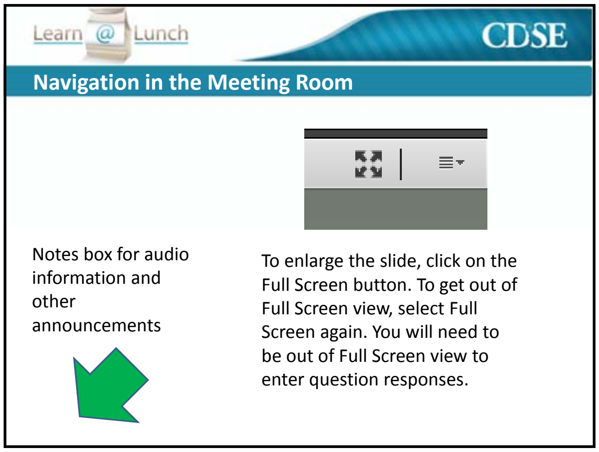
Cybersecurity **Webinar Series**

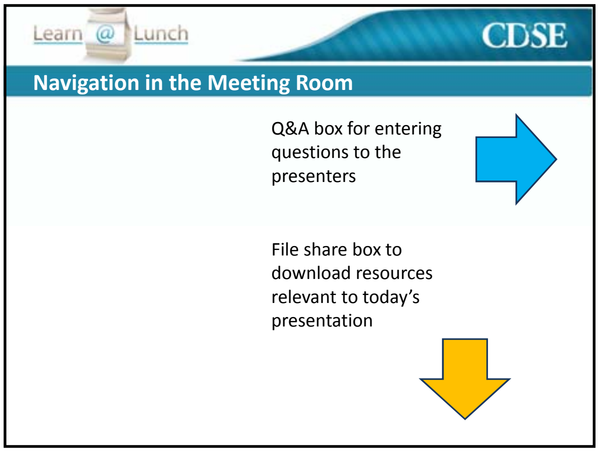
## DSS Cyber Insider Threat


Learn @ Lunch
CDSE

## Navigation in the Meeting Room

Notes box for audio information and other announcements

To enlarge the slide, click on the Full Screen button. To get out of Full Screen view, select Full Screen again. You will need to be out of Full Screen view to enter question responses.


Learn @ Lunch
CDSE

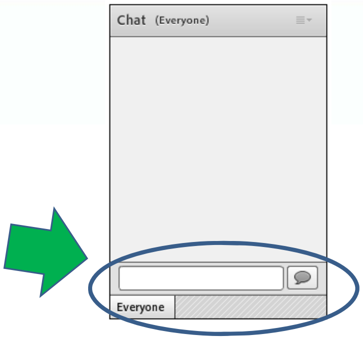
## Navigation in the Meeting Room

Q&A box for entering questions to the presenters

File share box to download resources relevant to today’s presentation

Learn @ Lunch CDSE

## Example of a Chat Question



Learn @ Lunch CDSE

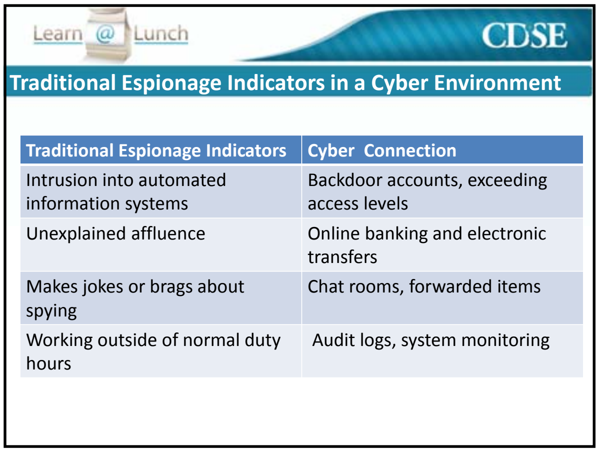
## Overview

- Discuss cyber insider threats and indicators
- Identify commonalities of insider IT and espionage threats
- Discuss observable and reportable characteristics of cyber insider threat
- Identify best practices for the prevention and detection of cyber insider threats

Learn @ Lunch CDSE

## Traditional Espionage Indicators in a Cyber Environment

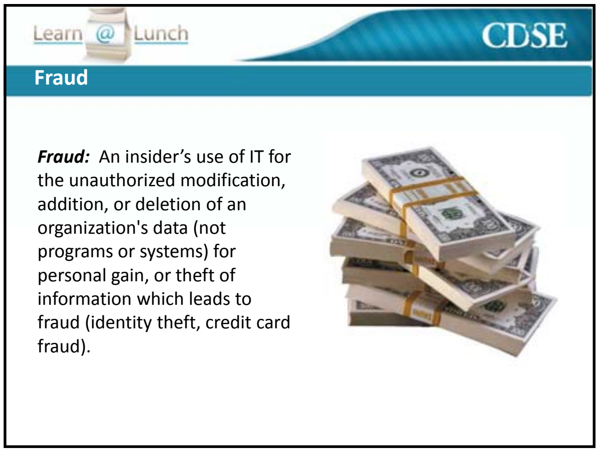
| Traditional Espionage Indicators | Cyber Connection |
|---|---|
| Foreign contacts | Social media, email, texting |
| Foreign preference/loyalty | Blogs, posts, social media |
| Intentional mishandling of classified information | Thumb drives, illicit downloading/uploading, unauthorized Copies |
| Repeated involvement in security violations | Misuse of information systems, unauthorized access, sharing passwords |



Learn @ Lunch CDSE

## Traditional Espionage Indicators in a Cyber Environment

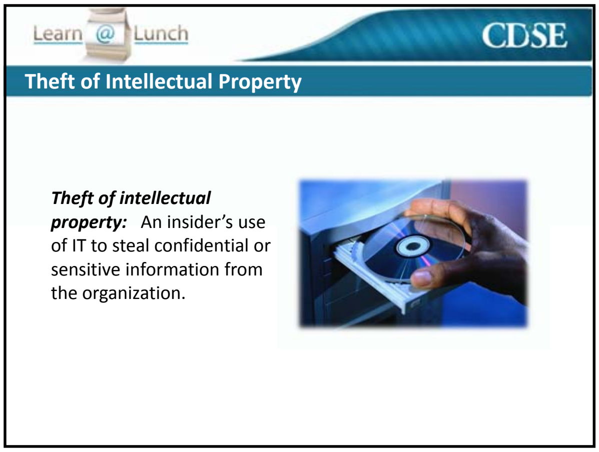
| Traditional Espionage Indicators | Cyber Connection |
|---|---|
| Intrusion into automated information systems | Backdoor accounts, exceeding access levels |
| Unexplained affluence | Online banking and electronic transfers |
| Makes jokes or brags about spying | Chat rooms, forwarded items |
| Working outside of normal duty hours | Audit logs, system monitoring |



Learn @ Lunch CDSE

## Fraud

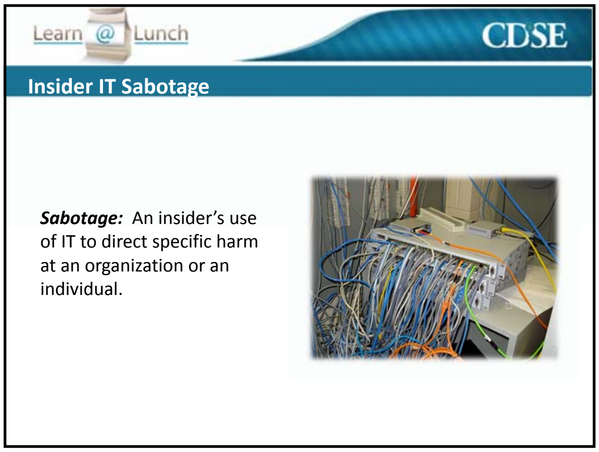
***Fraud:*** An insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information which leads to fraud (identity theft, credit card fraud).



Learn @ Lunch CDSE

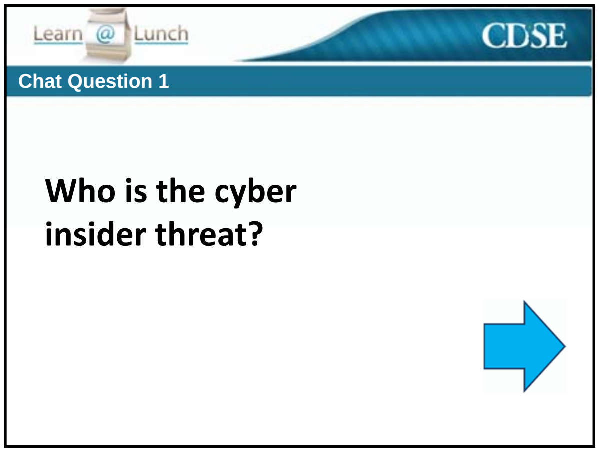
## Theft of Intellectual Property

***Theft of intellectual property:*** An insider's use of IT to steal confidential or sensitive information from the organization.



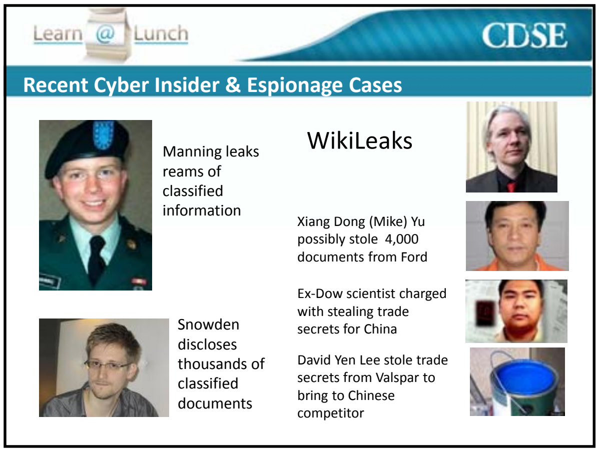
## Insider IT Sabotage

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



## Chat Question 1

**Who is the cyber insider threat?**



## Recent Cyber Insider & Espionage Cases

Manning leaks reams of classified information

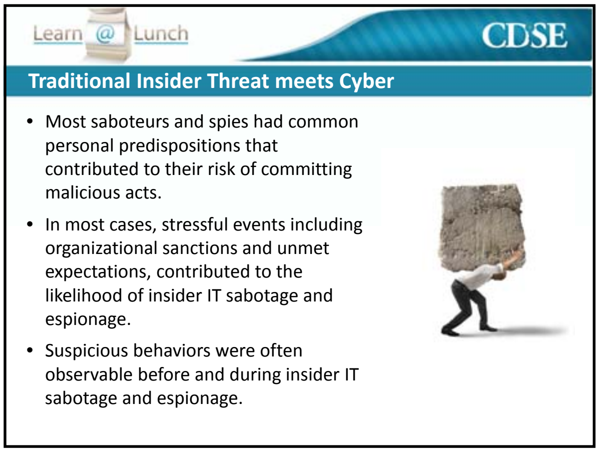
WikiLeaks

Xiang Dong (Mike) Yu possibly stole 4,000 documents from Ford

Ex-Dow scientist charged with stealing trade secrets for China

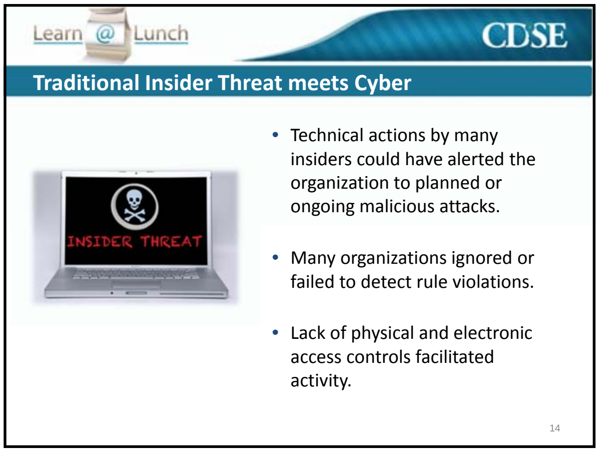
Snowden discloses thousands of classified documents

David Yen Lee stole trade secrets from Valspar to bring to Chinese competitor



## Traditional Insider Threat meets Cyber

- Most saboteurs and spies had common personal predispositions that contributed to their risk of committing malicious acts.
- In most cases, stressful events including organizational sanctions and unmet expectations, contributed to the likelihood of insider IT sabotage and espionage.
- Suspicious behaviors were often observable before and during insider IT sabotage and espionage.

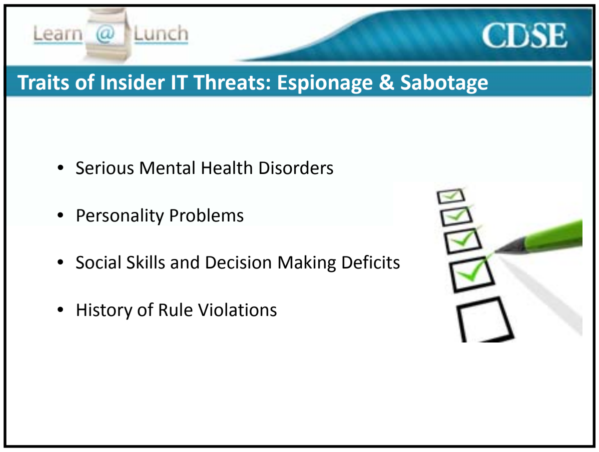


## Traditional Insider Threat meets Cyber

INSIDER THREAT

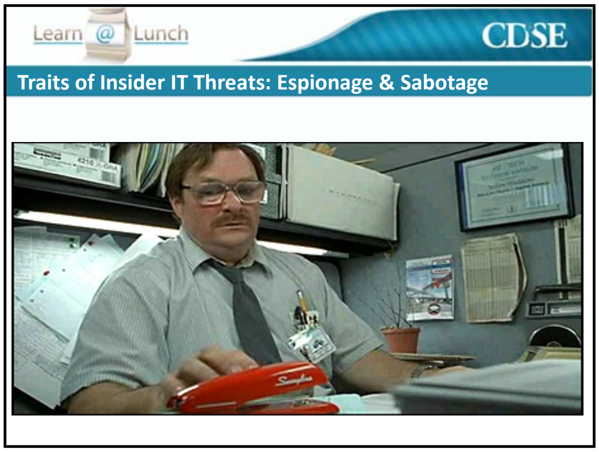
- Technical actions by many insiders could have alerted the organization to planned or ongoing malicious attacks.
- Many organizations ignored or failed to detect rule violations.
- Lack of physical and electronic access controls facilitated activity.

14

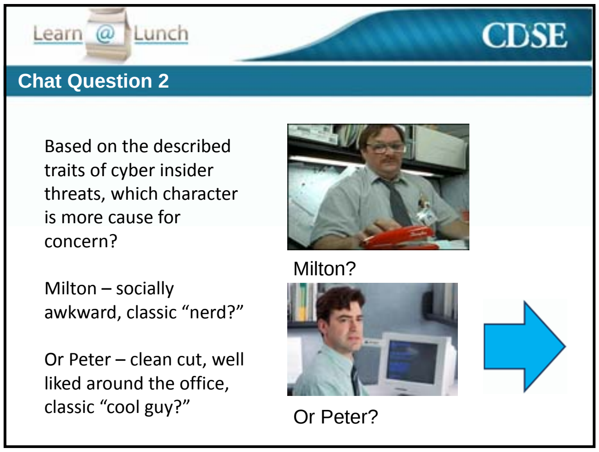


## Traits of Insider IT Threats: Espionage & Sabotage

- Serious Mental Health Disorders
- Personality Problems
- Social Skills and Decision Making Deficits
- History of Rule Violations



## Traits of Insider IT Threats: Espionage & Sabotage



## Chat Question 2

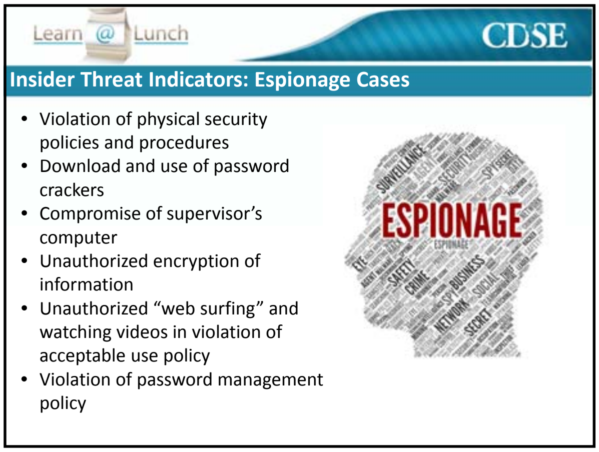
Based on the described traits of cyber insider threats, which character is more cause for concern?

Milton – socially awkward, classic “nerd?”

Or Peter – clean cut, well liked around the office, classic “cool guy?”

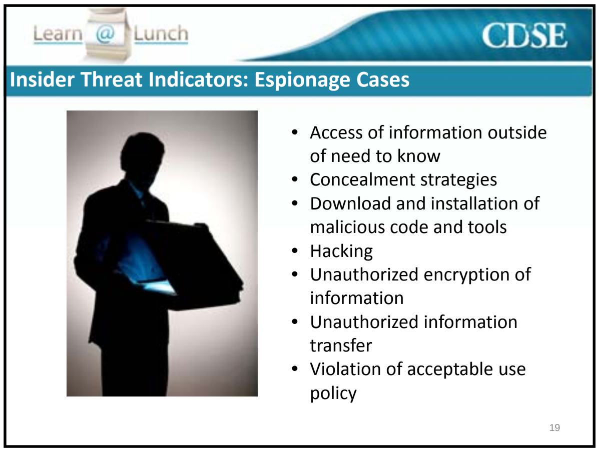
Milton?

Or Peter?



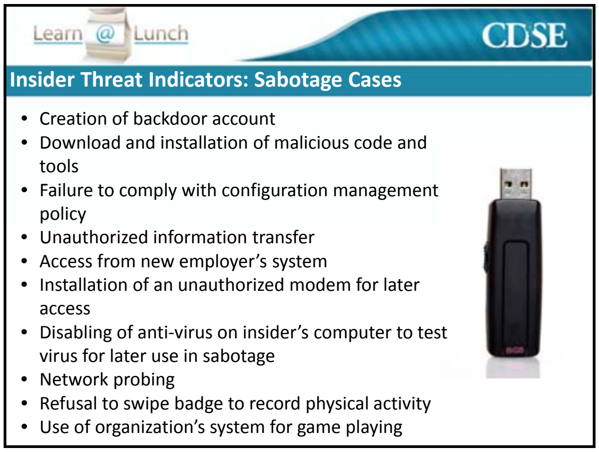
## Insider Threat Indicators: Espionage Cases

- Violation of physical security policies and procedures
- Download and use of password crackers
- Compromise of supervisor’s computer
- Unauthorized encryption of information
- Unauthorized “web surfing” and watching videos in violation of acceptable use policy
- Violation of password management policy



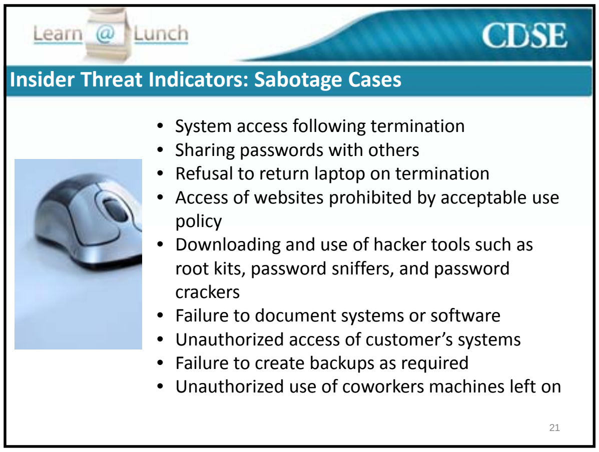
## Insider Threat Indicators: Espionage Cases

- Access of information outside of need to know
- Concealment strategies
- Download and installation of malicious code and tools
- Hacking
- Unauthorized encryption of information
- Unauthorized information transfer
- Violation of acceptable use policy



## Insider Threat Indicators: Sabotage Cases

- Creation of backdoor account
- Download and installation of malicious code and tools
- Failure to comply with configuration management policy
- Unauthorized information transfer
- Access from new employer’s system
- Installation of an unauthorized modem for later access
- Disabling of anti-virus on insider’s computer to test virus for later use in sabotage
- Network probing
- Refusal to swipe badge to record physical activity
- Use of organization’s system for game playing



## Insider Threat Indicators: Sabotage Cases

- System access following termination
- Sharing passwords with others
- Refusal to return laptop on termination
- Access of websites prohibited by acceptable use policy
- Downloading and use of hacker tools such as root kits, password sniffers, and password crackers
- Failure to document systems or software
- Unauthorized access of customer’s systems
- Failure to create backups as required
- Unauthorized use of coworkers machines left on

Learn @ Lunch CDSE

## Insider Indicators Plus:

- Opportunity
- Motive
- Lack of Inhibition for Betray
- Trigger

Learn @ Lunch CDSE

## Unwitting/Careless Insiders

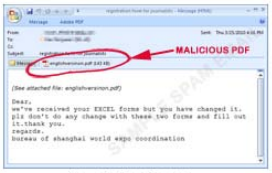
"There is No Patch for People"

Learn @ Lunch CDSE

## Chat Question 3

Despite your aggressive efforts in Cybersecurity Training and Awareness, an employee reports that they downloaded an attachment to an email which they now suspect may have been malicious.

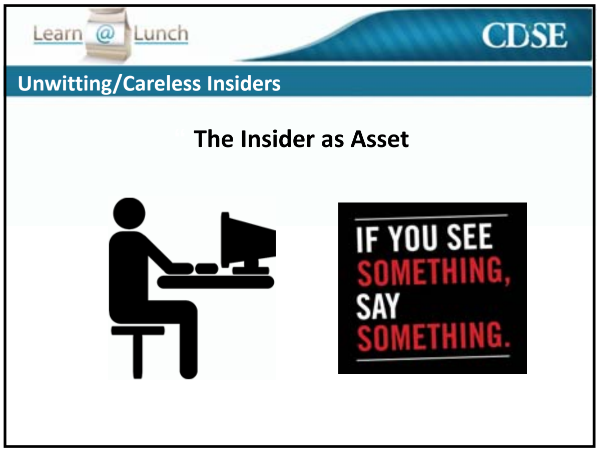
How do you respond?



(See attached file: englishversinon.pdf)

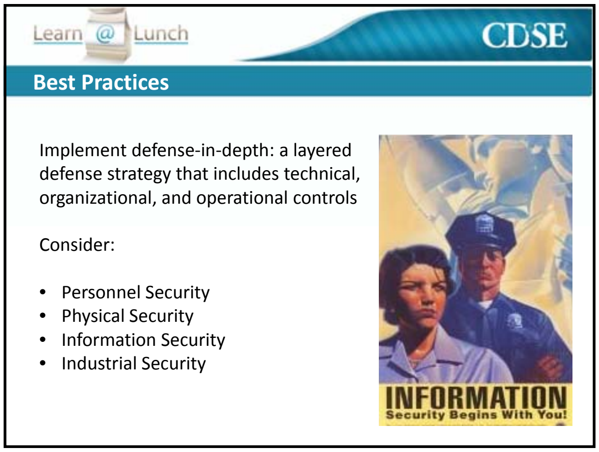
Dear,
we've received your EXCEL forms but you have changed it.
plz don't do any change with these two forms and fill out it.thank you.
regards.
bureau of shanghai world expo coordination

Figure 1. Sample spam



## Unwitting/Careless Insiders

### The Insider as Asset

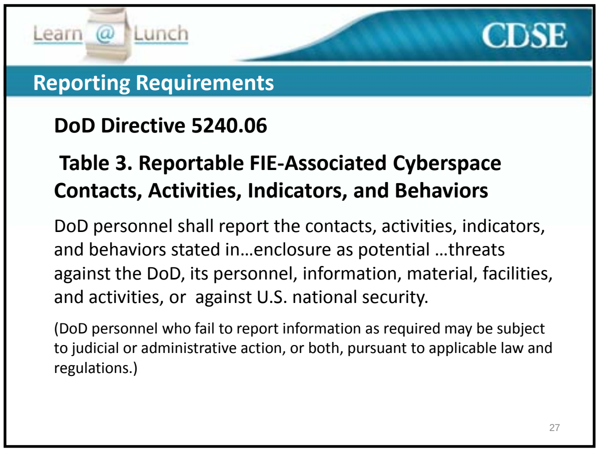


## Best Practices

Implement defense-in-depth: a layered defense strategy that includes technical, organizational, and operational controls

Consider:

- Personnel Security
- Physical Security
- Information Security
- Industrial Security



## Reporting Requirements

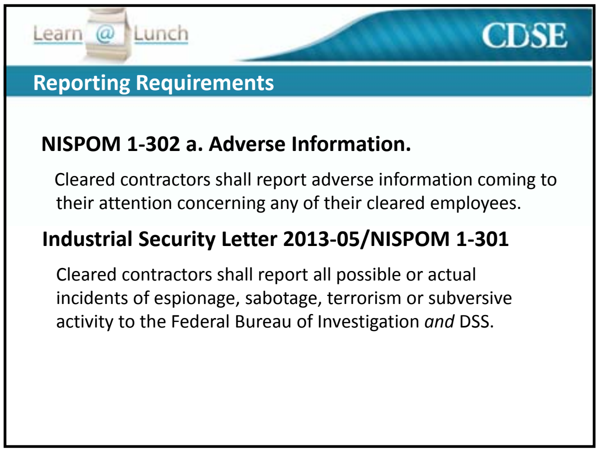
**DoD Directive 5240.06**

**Table 3. Reportable FIE-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors**

DoD personnel shall report the contacts, activities, indicators, and behaviors stated in…enclosure as potential …threats against the DoD, its personnel, information, material, facilities, and activities, or against U.S. national security.

(DoD personnel who fail to report information as required may be subject to judicial or administrative action, or both, pursuant to applicable law and regulations.)

27



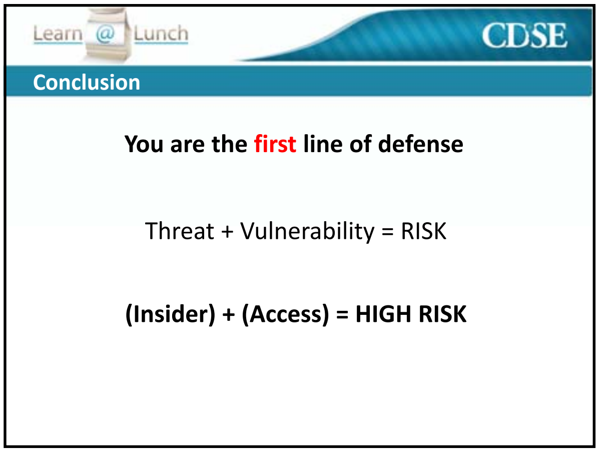
## Reporting Requirements

**NISPOM 1-302 a. Adverse Information.**

Cleared contractors shall report adverse information coming to their attention concerning any of their cleared employees.

**Industrial Security Letter 2013-05/NISPOM 1-301**

Cleared contractors shall report all possible or actual incidents of espionage, sabotage, terrorism or subversive activity to the Federal Bureau of Investigation *and* DSS.



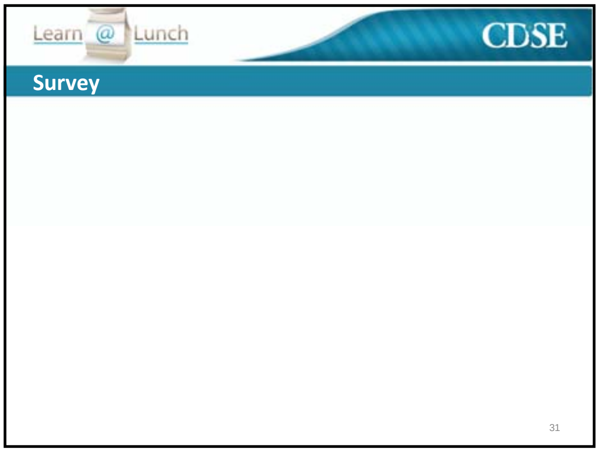
## Conclusion

**You are the first line of defense**

Threat + Vulnerability = RISK

**(Insider) + (Access) = HIGH RISK**

## Questions



## Survey

31

## Cybersecurity Training Products

**Past Webinars**

- Insider Threat
- Potential Espionage Indicators (PEI): Detecting Actions Outside the Norm

**All Other Training**

- CDSE Cybersecurity