Chapter 40 –IFPO –CPO

Information Security and Counterintelligence

Purpose

Studies have concluded that as much as 75% or more of a company's value may lie in intellectual property, or information, and intangible assets. Security professionals should understand how to defend the organization's proprietary information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Key Terminology

- **Information Assets:**
  - Consist of sensitive and proprietary information, privacy-protected data, intellectual property, intangible assets, and information defined under international, federal, and state laws governing trade secrets, patents, and copyrights.
  - Examples:
    - Intellectual property: R&D, technical data, formulae, processes.
    - Competitive information: Pricing, marketing strategies.
    - Information protected under regulatory requirements: Personal ID, health data, financial and legal.

- **Information Asset Protection (IAP):**
  - defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- **Intangible Assets:**
  - These are assets of any organization (including companies and government agencies) that are not physical in nature.
  - Examples of intangible assets are an organization's reputation, brand, relationships, management style, knowledge, and processes.

Key Terminology

- **Competitive Intelligence vs. Economic Espionage:**
  - *Competitive intelligence* is a normal business function, which can include completely benign activities such as market research.
  - *Economic espionage* is on the other end of the spectrum and includes illegal activities such as electronic eavesdropping.
- **Compromise**:
  - Refers to a situation where sensitive, controlled, or classified information falls into the hands of an unauthorized person or organization.
- **Counterintelligence**:
  - Any measures taken to negate intelligence collection efforts against an organization or its people.
    - In the federal sector, counterintelligence relates to programs designed to counteract foreign intelligence services.
    - In the private sector, it is focused on protecting against actions ranging from simple market research up to and including industrial espionage.
- **Economic Espionage:**
  - Knowingly performs targeting or acquisition of trade secrets to knowingly benefit any foreign government, foreign instrumentality, or foreign agent.

Key Terminology

- **Sensitive Information:**
  - Information or knowledge that might result in loss of an advantage or level of security if disclosed to others.
- **Technical Surveillance Countermeasures:**
  - Services, equipment, and techniques designed to locate, identify, and neutralize technical surveillance activities such as covert listening devices.
- **Trade Secret:**
  - Trade secrets are defined by laws, at the federal level, as well as by state and local laws.
  - Generally, trade secrets are designated by the owner but must meet certain criteria to qualify for applicable legal protections.

Threats to Information and Intangible Assets

- Three categories of Threats:
  1. Intentional (deliberate)
  2. Natural
     - Hurricane, earthquake, tsunami, flood, etc.
  3. Inadvertent (accidental)
- Like any tangible asset such as a building or piece of equipment, information will be subject to all three categories.

Threats to Information and Intangible Assets

- Commonly reported information collection methods are:
  - Open source collection of public information
  - Data mining and/or the use of information brokers
  - Social engineering and other elicitation techniques
  - Hiring key employees away from the targeted organization
  - Targeting meetings and conferences
  - Electronic eavesdropping
  - Theft of hard-copy information
  - Theft of soft-copy information/media (e.g., thumb drives, laptop computers, mobile devices, etc.)

Threats to Information and Intangible Assets

- One specific threat is that of laptop computer theft.
  - 81% of companies responding reported the loss of one or more laptop computers in the preceding 12 months.
  - 97% of stolen laptops are never recovered.
- Insiders (employees and others with a trusted relationship) working with outside attackers cause the most data breaches.
- Insiders have some level of authorized access, they know "the system," and they know where to look for valuable information.
- It is important for the professional protection officer to understand who the adversaries might be in terms of threats to an organization's information assets.
- The largest threats to proprietary information are from those with a *trusted relationship* with the organization—current and former employees and those partners, outsourced providers, and customers with a trusted relationship.

Threats to Information and Intangible Assets

- *Collectors* are those who steal the information or intangible asset.
- *End users* are those who will put the stolen information and/or intangible asset to use.
- End users may be the same as the collectors but often are not.

Threats to Information and Intangible Assets

- Among common end users for compromised information assets are:
  - Domestic and foreign competitors
  - Foreign governments
  - Organized criminal enterprises
  - Activist groups (environmental, animal rights, etc.)
  - Terrorist groups
  - Political advisors
  - Financial or business cartels and/or Narcocapitalists
  - Product counterfeiting operations
  - Targets of law enforcement activities

How Technology is Changing the Threat

- Once information is lost, **it is lost permanently and globally**—and can happen in an instant.
  - **Miniaturization of Media**:
    - More and more data is being stored on smaller and smaller devices.
  - **Social Networking Media:**
    - this type of media provides another outlet for instantly sharing information (including possibly sensitive/proprietary information or destructive false rumors/news) across wide audiences—and in some cases, anonymously.
- **Volume and Dispersal of Data:**
  - The enormity of the current volume of data makes it far more difficult to identify a data breach in real time or to determine if sensitive information has been compromised.
- **Data Mining and Information Brokers:**
  - An industry that collects data from a multitude of sources and selling it to whoever is willing to pay for it.
- **Wireless and Remote Computing Environments**:
  - Sensitive information can be exchanged through hot spots in public locations, hotel networks, or even home networks.
- **Security of Security Systems:**
  - Is a growing concern as security systems for surveillance, access control, facility management, intrusion detection, and other functions increasingly ride on the Internet and can be managed remotely.

Protective Measures

- The measures employed to protect information and intangible assets fall into three categories:
  1. Security
  2. Legal,
  3. Management

Security Measures

- Assessment (possibly including penetration testing or “red teaming”)
- Need-to-know controls (limited access, separation of duties)
- Information storage and handling
- Physical security (surveillance, access control, and intrusion detection)
- Premise access controls procedures (card management, visitor control and escorts)
- Design and layout of facility security zones (controlled versus open/public areas)
- Security officers/response forces
- Information destruction processes and standards

Security Measures

- Technical security measures
- Technical Surveillance Countermeasures (TSCM)
- Communications, emanations, and signals security measures
- Information systems security (IT security)
- Cybersecurity awareness training
- Product security
- Travel security programs
- Training and awareness (for employees, users, contractors, vendors, partners, and trusted third parties)
- Investigation capabilities

Training and awareness are essential tools.

Legal Measures

- Most legal measures are *reactive* in nature.
- For legal means to be useful, the organization must be willing to enforce the tools in a court of law.
- Examples of legal measures include the following:
  - Patents, copyrights, and trademarks
  - Trade secrets
    - The most restrictive or protective measure. Trade secrets have the advantage of not requiring registration but are subject to strict interpretation in court.
- 1996 Economic Espionage Act (EEA)
  - Allows the FBI to investigate such cases even if a foreign intelligence service is not involved.

Management Measures

- Insider threats are the most serious.
- In 80% of the insider cases, the perpetrator had come to the attention of management due to inappropriate behavior before the incident .
- This statistic highlights the importance of “management measures” as part of an overall IAP strategy.

Management Measures

- Management measures that should be considered, and generally be coordinated with the security program, include the following:
  - Effective employee screening (preemployment and periodic)
  - Drug screening
  - Establishing relevant policies and procedures
  - Offering a reporting mechanism that allows employees and others to provide information and make allegations.
    - Be sure that the organization is responsive to calls and allegations.
- The best approach to addressing risks to information assets is to apply defense in depth (layered security) by incorporating both IT and traditional protection measures.
- Examples of these layers are as follow:
  - Strong password protection
  - Encryption
  - Biometric authentication
  - Physical security measures
  - Personnel screening
  - Employee training
  - Password-protected screensavers.

The Role of the Protection Officer

- The most effective protection officers are those who know their client (the organization they serve)and tailor the way they provide security services to the client's DNA, mission, and culture.
- In general, professional protection officers place most of their emphasis on protecting people and property, but it is important to support the third asset category as well: information.
- Information asset and intellectual property protection should be included in officer and supervisor training.