MITIGATION

KNOW AND PROTECT YOUR CRITICAL ASSETS

Identify and document your critical assets and infrastructure (e.g., valuable property, proprietary information, data, and other physical, technical, and human resources). Assess potential risks, threats, and vulnerabilities, and identify high-value targets to prioritize your insider threat prevention and mitigation strategy.

ACTION STEPS

+ Conduct a risk assessment to identify your most important assets, potential threats, and the consequences of critical infrastructure being damaged or stolen.
+ Consider threats from insiders and business partners in enterprise-wide risk assessments.
+ Use assessment results to develop and prioritize security goals in your overall mitigation strategy.

MITIGATION

ESTABLISH POLICIES AND PROTOCOLS FOR ADDRESSING THREATS

Use best practices to develop insider threat policies that include HR, legal counsel, security, management, and internal affairs. Connect policies, procedures, and protocols to the overall safety and security of your organization.

ACTION STEPS

+ Enforce policies consistently to demonstrate fairness and prevent any favoritism or injustice.
+ Ensure that leadership and senior management advocate and comply with all organizational policies, procedures, and expectations.
+ Reinforce key directives and codes of conduct through ongoing communication and education.

MITIGATION

DEVELOP A FORMALIZED COUNTER-INSIDER THREAT (C-INT) PROGRAM

A C-InT program includes actionable information, guidance, and protocols to proactively detect potential threats, deter progression through effective interventions, and mitigate the consequences of a harmful act. Effective programs utilize a multidisciplinary team of internal and external stakeholders, and empower everyone to take shared responsibility for the organization's safety and security.

ACTION STEPS

+ Ensure program alignment with policies for addressing threats.
+ Designate a multidisciplinary insider threat team to support effective incident response capabilities.
+ Develop a confidential process for reporting threatening or concerning behaviors and actions.
+ Document incident management; assess, manage, and mitigate all reported concerns.

MITIGATION

INTEGRATE INSIDER THREAT AWARENESS INTO SECURITY TRAINING FOR EMPLOYEES

Increase organizational awareness of the warning signs and indicators of potential insider risk. Use regular training to reinforce cultural principles, and emphasize the shared responsibility to speak up, allowing for proactive intervention and mitigation measures.

ACTION STEPS

+ Develop and implement a training program that discusses diverse topics related to insider threat.
+ Design foundational curricula for all levels of employees, as well as specialized training for leadership and threat assessment team members.
+ Use training to reinforce a culture of trust and shared responsibility; encourage employees to feel safe speaking up about behavioral concerns.

MITIGATION

EMPLOY SAFE HIRING AND ONBOARDING PRACTICES

Reducing insider risk begins with your hiring process. Every potential new hire should go through a rigorous interview process and be subject to a thorough background check. When interviewing and onboarding new employees, ensure that conduct and performance expectations are clearly documented and understood.

ACTION STEPS

+ Ensure potential employees, contractors, and vendors have undergone a background investigation, including: a criminal background check, credit check, and education/employment history.
+ Employ a comprehensive vetting process for positions with security clearance, access to national intelligence, and frequent foreign travel and relationships.
+ Communicate clear guidelines for acceptable behavior, dress code, computer usage, career development, nondisclosure agreements, and when and how to notify HR, security, and others of potential violations or concerns.

MITIGATION

PROTECT AND SECURE YOUR PHYSICAL ENVIRONMENT

It is important to protect your physical environment and critical infrastructure, and keep employees, contractors, and visitors safe from internal and external threats. Always safeguard the environment with active security protocols and protective measures at all points of entry and exit hallways, elevators, lobbies, stairwells, and parking lots.

ACTION STEPS

- Employ strict access control measures and require all employees, contractors, vendors, and visitors to wear organizational badges to access areas of the office environment.
- Use alarms to notify security if unauthorized individuals attempt to access the premises.
- Use video surveillance or closed-circuit television to monitor facility entrances and exits and other critical infrastructure.

MITIGATION

PREVENT AND MITIGATE WORKPLACE CONFLICTS AND CONCERNS

If employees experience conflict or other workplace issues, they should feel comfortable talking to managers or HR without fear of negative consequences. Establish several ways to report concerns, and be transparent about the steps to address and resolve issues related to performance, work relationships, and job satisfaction.

ACTION STEPS

+ Investigate and document all suspicious or disruptive behavior.
+ Implement an Employee Assistance Program to provide support to employees dealing with personal stressors.
+ Train managers to recognize and respond to employees' concerning or inappropriate behavior and address the problem before it turns into a serious risk.
+ Provide safe, anonymous communication outlets for employees to address workplace conflicts or report security incidents or other concerns; provide incentives for speaking up.

MITIGATION

DEVELOP SOUND PASSWORD AND ACCOUNT MANAGEMENT PROTOCOLS

Protect your organization's computer network and confidential data from theft or sabotage with secure password- and account-management protocols. Strict network access control and ongoing monitoring can impede unauthorized access and detect targeted social engineering attacks and suspicious employee actions or account activity.

ACTION STEPS

+ Require employee passwords to be strong and changed at regular intervals; employees should never share their passwords with anyone else.
+ Program computers to automatically log off after a period of inactivity on the system.
+ Perform regular audits of the network to identify any unauthorized or backdoor accounts, or accounts and passwords known by terminated employees or former partners.

MITIGATION

IMPLEMENT PROACTIVE SECURITY PROTOCOLS

To protect critical infrastructure and limit opportunities for fraud or theft, organizations should implement “separation of duties,” which requires two individuals to complete an important task. Organizations should also implement “least privilege” in their digital security controls, which provides employees with only the access required for them to do their work.

ACTION STEPS

- Require two electronic signatures to sign off on transfers of funds or changes to the network, and require a manager’s authorization for any important data entry functions.
- Implement code reviews for new system software or maintenance.
- Control employee access to software/ system modification through configuration controls.
- Perform regular audits and to detect and prevent theft or fraud.

MITIGATION

MITIGATE INSIDER RISK IN THE SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC)

The SDLC is the process of designing, testing, and implementing new software for use in an organization. Organizations should eliminate defects and vulnerabilities in the SDLC and automated processes to minimize internal malicious actions such as theft or fraud attempts.

ACTION STEPS

- For system design, implement separation-of-duties protocol and limit opportunities for automatic system overrides.
- Never have a shared log-on account for for administrators or database users.
- For implementation and installation of new software, require new passwords to prevent unauthorized developer access to the organization's critical information.
- For system maintenance, maintain strict authorization protocols for employees updating code and new system releases.

MITIGATION

BE HYPERVIGILANT WITH SYSTEM ADMINISTRATION AND ACCESS

To protect the organization from IT sabotage and other malicious actions, additional oversight should be focused on system administrators and technical or privileged employees, who have specialized access and knowledge to control the network.

ACTION STEPS

+ Implement a separation-of-duties policy that requires multiple privileged authorizations for designs and changes to the system.
+ If possible, employ two system administrators.
+ Disable access to the network by all former system administrators and other technical or privileged employees.

MITIGATION

FORMALIZE THE SYSTEM CHANGE CONTROL PROCESS

Change controls for modifying a product or system should be a formalized process, and any unauthorized changes should be prohibited to prevent malicious code or programs.

ACTION STEPS

+ Identify and catalog the baseline software/hardware configurations that apply to each employee, so there is a reference point when changes are required.
+ Ensure that changes to the system and validation of those changes are carried out by different employees.
+ Protect change logs, create safe system backups, and use file integrity checkers when making changes to the system; avoid unauthorized modifications and safeguard against malicious attacks.

MITIGATION

MONITOR ONLINE ACTIONS IN THE ORGANIZATION

Organizations should track employees' online behavior to monitor for suspicious actions. User activity monitoring (UAM) provides the ability to observe and record the activities and actions of employees on the organization's computer network. For example, UAM can flag when employees access secure data or systems. Monitoring systems can both detect anomalous behaviors in employees and reinforce mitigation responses.

ACTION STEPS

- Implement UAM to verify changes to critical infrastructure or financial accounts, or to detect unauthorized backdoor accounts.
- Conduct scheduled and periodic random audits of employee transactions.
- Use UAM to detect suspicious emails or the sending of large attachments; prevent the copying, downloading, or printing of sensitive information.
- Be transparent about any monitoring and tracking of employees' work and social media activity.

MITIGATION

PROTECT AGAINST REMOTE ATTACKS

To minimize risk of remote cyberattacks, organizations should consider limiting remote access to critical data and operations and only allow access through a workplace device. Network administration should be conducted onsite at the physical organization, if possible.

ACTION STEPS

+ When remote access to critical information is necessary, monitor logins closely and conduct more frequent audits of remote transactions.
+ Give remote employees organization laptops to better control access and monitor online activities including login account, IP address, date and time connected, and failed login attempts.
+ When employees leave the organization, retrieve their company laptop and other equipment, disconnect their remote access, change open account passwords, and close any open connections.

MITIGATION

ADHERE TO SAFE TERMINATION PROCEDURES

Terminations are a known critical point of insider risk. Development and execution of thorough procedures for safe terminations protect and secure multiple points of human and technical vulnerabilities.

ACTION STEPS

+ Select a safe location and have security and other support teams on hand.
+ Deactivate the employee's access to all administrator, DBA, training and development, and external accounts.
+ Keep a list of all shared accounts with multiple users and disable the employee's access from those accounts.
+ Deactivate all remote access to the organization's network and information.

MITIGATION

PLAN FOR SECURE BACKUP AND RECOVERY IN CASE OF A MALICIOUS ATTACK

If an insider threat to an organization's network does occur, secure backup and recovery plans should be in place to increase the organization's resiliency and prevent costly data recovery time. These processes should be updated and tested regularly.

ACTION STEPS

+ Control access to the location where backups are stored and apply the two-person rule, requiring that two different people are responsible for making changes to the backup process.
+ Require accountability and transparency from third-party partners that provide support, especially with storage of the organization's data or media.
+ Create multiple backup copies and store them in different off-site locations.

MITIGATION

DEVELOP A RESPONSE PLAN TO INSIDER THREATS

Having an established response team and action plan is essential to an effective response to an insider threat or incident. The response plan should keep in mind the rights of everyone in the organization, and should be documented clearly and approved by the legal team and managers.

ACTION STEPS

+ Identify ways to mitigate risk and determine how/when these actions should be taken.
+ Assign a trusted mediator to communicate information to department leaders.
+ Share incident response plans only with the individuals responsible for carrying it out.
+ Train employees and managers to recognize and report suspicious behavior; update training materials based on lessons learned.

MITIGATION

LEAD WITH TRUST, FOLLOW WITH CONTINUOUS SUPPORT

An effective C-InT mission depends on organizational trust; an organization's people, assets, and environment are all interdependent. Trust and transparency should be combined with ongoing support and empowerment for all members of the organization.

ACTION STEPS

+ Promote an environment where interpersonal relationships are valued, toxicity is weeded out, professional development opportunities are available, and decision-making is transparent.
+ Create flexible work schedules to balance professional and personal responsibilities; promote workplace morale, enhance recruitment/retention, and reduce absenteeism.
+ Develop an Employee Assistance Plan to support employees' work performance, health, and well-being. Programs can include assessments, counseling, and referrals for additional assistance for work or personal issues and stressors.