Carnegie Mellon University
Software Engineering Institute

Insider Threat Vulnerability Assessment (ITVA)

Physical Security Capability Area

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

https://www.sei.cmu.edu

Copyright 2023 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM23-0882

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Table of Contents

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

1 Parts of an SEI Report

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Introduction

The insider threat vulnerability assessment was developed by staff in the CERT® Division at the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University. The assessment, which is based on hundreds of actual insider threat cases, enables organizations to gain a better understanding of insider threat and an enhanced ability to assess and manage associated risks. The assessment was designed to be completed over a period of three weeks. Week one is the pre-assessment week, where assessment team members review organization-supplied documents to become familiar with organization practices and policies. During week two, the assessment team spends three to five days onsite at an organization. During that time, the assessment team reviews documents, interviews key personnel, and observes processes to substantiate each capability. During the final week, the assessment team prepares an insider threat vulnerability assessment final report, describing how prepared an organization is to prevent, detect, and respond to insider threats.

This module measures the vulnerability of an organization to insiders' physical exploits as featured in cases in the CERT® insider threat database. In this context, "physical security" refers to controls, such as doors, locks, and cameras, designed to physically impede or prevent an insider from carrying out an attack.

® CERT® is a registered mark owned by Carnegie Mellon University.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Generic Clarifications

An insider is defined as any person who supports the organization, including contractors, subcontractors, and business partners.

All capabilities containing the phase ***"prevent, detect, and respond to"*** require that the organization can do all three: prevent insider threat incidents, detect incidents if they occur, and respond to incidents when they occur.

A ***policy*** is an administrative control commonly used as a prevention method. However, for an organization to achieve a capability involving a policy, the policy's existence is not sufficient on its own. The assessment team will be looking for the following attributes of a policy:

- documented
- communicated
- maintained
- routinely and consistently applied
- enforced
- monitored

Without defined policies and procedures, it can be difficult to discipline, terminate, or prosecute employees who engage in insider threat activity. To be effective, the policies and procedures must be consistently and routinely enforced.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Capability Sequence # PS1.1: Unauthorized Facility Access

The organization prevents, detects, and responds to unauthorized facility access by insiders.

Clarification/Intent

This capability deals with the organization having controls and processes in place to allow only authorized entrance to a facility and to restrict unauthorized access. To successfully meet this capability, the organization must show that they have a physical security plan in place that includes but is not limited to

- policies, processes, and procedures in place governing facility access for employees and visitors
- physical controls deployed to restrict unauthorized facility access, such as the use of mantraps, turnstiles, antipassback, guards, sign-in procedures, or credential gathering procedures.

Assessment Team Guidance

This capability only deals with ingress and egress of the facility itself; other capabilities deal with restricting access to areas within the facility.

Insiders have exploited lack of physical controls to gain unsupervised access to facilities. They have also walked out with equipment and data when not adequately monitored.

The organization should

- employ additional measures for controlling physical access outside normal working hours
- employ additional physical access monitoring for an employee whose termination is pending, whether from voluntary resignation or not
- train its employees to prevent social engineering to gain unauthorized physical access to facilities (e.g., a terminated employee using his previous work relationships, or piggybacking on the card key of a current employee)
- prohibit access by members of employees' social networks, such as employees' relatives
- monitor access to facilities by insiders while they are being investigated for policy violations

MERIT Example

The insider was employed as a claims representative by the victim organization, a government agency. As a function of his job, the insider had access to a Social Security Administration (SSA) database. The insider used an unattended computer to make an unauthorized query and also modified a record in the database. The insider modified the record of an online acquaintance to reflect that she was deceased. The insider was apparently retaliating for a moderator kicking him out of an online chat room. The insider had threatened to "get even" with the moderator. The incident was detected when the moderator tried to open a bank account and discovered that her records had been changed. The insider was connected to the incident by the victim, who identified the insider by the picture he used in the chat room. The insider was apologetic and stated he did not realize the extent of the damage he would be causing by his actions. The insider was arrested, convicted, ordered to pay $700 restitution, and sentenced to 1 year of probation.

Organization Response

Evidence Sought

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Auto Verification

Additional Information

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has a physical security plan that details

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ protected areas of the facilities and corresponding access restrictions

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ prohibitions against social engineering attempts to gain unauthorized physical access to facilities (e.g., piggybacking)

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ prohibition of employees' friends and relatives from entering the facility (with limited exceptions for special circumstances)

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ requirements for escorting or limited access for employees performing support duties (e.g., custodial staff)

  Doc Rev _____

  Dir Obs _____

  Intvw _____

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

☐ requirements for visitor access

Doc Rev

Dir Obs

Intvw

☐ The organization has defined physical access requirements commensurate with the job responsibilities of employees, trusted business partners, and other types of personnel who have any degree of physical access to facilities.

Doc Rev

Dir Obs

Intvw

☐ The organization has access control systems to prevent unauthorized physical access to organizational facilities.

Doc Rev

Dir Obs

Intvw

☐ The organization monitors employee access to and exiting of facilities.

Doc Rev

Dir Obs

Intvw

☐ The physical access control systems log all access attempts.

Doc Rev

Dir Obs

Intvw

☐ Alarms or CCTV are used to alert the organization of unauthorized access attempts.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization has a response plan to address physical security incidents.

Doc Rev

Dir Obs

Intvw

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

☐ Personnel (such as guards or security) are identified and trained to respond to physical security incidents.

Doc Rev

Dir Obs

Intvw

☐ Violations of physical security are addressed and resolved.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has a physical security program established.

Doc Rev

Dir Obs

Intvw

☐ The organization has a process or system to prevent recently terminated employees from regaining access to the facility.

Doc Rev

Dir Obs

Intvw

☐ The organization engages in enhanced monitoring of physical access control systems when employee termination is pending, whether voluntary or involuntary.

Doc Rev

Dir Obs

Intvw

☐ The organization engages in enhanced monitoring of physical access control systems when employees are being investigated for policy violations.

Doc Rev

Dir Obs

Intvw

☐ The organization provides employee training to address

Doc Rev

Dir Obs

Intvw

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

☐ social engineering attempts to gain unauthorized physical access to facilities (e.g., piggybacking)

Doc Rev

Dir Obs

Intvw

☐ escorting or limited access for employees performing support duties (e.g., custodial staff)

Doc Rev

Dir Obs

Intvw

☐ prohibition of employees' friends and relatives from entering the facility (with limited exceptions for special circumstances)

Doc Rev

Dir Obs

Intvw

☐ requirements and procedures for admitting and escorting visitors

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Capability Sequence # PS1.2: Unauthorized Access to Employee Workspaces

The organization prevents, detects, and responds to unauthorized physical access to other employees' workspaces.

Clarification/Intent

The organization should have physical and technical controls as well as provide education to prevent unauthorized physical access to others' workspaces.

The scope of this capability applies to both organizational employees and trusted business partners (i.e., contractors, sub-contractors, etc.) who have a workspace on-site, within the organizational facilities.

All levels of employees and trusted business partners should be covered by the same controls and receive the same education regardless if they are contracted or direct employees, this includes but is not limited to

- custodial or janitorial staff who may clean public and individual office spaces and employee work areas
- security staff who monitor facilities
- visitors who may temporarily be in the facilities
- vendors who may service equipment or infrastructure within the facilities
- remote employees who may be on-site for meetings or other temporary assignments
- employees who work daily in the facilities
- managers, supervisors, and C-level staff who work or visit the facilities

The organization should have controls that govern these types of employees and trusted business partners based on the nature and extent of the access they require to perform their jobs.

Assessment Team Guidance

Insiders have taken advantage of employees who left their workspace unattended. The team should look for evidence that

- requirements have been identified for who can access which areas of the facility employee workspaces and under what conditions based on job responsibilities
- appropriate controls, policies, and processes are in place to prevent unauthorized access including, badging access; locked doors, key-card entry mechanisms, monitoring of custodial staff access, etc.
- employees and trusted business partners have been educated on the policies regarding unauthorized access of other's workspaces
- a process is in place to report and address violations

MERIT Example

The insider was employed by a financial institution that handled internet banking for other organizations. She was responsible for validating authorized wire transfers and internet banking troubleshooting. The organization placed holds on two suspicious transactions. The insider distracted the coworker by pretending to be hurt and asking the coworker to get her a glass of water, and she then used the co-worker's computer to approve the transfer. A month later, she began wearing very expensive clothing. Six accomplices were involved. She failed to report previous arrests on her application.

Organization Response

Evidence Sought

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Auto Verification

Additional Information

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ A policy exists requiring all employees to respect the workspaces of other employees and on-site trusted business partners, and forbids unauthorized access.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ A policy exists requiring all employees and on-site trusted business partners to lock their doors and cabinets in their workspaces before leaving their work area.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a “clear desk” policy and requires employees and on-site trusted business partners to comply with it.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization requires employees and on-site trusted business partners to lock their workstations when leaving them unattended.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has defined physical access requirements commensurate with the job responsibilities of employees, trusted business partners, and other types of personnel who have any degree of physical access to workspaces.

Doc Rev _____

Dir Obs _____

Intvw _____

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Level 3

☐ Workstations are set to lock after a period of inactivity.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Violations of workspace policies are addressed and resolved.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization provides formal training for workstation security.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization trains employees to challenge individuals located in other employees' or trusted business partners' workspaces.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Security performs periodic sweeps of work areas and informs employees when they fail to adhere to workspace security policies.

Doc Rev _____

Dir Obs _____

Intvw _____

Dir Obs _____

Intvw _____

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Capability Sequence # PS1.3: Unauthorized Access to Critical Areas

The organization prevents, detects, and responds to unauthorized physical access by employees to critical or sensitive areas.

Clarification/Intent

This capability looks to ensure that there are controls, policies, and processes in place to restrict unauthorized physical access to critical or sensitive areas within facilities.

Critical or sensitive work areas may include

- off-site locations (customer sites, backup sites, external facilities, radio towers, kiosks)
- machine rooms
- server rooms
- data centers or other data storage areas
- any other area designated as critical

As part of meeting this capability the organization should identify the sensitive areas of its facilities and ensure it has policy and procedures to restrict access to them.

Employees should also be educated on the requirements and prohibitions for unauthorized access.

Assessment Team Guidance

Insiders have stolen identity badges and used social engineering to gain unauthorized entry to sensitive areas to harm their organizations.

MERIT Example

A senior financial analyst for a financial institution came to the organization's offices and downloaded 20,000 mortgage applicant records to a USB flash drive every Sunday. Over a two-year period, the insider downloaded and sold over 2 million records that contained personally identifiable information (PII). The organization had a policy that prohibited flash drives or other storage devices. He located the one computer that lacked this security feature.

Organization Response

Evidence Sought

Auto Verification

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Additional Information

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has identified sensitive areas of its facilities, both on-site and off-site.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has defined physical access requirements commensurate with the job responsibilities of employees, trusted business partners, and other types of personnel who have any degree of physical access to critical or sensitive areas.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization's access control system logs all access attempts of sensitive areas.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization's access control system alerts upon unauthorized attempted access to sensitive work areas.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Alarms or CCTV are used to alert the organization of unauthorized access attempts to sensitive areas.

Doc Rev _____

Dir Obs _____

Intvw _____

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

☐ The organization periodically reviews access logs for suspicious activity.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has an incident response plan in place to address physical security incidents relating to unauthorized access or attempted access to sensitive work areas.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization monitors egress of sensitive work areas to prevent unauthorized removal of information and equipment.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Access violations of sensitive work areas are addressed and resolved.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization requires multifactor authentication for entrance to sensitive work areas.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization limits access to sensitive work areas by time of day.

Doc Rev _____

Dir Obs _____

Intvw _____

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

☐ The organization limits access to sensitive work areas by job function.

Doc Rev

Dir Obs

Intvw

☐ The organization provides employee training on access requirements and restrictions for sensitive areas.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Capability Sequence # PS1.4: Notification of Employee Separation

The organization notifies appropriate parties of employee terminations or separations.

Clarification/Intent

The organization should have designated, trained employees who are responsible for notifying appropriate parties of employee separation whether voluntary or not. The scope of the separation notification includes organizational employees and trusted business partner employees.

If a trusted business partner notifies the organization of an employee separation from the trusted business partner company, the organization then should notify any other affected parties. (Organization in this context is the organization being assessed.)

Other parties can include but not be limited to current

- employees
- managers, supervisors, and C-level staff
- security staff or guards
- other trusted business partners as appropriate such as contractors, sub-contractors, vendors, etc.

Assessment Team Guidance

Insiders have exploited a lack of communication, or delayed communication, about their terminations to harm their organization following termination.

To meet this capability, the organization should have an institutionalized policy requiring notification of employee terminations, a mechanism for communicating the terminations or separations, and a trained staff who perform the notification function.

The team should look for evidence that

- a policy exists and has been communicated to the organizational staff
- a mechanism and process is in place to perform the notifications
- notifications have occurred – this could include but not be limited to copies of memos, announcements, or emails

MERIT Example

Insider was a former IT employee with a pharmaceutical company. After a dispute with senior management, the Insider resigned. The Insider's Supervisor, a close friend, convinced the Victim Organization to keep the Insider on as a contractor. A few months later, the Insider left the company completely. Due to company layoffs, the Supervisor found that he was about to be let go. The Supervisor tried to prevent management from obtaining certain passwords, leading to his suspension and subsequent firing. Sometime prior to the attack, the Insider uses his home network to install a piece of software on the Victim Organization's server. The Insider used a restaurant's internet connection and a Victim Organization user password to access Victim Organization server. Then, the Insider used the previously installed piece of software to delete virtual machines which hosted the organization's email, order tracking, and financial management systems. This halted the organization's operations for several days. The Insider's connection to the attack was discovered via his purchases in the restaurant near the time of the attack. Insider was arrested and plead guilty.

Organization Response

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Evidence Sought

Auto Verification

Additional Information

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has a policy that requires notification of employee terminations to appropriate parts of the organization, including trusted business partners, and other appropriate parties.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization performs notification of terminations to appropriate parties.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ A detailed process is in place for communicating information about insider termination to appropriate parts of the organization.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has designated employees who communicate terminations to appropriate parts of the organization.

Doc Rev _____

Dir Obs _____

Intvw _____

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Level 4

☐ The appropriate employees are trained on when, how, and whom to communicate with upon insider termination.

Doc Rev

Dir Obs

Intvw

☐ The organization has a detailed process for communicating with trusted business partners about relevant insider terminations.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Capability Sequence # PS1.5: Reporting of Physical Security Breaches

The organization has a method enabling employees to report physical security breaches.

Clarification/Intent

Physical security breaches describe insiders violating physical security policy, such as attempts to piggyback on other employees' access and attempting to enter areas to which they do not have authorized access. It can also include potential security breaches caused by lost credentials or identification, such as badges or card keys. It can also include unauthorized removal of information or equipment.

The organization should have channels for employees to report suspicious activity. This reporting may be automated.

Mechanisms should also be in place to report loss or theft of access devices, such as identification badges and/or card keys.

Employees should have the ability to report direct violations of policy, as well as suspicious or concerning behaviors, especially outside of normal working hours.

Employees should be trained on what actions to take when witnessing an unauthorized access to a logged-in workstation or unauthorized removal of information or equipment

Assessment Team Guidance

Employees sometimes see coworkers engaging in suspicious activities but often refrain from reporting them. Having a defined process and mechanism that is promoted to employees can help staff understand their responsibilities and what to do when they see suspicious activity.

The assessment team should look for evidence that the reporting mechanism is easily available and known to the employees. The team should verify that the mechanism is used and that reports are appropriately gathered, handled, and resolved.

MERIT Example

The insider was employed as a police officer by a school district. Over 6 years, he committed multiple crimes. Initially he broke into vehicles and stole expensive items, including electronics and credit cards. He had two teenage accomplices and committed credit card fraud and burglary. It was discovered that he used law enforcement and school district databases to steal the identities of people. He had previous arrests for breaking into cars, credit card fraud, and burglary.

Organization Response

Evidence Sought

Auto Verification

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Additional Information

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has a policy that requires employees to report physical security breaches, violations of policy, suspicious or concerning behaviors, and loss of credentials or access mechanisms (such as key cards or badges).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a website, email address, or other mechanism for employees to report physical security breaches, violations of policy, suspicious or concerning behaviors, or loss of access mechanisms or credentials.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a defined process for handling reports of physical security breaches, violations of policy, suspicious or concerning behaviors or loss of access mechanisms or credentials.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization handles any reports in a timely manner.

Doc Rev _____

Dir Obs _____

Intvw _____

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Level 4

☐ Training programs are in place to inform employees about

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ their responsibility for reporting physical security breaches, violations of policy, suspicious or concerning behaviors or loss of access mechanisms or credentials

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ the mechanisms for reporting physical security breaches, violations of policy, suspicious or concerning behaviors or loss of access mechanisms or credentials

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ the process for handling reports of physical security breaches, violations of policy, suspicious or concerning behaviors or loss of access mechanisms or credentials

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ Training programs are in place for those responsible for handling reports of physical security breaches, violations of policy, suspicious or concerning behaviors, or loss of access mechanisms or credentials which detail

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ the mechanisms for reporting

  Doc Rev _____

  Dir Obs _____

  Intvw _____

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

☐ the process for handling reports

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Capability Sequence # PS1.6: Tampering of Physical Security Systems

The organization prevents, detects, and responds to tampering with physical security systems.

Clarification/Intent

Tampering with cameras, access control systems, and ID badges can interfere with damage assessments, decrease likelihood of litigation, and damage assets. The organization should have controls to prevent, detect, and deter damage or unauthorized modification to these security components. Security guards should be aware of what is occurring on CCTV, and respond quickly to any disruption in video. Cameras should be placed in known entry and exit areas and in front of sensitive areas (such as backup tape storage). Automated notifications should trigger whenever a particular component is damaged or destroyed, and a clear response procedure must be documented.

Assessment Team Guidance

Insiders have exploited physical security systems to cover their tracks and reduce the likelihood of identification.

The assessment team should look for evidence that surveillance equipment is installed and used daily. If possible discussions with staff responsible for viewing the footage and responding to alerts can be held to collect information on how well this process is implemented and followed.

MERIT Example

The insider was formerly employed as a network administrator by the victim organization, a visual technology manufacturer and provider. At the time of the incident, the organization hired a new supervisor. The new supervisor fired 12-16 employees, but promoted the insider. The insider told co-workers that he had installed backdoors and planned to use them to harm the organization, but the co-workers were afraid to speak up due to the recent terminations. The insider displayed bizarre workplace behavior. The insider would answer his phone as “the king” or “the president,” and claimed to coworkers that he was building a hydraulic chair he could control with his computer-connected joystick. The insider put up a video camera in the organization’s computer room and would call in to say that he “was watching.” The insider was a very deceptive individual. At the time of hire, the insider falsely claimed to be a certified Cisco Network Engineer and to be recommended by a headhunter. The organization failed to verify this certification. The insider also concealed his violent criminal history, including assault with a deadly weapon, corporal injury to a spouse, and other prior felonies, including possession of a firearm and fraudulent use of 2 social security numbers (SSNs). The insider also had assault weapons at his home, which had been previously seen by a co-worker from the organization. The organization became suspicious of the insider when he became resistant and evasive after being asked to travel abroad for business. The insider claimed that he did not like flying, but actually had a pilot's license. The insider also claimed that he did not have a proper birth certificate due to a bizarre instance of identity theft. The organization discovered that the insider was not Cisco certified and subsequently terminated the insider. The insider did not return his company-assigned laptop after termination. The organization refused to give the insider his severance pay until the laptop was returned. The insider complied, but turned in the laptop physically damaged and with the memory wiped. During his employment, the insider managed the organization’s remote access equipment, even though the organization had technical staff for this purpose. After the insider’s termination, the organization noticed that the insider repeatedly attempted to remotely access their servers. When called the insider denied that he was accessing the servers. The organization hired a computer security consulting firm. The consultants blocked the insider’s IP address at the organization’s firewall, deleted his accounts, checked for backdoors, and watched for illicit access, but failed to check one server that the insider had access to. From a forensic examination they determined that the insider had used VPN accounts in the names of senior managers to log in over the 2 week period between the insider’s termination and the incident. For unknown reasons, the consultants did not consider the accounts suspicious and also failed to disable the insider’s Citrix access, allowing him to dial in. The VPN accounts were used by the insider to remotely access the organization’s Citrix server and rendered the server inoperable. The insider was arrested, convicted, sentenced to 1 year imprisonment, and ordered to undergo mental health counseling.

Organization Response

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Evidence Sought

Auto Verification

Additional Information

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has cameras monitoring known entry and exit areas.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has cameras monitoring known sensitive areas.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has security staff monitoring CCTV footage for tampering with physical security systems.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ There is a documented response process for handling tampering of physical security systems.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Employee violations regarding tampering with physical security systems are addressed and resolved.

Doc Rev _____

Dir Obs _____

Intvw _____

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

☐ Security staff check on failures of physical security equipment to determine cause.

Doc Rev

Dir Obs

Intvw

Level 4

☐ Physical security systems are regularly tested.

Doc Rev

Dir Obs

Intvw

☐ Security staff are trained to check on failure of equipment supporting physical security.

Doc Rev

Dir Obs

Intvw

☐ Security staff are trained on the process for handling tampering of physical security systems.

Doc Rev

Dir Obs

Intvw

☐ Automated notifications are triggered whenever a particular physical security component is modified, damaged, or destroyed.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Capability Sequence # PS2.1: Theft of Organization Property

The organization prevents, detects, and responds to the physical theft of organizational property.

Clarification/Intent

The organization has controls governing software, loaned property, removable media, and intellectual property (IP).

The organization has controls governing property used by, loaned to, or assigned to all staff, including permanent employees, trusted business partners such as contractors, subcontractors, or vendors.

Assessment Team Guidance

Insiders have been found to steal laptops, USB drives, and software from organizations to sell or personally use. This includes IP that may be stored on the media itself.

Security controls should exist to protect

- organization property loaned to employees as part of their job (e.g., laptops)
- removable media (especially backups of critical systems or data)
- information that exists on paper during its lifecycle, in particular its use (e.g., in the office), storage (e.g., in a file cabinet or safe), and disposal (e.g., through shredding)

MERIT Example

The insider was employed as an internet-technology worker in the network support department of the victim organization, a telecommunications company. The organization administered an emergency 911 system. While on site, the insider physically stole 55-77 backup tapes for the UNIX system that handled emergency calls. The insider also used local terminal access, and an open and logged-in session with root privileges, to delete data and software on three critical servers. The insider entered a command that prevented anyone from halting the destruction. The incident took place outside of working hours. The incident was detected when the systems failed. The insider was arrested, convicted, ordered to pay $233,000 restitution, and sentenced to 5 years of probation, including 6 months of home detention. The insider turned himself in and physical access logs connected the insider to the incident. The incident related impact was $209,000 - $233,000. At the time of the incident, the insider was being medicinally treated for schizoaffective personality disorder and manic-depression. The insider claimed he had found a contractor's badge that allowed him access to both the off-site backup tapes and the network operations center where he launched the software deletion attack.

Organization Response

Evidence Sought

Auto Verification

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Additional Information

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has a policy that governs the use and ownership of organizational property.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a physical asset inventory system and process including, at a minimum, laptops and removable media.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The asset inventory system and process is updated at least annually.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has an asset check-in and check-out process for all organizational property issued to permanent employees, business partners, contractors, or sub-contractors.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has process for reporting lost or stolen organizational property.

Doc Rev _____

Dir Obs _____

Intvw _____

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Level 3

☐ The organization has a mechanism for reporting lost or stolen property.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a process for recovering lost or stolen property.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Reports of lost or stolen organizational property are addressed and resolved.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Employees are trained on the appropriate use and ownership of organizational property.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Employees are trained on the process for checking in and checking out organizational property.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Trusted business partners are trained on the appropriate use and ownership of organizational property.

Doc Rev _____

Dir Obs _____

Intvw _____

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

☐ Trusted business partners are trained on the process for checking in and checking out organizational property.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.