Human Spies Enabling Cyber Attacks

Solutions to Real-World Problems

Thomas F. Pike
CEO
Spectrum Shield, LLC

Thomas Pike

- CEO of Spectrum Shield, LLC
  - Risk Management, Competitive Intelligence, Corporate Continuity
- Connect on LinkedIn: linkedin.com/in/thomas-pike-spectrumshield

- Retired Army Colonel in the U.S. Intelligence Community
- Human Intelligence (HUMINT) and Counterintelligence (CI)
- Director of HUMINT and CI in Afghanistan (ISAF)
- DIA, CIA fellowship, ODNI, Army
- Supported FEMA, CISA and Security for UN General Assembly

A Few Points

- “Multi-Vectored Threat”
  - Outside the scope of negligence, mistakes or being outsmarted.
  - Insider-Outsider Threats.
  - Convergence of non-cyber and cyber activities.
  - Human espionage and human facilitation of malicious activity.
- Laws, Policies & Ethics
  - Know when to involve HR, Legal and other authorities.
  - Understand the risk-tolerance of the C-Suite and the organization.
  - Organizations can have different security requirements.
- Be cautious with human indicators & activities.
- Terms:
  - Proprietary information, sensitive data, classified information
  - Adversaries: individuals, competitors and other nations.

Understand the Risk to Find the Threats

- **Designed not to be seen.**
  - To enable fraud, intellectual property theft, espionage, or a combination of the three.
- **Insider-Outsider Collusion**– Insiders collaborate with an external threat actor to compromise an organization.
  - Unscrupulous competitors, criminals. or nations: China, Russia and other adversaries.
  - Nations. Foreign Intelligence Entities: training, resources and determination.
- **Programs** (Ponemon Inst Study)
- 88% of organizations devoted less than 10% of their security budget to insider risk management.

Understand the Risk to Find the Threats

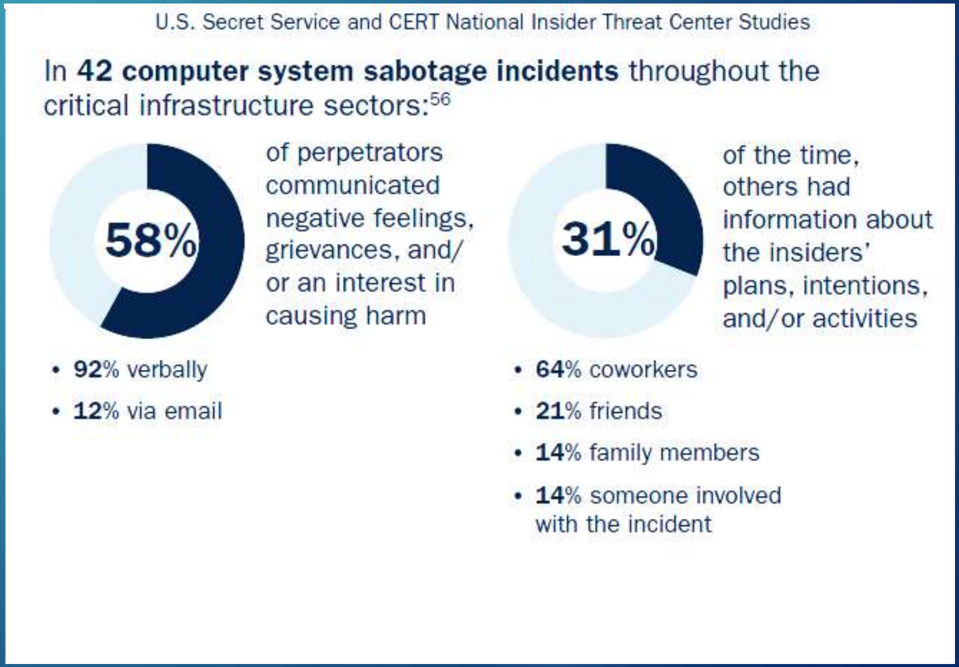
- A new counterintelligence investigation related to China every *10 hours* (FBI)
  - More than 2,000 current active cases.
  - Majority relate to economic espionage; a 1,300% increase since 2015.
- **The Human Element.**
- 74% of all breaches include the **human** element. (Verizon 2023 Data Breath Report)
  - Human Error, Privilege Misuse, Use of Stolen Credentials, Social Engineering.
- Malicious insiders caused 25% of incidents in 2022 which were the most costly (Ponemon Institute study)
  - Generally harder to detect due to their placement and access compared to external hackers.
  - Average cost of $701,500 per incident
- 86 days average time to contain an insider incident

Case Study: 40,000 employees

- .1% (.001) x 40,000 employees = 40 employees
- 1 employee is 0.0025% (.000025) of 40,000 employees

Vulnerabilities

- What you see, is what you see.
- Statistically, assume there may be more.
- Know the difference: Vulnerable vs Disgruntled.



U.S. Secret Service and CERT National Insider Threat Center Studies

In **42 computer system sabotage incidents** throughout the critical infrastructure sectors:[56]

58% of perpetrators communicated negative feelings, grievances, and/or an interest in causing harm

- **92%** verbally
- **12%** via email

31% of the time, others had information about the insiders' plans, intentions, and/or activities

- **64%** coworkers
- **21%** friends
- **14%** family members
- **14%** someone involved with the incident

The “Cold Pitch”

Playing The Numbers

- In 2021, cybercriminals targeted employees in a large company with direct emails.
- The initial email did not contain any suspicious attachments or links.
- This was a “Cold Pitch” for a human enabled ransomware attack.
- Quid Pro Quo: Employee installs ransomware on their work computers and they get 40% of the ransomware payment via bitcoin.
- Ransomware actors asked the recipients to enable Remote Desktop Protocol (RDP) or engage in direct collaboration.
- Example: 1,000 employes x 0.001=1

SPECTRUM SHIELD

How?

The “HUMINT Cycle”

Human Intelligence Cycle

Spot and Assess

- Where: Social media, trade shows, business contacts, social events, etc.
- Who: High level of access often *not* necessary.
- Approach: Non-threatening and natural.
- Adversary explores exploitable weaknesses such as drugs, alcohol, gambling, adultery, financial problems, or other vulnerabilities.

Develop

- Potential for recruitment identified.
- Learns about motivations & vulnerabilities.
- Adversary cultivates a relationship.
- Meetings become more private and discrete.
- Movement toward recruitment.

Motivations & Vulnerabilities

1. Money: This is usually wanted for something else such as dept, greed, desire to “keep up with the Joneses,” send children to college.

2. Anger/Revenge: deep dissatisfaction or resentment towards their organization; contemplating retaliation.

3. Work-related issues: fear of layoff, lack of recognition, disagreements with colleagues or managers, job dissatisfaction.

4. Ideology/Identification: Desire to champion the cause of the underdog or support a particular ideology. This includes foreign countries.

5. Divided Loyalty: allegiance lies with someone or something other than their organization, such as another person, company, or even a different country.

6. Adventure/Thrill: excited by clandestine activities, akin to a 'James Bond Wannabe' mindset.

Motivations & Vulnerabilities

7. Vulnerability to blackmail: extramarital affairs, gambling, or fraudulent behavior, susceptible to manipulation.

8. Ego/Self-image: “Above the rules” attitude, narcissism, sense of superiority, insecurity.

9. Ingratiation: seeking to please and gain the approval of others who could benefit from insider information, with the expectation of receiving favors in return.

10. Compulsive and destructive behavior: drug or alcohol abuse, gambling, other addictive behaviors

11. Family problems: Marital stress, loneliness from being separated from loved ones can increase susceptibility.

Social Engineering

Coercion to promote action

- The psychological manipulation of people into performing actions or divulging sensitive information.
  - Elicitation techniques
  - Development of rapport
  - Neurolinguistic Programming (NLP)
  - Emotional manipulation: guilt, friendship, favor-building.
- A component of cyberattacks today:
  - Build trust with targets through extended conversations.

Recruitment

Based on:

- Friendship
- Appeals to ideological leanings
- Financial gain
- Blackmail or coercion, etc.

Christopher Metsos
Russian Handler
“The Illegals”

Why Enable?

Foreign Governments, Criminal Groups, Radical Organizations

- Conduct Multi-vectored attacks.
- Enhanced effort to defeat strong cyber defenses or remain non-attributable.
- Seeking deep penetration to steal, deny, disrupt, destroy operations.
- Seek to inflict irreparable damage.

3 Basic Categories

- Protected Information
  - PII, customer information, SSNs, credit card numbers
- Trade Secrets (including sensitive activities)
  - Information that gives an organization an advantage
  - Business plans, customer data
- Intellectual Property
  - Patents, copyrights, trademarks

Enabling

- Why this is different
  - Well-planned, orchestrated, targeted victims and information
  - Well-trained Handler
  - Multi-Vectored Threat; enabling multiple points of entry
- Two Basic Ways
  - Facilitation
  - Direct Enabling (Action)

Facilitation

- Clandestine operations: designed not to be discovered.
- Provides what a hacker wants to make their job effective.
- Collecting & Reporting
  - Cyber security policies, systems, processes, technology, corporate security environment
  - Un-patched security flaws.
    - A printer has a "print from anywhere" feature turned on. The spy helps to find the open port on the printer that enables this feature, enabling a hacker to remotely hack into it.
  - Access codes for scheduled virtual meetings for IT discussions, for eavesdropping/monitoring.
  - Learn the passwords of other employees.
    - Observing, finding passwords written down, eliciting password information.
  - Determining what encryption system is used.
  - Listening in on IT discussions during meetings, in the lunch room, etc.
  - Place an infected flash drive in the office.

Direct Enabling

- The spy is an insider and has access to the system.
- Further an attack plan via access to IT systems.
  - Changing data
  - Inserting malware or other pieces of offensive software to disrupt systems and networks.
  - Use technical means to disrupt or halt an organization’s regular business operations.
- Steal a crypto card from that system.
- Take digital pictures of equipment; server rooms, etc.

t

Solutions

Steps to Mitigation

- Conduct a Risk Assessment
- ID and secure your “Crown Jewels.”
- Address employee issues *before* there are problems
- Establish/Uplift Insider Risk Program
  - Proactive, Predictive and ultimately, optimized
  - Training
  - Address “Human Risk.” Criminal & civil background checks
  - Address Security Silos. Cyber and physical threats are interconnected
  - Converged approach: Foster IT/security collaboration
- Remain aware of employee welfare
- Manage data access
- Create an Incident Response Plan

Remember Security Convergence: A lack of communication between security stakeholders can create vulnerabilities.

Risk Assessment

Things to Consider

What's the risk tolerance in the C-Suite?

Do they understand the Human and Technological risks?

How do policies define home/remote work using sensitive/ proprietary data?

What is being targeted? Your Crown Jewels?

Is an outside assessment beneficial?

The Office.

How is the welfare of employees?

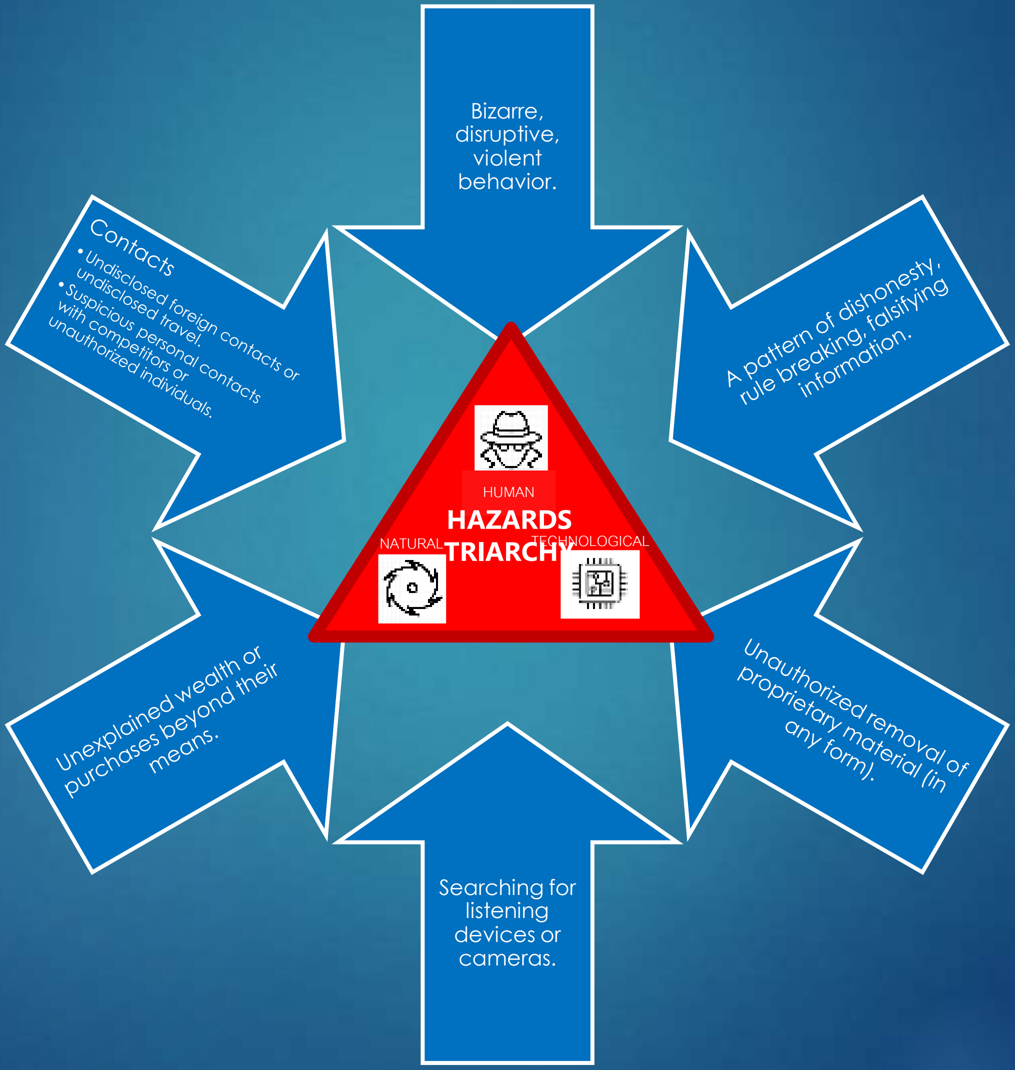
How easy is it for someone to exit the office with sensitive equipment or information?

What's the perception of security in the office? Is it relaxed? Too harsh?

Are employees rushed/pressured, or too busy to take accurate security measures?

SPECTRUM SHIELD

Behavioral Concerns



Bizarre, disruptive, violent behavior.

A pattern of dishonesty, rule breaking, falsifying information.

Unauthorized removal of proprietary material (in any form).

Searching for listening devices or cameras.

Unexplained wealth or purchases beyond their means.

Contacts

- Undisclosed foreign contacts or undisclosed travel.
- Suspicious personal contacts with competitors or unauthorized individuals.

Know The Signs

5 Potential Early Warning Indictors

Unexplained activity at unusual times, particularly when compared to their peer group.

Collecting data; accessing, sensitive data that is uncommon based on the individual's job function.

Seeking increased placement & access; especially falling outside the scope of their role or department.

Behavior; indications of unauthorized or inappropriate employee behavior, regardless of its significance.

Questionable methods, timing, or frequencies re: searching corporate networks.

An Effective Insider Threat Program

Leverage Experience, Awareness and a Measured Response

- Remember employment & regulatory laws, ethics, policies, etc.
- Identify and prioritize critical assets, data, and services for the organization.
- Implement a comprehensive monitoring system to detect and identify threats.
- Conduct thorough threat assessments to determine the level of risk associated with individuals of concern.
- Implement targeted strategies to manage the entire spectrum of risk for insider threats.
- Deter, detect, and mitigate any potential harm by proactively engaging individuals at risk.
- Takes prompt action: alerting behavior, suspicious activities, etc.

Focus Areas

- Screening. Employ thorough screening procedures when recruiting new staff.
- Monitoring. Regularly monitor computer networks for signs of suspicious activity.
- Training. Implement comprehensive employee education and training programs that include human espionage and enabling cyber risk.
- Safeguarding. Establish stringent measures to adequately safeguard proprietary information and access points (ie: server rooms).
- Resourcing. Furnish security personnel with the necessary skills to effectively fulfill their roles.
- Reporting. Establish accessible and confidential channels for employees to report suspicious activity.
  - 31% of the time, others had information on an Insider Threat’s plans, intentions or activities.
  - Encourage employees to promptly report any observed irregularities for safety and security reasons.

Summary

Remember employment & regulatory laws, ethics, policies, etc.

Acknowledge the potential for risk/threat.

Conduct a Risk Assessment.

Insider Risk Program: address **human** espionage & enabling.

Know the signs: employee awareness.

Address employee issues before there are problems.

SPECTRUM SHIELD

Questions?

- Thomas Pike, CEO of Spectrum Shield, LLC
  - Risk Management, Competitive Intelligence, Corporate Continuity
- linkedin.com/in/thomas-pike-spectrumshield
- tpike@spectrumshield.com