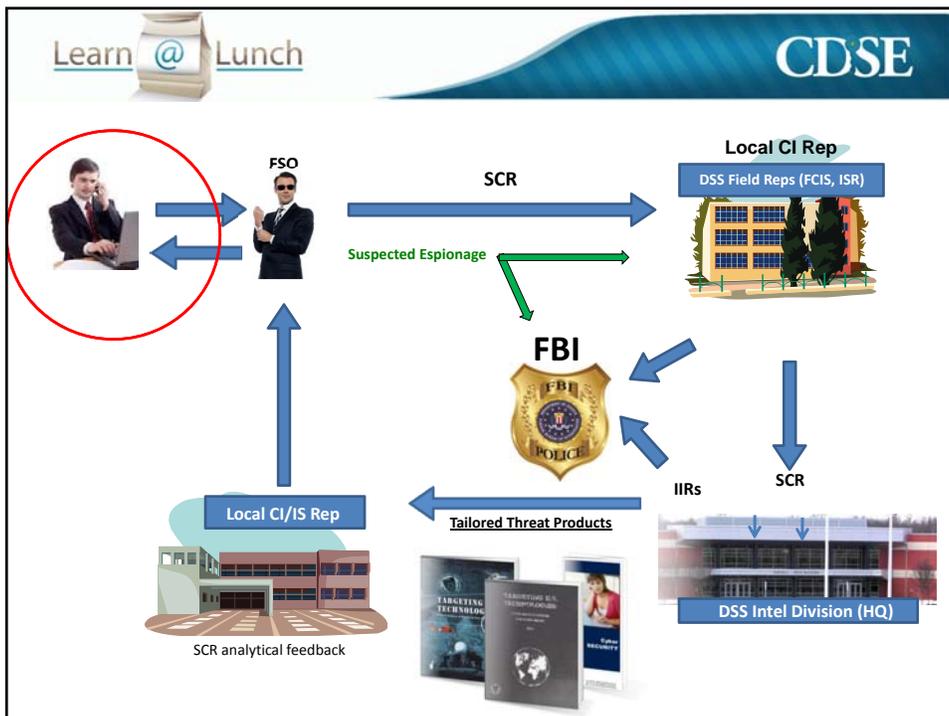


Industrial Security Webinar Series

Learn @ Lunch



Reportable Cyber Events



Learn @ Lunch 

## Most Commonly Used Collection Methods

- A. Unsolicited requests for information
- B. Suspicious network activity
- C. Targeting at conferences, conventions, and trade shows
- D. Insider threat
- E. Solicitation and employment
- F. Foreign Visits

Learn @ Lunch 

## Quick Poll

Have you reported a discovered cyber threat in the past year to your DSS office?

- A. Yes
- B. No
- C. I know some else who did

Learn @ Lunch UNCLASSIFIED CDSE

## What are Reportable Cyber Issues?

Recognizing categories of e-mails:

- Valid SCRs
- Potential cyber threat
- Spam or bulk e-mails



UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

## What are Reportable Cyber Issues?

- A cyber event represents a potential risk, and is reportable to DSS as part of the SCR process
- Cyber issues are the suspicious network activity component of SCR reporting, and touch on other areas as well

UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

---

## Poll Question 1

Which of the following are reportable Cyber Events?

- A. Exfiltration of protected program data
- B. Failed log-in attempts by an authorized user
- C. Spam e-mails
- D. Spam e-mails with attachments
- E. Introduction of unauthorized software or hardware to a protected system

UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

---

## What is Suspicious Network Activity?

- Any attempts to carry out intrusions into cleared industry networks and/or the exfiltration of protected information
  - Cyber intrusions
  - Viruses
  - Malware
  - Backdoor attacks
  - Unauthorized acquisition of usernames and passwords



UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

## Two Categories of Reportable Cyber Issues

Human & Cyber Activity



UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

## Human Activity

- Suspicious questioning
- Unauthorized system changes
- Unauthorized use
- Accessing files without a need-to-know
- Discovery of a “backdoor”
- Poor IT security practices

UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

## Suspicious Network or Cyber Activities

- Suspected intrusions or data exfiltration
- Root level compromises
- User level compromises
- Log-in attempts from an unauthorized user/unauthorized system access attempts
- Port scans
- Discoveries of malicious code
- Unauthorized hardware and software introductions or modifications

UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

## Poll Question 2 – What Do You Do?

- An employee of your firm forwards you an e-mail item, and reports it as suspicious.
- You look at the e-mail, and note that it is from an overseas investment firm.
- It discusses an investment opportunity, and asks the recipient to provide an unspecified list of projects that can be invested in.
- (more)

UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

**Poll Question 2 (cont.)– What Do You Do?**

- You notice that the e-mail doesn't list anything specific to your company.
- The e-mail did not directly address the recipient, indicating that the e-mail may have been sent in bulk.
- The e-mail contains an attachment.

UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

**Poll Question 2 – What Do You Do?**

- A. Report this as a suspicious item to DSS
- B. Report this as SPAM to DSS
- C. Inform the employee that this is SPAM, and don't report it

Learn @ Lunch UNCLASSIFIED CDSE

---

### Report to DSS if...

- The e-mail contains a request for information, or a request to purchase, and you either don't know the sender, or can't verify that the request is legitimate

AND

- The e-mail is apparently addressed directly to your firm, and/or mentions your specific products or services



UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

---

### Do Not Report to DSS if...

- The e-mail is a SPAM e-mail

An e-mail is likely to be SPAM if it is sent in bulk, and if it is impersonal in nature



UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

---

**Dear Sir/Madam:**

We got your contact through our buying source, and we therefore deemed it wise to know more about you and your esteemed company or organization and as we hope to have a good business relationship with you and your able firm. We are a fast growing supplier, and we are interested in your product please do send to us details of your products and company. And Please Quote below:

1. Prices FOB	4. MOQ
2. Payment terms	5. Your website
3. Delivery Period	6. Specified delivery date assuming from the Date of Order.

UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

---

**Identifying Spam and Scam E-mails**

- Know some of the characteristics of SPAM e-mail
  - SPAM doesn't need to be reported to DSS
- Defense Industry needs to be aware of the risks of spam e-mails
  - DON'T respond to SPAM e-mails
  - SPAM may be a "scam," or an attempt to defraud you.
  - Suspected fraud can be reported to the Internet Crime Complaint Center (IC3) at [www.ic3.gov](http://www.ic3.gov)

UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

## Identifying Spam and Scam E-mails

- As a general rule of thumb:
  - A true SCR will generally be addressed directly to you, or your firm, and will ask for something specific from you
  - A spam/scam e-mail may be generic in nature, may be addressed in bulk, and may offer something

UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

## Tips for Identifying Typical Spam E-mail

- Many spam e-mails are well known, such as the Nigerian scam
- These “advance fee fraud” scams ask you to provide a fee up front
- Spams/scams are always evolving, and you may not readily recognize them



UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

---

## Tips for Identifying Typical Spam E-mail

- Check to see if they are asking for anything specific from your firm
- If there is no indication of that, do a quick internet search
- Check the sender's name, e-mail address, other information – they may come up as a known spammer



UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

---

## Other Tools

- FBI's website:  
[www.fbi.gov/scams-safety/fraud/internet\\_fraud](http://www.fbi.gov/scams-safety/fraud/internet_fraud)
- IC3's website: [www.ic3.gov/media/default.aspx](http://www.ic3.gov/media/default.aspx)
- Be aware of some common tactics, such as creating a sense of urgency

Spammers use “trigger words” to create that urgency

UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

---

**Poll Question 3 – What Do You Do?**

- An employee of your firm forwards you an e-mail they received on their work account, that appeared to be from their bank.
- It contained an official bank logo, and told the employee to click on a link to re-set their Internet banking password.
- The employee questions the legitimacy of the e-mail, but was concerned, because the e-mail was sent directly to the employee by name.

UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

---

**Poll Question 3 – What Do You Do?**

- A. Report the item promptly to DSS as a “phishing scam”
- B. Do not report it to DSS, but inform the employee that this is a potential criminal concern, and they should report it to their bank

Learn @ Lunch UNCLASSIFIED CDSE

---

**Poll Question 4 – What Do You Do?**

- You receive an e-mail from a co-worker that asks you to take a look at an attached product development schedule.
- You know this co-worker, and something about the wording of the e-mail seems strange.
- You call this co-worker, and determine that she did not send the e-mail.
- You recognize that you are dealing with a spear-phishing e-mail.

UNCLASSIFIED

Learn @ Lunch UNCLASSIFIED CDSE

---

**Poll Question 4 – What Do You Do?**

- A. You report the item to your IT department
- B. You have the employee respond to the e-mail, and ask the sender to divulge who they really are
- C. You forward the e-mail, with attachment, to DSS as an SCR
- D. You forward only the e-mail header data and text to DSS, and use a secure file sharing system to send the attachment

Learn @ Lunch 

## Conclusion

- Cyber threats to cleared industry are a real and growing threat
- Your vigilance to identify the threat, and your reporting, is vital!



Learn @ Lunch 

## Questions...

