



What is Physical Security?

Physical Security are the measures a company or organization takes to protect its' assets namely information. If a company secret is stolen, then the competitive playing field is leveled or worse, it's tipped in favor of the competitor. Corporate theft costs US companies **\$100 billion annually** in lost sales. Most crimes are perpetrated by employees, which are about eighty five percent of corporate espionage. To complicate the problem even more, trade secrets are not only being sought after by a company's competitors, but from foreign nations as well. They are hoping to use stolen corporate information to increase that nation's competitive edge in the global marketplace. (The SANS Institute)

Power Find specializes in providing your company with the tools to prevent breaches in information security. We have over eight years of experience with Department of Defense background investigations, industrial, government standards, and procedures that deal with the protection of sensitive materials or data. We can assist your company by evaluating your current physical security procedures, design, and help implement "Standard Operating Procedures" to prevent corporate information theft or espionage. We can train key employees or departments on how to implement these procedures. <<[Contact us to find out more](#)>>



The Benefits:

- ▶ **Lowers Risk**- Controls who has access to sensitive information, reduces the possible negative perception of your customers and suppliers, prevents further monetary loss, creates a stronger more stable business environment, and eliminates further theft.
- ▶ **Strengthens Business Relationships** – Increase the confidence of your customers and suppliers, assures the safety of private confidential information of your customers and suppliers, strengthens your position in the market place, creates a better awareness and reassures management of internal security.

- ▶ **Prevents Loss-** Reduces monetary loss, prevents sensitive information from going to a competitor, decreases the loss of trade secrets, intellectual property, prototypes, research documents etc. Prevents the loss of market share, market, or industry position of your company.
- ▶ **Increases Awareness-** Gives management and executives the insight and responsiveness in order to deal with and stop further damage to your company.
- ▶ **Denies-** Decreases the chance of infiltration, exploitation, and influence of information theft.

Business Operations

Precautions

Trade Secrets

Vital Documents

Power Find

Providing The Training Tools For Better Security

___What are the factors that may influence theft? ___

There are certain key factors and influences that may contribute to the motivation of a person to commit theft or espionage. Depending on the acceptability of how much risk a company or organization may want to take, there are issues that have to be considered in order to lower the threat of loss.

These factors and influence must be considered before anyone is hired or put in a position of trust. They include the following and are guidelines in order determine suitability before hiring. They include:

- ▶ **Conduct-** This involves questionable judgment, untrustworthiness, unreliability, and lack of candor, dishonesty, and unwillingness to comply with rules.
- ▶ **Allegiance-** If a person has association or sympathy with persons, a foreign country or organizations or who openly support chaos, subversion, or violence and who try to deny the rights of others.
- ▶ **Foreign Influence-** If a person is bound by affection, obligation, or influence through family or close association to citizens or governments of foreign nature.
- ▶ **Financial-** An individual who is financially over extended is at risk at having to engage in illegal acts to generate funds. [Read an about an actual spy case on this reason!](#)
- ▶ **Behavior-** It involves a criminal offense, personality, or emotional disorder and involves lack of judgment or indiscretion.

These are just some of the known factors that may increase the risk or potential of someone committing a crime against your company or organization. The [SANS Institute](#) writes that the basic reasons for insiders to "sell out" to a competition are: lack of loyalty, disgruntled, boredom, mischievousness, blackmail, and most importantly, money ([Corporate Espionage 101](#)). Employees that perpetrate most crimes that involve theft fall into one or more of the above influences that contribute to these behaviors and motivations. A company must have full disclosure of a persons past from a potential employee and even current employees. They must be willing to submit to a background investigation and periodic reinvestigation to determine there are no issues that can motivate them to become a thief or spy.

The other side of the coin is the outsider. These would include spies, attackers, or hackers who enter from outside a company. Since the end of the Cold War, a number of countries have been using their intelligence-gathering capabilities to obtain proprietary information from many of America's major corporations as well. Outsiders can enter from the Internet, dial-up lines, physical break-ins, or from partner (vendor, customer, or reseller) networks that are [linked to another company's network](#).

TEST YOUR COMPANY'S SECURITY!

1. Do you have current security measures? YES NO

2. Does your company have standardized operating procedures? Yes No

If yes: What are the general addendums or sections of your procedures? _____

_____.

3. Does your company have pre-hiring procedures or requirements? Yes No

If yes: What procedures are they? Such as; drug screening, background investigation, local Police Department Records checks.

4. Does your company have pre-hiring interviews? This would include a scripted list of questions or based on acceptable or mitigating factors such as; financial situation (any bankruptcies, debts more that 120 days, or large indebtedness) psychological consideration (suffering from a mental condition including schizophrenia, bi-polar disease or depression) or if a person is being medicated that might affect there judgment or mental process, behavior or conduct (such as criminal activity, reliability, trustworthiness)
Every Hire Seldom Never

5. Does your company currently have access controls? (Not including network passwords)
Yes No

6. Does your company restrict access into certain or designated parts or your office?
Yes No Limited Controlled

7. Does your company have regular security training? Yes No Annually Bi-Annually

8. Do you conduct vulnerability assessments? (This would include inspecting physical equipment, security checks and covertly testing security measure or procedures)Yes No Never Have

9. Does your company mark or classify documents or separate designated sensitive company intellectual property (i.e. labeling documents by either "trade secret," "confidential" or a special mark created by your security department)
Yes No Some Never have

10. Does your company have locking file cabinets, safes, controlled entry section or office?
None Locked Cabinets Safes Controlled Room

11. Do your employees leave items or documents out in the open while at work or after hours? Yes No File or Lock them up

Scoring: Yes questions=2 pts. No questions= -1 pts.

Total your points: Yes_____ No_____

Rate your company:

There are a total of +18 "Yes Points" and a total of -18 "No" Points

Add your total "Yes" and "No" points then subtract your "No" points from the "Yes" points to get your final score.

Excellent: 10-18 points Good: 5-9 Poor: 1-4

Deliverables



What We Deliver:

Our services deliver a valuable, high interest specific methods, and procedures that facilitate the management's business information protection needs. You will receive comprehensive guidance, consultation, and custom exclusive SOP's for your company. Some of them include:

- ▶ **Exclusive Methodologies & Procedures-** Power Find will develop specific Standard Operating Procedures and Methodologies tailored to your exact information protection needs. This is done by evaluating your company's current SOP, methods, and history in order to initiate strategies that are more productive.
- ▶ **Assessments-** We will identify specific requirements, identify core issues, and interview your project team to develop and implement your company's needs.
- ▶ **Situational Analysis-** What impact your current strategies have on your company, level of threat, and how you can improve your situational awareness in order to reduce a possible threat or breach of security.
- ▶ **Professional Development-** We can create the training tools that your company can use to enhance your awareness, provide security briefings to your employees, and develop on going educational instruction.



Support Services:

Project Team- We can organize as well as coordinate evaluations, inspections, and assessments in order to provide your company with the protection it needs.

Recommendations Report- Based on the findings and any other projects Power Find has completed for your organization, we can create a report designed to be used by your executives to help them increase their security awareness!

Onsite / Online Workshop- Designed to help those that participate leverage the results towards future improvements for your organization by remote learning. We use the latest online technology to provide your company with quality seminars, professional development, and learning tools on Strategic Management.

[Learn how to do a proper background check!](#)

[Contact us so that we can get started right away!](#)

[Strategic Information Management](#) | [Information Security](#)
[Online Learning Center](#)

Power Find Business Intelligence Services (Copy right 2002)

270 E. Douglas Avenue * El Cajon, CA 92020

Office: (619) 401-4022

Fax: (619) 442-7439

E-mail: service@power-find.com