Chapter 28 – IFPO – CPO

Espionage – A Primer

Purpose

- As information becomes more portable, it also becomes easier to corrupt, delete or steal. Organizations must be aware that adversaries will take advantage of any vulnerability in their systems. Security professionals are the front-line of the protection of organizational information; thus, must be familiar with methods used by adversaries to access proprietary information.

Espionage

- Espionage, in essence, is stealing secrets.
- Secrets can be found in many forms such as:
  - Documents
  - E-mails
  - Recorded conversations
  - Telephone calls
  - Text messages
- Secrets must be protected
- Sabotage is a form of espionage.
- Sabotage occurs when an individual takes an action that interferes with normal business or government operations.
- Being able to commit sabotage requires many of the same elements that committing espionage requires—particularly opportunity or access to items or systems that can be sabotaged.

How is Espionage Conducted?

- The practices involved in committing espionage is referred to as *tradecraft.*
- In the days before computers, information had to be memorized and transmitted verbally, written down, or transmitted via a communication device.
- To protect information, governments devised codes to deter eavesdroppers from intercepting it. The discipline that evolved from this practice is referred to as *cryptography*.
- One of the simplest ways, and riskiest, is to pass information from person to person via a handoff:
  - Microfilm, thumb drives, CD's, etc.
- Another method to pass information is by using a "dead drop."
  - Occurs when one party leaves an item or package in a prearranged place that is retrieved by another party.
- Tapping phone line, electronic bugs, microphones
- Use of cell phones to record or photograph secrets.

Security Against Espionage

- Use of a cipher to create a code that encrypts information.
- When transporting information, an additional level of safety is provided by encryption, such as a “one-time pad” (OTP).
- A “one-time pad” is a cipher. It is defined as “a series of numbers randomly keyed to letters that can be put into clear text only by someone having an identical OTP”
- Use of encrypted communication and information systems.

Social Engineering

- A form of espionage that uses both technology and person-to-person techniques in order to elicit information.
- Defined as “the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data.”
- In simpler terms, it’s a confidence game. The social engineer tries to bluff his/her way into the information being sought.

Motivations

Reasons that a person might engage in espionage:

- **Increasing prevalence of personal financial problems and/or compulsive gambling**.
  - Secrets are worth a lot of money to the person who possesses them.
- **Diminishing organizational loyalty**.
  - Lack of company loyalty enables the rationalization of taking something from the company.
- **Ethnic diversification and/or allegiance to a global community.**
  - A person does not have allegiance to the country where they live but rather still hold allegiance to their “home” country.
  - The question becomes if the emigrant must choose between (a) the country they’ve emigrated to and (b) the country they’ve emigrated from, with whom will they place their loyalty?

Security Clearances/Classifications

- Security classifications generally are used to restrict government-held or government-related information. These classifications are applied to any information that, if exposed, would adversely affect national security.
- In order to obtain access to classified information, a security clearance is required.
- There are different levels of security clearance, depending on the nature and sensitivity of the information classified at that particular level.
- Regardless of their employer, if a person requests a security clearance, a background investigation will be conducted.

Trade Secrets

- Trade secrets are information which, if exposed, would impact the health and very existence of the company that possesses them.
- Information that is valuable because of the resources used to develop it can be a trade secret as long as it is known to the minimum necessary number of people and is protected via encryption, a safe, armed guards, or some other method.
- Information that is not protected (i.e., open-source information) cannot be a trade secret.

Security Against Espionage in the 21st Century

- Some methods can only be detected by IT professionals:
  - The introduction of an unauthorized thumb drive onto the company network or the attempted accessing of restricted files.
- Cultivating of relationships:
  - Corporate IT department,
  - Corporate HR department
  - Law enforcement agencies
- Use of tactics such as “red teaming” or conducting penetration exercises:
  - Security professionals deliberately try to penetrate an organization in order to identify weaknesses.
- Security awareness:
  - Company employees will supplement good security practices if they understand why they need to do something.
  - Security professionals can support that by making periodic presentations to the employees.
  - If presentations can include the corporate IT department or law enforcement, that will have additional impact.