Draft
Title: Incident Response and Reporting Procedure for State Government

(Date of last revision: 4/5/2002)

State Agencies shall prepare procedures for reporting security breaches and incidents. Documentation on security incidents shall be filed with the Chief Information Officer for the State of Nebraska.

Explanation / Key Points

Security is a growing problem. Effective response and collective action are required to counteract security violations and activities that lead to security breaches. Agency management, law enforcement, and others must know the extent of security problems in order to make proper decisions pertaining to policies, programs and allocation of resources. Responding to security alerts will help to prevent incidents from occurring. Quick reporting of some incidents, such as new viruses, is essential to stopping them from spreading and impacting other systems. Reporting computer crimes is the only way for law enforcement to deter and apprehend violators.

These guidelines incorporate most of the "CIO Cyberthreat Response and Reporting Guidelines" jointly sanctioned by the FBI and U.S. Secret Service. A copy of those guidelines is available at: http://www.cio.com/research/security/incident_response.pdf, http://www.usss.treas.gov/net_intrusion.shtml, or http://www.fbi.gov/pressrel/pressrel02/cyberguidelines.htm.

Effective response to security incidents requires quick recognition of problems and fast mobilization of skilled staff to return systems to normal. This requires prior documentation of procedures and responsibilities of everyone with a role in responding to the emergency. Continuous improvement by eliminating points of vulnerability and applying lessons learned is an essential component of incident response.

Centralized reporting serves the goal of increasing awareness of vulnerabilities and threats to state government as a whole. In particular, centralized reporting is necessary to discern patterns, identify areas of vulnerability, allocate resources, and develop statewide solutions. Centralized reporting does not substitute for internal reporting to management, reporting to law enforcement, or mobilizing a computer security incident response team (CSiRT). Agencies should develop procedures for internal and external reporting that will meet the needs of centralized reporting with little or no additional work. The centralized reporting is designed to mesh with the postmortem analysis that should follow each incident.

Security incident response should never include retaliation. Defending a system should

emphasize preventing security breaches. If there is an intrusion, a defensive response should focus on containing and eradicating the problem, plugging the security hole and getting back to business. Security incident response should never include striking back against attackers. The appropriate law enforcement authorities should handle all punitive actions.

Applicability

These guidelines apply to all non-education state agencies, boards, and commissions, which receive a direct appropriation from the Legislature or any state agency that has a direct connection to the state's network. Educational institutions and other entities are encouraged to develop their own security incident and centralized reporting procedures.

Planning and Preparation

Develop an incident response plan and designate people to carry it out. The plan should include details for how you will:

1. Detect the incident
2. Analyze the incident
3. Contain or eradicate the problem
4. Provide workarounds or fixes
5. Prevent re-infection
6. Log events
7. Preserve evidence
8. Conduct a post-mortem and apply lessons learned

Educate users to raise security awareness and promote security policies. Build a centralized incident reporting system. Establish escalation procedures that lay out actions the agency should take if an attack turns out to be protracted or especially damaging. Make sure your service-level agreements include provisions for security compliance, and spell out reporting requirements and maintenance of systems (including contingency plans) in the event of a cyberattack. Decide in advance under what circumstances you would call the authorities. Plan how and when employees, customers and strategic partners will be informed of the problem. Establish communication procedures, if the media become involved.

Have a single contact to whom employees should report suspicious events and who will track changes in contacts or procedures. Have a single contact that will report incidents to outside agencies, including law enforcement, regulatory bodies and information sharing organizations such as InfraGard.

Keep a list of the incident response team members' names, titles and 24/7contact information, along with their role in a security breach. Have contact information for vendors contracted to help during a security emergency, as well as ISPs and other relevant technology providers. Have contact information for major customers and clients who might be affected. In advance, establish contacts at the relevant law enforcement agencies: typically, the national infrastructure protection and computer intrusion squad

at the local FBI field office; the electronic crimes investigator at the local Secret Service field office; and the electronic crimes investigator at the Nebraska State Patrol. Have their contact information easily accessible.

Perform a risk analysis on your plan. Test and rehearse procedures periodically. Develop contingency Plans in case your response infrastructure is attacked.

What to Report

The ultimate goal of security incident response and centralized reporting is to protect data and prevent obstruction of government operations. It is important to distinguish between problems that stem from mistakes or miscommunications and true security incidents that involve either malicious intent or intent to circumvent security measures. Security incident reporting should be used only for true security incidents. You should report events that have a real impact on your organization (such as when damage is done, access is achieved by the intruder, loss occurs, web pages are defaced, malicious code is implanted) or when you detect something noteworthy or unusual (new traffic pattern, new type of malicious code, specific IP as source of persistent attacks). Do not report routine probes, port scans, or other common events.

A security incident includes, but is not limited to the following events, regardless of platform or computer environment:

1. Evidence of tampering with data;
2. Denial of service attack on the agency;
3. Web site defacement;
4. Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources);
5. Social engineering incidents;
6. Virus attacks which adversely affect servers or multiple workstations;
7. Other incidents that could undermine confidence and trust in the state's information technology systems.

When and How to Report an Incident

If an attack is under way, you should call your previously established law enforcement contact immediately and communicate the basic information that is included in the Computer Incident Reporting Short Form. There is additional information that will be required to effectively conduct the investigation (see bullet points below), but the form is a good place to start. Sometimes you will report an incident to law enforcement after the fact—you have detected that something happened, but your systems are functioning normally and whatever damage is likely has already been done. In this case, you will want to gather as much information as possible for the law enforcement agents before you make the call. Here is some additional information that will help law enforcement agents in their investigation:

1. What are the primary systems involved?
2. How was the attack carried out?
3. What steps have you taken to mitigate or remediate?
4. Does a suspect exist? If so, is it a current or former employee/contractor?
5. What evidence is available to assist in the investigation (e.g., log files, physical

evidence, etc.)? To track the status of your case once you've filed a report, contact the field office that is conducting the investigation.

Who to Notify

FBI – Omaha Office
InfraGard Coordinator
Phone (405) 290-3685
Fax (405) 290-3885
infragard-om@fbi.gov

Nebraska State Patrol
Capt. Robert E. Thorson
Investigative Services
Nebraska State Patrol
1600 Highway 2
Lincoln, Nebraska 68509-4907
Ph. 402-479-4947; Fax:
rthorson@nsp.state.ne.us

Sgt. Scott Christensen
Coordinator
Internet Crimes Against Children Unit
Nebraska State Patrol - Omaha
4411 So. 108th Street
Omaha, Nebraska 68137
Ph. 402-595-2410; Fax: 402-697-1409
24 hr dispatch number is 402-331-3333.
schriste@nsp.state.ne.us
www.nsp.state.ne.us

Office of the CIO / NITC (state agencies, only)
Steve Schafer
Chief Information Officer
521 South 14th Street, Suite 200
Lincoln, Nebraska 68508-2707
Ph. 402-471-4385; Fax: 402-471-4608
slschafe@notes.state.ne.us

Step-by-step procedure(s)

The Incident Response and Centralized Reporting Procedure for State Government requires that the agency implement the following steps for a complete security incident handling process.

1. Establish general procedures for responding to incidents;
2. Prepare to respond to incidents;
3. Analyze all available information to characterize an incident;
4. Communicate with all parties that need to be made aware of an incident and its

progress;

5. Collect and protect information associated with an incident;
6. Apply short-term solutions to contain an incident;
7. Eliminate all means of vulnerability pertaining to that incident;
8. Return systems to normal operation;
9. Closure: Identify and implement security lessons learned.

Step 1: Establish a computer security incident response team (CSIRT) that can take responsibility for managing security incidents. The CSIRT can be a virtual team that includes people with a wide range of expertise. Agencies should consider forming a CSIRT that serves multiple entities. A clear description of roles and expectations is essential.

Step 2: Set methods for placing the CSIRT on alert status and ready to take preventative measures. It should include procedures for activating the team once an incident occurs.

Step 3: Identify and understand the incident. Use the Information Systems Administrator's Incident Reporting form to document the incident.

Step 4: Contact managers and users affected by an incident, security personnel, law enforcement agencies, vendors, the CERT Coordination Center (**http://www.cert.org/**), and other CSIRTs external to the organization as necessary. It is essential that each agency establishes and follows a single channel of communication. Multiple sources of information while the incident is underway creates confusion, interrupts the work of the response team, and increases vulnerability if the perpetrator is monitoring communications within the agency. It is required that the Computer Incident Reporting Short Form be completed and forwarded to the Nebraska State CIO.

Step 5: Collect and preserve as much evidence in its original form as possible. Take detailed notes of all evidence found and record each piece of evidence. It is important not to rush. Be aware not to destroy or modify any evidence. If necessary, use low-level copying methods to make a complete copy of the disk and memory state of the affected host(s).

Step 6: As necessary the CSIRT should, (A) physically isolate the affected host(s); (B) change all passwords or disable all accounts on all systems to which the attacker may have had access; (C) disable access to compromised file or date systems that are shared with other computers. Continue to monitor system and network activities

Step 7: The CSIRT should review local operating system and configuration files for signs of intrusion and remove any means for intruder access including changes made by an intruder. Next, determine if there are uncorrected system or network vulnerabilities and correct them. Last, improve protection mechanisms to limit the exposure of networks and systems.

Step 8: Determine the requirements and timeframe for returning the system to normal operation. Members of the CSIRT should restore the operating system, applications

and data from trusted media and reconnect the restored system to the network. The CSIRT should validate the restored system for potential vulnerabilities.

Step 9, "Closure" is intended to give the organization an opportunity to learn from the experience of responding to an incident. Every successful intrusion or other incident indicates potential weaknesses in systems, networks, operations, and staff preparedness. These weaknesses provide opportunities for improvement. Steps should include the following points (from CERTCC security practices, http://www.cert.org/security-improvement/practices/p052.html):

1. Hold a post mortem analysis and review meeting with all involved parties. Do this within three to five working days of completing the investigation of an intrusion. Use the attached Information Systems Administrator's Incident Reporting Form to gather information and guide discussion.
2. Prepare a final report for senior management. This ensures awareness of security issues. Use either the Computer Incident Reporting Short Form or the Information Systems Administrator's Incident Reporting Form to report information about the security incident to the Office of the Chief Information Officer. Incidents should be reported no later than 5 working days after returning systems to normal operation.
3. Revise security plans and procedures and user and administrator training to prevent future incidents. Include any new, improved methods resulting from lessons learned.
4. Determine whether or not to perform a new risk analysis based on the severity and impact of an intrusion.
5. Take a new inventory of your system and network assets.
6. Participate in investigation and prosecution, if applicable.

Related Rules

Draft security standards for the federal Health Insurance Portability and Accountability Act (HIPAA) would establish administrative procedures to guard data integrity, confidentiality, and availability. These include security incident procedures (45 CFR Part 142.308 (a)(9):

"(9) Security incident procedures (formal documented instructions for reporting security breaches) that include all of the following implementation features:

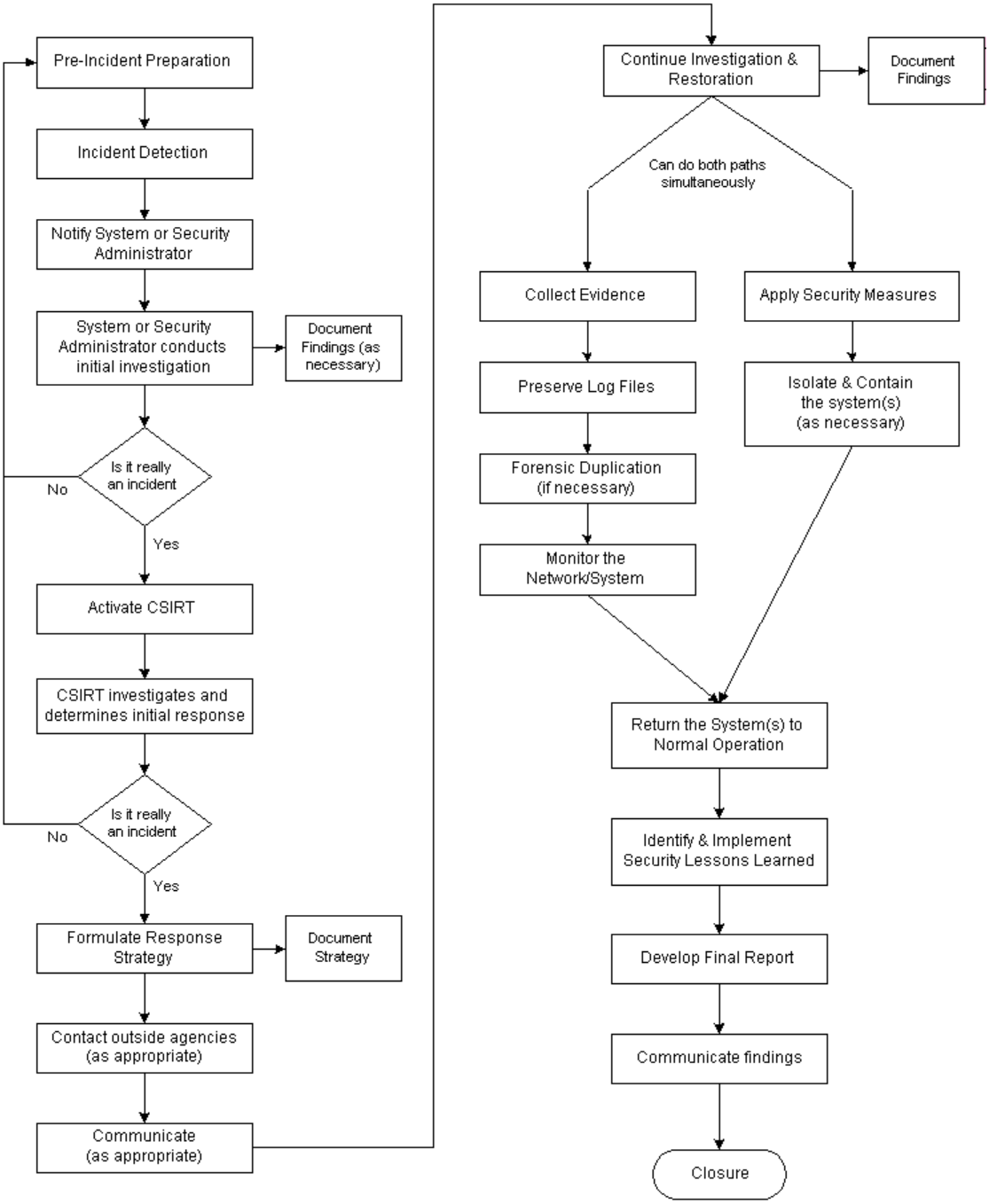
"(i) Report procedures (documented formal mechanism employed to document security incidents).

"(ii) Response procedures (documented formal rules or instructions for actions to be taken as a result of the receipt of a security incident report)."

Attachments/ Forms

Incident Response Process Flow Chart
Computer Incident Reporting Short Form
Information Systems Administrator's Incident Reporting Form

Incident Response Process



COMPUTER INCIDENT REPORTING SHORT FORM

Use this form to report incidents to the Office of the Chief Information Officer of the State of Nebraska. State agencies should send an electronic copy to slschafe@notes.state.ne.us, or fax it to (402) 471-4608. This form also outlines the basic information that law enforcement needs on a first call.

STATUS

☐ Site Under Attack ☐ Past Incident ☐ Repeated Incidents, unresolved

CONTACT INFORMATION

Name_____Title_____
Organization_____
Direct-Dial Phone_____E-mail_____
Legal Contact Name_____Phone_____
Location/Site(s) Involved_____
Street Address_____
City_____State_____ZIP_____
Main Telephone_____Fax_____
ISP Contact Information_____

INCIDENT DESCRIPTION

☐ Denial of Service
☐ Distributed Denial of Service
☐ Intrusion/Hack
☐ Malicious Code (virus, worm)
☐ Misuse of Systems (internal or external) (Includes inappropriate use by employees)
☐ Probe/Scan
☐ Unauthorized Electronic Monitoring (sniffers)
☐ Website Defacement
☐ Other (specify)_____

DATE/TIME OF INCIDENT DISCOVERY

Date_____Time_____
Duration of Attack_____

IMPACT OF ATTACK

☐ Loss/Compromise of Data
☐ Damage to Systems
☐ Financial Loss (estimated amount: $_____)
☐ Damage to the Integrity or Delivery of Critical Goods, Services or Information
☐ System Downtime
☐ Other Organizations' Systems Affected

SEVERITY OF ATTACK, INCLUDING FINANCIAL LOSS OR INFRASTRUCTURE

☐ High ☐ Medium ☐ Low ☐ Unknown

SENSITIVITY OF DATA

☐ High ☐ Medium ☐ Low ☐ Unknown

How did you detect This?_____
Have you contacted law enforcement about this incident before? Who & when?_____
Has the incident been resolved? Explain_____

State of Nebraska
Information Systems Administrator's Incident Reporting Form

Point of Contact Information

Name	
Title	
Telephone/Fax Numbers	
Email	
Agency	

B. Incident Information

1. Background Information:	
a. Agency (if same as above, enter "SAME":	
b. Physical Location(s) of affected computer system/network (be specific):	
c. Date/time of the incident:	
d. Duration of the incident:	
e. Is the affected system/network critical to the agency's mission? (Yes/No)	

2. Nature of Problem (check all that apply):	
a. Intrusion	
b. System impairment/denial of access	
c. Unauthorized root access	
d. Web site defacement	
e. Compromise of system integrity	
f. Hoax	
g. Theft	
h. Damage	
i. Unknown	
j. Other (provide details in remarks)	
k. REMARKS:	

3. Has your agency experienced this problem before? (Yes/No; If yes, please explain in the remarks section.)
a. REMARKS:

4. Suspected method of intrusion/attack:	
a. Virus (provide name, if known)	
b. Vulnerable exploited (explain)	
c. Denial of Service	
d. Trojan Horse	
e. Distributed Denial of Service	
f. Trapdoor	
g. Unknown	
h. Other (Provide details in remarks)	
i. REMARKS:	

5. Suspected perpetrator(s) or possible motivation(s) of the attack:	
a. Insider/Disgruntled Employee	
b. Former employee	
c. Other (Explain remarks)	
d. Unknown	
e. REMARKS:	

6. The apparent source (IP address) of the intrusion/attack:

7. Evidence of spoofing (Yes/No/Unknown)

8. What computers/systems (hardware and software) were affected (Operating system, version):	
a. Unix	
b. OS2	
c. Linux	
d. VAX/VMS	
e. NT	

f. Windows	
g. Sun OS/Solaris	
h. Other (Please specify in remarks)	
i. REMARKS:	

9. Security Infrastructure in place. (Check all that apply)	
a. Incident/Emergency Response Team	
b. Encryption	
c. Firewall	
d. Secure Remote Access/Authorization Tools	
e. Intrusion Detection System	
f. Security Auditing Tools	
g. Banners	
h. Packet filtering	
i. Access Control Lists	
j. REMARKS:	

10. Did intrusion/attack result in a loss/compromise of sensitive or information classified as private?	
a. Yes (provide details in remarks)	
b. No	
c. Unknown	
d. REMARKS:	

11. Did the intrusion/attack result in damage to system(s) or data?	
a. Yes (provide details in remarks)	
b. No	
c. Unknown	
d. REMARKS:	

12. What actions and technical mitigation have been taken?

a. System(s) disconnected from the network?	
b. System Binaries checked?	
c. Backup of affected system(s)?	
d. Log files examined?	
e. Other (Please provide details in remarks)	
f. No action(s) taken	
g. REMARKS:	

13. Has law enforcement been notified? (Check all that apply.)	
a. Yes-local law enforcement	
b. Yes-Nebraska State Patrol	
c. Yes-FBI field office	
d. Not	
e. REMARKS:	

14. Has another agency/organization been informed as assisted with the response?	
a. Yes-Information Management Services	
b. Yes-Division of Communications	
c. Yes-CERT-CC	
d. Yes-Other (provide details in remarks)	
e. No	
f. REMARKS:	

15. Additional Remarks:

If the reported incident is a criminal matter, you may be contacted by law enforcement for additional information.

C. Closure Information (Optional, Except 9 & 10)

1. (Optional) Did your detection and response process and procedures work as intended? If not, where did they not work? Why did they not work?
REMARKS:

2. (Optional) Methods of discovery and monitoring procedures that would have improved your ability to detect an intrusion.
REMARKS:

3. (Optional) Improvements to procedures and tools that would have aided you in the response process. For example, consider using updated router and firewall filters, placement of firewalls, moving the compromised system to a new name or IP address, or moving the compromised machine's function to a more secure area of your network.
REMARKS:

4. (Optional) Improvements that would have enhanced your ability to contain an intrusion.
REMARKS:

5. (Optional) Correction procedures that would have improved your effectiveness in recovering your systems.
REMARKS:

6. (Optional) Updates to policies and procedures that would have allowed the response and recovery processes to operate more smoothly.
REMARKS:

7. (Optional) Topics for improving user and system administrator preparedness.
REMARKS:

8. (Optional) Areas for improving communication throughout the detecting and response processes.
REMARKS:

9. (Required) A description of the costs associated with an intrusion, including a monetary estimate if possible.
REMARKS:

10. (Required) Summary of post mortem efforts.
REMARKS: