Counterintelligence and Insider Threat Awareness

WHAT IS COUNTERINTELLIGENCE?

"Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities."

C - Countering

A - Adversarial

I - Intelligence

T - Threats

16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

ECONOMIC ESPIONAGE & TRADE SECRET THEFT

ECONOMIC ESPIONAGE

Defined under §1831 of the Economic Espionage Act of 1996 and comprises behavior that denies the rightful owner of the economic benefit of property that the owner has gone to reasonable means to protect and does so with the **intent to benefit a foreign entity**.

TRADE SECRET THEFT

Defined under §1832 of the Economic Espionage Act of 1996 and covers the conversion of a trade secret to the economic benefit of anyone other than the rightful owner. There is **no requirement for a foreign nexus** in Trade Secret Theft.

WHAT DO THE BAD GUYS WANT?

- Construction Techniques & Technical Drawings
  - **“How we build what we build”**
- Personnel Information
- Supply Chain Information
  - **Vendor Names, Costs, Quantity, Quality Control Info, Vendor Issues, Clearance and Security Requirements**
- Dual Use and Export Restricted Items
- Product Vulnerabilities
- Controlled Unclassified Information (CUI)
- Research, Development, Technology
- Company Proprietary Technology, Methodology, and Information

WHAT MAKES YOU A TARGET?

Placement, Access, Culture:

- **You don't need to be the most valuable target or person – just the most available one**
- **Retired/Resigned?**
  - **Information/knowledge doesn't magically remove itself from your brain**

POSSIBLE RISK INDICATORS

- Extreme Disgruntlement
- Working Odd/Unusual Hours
- Technical Activity
  - Unauthorized access or attempt to access IT systems
- Need-To-Know
- Unnecessary Copying
- Unexplained Affluence
  - Financial Considerations
- Substance Abuse and Addictive Behaviors
- Unreported Foreign Travel
- Unreported Foreign Contacts
  - Affiliation Considerations
- Security and Compliance Incidents
  - Unauthorized Removal
  - Unauthorized Devices
- Criminal, Violent, or Abusive Conduct
- Judgement, Character, and Psychological Conditions

- Most individuals convicted of espionage exhibited multiple indicators over a period of time, coupled with some type of significant life event
- * Existence of PRIs ≠ Insider Threat

HOW DO "THEY" DO IT?

METHODS OF CONTACT

List of Methods

- Conferences / Conventions
- Cyber Operations
- Email
- Foreign Visit
- Mail
- Personal Contact
- Phishing Operation
- Resume (Academic)
- Resume (Professional)
- Social Networks
- Telephone
- Web Form

KEY TAKEAWAYS:

- American service members, academics, and professionals receive unsolicited communications from China.
- These communications often seem innocent and do not appear to come from China or state affiliates.
- These communications often ask for personal information, professional favors, or proprietary data.

OPEN SOURCES

- **What is it?**
- Publicly available information:
  - News articles, Google results, Social Media, Academic papers, research papers, company's public website, etc.

- **How is it Used?**
- Identifies:
  - Personal interests, preferences, motivations, activities; vulnerabilities
- Social Engineering through Social Media
  - Used to develop "Target packages"

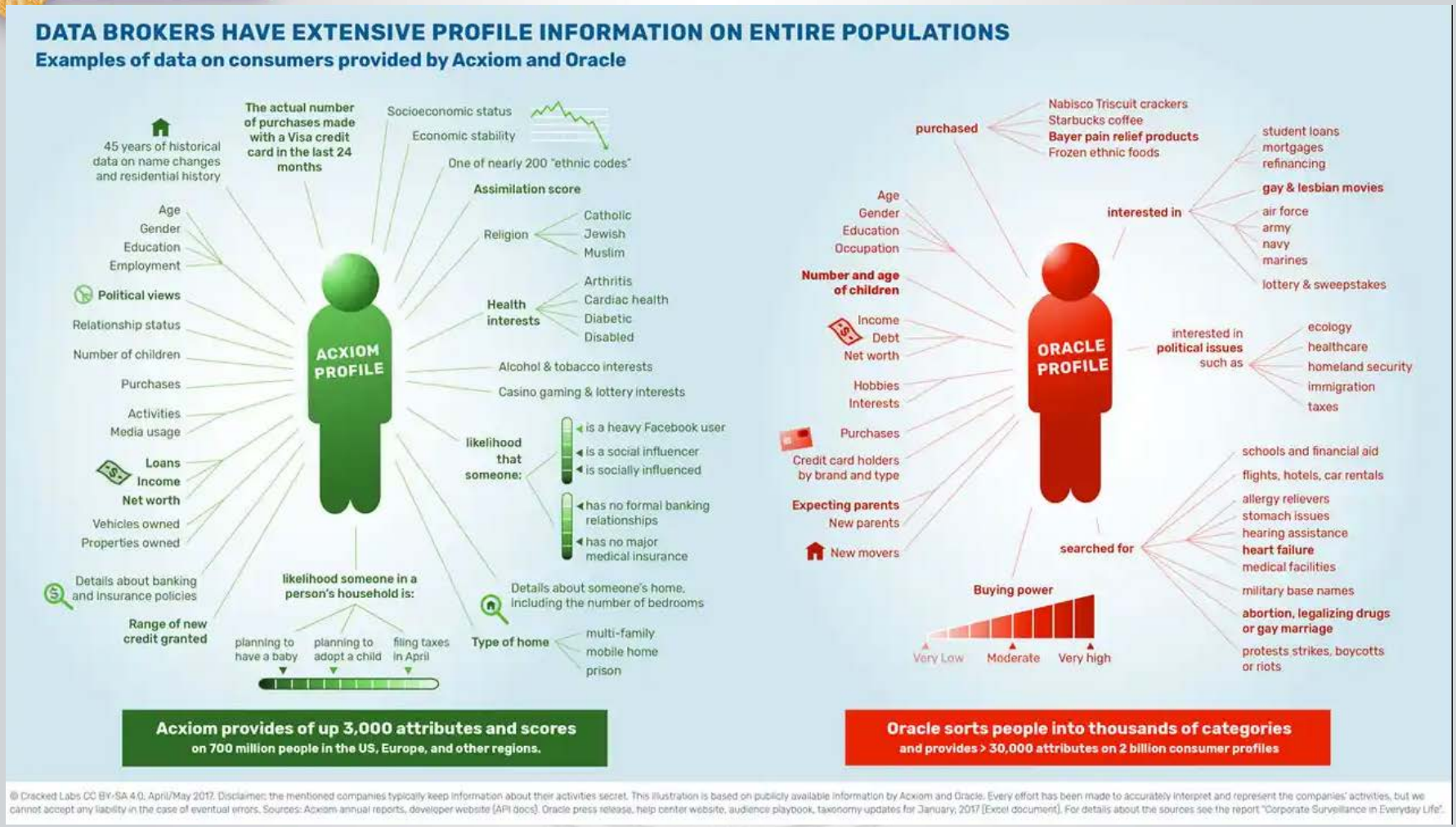
- **Why is it Valuable?**
- It provides a customized picture of a "target"

- **Data brokers buy and sell our information everyday-*TO ANYONE***
- **We are data mined in every facet of our lives:**
  - Hobbies
  - Clubs
  - Grocery purchasing history
  - Social media
  - Bills
  - Internet web browsing history
  - Search engines
  - Applications
  - Online accounts and purchases
  - *You get the point*

-The data broker industry – 2021 earnings - $319B

-Expected to surpass $545 billion by 2028 *(historical 10% growth rate annually)*

-The total revenue of the United States' oil and gas industry came to $332.9 billion in 2022



- **ACXIOM now collects 12,000 “global attributes” on an individual**
  - **Can you name 12,000 attributes about yourself?**

NON-TRADITIONAL COLLECTORS (NTC)

- **What are they?**
  - Persons outside of the “traditional intelligence spheres”
    - (i.e. – not a “spy,” not intelligence officer, no formal training)
  - Utilized to collect sensitive information on behalf of foreign government
    - WITTING or UNWITTING
- **Who are they?**
  - Business people, students, engineers, scientists, professors
  - Legitimate in their trade, skill, experience
- **How does it work?**
  - Collect information, “recruit” agents, and co-opt individuals
  - Overwhelm
    - Allows FIE to exponentially expand their reach
    - Different tactics/threat than historically faced
- **How do we counter it?**
  - Understand their tactics, raise awareness

Fwd: Paid Consultation Opportunity | Panel Building Value Chain

---------- Forwarded message ---------
From: [redacted]
Date: Tue, Oct 24, 2023 at 11:30 AM
Subject: Paid Consultation Opportunity | Panel Building Value Chain To:
[redacted] >

Hi [redacted],

I appreciate that you must be busy so I will get straight to the point:
I'm working with a client who would like to speak to a profile like yours in a 1 hour paid phone consultation to understand the value chain of building control panels, from the request until the delivery.

Would $230 per hour be suitable?

Do you have a few moments for a quick call today to provide full context and details? Let me know which number would be best to reach you on. If you could also let me know what is the best time for this initial call, I am in London so any UK-friendly time works for me.

Many thanks in advance,
[redacted]

[redacted]
Associate, Client Services
[redacted]

ELICITATION

"The strategic use of conversation to extract information from people without giving them the feeling they are being interrogated"

ELICITATION

Why it works:

Plays on Natural Human Tendencies:

- *Humans desire to:*
  - Be polite and helpful
  - Appear well informed, especially about our profession
  - Believe we are contributing to something important
- *Humans tend to:*
  - "Show off"
  - Correct others
  - Underestimate the value of the information being sought or given
  - Desire to convert someone to our opinion

ELICITATION

• RECOGNITION AND DEFENSE

- ***Know what information should NOT be shared and what is normal questioning***
  - ***Establish "base line"***
  - ***Each event/circumstance will be different***
    - **Recognize questions outside scope of the event**
- Do not tell people any information they are not authorized to know

- You can politely discourage conversation topics and deflect possible elicitation by:
  - Referring them to public sources (websites, press releases)
  - Ignoring any question or statement you think is improper and changing the topic
  - Deflecting a question with one of your own
  - Responding with "Why do you ask?"
  - Giving a nondescript answer
  - Stating that you do not know/can't discuss

PROACTIVE COUNTERMEASURES

- Complete annual trainings
  - Pre and post briefs for conferences/events
- At events, display mockups, not actual working versions
- Prepare responses for questions going
  - Specifically CUI or classified aspects of your product

FOREIGN VISITOR CONCERNS

COMMONLY OBSERVED TECHNIQUES:

-**Peppering:** *Visitors asking the same question in different styles or one visitor asking the same question to multiple employees.*

-**Wandering Visitor:** *The visitor uses the distraction provided by a large group to slip away, out of the escort's control.*

-**Divide and Conquer:** *Visitors take the US team members into different areas to discuss issues in order to deprive the USPER of his safety net of assistance in answering question*s.

-**Switch Visitors:** *A collector is added to the group without leaving enough time for a background check or proper vetting of the new visitor (check IDs before issuing).*

-**Bait and Switch:** *The visitors say they are coming to discuss business that is acceptable for discussion, but after they arrive their agenda switches to different questions and discussion topics (asking questions outside the scope of the planned visit).*

-**Distraught Visitor:** *When the visitor's questions are not answered s/he acts insulted or creates an uncomfortable scene in an attempt to psychologically coerce information from the target.*

COMBATING THE CYBER THREAT

- Limit the personal info you post online.
- Remember what you post online is public.
- Be wary of people you meet online.
- Be skeptical of links/messages asking you to update info.
- Actively manage your privacy settings.
- Use strong passwords and use care where you enter them.
- Use care on unsecured wireless networks.
- Check privacy policies of sites you use regularly.
- Keep all software, especially security software, updated.

2018: NAVAL UNDERSEA WARFARE CENTER CONTRACTOR HACKED BY CHINA

- *Unclassified network* of USN contractor breached by PRC (614 GB data stolen)
  - Plans for supersonic anti-ship missile, signals & sensor data, submarine cryptography systems, electronic warfare library for Navy Submarine Development Unit
  - Aggregated data “could be” classified
- No indication of classified networks breached or probed
- Changed cybersecurity protocols for DoD contractors
  - Cybersecurity Maturity Model Certification (CMMC)

NAVSEA
WARFARE CENTERS
NEWPORT

SA Colton Plumb
NCIS – Pittsburgh | FBI Pittsburgh TFO
Office: 412-476-7224
Cell: 412-377-7337
Email: colton.plumb@ncis.navy.mil