INSIDER THREAT
Awareness


SEI Copyright

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.

DM19-0489

Course Introduction

Course Introduction

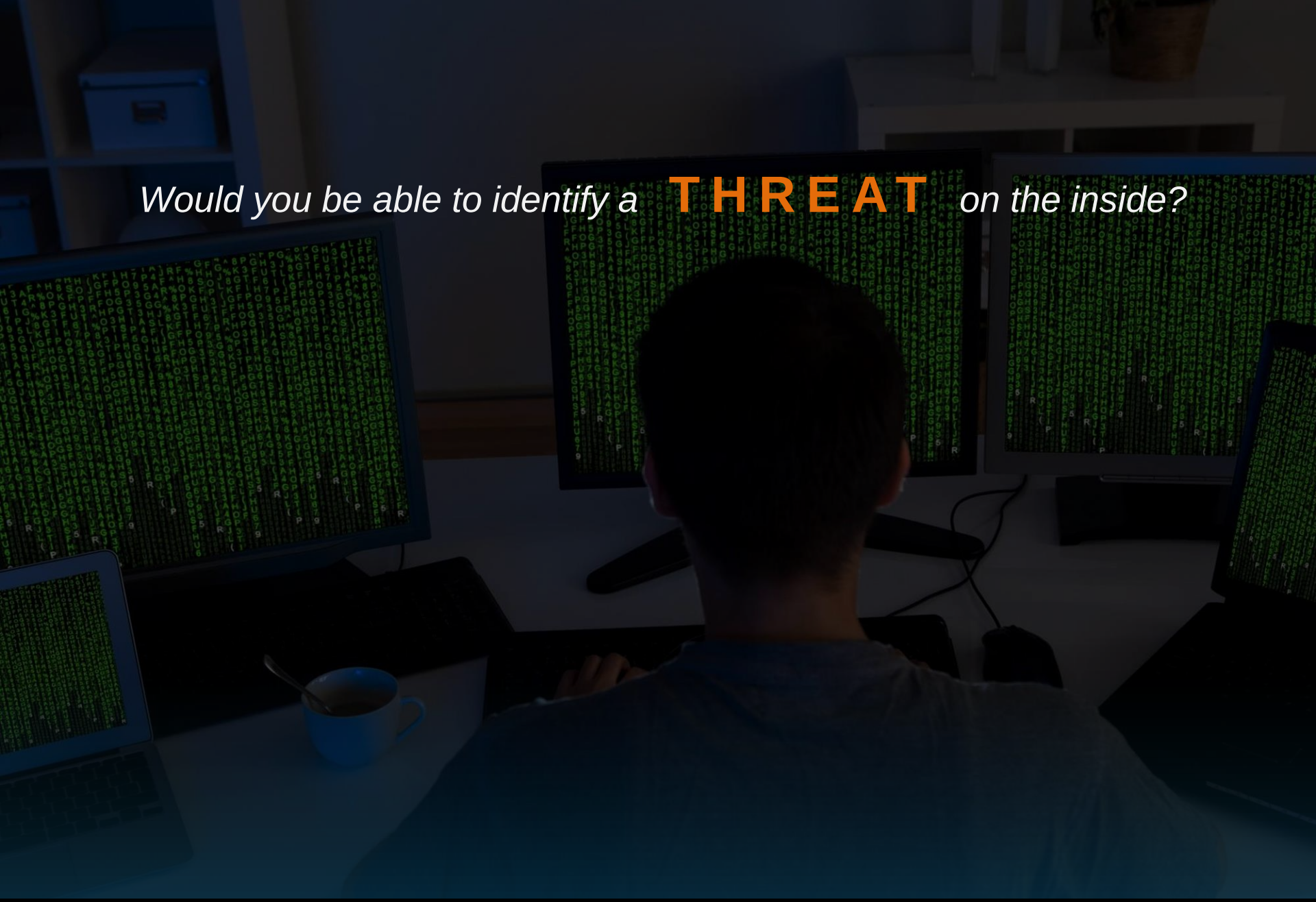
Learning Objectives

After completing this training you should be able to:

- Define an Insider and the threats they impose to critical assets
- Name different types of Malicious Insider Threat incidents
- Discuss impacts to your organization and to the general public
- Recognize how you can become an Unintentional Insider Threat to your organization and identify steps you can take to protect yourself
- Understand how you can be targeted by a malicious individual or adversary
- Identify reportable behaviors of Malicious Insiders
- Understand common motivations of Insider Threat incidents
- Describe the consequences of being a Malicious Insider or an Unintentional Insider
- Know what actions to take if you see or suspect an Insider Threat

Insider Threat: It may not be what you think

Module 1



What if someone on the outside **TARGETED** *you through email phishing?*

How could your work be **IMPACTED** *?*

Send

From ▾ chiefsecurity@yourorganization.com

To...

Cc...

Subject:

Hello,

I work with the director of your organization's security team. I need you to send me your login ID and user password for your computer.

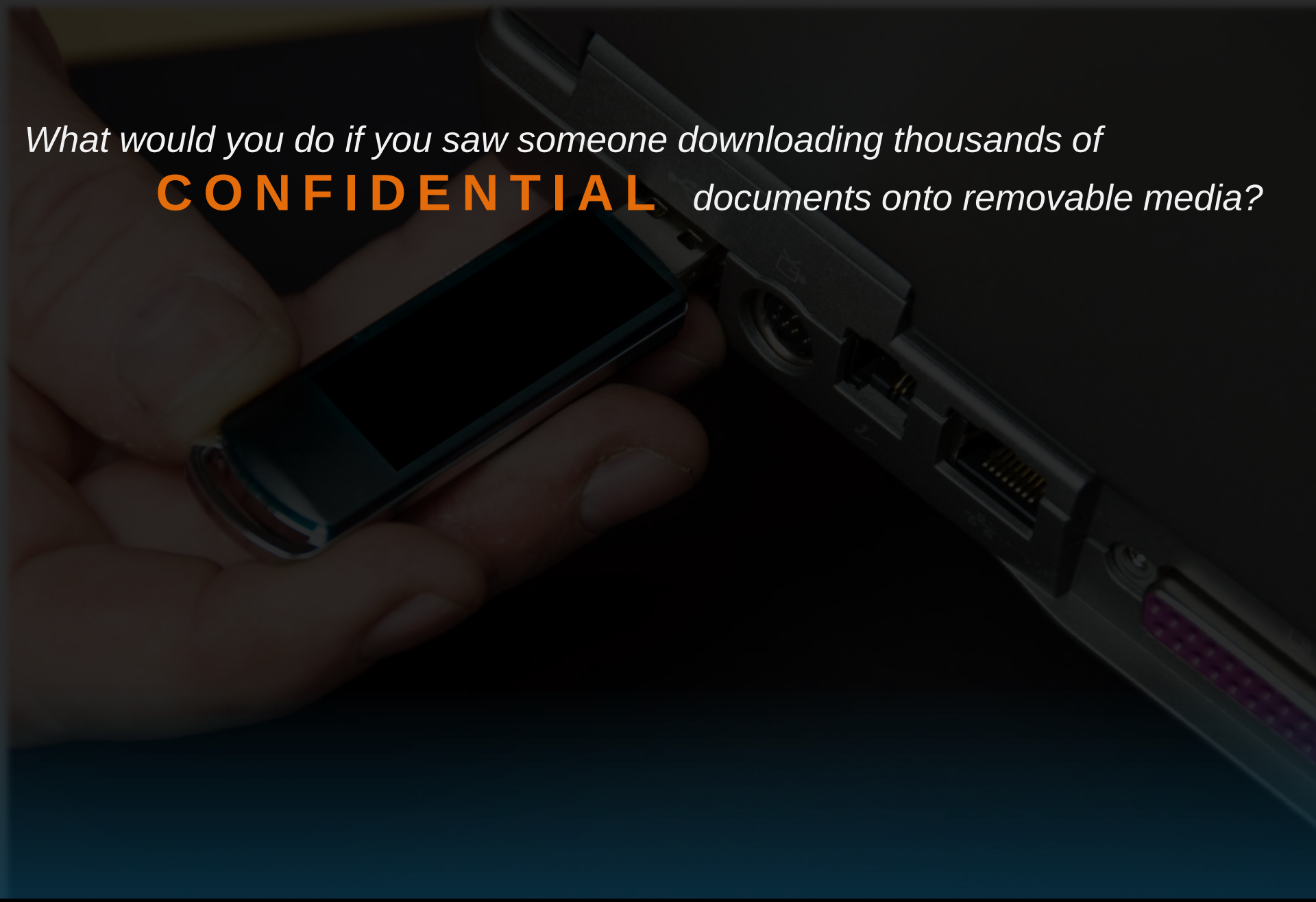
Thank you,

John Doe

What if the worker in charge of your medical records assumed the identity of the doctor to

TAMPER

with the results?



What do you think the

CONSEQUENCES

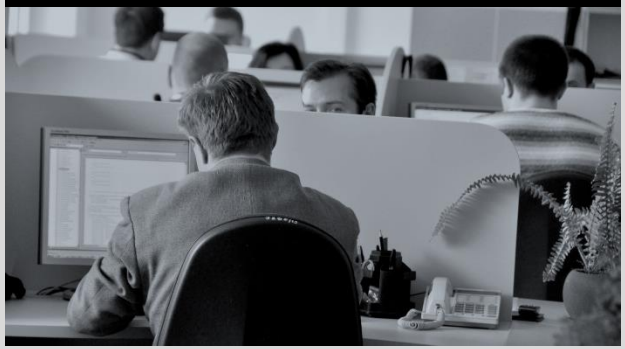
are for being an insider threat?

Insider Threat: It may not be what you think

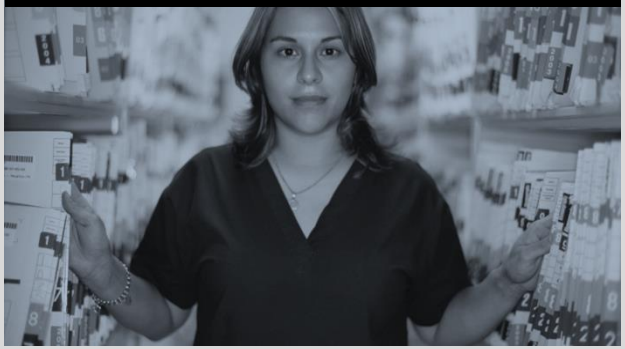
Module 1

Common Terms

Insiders



Insider Threats

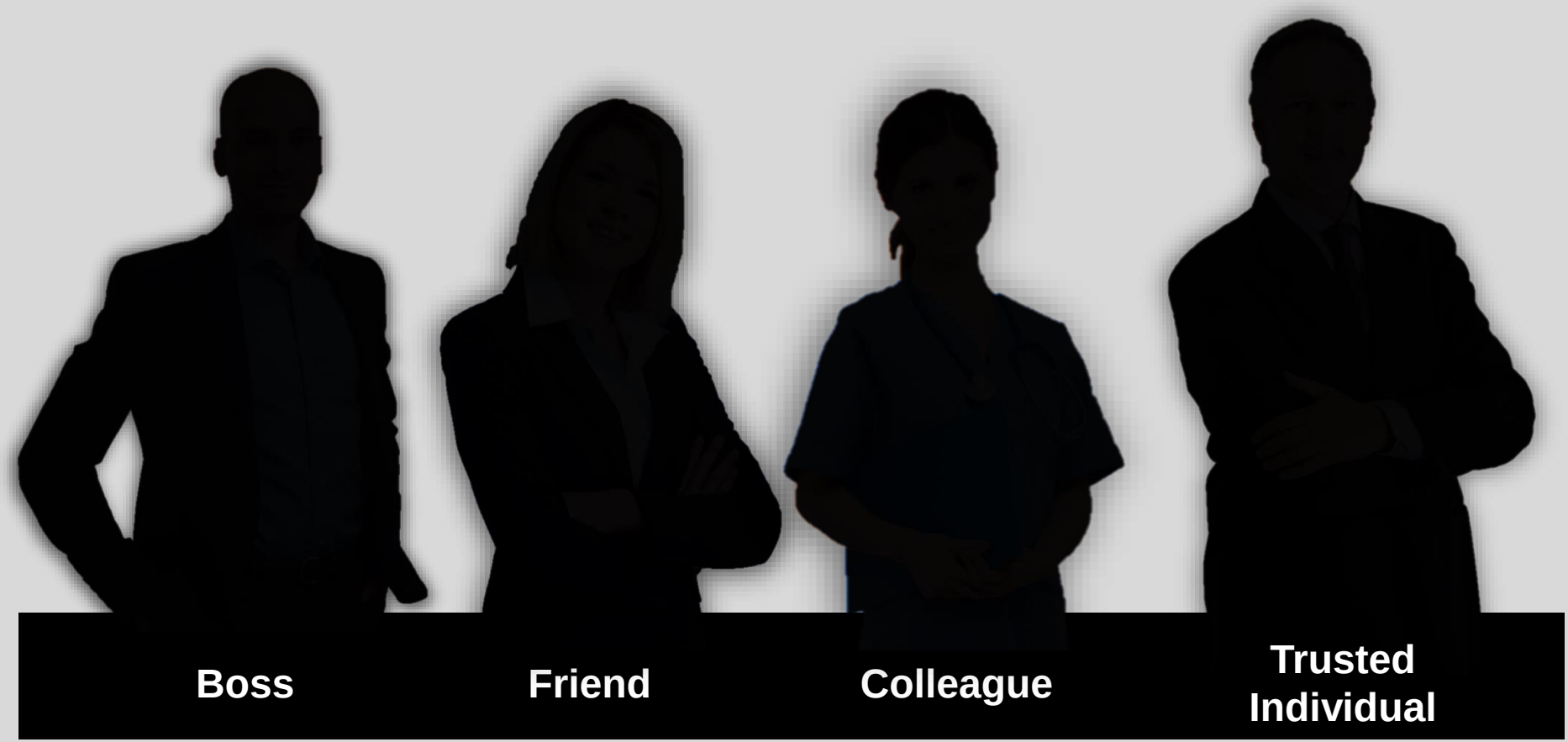


Insider Incidents

Insider Threat: It may not be what you think

Module 1

What does an Insider Threat look like?



Insider Threat: What it is

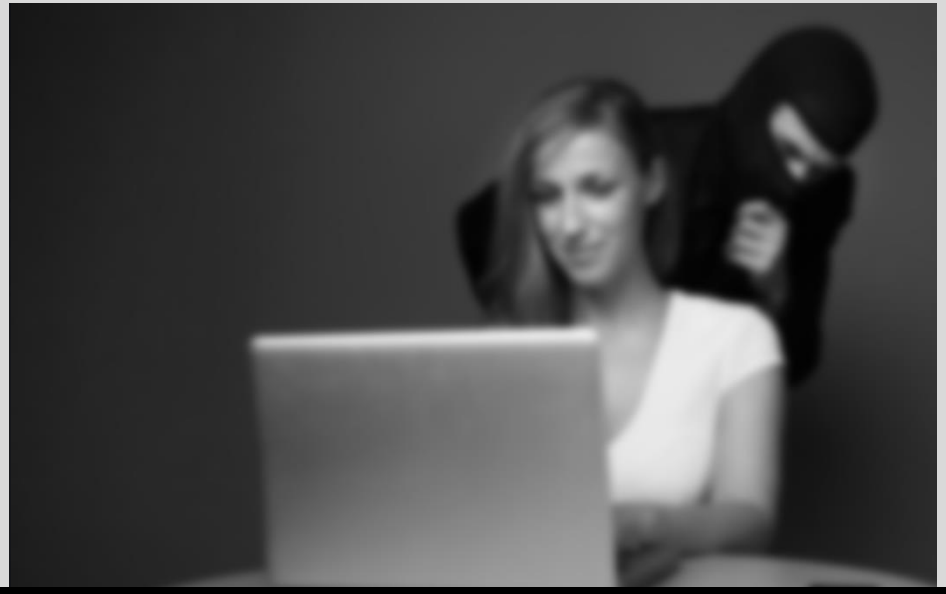
Module 2

The CERT Insider Threat Definition

A malicious insider is a **current** or **former employee**, **contractor**, or other **business partner** who has or had authorized access to an organization's network, system or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, availability, or integrity of the organization's information or information systems.

Another Type of Insider: Unintentional

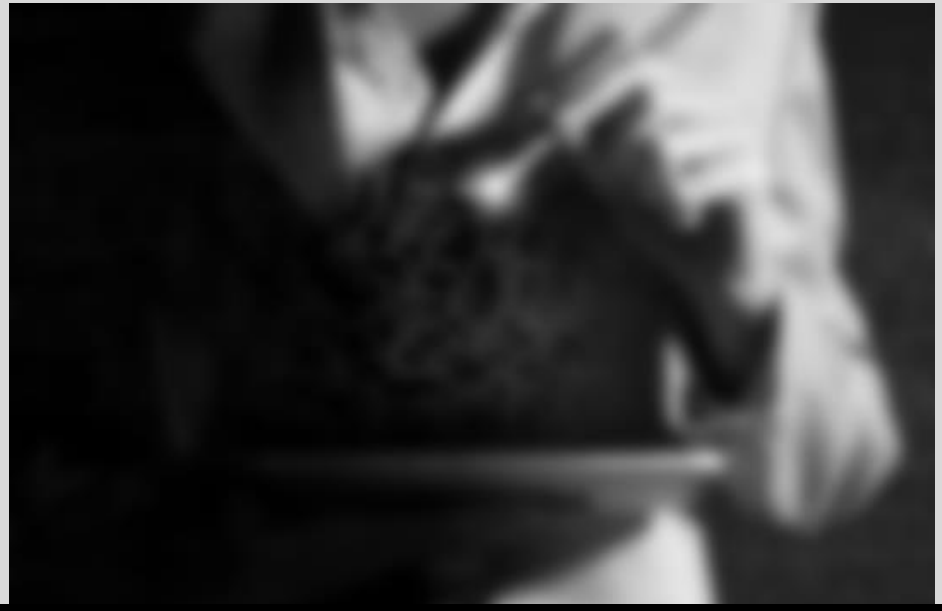
An unintentional insider is a **current** or **former employee**, **contractor**, or other **business partner** who has or had authorized access to an organization's network, system, or data and who, through their action/inaction without malicious intent causes harm or substantially increases the probability of future serious harm to the confidentiality, availability, or integrity of the organization's information or information systems.



Why is Insider Threat different from other types of threats?

Insiders pose a substantial threat by virtue of their knowledge of, and access to, their employers' systems and/or databases

Insiders can bypass existing physical and electronic security measures through legitimate measures



The Insider Threat

There is not one “type” of insider threat

- Threat to an organization’s critical assets:
  - People
  - Facilities
  - Information
  - Technology

- Impact is to Confidentiality, Availability, Integrity
- Based on the motive(s) of the insider

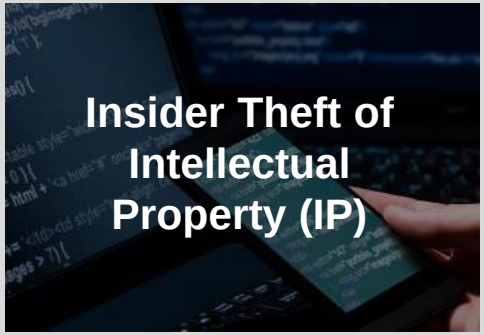
It is up to the organization to identify which of their assets are critical and apply protection strategies appropriate to the value of the asset

Insider Threat: What it is

Module 2

Types of Insider Threats?

You will learn more about each insider threat type in the next module



There are also other types of insider threats that do not necessarily fit into any one category. These miscellaneous forms of insider threats can be:

- Disclosure of information the insider believed should be in the public domain
- Query of high-profile individuals to access personal information

Types of Insider Threats

Module 3

INFORMATION TECHNOLOGY(IT) SABOTAGE

Consider the following real-life event….

Information Technology (IT) Sabotage

An insider's use of IT to direct specific harm at an organization or an individual

- Deletion of information
- Bringing down systems
- Web site defacement to embarrass organization

Patterns of Information Technology (IT) Sabotage Crimes

From the research performed by the CERT Insider Threat Center, typically IT sabotage events occur over time, and typically are the result of disgruntled people seeking revenge for some perceived injustice by the organization.

INSIDER THEFT OF INTELLECTUAL PROPERTY (IP)

Consider the following real-life event….

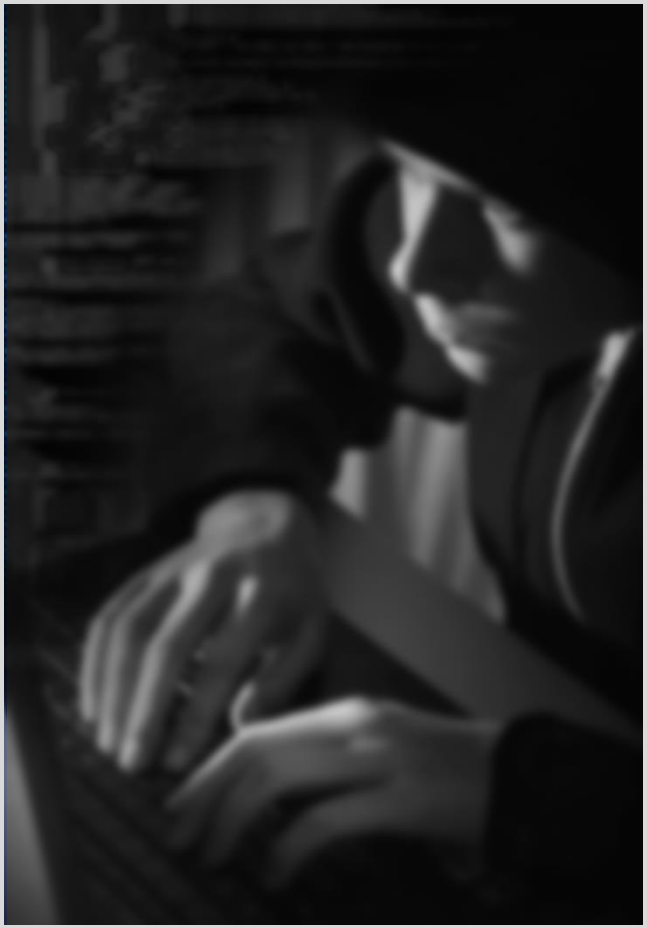
Victim Organization

Competitor Organization

Insider Theft of Intellectual Property (IP)

An insider's use of IT to steal intellectual property from the organization

- Proprietary source code
- Proprietary engineering designs
- Scientific formulas
- Confidential customer information
- Industrial Espionage



Patterns of Theft of Intellectual Property (IP) Crimes

From the research performed by the CERT Insider Threat Center, theft of Intellectual Property coincides with someone leaving the organization and wanting to take something with them. They may take physical assets and/or electronic assets. They display unusual behavior prior to leaving the organization.

INSIDER FRAUD

Consider the following real-life event….

Insider Fraud

An insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information which leads to fraud (identity theft, credit card fraud)

- Theft and sale of confidential information (SSN, credit card numbers, etc.)
- Modification of critical data for pay (driver's license records, criminal records, benefit status, etc.)

Patterns of Insider Fraud Crimes

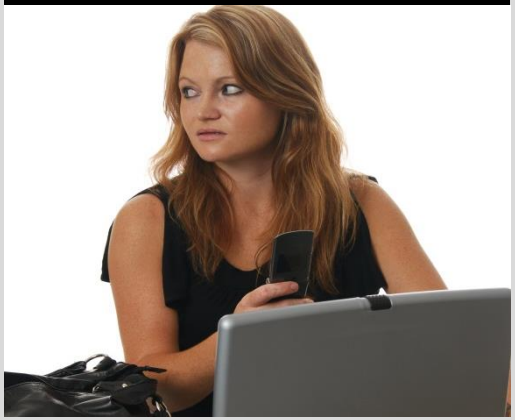
From the research performed by the CERT Insider Threat Center, Insider Fraud is performed using both electronic and physical records. Typically it involves stealing, or modifying personal information.

Types of Insider Threats

Module 3

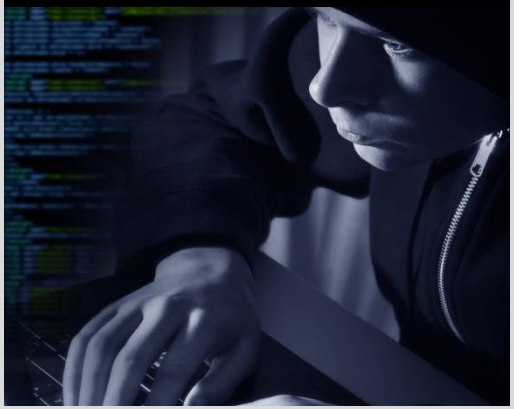
What motivates an Insider Threat?

Theft of Intellectual Property (IP)



Information Gain

Information Technology (IT) Sabotage



Revenge

Fraud

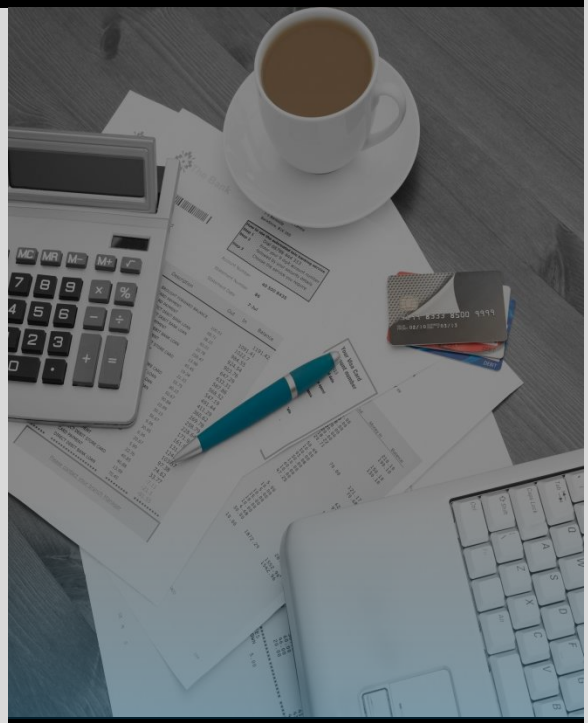
Financial Gain

Types of Insider Threats

Malicious vs. Unintentional

Fraud

Malicious



Unintentional

UNINTENTIONAL INSIDER THREAT

Consider the following real-life event….

Unintentional Insider Incident

An Unintentional Insider Incident occurs when an insider, who has or had authorized access, causes harm without malicious intent.

- Current and former employees, contractors and subcontractors, and trusted business partners
- Who have or had authorized access to any of the organization's critical assets
- Who harm the confidentiality, availability, or integrity of the organization's information and systems
- Who increase the probability of future serious harm to the confidentiality, availability, or integrity of the organization's information and systems

Patterns of Unintentional Insider Threat Crimes

Four patterns of incidents were identified based on the CERT Insider Threat Center research:

- Accidental disclosure
- Malicious code
- Improper/accidental disposal of physical records
- Portable equipment no longer in possession

When working remotely be cautious of accessing sensitive information

Impacts and Consequences of Insider Incidents

Module 4

Impacts to Individuals – of malicious and unintentional insider incidents

Even if you are an unintentional insider threat due to carelessness/ignorance there are still consequences:

- Security violation
- Difficulty finding future employment
- Loss of employment
- Fines/penalties
- Loss of freedom/liberties
- Prison

Impacts and Consequences of Insider Incidents

Module 4

Impacts to Organizations – of malicious and unintentional insider incidents

Loss of contracts

Damaged reputation

Organizational vulnerability

Loss of money

Layoffs

Loss of market share

Personal information leaked

Organization goes out of business

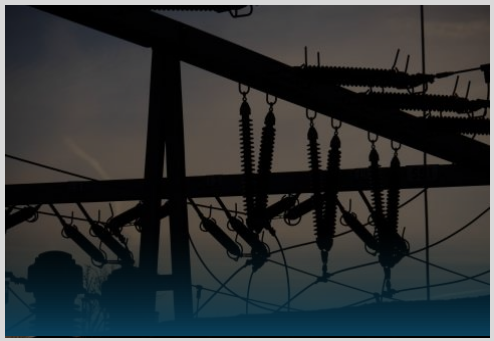
Impacts and Consequences of Insider Incidents

Module 4

Impacts to General Public – of malicious and unintentional insider incidents

Emergency Services

Safety and health

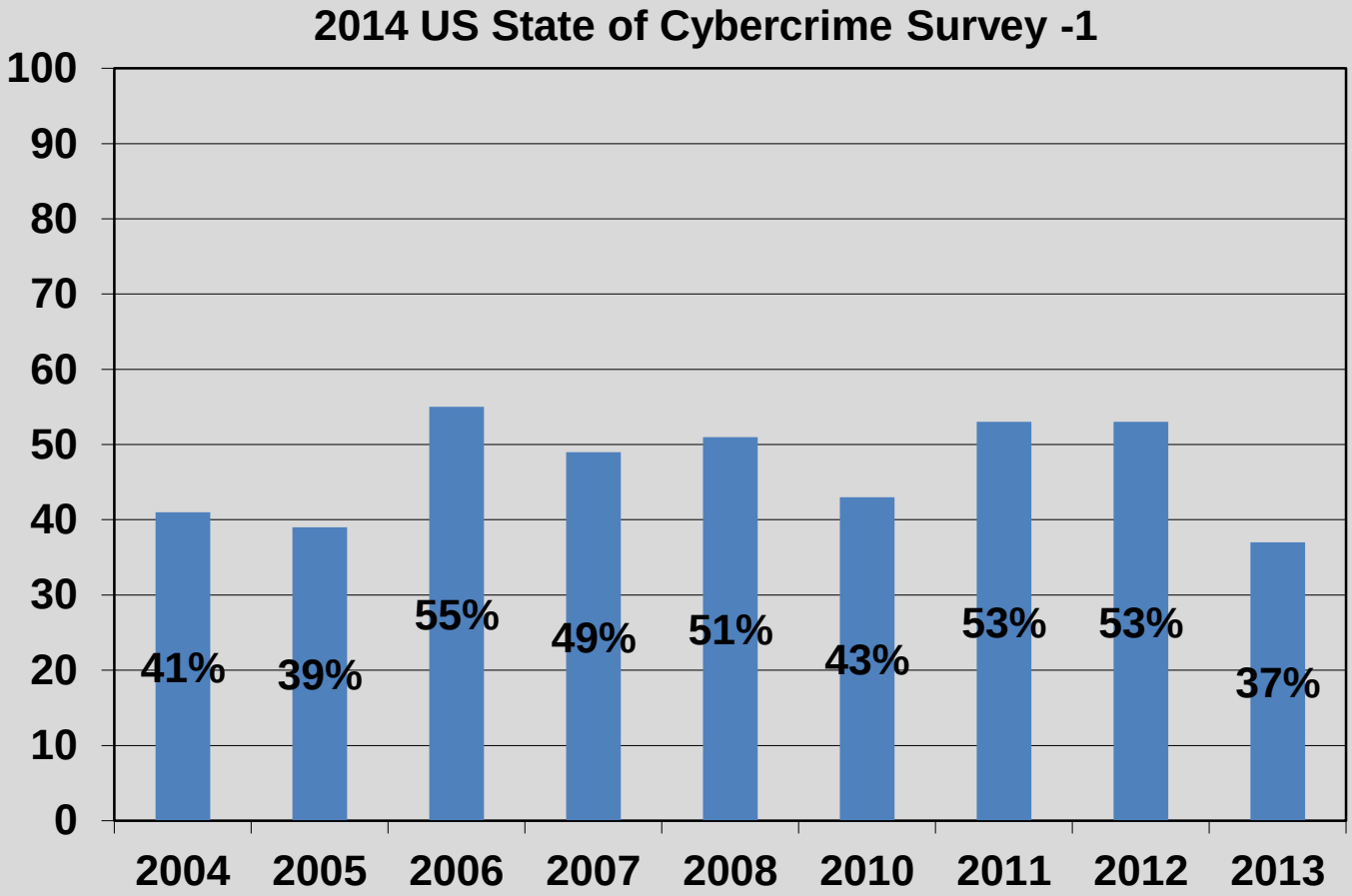


Environmental

Impacts and Consequences of Insider Incidents

Module 4

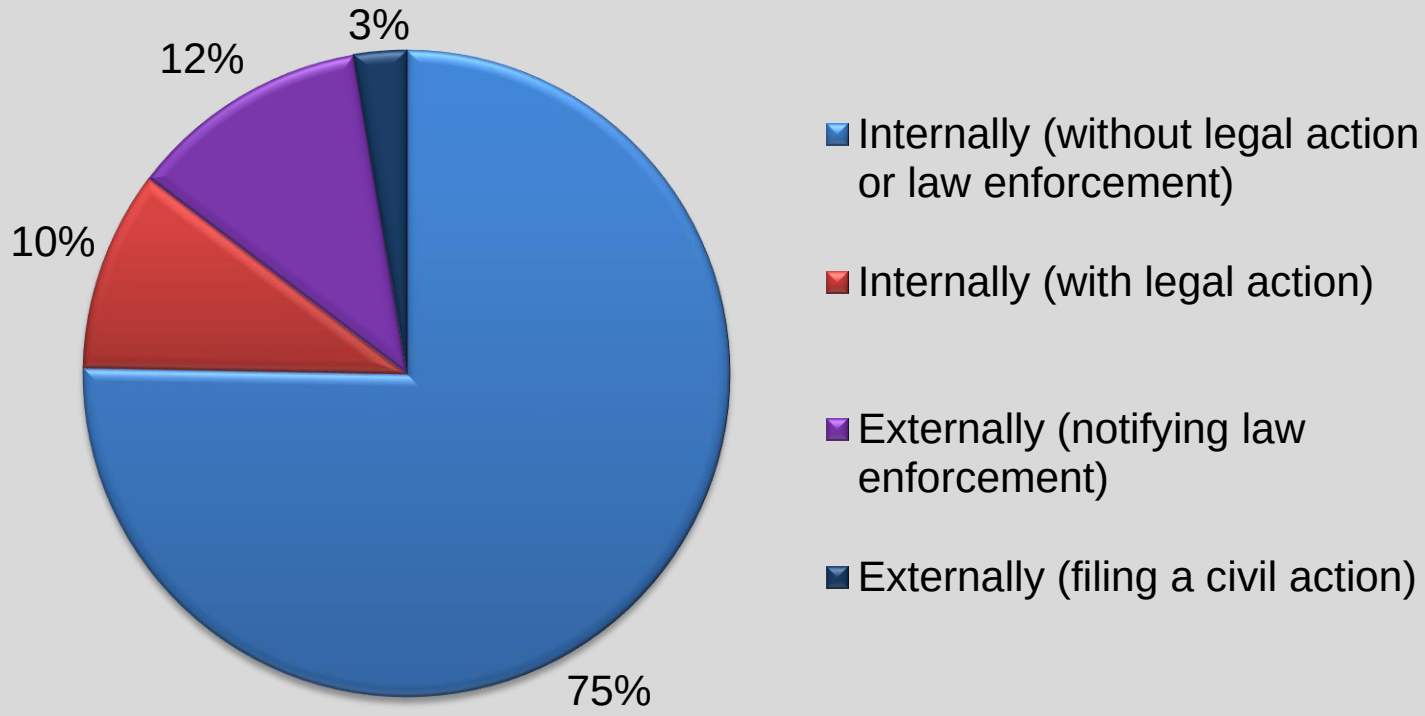
How frequently do insider incidents occur?



Source: 2014 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014

2014 US State of Cybercrime Survey - 2

How Insider Intrusions are Handled



Source: 2014 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014

Impacts and Consequences of Insider Incidents

Module 4

Reasons Cyber Crimes were not referred for legal action			
	2013	2012	2011
Damage level insufficient to warrant prosecution	34%	36%	40%
Lack of evidence/not enough information to prosecute	36%	36%	34%
Could not identify the individual/ individuals responsible for committing the eCrime	37%	32%	37%
Concerns about negative publicity	12%	9%	14%
Concerns about liability	8%	7%	9%
Concerns that competitors would use incident to their advantage	7%	6%	7%
Prior negative response from law enforcement	8%	5%	6%
Unaware that we could report these crimes	6%	5%	4%
Law enforcement suggested incident was national security related	3%	4%	4%
Other	8%	12%	11%
Don't know	21%	28%	20%

Source: 2014 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014

The Insider Incident

There is not one solution for addressing the insider threat

- Technology alone may not be the most effective way to prevent and/or detect an incident perpetrated by a trusted insider
- You can be part of the solution

Insider Incidents are infrequent, but the impacts can be substantial:

- Financial
- Operational
- Environmental
- Safety

What can you do to protect yourself?

Module 5

Remember that **YOU** *are the first line of defense against*

INSIDER INCIDENTS

Employee Responsibilities

What can I do?

As an employee of your organization, there are two crucial components to keep in mind:

- Protecting critical assets
- Reporting

What can you do to protect yourself?

Module 5

Employee Responsibilities – Protect the well-being of your organization and yourself

Protect your job and the well-being of your organization—disclosing critical information can cause your organization to close or lose its competitive edge

Don’t be a target--It is your duty to protect yourself. Always ensure you are in compliance with your organization’s policies and rules, and tell your security program immediately about any reportable behaviors you may witness

Every organization is different--consult your organization’s security program about reporting guidelines and processes

Employee Responsibilities - Reporting

Reporting - Consider behaviors that are reportable and tell your security program immediately

Reportable Behavior – is a violation of a practice, policy or procedure

Someone who *(common examples)*…..

- Attempts to access sensitive information without authorization
- Engages in suspicious personal contracts outside of the organization
- Discusses classified or sensitive information in a non-secure area
- Frequently works outside of normal hours
- Seeks to obtain clearances outside of job scope
- Obtains sensitive information that is inconsistent with job role
- Keeps sensitive information in an unauthorized area
- Attempts to access restricted areas

What can you do to protect yourself?

Module 5

Employee Responsibilities – Protecting Critical Assets

Protect your organization's critical assets - understand what you need to do to avoid becoming an unintentional insider threat:

- ***Report harassing behavior***
- ***Know and follow your organization's policies and procedures***
- ***Talk to your security team about reportable behaviors***
- ***Never share your password***
- ***Lock your computer***
- ***Do not admit anyone without a badge***
- ***Do not click on suspicious links or attachments***
- ***Avoid posting to social media***

What can you do to protect yourself?

Module 5

Best Practices for Managers and Supervisors

If you are a manager or supervisor within your organization, here are a few recommended best practices to protect yourself, employees and your organization's critical assets:

- Incorporate insider threat awareness into periodic security training for all employees
- Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior
- Anticipate and manage negative issues in the work environment
- Know your assets
- Implement strict password and account management policies and practices
- Be especially vigilant regarding social media

The Best Practices outline above are from CERT's "Common Sense Guide to Mitigating Insider Threats". For the complete list of best practices, please reference the attachments area of this course

What would you do if someone **TARGETED** *you?*

What if they **COERCED** *you?*

Promised you monetary gain?

Report suspicious behaviors!

Contact your security team about reportable behaviors!

Has anyone ever asked you for your password?

Never share or email your password!

organization asked you to let them

Direct people trying to enter your organization to your security team!

What if someone sent you a link you were unsure of?

What would you do?

Subject:

Never click on suspicious links!

Do you post anything about your organization on social media?

Avoid posting about your organization on social media!

Remember that **YOU** *are the first line of defense against*

INSIDER INCIDENTS

Be aware of the actions of others around you and tell your security program Immediately about any reportable behaviors

Understand reportable activity guidelines—consult your security program

Please consult the attachments area of this course for printable resources

If you *SEE* something,

SAY something

What can you do to protect yourself?

Final Thoughts

An insider threat can be anyone: someone you know and trust
Even YOU can be an insider threat

Everyone can be a target—whether intentionally or unintentionally

Be aware of reportable behaviors—***If you see something, say something***

Don’t be an unintentional insider threat—protect your organization’s critical assets

Tell your security program immediately about reportable behaviors—YOU are the first line of defense against insider threats!

For additional information visit the CERT website at www.cert.org, or follow the link on the course description field of this course player