California
DEPARTMENT OF TECHNOLOGY
Office of Information Security

(916) 445-5239
HTTPS://CDT.CA.GOV/SECURITY/

INSIDER THREATS
INFORMATION SHEET NO. 5
MAY 2017 (REVISED)

The Hostile Takeover

Time for some introspection. Do your disaster recovery and incident response plans consider a rogue insider who commandeers your network? Is this a risk your organization has assessed and taken steps to mitigate? Recent events in the media about the "Insider Threat" validate the need for more thoughtful attention to the assessment and mitigation of a "hostile takeover" and other security risks associated with insider threats. If there was ever a time to "trust but verify", it is now.

The following are some proactive steps that will help minimize the likelihood that this may occur to your organization and additional guidance on post-event actions to take if an organization finds themselves in this situation.

Human Resources Perspective

- Screening: Satisfactory character references, confirmation of claimed academic and professional qualifications, identity check, credit/criminal background check.
    - Consider re-occurring background checks or supplemental arrest/criminal conviction notices.
- Terms and conditions of employment:
    - Subscribe to a code of conduct that covers ethics, appropriate use and reputable practices expected.
    - Clearly define the roles, responsibilities, and boundaries (e.g., network administration versus server administration versus other security/audit) for the employee/contractor upfront.
    - Have employee/contractor acknowledge their receipt of agency policies and understanding of their responsibilities by signing confidentiality or non-disclosure agreements, and acceptable use and code of conduct agreements prior to being given access to any facility/system.
    - Identify actions to be taken if employee/contractor disregards the organization's security requirements.
- Level of position: Assign responsibility to an exempt high-level technical supervisory/management position.

Management Responsibilities

- Implement segregation of duties where appropriate to reduce the risk of negligent or deliberate system misuse. Care should be taken so that no single person can access, modify, or use assets without authorization or detection. Where difficult to segregate, implement additional monitoring controls, audit trails, and management supervision.
- Establish a fully trained backup for each key information technology function/role. Manager's should ensure that system documentation is maintained, and that multiple staff have been trained to support key systems, so that no single employee is considered the only "go to" person for resolving issues with an agency's critical systems.
- Document your expectations and share with the employee.
- Provide continuous performance evaluation and feedback to the employee.
- At the first sign of performance issues, take steps to protect your systems and minimize any potential damage (e.g., build a back door in case the employee takes control, limit the employee's access, closely monitor actions taken by the employee).
- Use a team management versus individual management approach – Example: Well trained employees will know how to recognize and report potential problems introduced by outsiders or insiders.
- Properly manage changes of responsibility or employment (transfer or separation from the agency) following a risk-based approach. Ensure immediate termination of access for separated employees.
- Implement strict change management controls on operating systems and application software.
- Limit access to assets to authorized personnel who require these assets in the performance of their assigned duties.
- Review authorizations for special privilege access rights more frequently (e.g., every three months versus every six months).
- Check privilege allocations to ensure that unauthorized privileges have not been obtained.
- Review logs for changes to privileged accounts and for inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls).
- Conduct routine independent risk vulnerability assessments/audits to provide early warning of potential problems. Security audit function must remain independent.
- Develop and implement an incident response plan.

Technology Perspective

- Establish central logging, an appropriate log retention policy and the faculties to ensure they are reviewed. Properly secure logs by offloading in read-only mode to prevent against modifications or deletions.
- Implement logical network segmentation (where possible two individuals with separate keys). Build a multi-layer security perimeter around the network.

- Establish a routine backup procedure that includes all network device configurations. Regularly test as part of your Disaster Recovery Plan.
- Establish delegated accounts for administrators (Tacacs, Radius or like product).
- Establish a password management policy for group devices and ensure appropriate staff have access, and provide for administrator/service account password expiration.
- Implement recording and alerting for the use of special system privileges (e.g., when network administrator password is changed notification is provided to a select security/audit group).
- Implement regular auditing of administrative accounts, information security management representation and oversight in the configuration management process and approval on all production changes.
- Implement data encryption strategy for confidential and sensitive information to prevent unauthorized access. Key management should be in place to support the use of these techniques.

Post Event Actions

Should a situation like this occur within your agency, your incident response plan should include the following important steps.

1) Conduct initial assessment of the situation. Implement your incident response plan. The security incident response team can best assist law enforcement by carefully preserving a crime scene. In this case the scene could stretch across the WAN. The main objective will be to document initial findings without altering the state of computer-based evidence. It is highly recommended that you seek the assistance of a certified computer forensic specialist.
2) Consider having each member of the incident response team, and any other individuals directly involved in the management of the incident, sign a confidentiality or non-disclosure statement.
3) State policy requires state entities to make notification to the California Office of Information Security (OIS) and the California Highway Patrol (CHP) immediately following discovery of an incident. Each state entity's Chief Information Officer (CIO), Information Security Officer (ISO), or the assigned incident reporting personnel (as designated on the Cal-CSIRS Designee Request (Incident Management) [XLSX]), collectively hereinafter referred to as authorized California Compliance and Security Incident Reporting System (Cal-CSIRS) user, is responsible for notifying the proper authorities.

   Immediately report the incident through the Cal-CSIRS. Cal-CSIRS will require specific information about the incident and will notify the OIS and the CHP Computer Crimes Investigation Unit (CCIU). A system generated e-mail confirmation will be sent to the authorized Cal-CSIRS users acknowledging the OIS and CCIU have received the Cal-CSIRS notification.

   IMPORTANT: Incident notification made to CHP or our Office outside of the Cal-CSIRS notification process by email or other means is NOT an acceptable

substitute for the required notification through Cal-CSIRS. Specific direction for reporting incidents can be found on OIS's Web site at https://cdt.ca.gov/security/policy/#Incident-Management.

4) Containment. It is imperative to recognize, protect, seize, and search the devices in accordance with applicable statutes, policies and best practices and guidelines. Depending on the situation and at law enforcement's direction, be prepared to do one or more of the following:
    a. Collect computer access policies and procedures, legal notifications (e.g., login banners, etc.)
    b. Collect all relevant logs, files, source code, hard drives, media, etc.
    c. Disconnect the device from the network.
    d. Suspend business retention rules for electronic and paper records involved in the incident.
    e. Set aside backup tapes (removing them from the normal tape cycle) so that valid evidence is not inadvertently overwritten.
    f. Preserve the state of the computer by making a backup copy of the system, logs, damaged or altered files, and/or files left by the intruder to new (unused) media.
    g. If attack is in progress, activate auditing in software and/or possibly keystroke monitoring software.
    h. Begin tracking and documenting losses suffered:
        i. Number of hours spent on response/recovery activity
        ii. Cost associated with hiring outside help/experts
        iii. Cost to replace damaged equipment
        iv. Loss of revenue/productivity
        v. Value of data lost
5) Document all steps taken in the initial assessment and in reviewing any logs or files. If at all possible, determine the normal function and level of activity on the network and computers before the event to detect the anomalies post-hack. Provide this documentation to CHP or the certified forensic specialist.
6) Brief executive management. Keep executive management informed, including your human resources, legal staff and other key stakeholders, as appropriate by involving them in key decision-making points.
7) Recovery. Review the Disaster Recovery Plan, and follow the strategy and steps for recovery. Begin procedures to rebuild the system, if necessary, and place it back into production.

Resources

- OIS – https://cdt.ca.gov/security/policy/#Incident-Management (Incident Management)
- State Administrative Manual (SAM) Chapter 20000 – Internal Controls Section 20050 – http://sam.dgs.ca.gov/TOC/20000.aspx
- SAM Security and Privacy Chapter 5300 - http://sam.dgs.ca.gov/TOC/5300.aspx
- ISO 27002 - http://www.iso27001security.com/html/27002.html

- California Government Code 13400 – 13407 - https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=GOV&division=3.&title=2.&part=3.&chapter=5.&article=
- National Institute of Standards and Technology (NIST) Special Publication 800-61, Computer Security Incident Handling Guide - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- NASCIO Publications, http://www.nascio.org/publications/
    - *Insider Security Threats: State CIOs Take Action Now!*, April 2007
    - *The Workforce Evolution: Recruiting and Retaining State IT Employees*, April 2008
- SANS – http://www.sans.org/reading_room/whitepapers/incident/