



How To Prevent Theft or Damage?

THE SPY WHO HACKED ME:

Corporate spies, infiltrators, or hackers can be classified into two basic categories; insiders and outsiders. Insiders are usually employees, executives, IT personnel, contractors (programmers, network penetrator or computer auditors), engineers, or janitors who have legitimate reasons to access facilities, data, computers, or networks. Outsiders are 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 too. ([Corporate Espionage 101](#))

Power Find specializes in providing your company with the tools to prevent breaches in information security. We have over five 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 also train key employees or departments on how to implement these procedures. [Contact us to find out more>>](#)

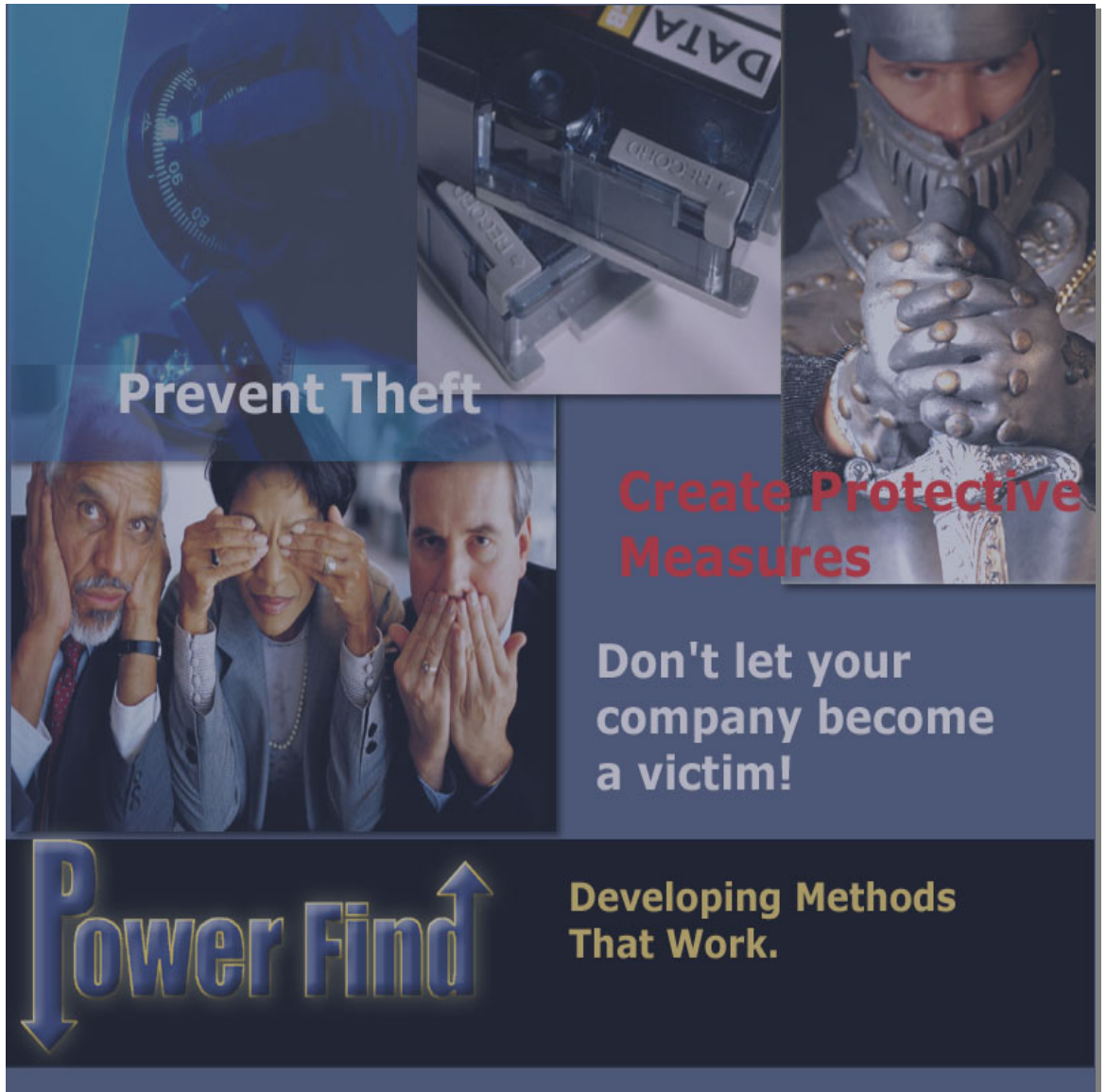
[Sign up to receive a FREE Security Evaluation>>](#)



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.



Prevent Theft

Create Protective Measures

Don't let your company become a victim!

Power Find

Developing Methods That Work.

___How Does Hacking or Spying Work?___

Consider the following:

An Internet worm that struck thousands of computers on Saturday January 2003, crashing bank cash machines and snarling Internet connections, caused limited disruptions as businesses in the United States and Europe fired up their computers Monday. In all, security firms estimated the "Slammer" worm, the worst act of Web sabotage in 18 months, affected tens of thousands of computers worldwide and caused millions of dollars in losses to Internet-related businesses. (CNN.com)

January 24, 2001

Microsoft's online services were disabled by a supposed Denial of Service attack. Further investigation by a Swedish network administrator reveals that all of Microsoft's DNS servers were behind one single network, therefore the problem was a result of poor network design. (Hacking and Network Defense / Verisign)

Corporate espionage is a threat to any business whose livelihood depends on information. The information sought after could be client lists, supplier agreements, personnel records and research documents, prototype plans for a new product or service. Any of this information could be of great financial benefit to a scrupulous individual or competitor, while having a devastating financial effect on a company. Just about any information gathered from a company could be used to commit scams, credit card fraud, blackmail, extortion, or just plain malice against the company or the people who work there. (Espionage 101)

Within the theft community, there are both hackers and crackers. Hackers have an interest in computers and networks and actually enjoy the game of discovering vulnerabilities or holes in systems. Hackers typically like to share their findings and never intentionally damage data. Crackers, on the other hand, are focused on maliciously violating systems with criminal intent. There are also spies that work to infiltrate a company by various means. A number of countries have been using their intelligence-gathering capabilities to obtain proprietary information from many of America's major corporations too. 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.

Their Tools & Methods:

1. Profiling

Profiling, or foot printing, is the process of gathering information about targets (your company or others). The result is a profile of an organization's security posture, also known as the infrastructure.

2. Scanning

After profiling a network, a hacker/spy will then scan the network for additional information. This will allow him or her to create a list of network devices active on the network.

3. Social Engineering

Social engineering is essentially a confidence game, in the old fashioned sense—a "con." The goal of social engineering is to gain access to network information from the people that run the network by creating a level of trust through deceit.

4. Observation

Observation can range from looking over someone else's shoulder as they login, to coming across passwords that people often keep written down.



Deliverables:

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



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.

[Sign up to receive a FREE Security Evaluation!](#)

[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 Ave * El Cajon, CA 92020

Office: (619) 401-4022 * Fax: (619) 442-7439

Web: www.power-find.com * E-mail: service@power-find.com