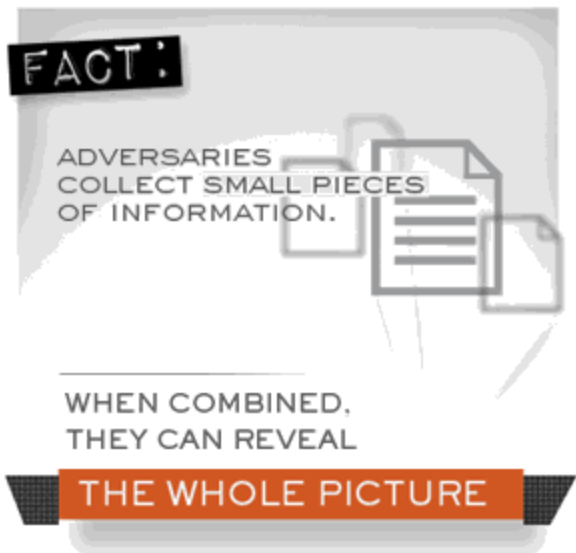


NCIS

SPECIAL AGENT JASON HENDERSON
NCIS REP TO STRATEGIC SYSTEMS PROGRAMS
JASON.HENDERSON3@NAVY.MIL
JBAB OFFICE: 202-433-6688

TYPES OF THREATS



Source // Interagency OPSEC Support Staff,
Intelligence Threat Handbook



FOREIGN INTELLIGENCE ENTITY

A foreign organization, person, or group that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, disrupt U.S. systems and programs, or gain a competitive edge.

Includes foreign intelligence and security services, international terrorist organizations, organized crime groups, and drug cartels.

TYPES OF THREATS }



INADVERTENT

“Loose tweets sink fleets.” You do not have to intend harm to create a threat. Lack of OPSEC can lead to non-intentional disclosures.

Adversaries often exploit personnel's lack of OPSEC through the monitoring of social media sites, using elicitation, and eavesdropping.



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

OVER

97
COUNTRIES



BOTH FRIENDS & FOES

target the United States seeking
information and technology.

Source // NSA Threat Briefing, 2008



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

OPEN SOURCES

- Al Qaeda Handbook encourages searching online for data about government personnel, officers, targets, etc.
- The Internet and other media are key sources of intelligence information
- Social networking sites, such as Facebook, Twitter, and blogs, are monitored and exploited



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

ELICITATION

WHY IT WORKS

THE ADVERSARY'S M.O.

A SUBTLE DEFENSE

- GET you talking and KEEP you talking
- Common, effective technique to subtly collect information through face-to-face or online interaction
- Often used during facility and ship tours and at conventions and seminars where participants are eager to share information
- Operates under the guise of think tanks, exchange students, research organizations, foreign liaison officers, and official delegations



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

ELICITATION

WHY IT WORKS

THE ADVERSARY'S M.O.

A SUBTLE DEFENSE

- Nonthreatening: Hard to recognize and easy to deny
- Easy to disguise: Seems like innocent conversation
- We're human: Exploits fundamental aspects of human nature. In general, we aspire to:
 - Be polite and helpful
 - Appear well-informed
 - Be appreciated
 - Trust others



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

ELICITATION

→ WHY IT WORKS

THE ADVERSARY'S M.O.

A SUBTLE DEFENSE

- Flattery/appeal to ego: Asks your opinion or values your insights
- Quid pro quo: Shares information with you in hopes you'll reciprocate
- Mutual interest: Focuses on details you have in common



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

ELICITATION

WHY IT WORKS

THE ADVERSARY'S M.O.

A SUBTLE DEFENSE

- Don't allow others to control the conversation
- Listen more than you talk
- Deflect a question with a question
- Change the topic
- Be general and nonspecific
- Plead ignorance
- Don't answer



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

EAVESDROPPING, ELECTRONIC SURVEILLANCE

- Operative positioned within earshot of a conversation or within view of a computer screen
- Communications intercepted when devices are connected to public Wi-Fi, unsecured networks, or unencrypted email systems



OPEN SOURCES



ELICITATION



EAVESDROPPING



RECRUITMENT

TRADITIONAL METHODS

RECRUITMENT

- Build personal relationship and gain trust, little by little
- Exploit personal weakness or circumstances
- Coerce or use inducements
- Start with small requests, then make bigger demands
- Praise and reward for accomplishments



OPSEC | REMINDERS

- ▶ Think before you talk and limit the information you post
- ▶ Never speak about sensitive info in public or on unsecured lines
- ▶ Shred sensitive information, including PII
- ▶ Never bring home classified information
- ▶ Create strong passwords for each account and change them often
- ▶ Update and use security software
- ▶ Follow the need-to-know principle
- ▶ Follow all security and IA policies



OPSEC | REMINDERS

THE SEA AIR SPACE EXPO BRINGS DOD AND FOREIGN ENTITIES INTO A COMMON SPACE. PLEASE REPORT ANY SUSPICIOUS ACTIVITY TO NCIS AS SOON AS POSSIBLE. THINGS NCIS WILL NEED:

- A DETAILED DESCRIPTION OF THE INCIDENT, INCIDENT LOCATION, AND PERSONS INVOLVED
- ON OCCASION, PERSONNEL MAY BE PROVIDED WITH A BUSINESS CARD OR CONTACT INFORMATION, PLEASE PRESERVE THIS INFO

Congratulations! You have completed this course.
You must continue to the next page to record
your training as complete and to view or print
your certificate.