8-802. Incident response plan.

All agencies that process, store, or access CONFIDENTIAL or RESTRICTED information are required to maintain an incident response plan. This plan must include operational and technical components, which provide the necessary functions to support all the fundamental steps within the incident management life cycle, including the following:

(1) Preparation.

(a) A security incident is any adverse event whereby some aspect of the state infrastructure is threatened (e.g., personal violation, loss of data confidentiality, disruption of data integrity, denial of service, security breach). It is important to note that even if there is no evidence of information being accessed by unauthorized personnel, exposing sensitive information in an unsecure manner is considered a security incident. For example, any unencrypted email containing CONFIDENTIAL or RESTRICTED information (e.g. Federal Tax Information, Personally Identifiable Information) sent outside the secured state network is a security incident and should be reported as such.

(b) All security incidents must be reported to the state information security officer, agency management, and the Office of the CIO Service Desk immediately. Security incidents will be tracked by the state information security officer. Any state staff who observe, experience, or are notified of a security incident, should immediately report the situation to the agency information security officer, state information security officer or the Office of the CIO Service Desk, but at the very least to their supervisor. All state management are responsible to ensure that their staff understand that awareness of the incident are to be reported immediately.

(c) State Information Security Officer and Agency Information Security Officer.

The security officers are responsible for assembling, engaging, and overseeing the incident response team. They will coordinate the management of security incidents and any identified follow-up activity, remediation, or countermeasures. They are also responsible for taking lead with information technology personnel to perform analysis and triage of incident impact and reportable conditions.

The security officers will finalize and sign off on any security incident reports, and determine follow-up activity, root cause analysis, long term mitigation, and updates to the security awareness training.

Agency information security officers are also responsible for ensuring that all technical areas within the agency have an understanding and ability to meet this standard. They are required to

perform education and training of this standard to all applicable agency personnel, and then test the incident response process annually.

(d) Incident Response Team.

The state information security officer will identify key personnel who will serve as members of the state incident response team. This team will be made up of knowledgeable staff that can rapidly respond to, manage, and support any suspected incident to minimize damage to state information systems, networks and data by identifying and controlling the incident, properly preserving evidence, and reporting to appropriate entities. This team may change from time to time, depending on the nature of the incident and the skills necessary to recover from it. Agencies may also identify additional incident response teams for their specific environment. The state information security officer or agency information security officer will maintain a contact list which includes the names, telephone numbers, pager numbers, mobile telephone numbers, email addresses, organization names, titles, and roles and responsibilities for all potential key incident response resources. Key responsibilities for the incident response team include:

(i) The state's priority is "prevention over forensics." In other words, do not allow a damaging incident to continue so that additional evidence may be collected;

(ii) Conduct the initial triage. Perform a damage and impact assessment and document the findings;

(iii) Report to state of agency management on a regular schedule with status and action plans;

(iv) Maintain confidentiality of the circumstances around the incident;

(v) Follow procedures to maintain a chain of trust and to preserve evidence;

(vi) Initiate the root cause analysis; bring in other resources as necessary; and

(vii) Initiate return to normal operations; bring in other resources as necessary.

(e) Incident Management Procedures.

Incident management procedures require, first and foremost, prevention of damage from the incident over forensics. This means that the priority is to shut off or terminate any potential damaging threat. It is strongly desired to perform this action in a manner that allows for detailed forensics or preservation of evidence, but if there is ANY doubt, all state personnel, whether employees or contractors, are required to disable the threat immediately. Following the assessment and termination of the threat, the next priority is containment, followed by recovery actions, damage determination, report documentation, lessons learned, and implementation of corrective actions.

All communication related to the incident should be carefully managed and controlled by the Office of the CIO and agency senior management. All personnel involved any incident management support activity will communicate only with the parties necessary for incident analysis or recovery activity, and to the state information security officer, Office of the CIO, or the agency information technology team. No other communication, unless explicitly authorized, is allowed.

A security incident report is classified as RESTRICTED information.

(f) Incident Management Training and Testing.

Annually, the state information security officer and agency information security officers shall provide training for appropriate identification, management, and remediation of an incident and shall facilitate a simulated incident response and recovery test for the state or agency security incident response team. This test will simulate a variety of security related incidents.

(2) Incident Triage and Identification.

As soon as an incident is suspected, personnel qualified and designated to respond shall be notified to take immediate action, determine incident impact, file a ticket, or prepare a report.

Initial triage will be conducted by the state information security officer/agency information security officer, Office of the CIO Service Desk, or the information technology team to understand the scope and impact of the incident and initiate appropriate action. Once an incident has been identified and reported, the state information security officer/agency information security officer will assume oversight of the incident response and will continually assess the incident conditions and determine if escalation of response actions is appropriate. Prevention of damage is given priority over forensics of incident source. Therefore, the state information security officer/agency information security officer and IT management may quarantine any potentially threatening system and terminate any threatening activity. The state information security officer will ensure that a security incident report is completed for all incidents.

For more complicated incidents that may require further analysis, the incident response team will be assembled via direction from the state information security officer, Office of the CIO, agency information security officer, or agency IT management. This team will take over the triage and impact assessment process.

A damage analysis of security incidents is to be initiated immediately after assessment by the state information security officer or the incident response team. They will determine if the incident impacts organizations outside of the agency's internal network. They will also determine if any reportable conditions, such as unauthorized disclosure of CONFIDENTIAL or RESTRICTED information exists. If the incident appears to have any citizen information compromised, immediate notification to the agency management, state information security officer, and agency information security officer is required. Agency management will oversee and coordinate all communication actions.

All forms of unauthorized disclosure of CONFIDENTIAL or RESTRICTED information, including the potential for unauthorized disclosure (such as information spillage), will be considered incidents. Information spillage refers to instances where either CONFIDENTIAL or RESTRICTED information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, an incident has occurred and corrective action is required.

(3) Incident Containment.

Any IT resources that are engaged in active attacks against other IT resources must be isolated and taken off the state network immediately. Incidents involving the exposure, or potential exposure, of CONFIDENTIAL or RESTRICTED information to unauthorized parties must also be contained immediately. Other compromises must be contained as soon as practical, considering impacts of service interruptions, recovery of equipment, and potential impacts of the incident itself.

Containment can be achieved by immediately disconnecting the resource from the network, revoking user access, or other means as appropriate. The state information security officer has the authority to coordinate with the Office of the CIO to block compromised services and hosts that present a threat to the rest of the state network. Notifications of outages or service interruptions will follow normal Office of the CIO or agency procedures if possible, but will not delay the outage or interruption if an attack or breach is underway or if the threat of an attack or breach is imminent.

(4) Incident Communication.

Reportable conditions, such as the breach of PHI, PII or FTI, require notification within specific timeframes as defined in state and federal law. It is the responsibility of the state information security officer and agency information security officers to understand these requirements and ensure the state and agency remain compliant in the event of a reportable incident.

Additionally, communication during a security incident must be carefully controlled to ensure that information that is disclosed is accurate, timely, and provided only to appropriate audiences.

It is the responsibility of the state information security officer, agency information security officer, Office of the CIO, and agency management to ensure that all communication regarding any security incident is managed and controlled.

(5) Preservation of Evidence.

In the event of a discovery of a breach of system security protections, an internal security investigation must be properly performed to preserve evidence. If the incident involves any type of law enforcement, the incident response team will work with law enforcement to secure the potential evidence without reviewing additional content. Network hardware, software or data may be considered potential evidence.

The chain of custody steps that should be taken to preserve all potential evidence in the event of a security breach are as follows:

(a) If possible, isolate the system from the network, either physically (unplug the network cable), or logically. Do NOT power the system off. Evidence in system memory may be lost;

(b) If the system cannot be taken off the network, take pictures and screenshots;

(c) Notify the agency information security officer immediately after initial steps, but no later than one hour after becoming aware of the possible incident;

(d) Make a bit copy of the drive before investigating (e.g., opening files, deleting, rebooting);

(e) Dump memory contents to a file;

(f) Label all evidence; and

(g) Log all steps.

(6) Incident Documentation and Root Cause Analysis.

An incident report is required for all incidents except those classified as having a low impact to the state network. The incident report should include entry of the root cause, actions taken and any remediation or mitigation strategy to reduce the risk of recurrence. Depending on the nature of the security incident, a post-mortem meeting may be conducted.

Documentation of information is critical in situations that may eventually involve authorities as well as provides documentation of the actions taken to resolve the event. Incident reports are RESTRICTED information.

A formal root cause analysis must be performed within two weeks of the occurrence of the incident. This analysis should identify the core issues of the incident in the affected environment and actions that can be taken to address these issues. This can include physical, logical, or environmental changes, operational or administrative control changes, or enhanced training, education, or awareness programs.

(7) Incident Recovery and Permanent Remediation.

The incident response team, working with technology, application and data owners, shall evaluate and determine when to return compromised systems to normal operations. Access to compromised systems will be limited to authorized personnel until the security incident has been

contained and root cause mitigated. Analysis and mitigation procedures must be completed as soon as possible, recognizing state systems are vulnerable to other occurrences of the same type.

The Office of the CIO, state information security officer, and agency information security officer shall define and prioritize the requirements to be met before returning an affected or compromised system to normal operations.

Recovery procedures:

(a) Reinstalling compromised systems from trusted backup-ups, if required;

(b) Reinstalling system user files, startup routines, or settings from trusted versions or sources, if required;

(c) Validating restored systems through system or application regression tests, user verification, penetration tests, and vulnerability testing and test result comparisons; and

(d) Increasing security monitoring and heighten awareness for a recurrence of the incident.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-802.pdf