# Security Incident Management Training

Tandem™

# Lesson 1

About Security Incident Management

# Introduction

To help the organization achieve its goals and comply with laws, every employee is responsible for doing their part to secure systems and data. In this course, you will learn about your role in security incident management, as well as how you can prevent, detect, and respond to security incidents.

# What is “Security?”

Security is all about preserving the confidentiality, integrity, and availability of systems and data.

- **Confidentiality** is about ensuring only the right people have access to systems and data at the right times. To ensure confidentiality, you must prevent unauthorized access and disclosure.
- **Integrity** is about ensuring systems and data are accurate. To ensure integrity, you must prevent unauthorized modification and misuse.
- **Availability** is about ensuring systems and data are accessible when you need them to be. To ensure availability, you must prevent unauthorized interruptions and destruction.

Together, these three elements are referred to as the “CIA triad,” and each part must be in place to ensure security is achieved.

# What is a “Security Incident?”

If an event compromises one or more aspects of the CIA triad, the event may be considered a security incident. Security incidents can occur when an organization’s policies and procedures are ignored, when natural or human interference causes harm, or when technology fails to perform as expected. In many cases, a security incident results from a combination of these things.

# How a Security Incident Affects the Organization

Security incidents have the potential to cause serious consequences for the organization. Depending on the nature of the incident, some of the more extreme effects could involve:

- The inability to perform business functions or provide services to clients.
- Sizeable financial costs for responding to the incident, paying legal fees, paying fines, etc.
- Severe reputation damage if clients and/or the public are notified or aware of the incident.
- Irreversible effects to organization systems or data.
- Increased regulatory oversight and penalties.

# How a Security Incident Affects You

When a security incident occurs, consequences of the incident may directly affect you, as well.

For example, if a security incident affects your workstation or compromises one of your accounts, this could cause a delay in the ability to perform your job. If negligence was a contributing factor in the incident, increased oversight or re-training may also be implemented.

Deliberate cause of a security incident (e.g., theft of assets, disabling security controls, intentional unauthorized disclosure of information, etc.) may lead to disciplinary action, up to and including termination of employment.

# The Incident Management Plan

To help identify, analyze, and correct incidents when they occur, the organization has implemented an incident management plan. The goal of the plan is to limit disruptions and restore operations as quickly as possible if an incident occurs.

**You play a key role in this plan.** For the incident management plan to be most effective, you must know how to prevent, detect, and respond to security incidents.

# Lesson 2

Preventing Security Incidents

# About Preventing Security Incidents

Taking steps to stop security incidents before they begin is the best way to ensure the organization remains secure. In this lesson, you will learn some common ways to prevent security incidents.

# Follow Acceptable Use Policies

One way to prevent security incidents is to follow the organization’s acceptable use policies, using systems and data only as they are intended. Some examples of inappropriate use include:

- Actions contrary to the organization’s best interest.
- Use for personal gain.
- Disregarding company policy.
- Violating laws.
- Representing yourself as another person.
- Communicating offensive, derogatory, harassing, or defamatory content.

# Install Patches and Updates

Install the latest updates on your systems and applications as soon as they become available to limit the time vulnerabilities can be exploited by malicious actors.

# Use Secure Networks

Do not connect your devices to unknown wireless (a.k.a., “Wi-Fi”) networks in airports, hotels, and restaurants, unless necessary. It is difficult to know the security levels of these networks and connecting could expose transmitted data to unauthorized viewers.

# Do Not Circumvent Security Systems

Certain security systems are installed or configured on your devices to stop malware, scan email, filter network traffic, and secure your logins. Do not attempt to go around or disable these security systems, so they can do their jobs most effectively.

# Other Prevention Measures

There are several other things you can do to help prevent security incidents, such as:

- Using strong passwords and not sharing them with anybody.
- Physically securing your devices to prevent them from being stolen.
- Locking your device screens when you walk away from your desk.

Any step you take to be careful with systems and data can be thought of as a security incident prevention measure. Additional prevention measures are covered in other training provided by the organization.

# The Downside to Preventing Incidents

Incident prevention is not foolproof. While taking steps to prevent security incidents is important, things can slip through, which is why a layered incident management plan is necessary. Regardless of how a security incident occurs, it is important for you to be prepared to detect and respond to these events.

# Lesson 3

Detecting Security Incidents

# About Detecting Security Incidents

There are several ways to identify different types of security incidents. In this lesson, you will learn some of the most common signs of security incidents and ways you can detect them.

# Account Takeover

Account takeover occurs when a malicious actor gains access to a legitimate user's account credentials and is often associated with identity theft. Some common signs of account takeover include:

- Emails being sent from your account which you did not send.
- Unauthorized transactions being performed.
- Notification from a client that their account has been compromised.

# Criminal Activity

Criminal activity can be thought of as illegal conduct by an individual or group of malicious actors. Examples of criminal activity include fraud and sabotage / vandalism.

# Criminal Activity: Fraud

Fraud is the deliberate, unauthorized manipulation of systems and data with the intent of financial gain. You may discover signs of fraud by accident or by notification from parties involved with the fraud. Signs of fraud may include detecting a counterfeit transaction, discovering embezzlement activities, or taking petty cash.

# Criminal Activity: Sabotage / Vandalism

Sabotage / vandalism is a deliberate action taken to disrupt operations by destroying or damaging systems or data. This form of criminal activity typically includes visible indicators, so if something appears to be damaged or destroyed when it should not be, it could be a security incident.

# Data Breach

A data breach involves data being accessed, modified, and/or exfiltrated by an unauthorized person. Some common signs of a data breach include the discovery of:

- Physical or electronic data in an unauthorized location.
- Missing or altered data.
- A team member accessing data to which they should not have access.
- A team member using data for unauthorized purposes.

A data breach often occurs as a result of another type of security incident, like malicious code, policy violation, or social engineering. If you detect signs of a data breach, look for other signs to understand how the breach happened.

# Lost or Stolen Resources

If systems, equipment, or data entrusted to you end up in the hands of an unauthorized person, either due to the resource being lost or stolen, this could be considered a security incident.

# Malicious Code

Malicious code (commonly referred to as “malware”) is an application designed to access a system without authorization, including forms of hostile, intrusive, or annoying code. Some common indicators of malware include:

- Files being deleted or their contents being changed.
- Internet searches being redirected.
- Cursor moving on its own.
- Windows opening and closing automatically.
- Popup messages either of a malicious nature or from your anti-malware system.

# Policy Violations

The organization’s policies and procedures serve as guiding principles for the security of systems and data. These principles are often communicated to you via acceptable use policies, employee handbooks, non-disclosure agreements, etc. Some examples of common policy violations include unauthorized use of organization resources and unauthorized disclosure.

# Social Engineering

Social engineering is an attack that exploits human nature and behavior to convince the target to perform an unauthorized operation or reveal proprietary information. Some common forms of social engineering include impersonation and phishing.

# Social Engineering: Impersonation

Impersonation occurs when a malicious actor attempts to gain physical access to the organization, systems, or data by pretending to be someone they are not. Commonly impersonated individuals include repair persons, IT support, trusted vendors, auditors, new employees, or even “friends” with coffee who need the door opened for them.

If someone claims to need access to organization resources because they fulfill one of these roles, this could indicate someone is trying to social engineer you.

# Social Engineering: Phishing

Phishing occurs when a malicious actor attempts to acquire sensitive information such as usernames, passwords, credit card details, etc. by masquerading as a trustworthy entity in electronic communication. While email is the most frequently used form of phishing, other forms of phishing include vishing (phishing via phone call) and smishing (phishing via text message).

If you receive unexpected emails, phone calls, or text messages which ask you to perform certain actions (e.g., click a link, open an attachment, share sensitive information, etc.), this could indicate someone is trying to social engineer you.

# System Failure

A system failure can happen due to vulnerabilities in the system or technology malfunctions. Some indicators of a system failure include power loss, slow system speeds, or loss of network connectivity. While a system failure may not be a security incident in-and-of itself, if the failure is caused by something like malicious code, signs of a system failure should always be noted and managed appropriately.

# Is it a Security Incident?

Except in certain obvious cases, it may be difficult to determine if the signs you observe are indicators of a security incident or not. For your role in incident management, it is better to err on the side of caution and respond accordingly. The organization can use the information you provide, correlate it with other data, and can determine if the event is, in fact, a security incident.

# Lesson 4

Responding to Security Incidents

# About Responding to Security Incidents

When a security incident happens, the longer it remains uncontrolled, the more damage it could cause. As such, when you detect signs of a security incident, you should respond in a timely and accurate manner. In this lesson, you will learn about general steps you can take to respond to a suspected incident.

# Be Safe

The first step in responding to a security incident is to assess your surroundings and ensure you are safe. This is particularly important in the event of physical security incidents, such as social engineering, criminal activity, or natural disasters. Depending on the type of incident, consider the following:

- Move to a more densely populated area to avoid being alone with a malicious actor.
- Vacate the premises as quickly as possible.
- Hide under a desk or lock yourself in an office.
- Call 9-1-1 or other emergency services.

Our team members are our most valuable asset. As such, your physical safety is of first and foremost importance.

# Report Suspicious Activity

If you detect signs of a security incident, it should be reported as soon as possible, so the damage it could cause can be limited. Report any suspicious activity to:

- **Your direct supervisor(s).** They will be able to help you assess the event, as well as provide detailed instructions over how to respond.
- **Your technology support group.** If you are not comfortable reporting to your supervisor or if your supervisor is unavailable, report the event to the organization’s designated technology support group (e.g., IT support, help desk, etc.).
- **The malicious actor’s supposed contact.** Often, a social engineer may try to use the name of one of your coworkers to make their request seem valid. Check with their supposed point-of-contact to find out if the request is legitimate or not.

# Provide Helpful Information

When reporting suspicious activity, be prepared to provide helpful information. The more information you can share, the better the chances are that your team will be able to verify if it is a security incident. Some items they may request include:

- Your name and contact information.
- The location of the suspicious activity.
- Details of any affected systems.
- The date and time the suspicious activity began and/or was noticed.
- A detailed explanation of what happened.

# Follow Their Instructions

When you report suspicious activity to a supervisor or technology support team member, they may provide specific instructions for you to follow, such as:

- **Disconnecting devices from the internet,** to help keep a security incident from spreading.
- **Shutting down (or not shutting down) your devices.** Turning off devices can help contain a security incident, but with certain types of malicious code, it may also trigger certain malicious behavior or delete valuable evidence.
- **Run a scan** using the anti-malware solution installed on your workstation to discover and remove any malicious code.
- **Install updates** to patch any of the vulnerabilities which may have allowed the security incident to occur.

# Do Not Share Information

Information about a security incident is considered proprietary and should only be shared with a small number of approved people, including your supervisor, the technology support group, and other involved parties.

**Do not share** information about a security incident with anyone else, including unaffiliated coworkers, third parties, or anyone outside the organization.

# Do Not Respond to Media Requests

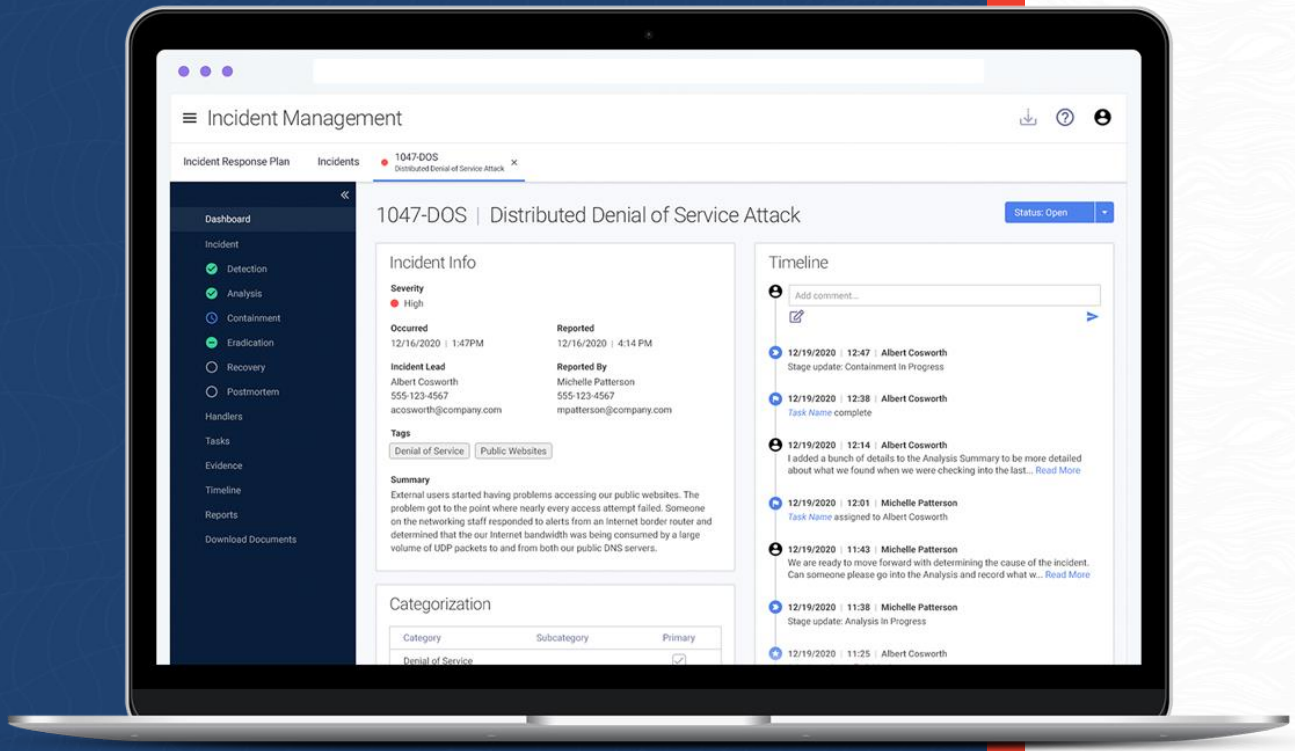
If a member of the media (e.g., television, newspaper, etc.) requests a comment from you on the security incident, you should not comment. Instead, escalate the request to your supervisor or to the organization’s public relations coordinator.

# Cooperate with the Incident Response Team

Some incidents can take a lot of time to investigate. As the organization’s Incident Response Team responds to a security incident which may affect you, it is important for you to be accommodating and do what you can to assist the response process.

# Conclusion

Security incidents can cause significant problems for the organization. As an employee, it is your responsibility to know how to prevent, detect, and respond to incidents in a timely and accurate manner. If you have any questions about security incident management, contact your supervisor.



1047-DOS | Distributed Denial of Service Attack

Incident Info

Severity
High

Occurred
12/16/2020 | 1:47PM

Reported
12/16/2020 | 4:14 PM

Incident Lead
Albert Cosworth
555-123-4567
acosworth@company.com

Reported By
Michelle Patterson
555-123-4567
mpatterson@company.com

Tags
Denial of Service
Public Websites

Summary
External users started having problems accessing our public websites. The problem got to the point where nearly every access attempt failed. Someone on the networking staff responded to alerts from an Internet border router and determined that the our Internet bandwidth was being consumed by a large volume of UDP packets to and from both our public DNS servers.

Categorization

| Category | Subcategory | Primary |
|---|---|---|
| Denial of Service | | ✓ |

Timeline

12/19/2020 | 12:47 | Albert Cosworth
Stage update: Containment In Progress

12/19/2020 | 12:38 | Albert Cosworth
Task Name complete

12/19/2020 | 12:14 | Albert Cosworth
I added a bunch of details to the Analysis Summary to be more detailed about what we found when we were checking into the last... Read More

12/19/2020 | 12:01 | Michelle Patterson
Task Name assigned to Albert Cosworth

12/19/2020 | 11:43 | Michelle Patterson
We are ready to move forward with determining the cause of the incident. Can someone please go into the Analysis and record what w... Read More

12/19/2020 | 11:38 | Michelle Patterson
Stage update: Analysis In Progress

12/19/2020 | 11:25 | Albert Cosworth

# LEVEL UP!

Tandem Incident Management can improve the quality and effectiveness of your security incident management training with our:

- Built-in quizzes to assess learning.
- User-friendly interface.
- Email reminders for employees.
- Reports and downloads to share results.

Learn more on our website:
Tandem.App/Incident-Management-Software

Tandem™