Cyber Enabled Threats to Cleared Industry

Agenda

• Counterintelligence, Cyber Counterintelligence, and the NISP
• The DSS Mission and Counterintelligence Role
• Cyber Enabled Intelligence Activities
• Reporting Requirements

What is Counterintelligence?
What is Cyber Counterintelligence?
How do these definitions apply to the NISP?
DSS Mission
DSS supports national security and the warfighter, secures the nation's technological base, and oversees the protection of U.S. and foreign classified information in the hands of industry.

CI Mission
DSS CI identifies unlawful penetrators of cleared U.S. defense industry and articulates the threat for industry and U.S. Government leaders.

Scope
- 10+K firms, 13+K facilities, 1.2m people
- 1 CI professional/261 facilities
- 12% of facilities report

Cyber Enabled Threats to Cleared Industry

How does Cyber enable intelligence activities at cleared industry?

Academic Solicitation
- Typically a foreign student contacts a professor
- Builds a trust through communicating via email
- Trust relationship is exploited by sending a weaponized academic paper to the target

Seeking Employment
- Foreign actor seeking employment with a cleared company
- Easily send a weaponized resume to the unsuspecting employer

Exploitation of Relationships
- Exploit the relationship to entice an employee to open a malicious email
- Can leverage trust to insert removable media into a company computer

Attempted Acquisition
- Front company attempting to acquire controlled technology
- Can hide true identity and intentions by communicating electronically

Request for Information
- Usually request is sent over email
- Typically involves multiple email exchanges between actor and company
- Actor can easily send weaponized document during one of the exchanges
Cyber Enabled Threats to Cleared Industry

How does Cyber enable intelligence activities at cleared industry?

Foreign Visits
- Can overtly/covertly insert malicious removable media into a company computer

Potential Espionage Indicators
- An Insider can use cyber means to elevate access on the network, easily gain access to files, and place malware on the network for foreign actors to leverage.

Cyber Enabled Threats to Cleared Industry

How does Cyber enable intelligence activities at cleared industry?

Suspicious Network Activity
- Spear phishing
- Compromised credentials
- Website compromise
- Social Networking Sites
- SQL injection

Cyber Enabled Threats to Cleared Industry

How Does the Company Protect Itself?

- Maintain good network hygiene!
- Implement good firewall rules
- Block file extensions at the email gateway
  - EXE, SCR, ZIP, VBS, etc.
- Block dynamic DNS domains
- Assume you will be compromised at some point
  - Shorten your mean time to know
How Does DSS Help?

- Defensive Cyber Operations
  - Threat products
  - Advise and assist
- Offensive Cyber Operations
  - Contractor Suspicious Contact Report referrals
- Strategic Analysis
  - Threat = Capability x Opportunities x Intent
  - Used to anticipate adversary operations

Suspicious Contact Reporting:

- NISPOM 1-302b
- NISPOM 1-301

Counterintelligence Training Products

- Protecting Your Facility's Technology
- Cybersecurity Awareness
- Suspicious Emails

Job Aids
- Counterintelligence Awareness Toolkit

Past Webinars
- Cyber Insider Threat
- Information Security Continuous Monitoring
- Reportable Unclassified Cyber Events

www.cdse.edu/catalog/counterintelligence.html
Feedback

Before we conclude today’s presentation, we hope you’ll take a moment to participate in our feedback questionnaire. Your feedback is very helpful to us and is greatly appreciated.

If you have ideas for future webinar topics, you can share these in the questionnaire.

Counterintelligence Training POC:

Peter DeCesare and Rebecca Morgan
(410) 689-1136    (410) 689-1294
Email: counterintelligence.training@dss.mil