U.S. Department of Justice
Federal Bureau of Investigation

Intellectual Property Protection

Safeguard Your Company's Trade Secrets, Proprietary Information and Research

Information That Could Be Targeted:

Proprietary formulas and processes

Prototypes or blueprints

Research

Technical components and plans

Confidential documents

Computer access protocols

Passwords

Employee data

Manufacturing plans

Equipment specifications

Vendor information

Customer data

Access control information

Computer network design

Software (including source codes)

Phone directories

Hiring/Firing strategies and plans

Negotiation strategies

Sales forecasts

Pricing strategies

Corporate strategies

Marketing strategies

Acquisition strategies

Budget estimates/ expenditures

Corporate financial data

Investment data

Domestic and foreign companies may try to illegally acquire your company's information. Foreign nations that seek to improve their economies and militaries target US technology companies.

Protect the programs and systems that support what makes your company successful and unique. If your company has a technological edge, expect your technology, and those with access to it, to be targeted. If your company has developed a process to manufacture an item at less cost than others, that manufacturing process may be targeted. If your company is negotiating with another company or country, the negotiators and negotiation strategy may be targeted. If your company has invested time and resources developing a product or idea—**Protect It!**

Common Tactics:

- Computer hacking! (Electronic-device hacking)
  - A visitor connects an electronic device to your system, such as a thumb drive, that adds malware or downloads your information
  - Someone hacks into your network via a spear phishing attack
  - An unattended laptop is accessed or stolen
- On-site visits to your company:
  - Unauthorized photography or computer access
  - Unauthorized entry into restricted areas
  - Asking questions outside the scope of the visit
- Review of publicly available sources. Are you sharing too much information?
- Obtains your surplus equipment. Thousands of pages of stored information may still reside in the memory of a copier, printer, fax machine, etc.
- Employment solicitation (try to hire your key employees)
- Theft or unauthorized photography of products at trade shows
- Burglary (including copying of restricted documents where the originals stay in-house)
- Dumpster diving – finding information in your company's trash
- Joint ventures
- Front companies
- Unsolicited requests for information
- Elicitation – developing a friendship with an employee with the intention of obtaining restricted data or products. The employee will see someone who appears non-threatening and interested in his/her work.
- Electronic surveillance (listening devices in your hotel room, cell-phone hacking, etc.)

Theft of Intellectual Property Could Result In:

- Lost revenue
- Lost employment
- Damaged reputation
- Health and safety concerns from counterfeit products
- Lost investment for research (R&D)
- Delays or interruption in production

Intellectual Property Protection

Who Might Steal Your Intellectual Property?

- Domestic and foreign commercial rivals
- Domestic and foreign start-up companies
- Foreign intelligence officers (spies)
- Disgruntled employees
- Opportunists (lone wolves)
- Organized criminals

Insider Threats

Look for warning signs that an employee may be gathering and passing information outside your company.

Foreign Travel

When traveling to a foreign country, you and your company's information are at greater risk.

- Many foreign countries do not have legal restrictions against technical surveillance.
- Some foreign governments help their domestic corporations collect competitive intelligence.

Protection Strategies

- Assess your company's information security vulnerabilities and fix or mitigate the risks associated with those vulnerabilities.
- Do not store private information vital to your company on any device that connects to the Internet.
- Use up-to-date software security tools. Many firewalls stop incoming threats, but do not restrict outbound data. Competitive intelligence hackers try to retrieve data stored on your network.
- Educate employees on spear phishing email tactics. Establish protocols for quarantining suspicious email.
- Ensure your employees are aware of and are trained to avoid unintended disclosures.
- Remind employees of security policies on a regular basis through active training and seminars. Use signs and computer banners to reinforce security policies.
- Document employee education and all other measures you take to protect your intellectual property.
- Ensure human resource policies are in place that specifically enhance security and company policies. Create clear incentives for adhering to company security policies.
- Ask the FBI or other security professionals to provide additional awareness training. The FBI can provide a vulnerability self-assessment tool.

Contact Law Enforcement

You are ultimately responsible for protecting your own intellectual property. Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights to protect innovation; however, you need to take reasonable steps to protect your intellectual property and products, and document those measures.

Violations that may apply: Economic Espionage, Theft of Trade Secrets, Mail Fraud, Wire Fraud, Interstate Transportation of Stolen Property, Export Control, and Intellectual Property Rights.

If you believe your company is a victim of these crimes, contact the FBI or the National Intellectual Property Rights Coordination Center. Investigators cannot act if they are not aware of the problem. The FBI will minimize the disruption to your business, and safeguard your privacy and your data during its investigation. Where necessary, the FBI will seek protective orders to preserve trade secrets and business confidentiality.

Safeguard Your Company's Trade Secrets, Proprietary Information and Research

www.fbi.gov www.ice.gov/iprcenter