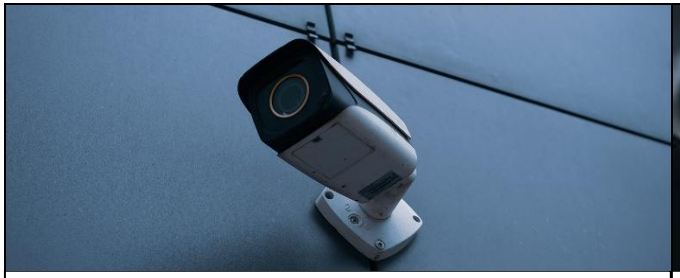


6 Common Mistakes Companies Make When Addressing Insider Threats

- **A**lways Assuming the Best in People while Ignoring the Indicators.
- **L**ackadaisical Physical Security Procedures.
- **I**ncomplete Risk Assessments.
- **D**eficiencies in Compartmentalization of Information.
- **S**hortfalls in Expedient Reporting Procedures.
- **S**uboptimal Security Refresher Training.

Potential Targets for Exploitation

- Supply Chains
- People
- Investments
- Equipment
- Facilities

Always Alert, Always Progress

Insider Threats and How They Can Impact Your Business

Insider Threats

An insider is a person that has placement within your organization and potential access to information, people, and key infrastructure that are vital for your business to function. An insider threat does not have to be a full-time employee, a temporary technician or even a janitor may pose a risk if left unsupervised with unimpeded access to what you value most. Food for thought, how does your partnerships' security standards align with your own?

Impacts to Your Business

- Loss of a Competitive Edge.
- Potential Damage to Key-Critical-Infrastructure.
- Degradation of processes or public image.
- Disclosure of Proprietary Information.

Espionage Indicators

- Attempting to obtain placement or access outside normal purview.
- Eliciting information that they do not need to know.
- Spending long hours alone in the workplace with no work to show for it.
- Expressing discontent and/or motive to do harm against the U.S. Government and businesses.
- Heard discussing workplace information outside the office with little regard for security practices.
- Random, unexplained wealth.
- Unreported foreign contacts or foreign travel.

Protect with Precision

Insider Threats

Offensive-Defense is the best defense.

Objectives of Exploitation

- Disrupting *supply chains* can interfere with production. Exploiting supply chains could also lead to other opportunities that have inferences on competitive advantages.
- Knowing your next move in *investment* strategy could cause unwanted turbulence.
- *Time* is money, thus waisted time costs you money. How could a competitor waist your time? Misinformation and Disinformation campaigns can discredit *people* and operations within your business, ultimately tarnishing your good reputation and affecting professional relationships.
- *Equipment* must be both acquired and maintained. Knowing the processes of how this occurs can affect consumer-supplier relations and supply chains, as mentioned above.
- Knowing the full capabilities of your business can also identify your shortfalls, thus providing gaps competitors can exploit to fill.

Resources

- Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information
- Executive Order 12333, Intelligence Oversight
- Department of Defense
  - -DoD Instruction 5205.16, The DoD Insider Threat Program
  - -DoD Directive 5240.06, Counterintelligence and Reporting
- Department of Homeland Security
  - -DHS/ALL/PIA-052(b)
- 118th Congress (2023-2024): Insider Threat Assessment Act

Be a Hard Target

Definitions

Placement: Being a part of an organization or positioned inside a specific facility, group, or project.

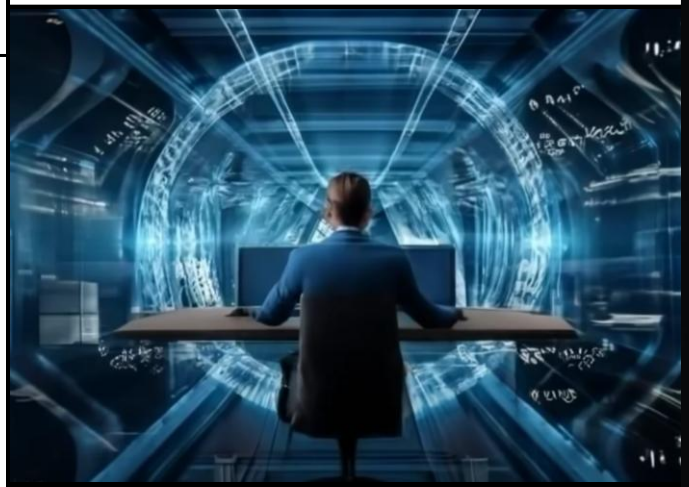
Access: Having the ability to walk freely into facility spaces with the appropriate credentials. This includes gaining normal-exposure to business servers with the ability to freely browse information not readily available to the public.

Elicitation: Casual conversations that result in the accidental disclosure of information without the target knowing they divulged such information.

Misinformation: Erroneous information.

Disinformation: Erroneous information used for an intended purpose (confusion, chaos, defamation, discreditation, etc.).

Hard Target: Exercising proper security procedures and maintaining a low profile, minimizing your risk to exploitation.



Make Things Difficult for Them

In Fact, Strive to Make it Impossible