31/2017	ed.toner@nebrask.gov	402-471-3717 C402-880-1122	Understand the root cause of the incident and any failures of compliance, which may have contributed to the incident.	
	Agency IT personnel					Assess any physical damage and investigate any physical theft of data. Document chain of custody for any physical evidence.	
	Agency Legal and Attorney General					Ensure that evidence collected is usable in a criminal investigation. Act as legal counsel to senior management.	
	Agency Human Relations Representative					Provide advice to senior management if an employee caused the incident.	
Char Scott	Treasury Management Director	5/31/2017	5/31/2017	char.scott@nebraska.gov	402-471-4146 C402-540-3595	Work with all members of the CIRT to understand the incident. Coordinate with senior management, acquirers, card brands, and law enforcement to develop a disclosure plan (if any).	

Appendix B - Incident Response Plan – Annual Review and Testing

Incident Response Plan will be reviewed annually and modified as necessary to ensure it is up to date according to lessons learned and industry developments. (Ref. Nebraska State Treasurer's Office Information Security Policy sec. 12.10.6)

The Incident Response Plan will be tested annually. (Ref. Nebraska State Treasurer's Office Information Security Policy sec. 12.10.2)

Annual Incident Response Plan Test

Test Date	CIRT Members Involved	Test Scenario	Test Results	Modifications Needed

Appendix C - Incident Reporting and Assessment Form

Incident Handler Contact Information

Last Name:		First Name:	
Job Title:		Email:	
Phone:		Alt Phone:	
Mobile:		Fax:	

Incident General Information

Incident #:	Type of Incident:	☐ Malicious Code	☐ SQL Injection
Source of Incident: ☐ External ☐ Internal		☐ Denial-of-Service	☐ Physical Theft
Date/Time of Incident Occurred:		☐ Unauthorized Access	☐ Phishing
		☐ Wireless Attack	☐ Cross Site Scripting
Discovered or Reported by:		☐ Rogue Wireless	☐ Inappropriate Usage
		☐ Network Probes	☐ Privilege Escalation
		☐ Others (Specify):	
Incident location:	Date/Time of Incident Detected:		

Personal Identifiable Information Affected?	☐ Yes	☐ No	Severity Level:	☐ Critical ☐ High ☐ Medium ☐ Low
Credit Card Information Affected?	☐ Yes	☐ No		
Number of Credit Cards Impacted	VISA: MC:		AMEX: DISC:	
Systems and Services Impacted:				

Incident Summary

Comments

Incident Mitigation

Comments:

Recommendation

Comments:

Additional Comments/Notes

Comments:

Appendix D - Incident Contact List

The IRP must include or reference the specific incident response procedures from the payment brands. (PCI-DSS Requirement 12.9.1)

This information must be kept up to date and validated as part of the annual Incident Response procedure review and training.

Organization	Website	Telephone Number	Email Contact Information	Comments
Elavon - Customer Representative – Amir Aslam	https://www.elavon.com/security-center/elavon-security/safe-t.html	(925) 683-9833	amir.aslam@elavon.com	
US Bank – Greer Almquist	https://usbank.com	(402) 536-5101 c (913) 484-6908	greer.almquist@usbank.com	
VISA	https://usa.visa.com/content/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf	(650) 432-2978	usfraudcontrol@Visa.com	Please see current Visa documents on the "What to do if Compromised" webpage.
MasterCard	http://www.mastercard.com/us/merchant/support/security_programs.html	(636) 722-4100	account_data_compromise@mastercard.com	Please see the current MasterCard "Account Data Compromise User Guide" located on the MasterCard website.
American Express	http://www.americanexpress.com/datasecurity	(888) 732-3750 (602) 537-3021	EIRP@aexp.com	Please see the current (American Express Data Security Operating Policy for Service Providers or American Express Data Security Operating Policy for U.S. Merchants) document located on the American Express data security website.
Discover	http://www.discovernetwork.com/fraudsecurity/disc.html	(800) 347-3083	N/A	
PCI Forensic Investigator	https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators			
NE State Patrol		(402) 471-2400	nsp.capitolsecurity@nebraska.gov	Capitol Security will refer us to the Investigative Division within the State Patrol
US Secret Service	http://www.secretservice.gov/field_offices.shtml			See website for the nearest US Secret Service office.

Appendix E – Legal Requirements

PCI DSS Requirement 12.10.1 requires analysis of legal requirements for reporting compromises.

The following law applies in Nebraska:

Nebraska Financial Protection and Consumer Notification of Data Security Breach Act of 2006

Neb. Rev. Stat. §87-803 Requires notice to the resident that personal information has been or might be use for unauthorized purpose.

Card Brands – security notifications guidelines

https://usa.visa.com/content/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

https://www.mastercard.us/en-us/merchants/get-support/security-training.html

http://www.discovernetwork.com/fraudsecurity/disc.html

https://www209.americanexpress.com/merchant/services/en_US/data-security