The Ultimate Guide to Intellectual Property Protection

From CSO Magazine and CSOonline.com

CONTENTS

I. Introduction to Intellectual Property

Definition: Intellectual Property

Intellectual property (IP) encompasses a wide range of documents, data and other assets that contain proprietary information. This can be anything from a particular manufacturing process or product design, to plans for a product launch, a trade secret like a chemical formula or algorithm, or a list of countries in which your patents are registered. It can also include proprietary ideas, inventions, industrial and architectural designs, literary and artistic works and Web pages. The formal definition, according to the World Intellectual Property Organization, is creations of the mind — inventions, literary and artistic works, symbols, names, images and designs used in commerce.

IP can also be something broader and less tangible, such as an idea. If the head of your R&D department has a "eureka" moment during his morning shower and then applies his new idea at work, that's intellectual property too.

Not protecting IP is a huge mistake for companies and countries alike. Intellectual property is what makes modern nations competitive in the world economy. It fuels innovation and development, and it keeps you ahead of the competition.

IP Theft: The Current Threat

Much attention has been paid to the seemingly never-ending stream of leaked or stolen personally identifiable information (PII). Stealing PII (in the form of credit cards, Social Security numbers and so on) used to be big business for cybercriminals. Then it started to get a bit harder because overall awareness increased; laws, regulations and industry standards were instituted; and organizations started to invest in controls to prevent and detect hacks.

The next big target for cyber-criminals, state governments, organized crime and hackers is IP. One stolen manufacturing process can be worth millions in saved development costs or billions in market share. Estimates show that IP theft costs U.S. businesses billions of dollars a year, while robbing it of jobs and lost tax revenues. The threat from emerging economies is of particular concern, as laws can be lax and enforcement more difficult.

William Boni, who coauthored Netspionage: The Global Threat to Information, calls it "the death of a thousand cuts." Because most organizations don't have a means of tracking the loss of proprietary information, they go on hemorrhaging, constantly losing market share.

Security pros need to understand the forces that are trying to filch IP from their company—whether legally or illegally. These forces range from competitors conducting corporate espionage, in which they might eavesdrop at trade shows, launch a social engineering ploy or dumpster-dive for IP, to criminals breaking into computer systems, bribing employees, maybe even hiding a pressure-activated tape recorder in the CEO's chair.

The threat of IP theft has not yet been fully understood by many organizations. One reason is that no one requires companies to disclose IP loss. When PII is exposed, laws such as HIPAA and HITECH demand companies disclose that information, but no similar laws exist for IP loss. Only the SEC has come out and said that if IP is stolen and it could have material financial impact on your company, you should disclose that.

Second, companies often have no idea when their IP is compromised. When credit card numbers and other PII is hacked, you tend to find out quickly because the bad guys make money on the breach. They quickly sell the credit card information on the black market, and that data gets used. At that point, the banks know the card numbers were stolen and the forensic trail leads back to the hack.

Two misconceptions exist among CEOs in regards to IP: One is that the threat of economic espionage or trade secret theft is a limited concern that it is only an issue if you are holding on to something like the formula for Coca-Cola or the design of the next Intel microprocessor. The other, held by many business leaders who acknowledge the danger to their trade secrets and other IP, is that the nature of this threat is sufficiently understood and adequately addressed. Often, on closer inspection, the information protection programs these business leaders rely on are mired in Industrial Age thinking; they have not been adapted to the dynamic and dangerous new environment forged by globalization and the rise of the Information Age.

Quick-Hit Examples of IP Theft

There are as many ways to gain access to corporate IP—legally and illegally—as there are assets to protect. Often, perpetrators operate in a gray zone. Here are three categories of IP loss.

When insiders and competitors target businesses: Economic espionage or IP theft conducted by insiders, competitors or combinations of the two are the most tangible, most common and most destructive threats. Such an attack can take many forms, like an employee, a member of the management team, a corporate board member, a third-party contract manufacturer or a collaborative partner in a joint venture. Here are several recent examples:

Lightwave Microsystems: The company IT director stole and sold trade secrets of the company as it was going out of business.

America Online (AOL): An AOL software engineer used a colleague's access codes to acquire information on 30 million AOL customers and sold it to spammers.

Corning Inc.: An employee found blueprints containing trade secrets within a container of material awaiting destruction. Instead of destroying them, he sold them to an Asian competitor.

When state-sponsored trade secret theft targets businesses: State-sponsored economic espionage and intellectual property theft are the most sophisticated and

formidable threats. Why do nation states engage in economic espionage and intellectual property theft? Primarily, to acquire technology to advance a military program, or to advance the economic competitiveness of the nation's industrial base, or simply to ensure that the major companies and contributors to the nation's GDP continue to make that contribution.

French Intelligence: Airbus attempted to muscle its way into the 1994 Saudi Arabian Airlines fleet modernization effort by offering bribes to individuals from both the Saudi airlines and government.

Russian Intelligence: In January 2005, Russian Prime Minister Fradkov requested Russia's internal security service (FSB) to increase its efforts to assist Russian commercial enterprises. This was tantamount to a public declaration that Russian government's intelligence and security services engage in collection and reporting activities in support of Russian commercial enterprises.

Cleveland Clinic Foundation: In May 2001, the U.S. attorney in Ohio indicted Takashi Okamoto and Hiroaki Serizawa for the theft of intellectual property belonging to the Lerner Research Institute of the Cleveland Clinic Foundation, charging that the two then provided the stolen research to a research facility owned by the government of Japan.

When counterfeiters, pirates and organized crime target products: The counterfeiting and piracy of products, activities often sponsored by organized criminals, make up the most insidious intellectual property threat, and certainly the most pervasive threat to the global economy as a whole. The U.S. Chamber of Commerce estimates that counterfeit and pirated products account for 5 percent to 7 percent of the global economy, and results in the loss of more than 750,000 jobs and approximately $250 billion in sales to the United States alone.

Software: According to a global study commissioned by the Business Software Alliance, piracy rates in 50 countries have increased over the prior year.

Technology: Counterfeiting, of course, isn't limited to software.

Shoes and Apparel: Counterfeit shoes are commonplace in the open markets of Southeast Asia.

Entertainment: A few successful cases against individuals for illegal file sharing do little to stanch the estimated $3 billion in losses due to piracy of motion pictures. According to the DOPIP Security Counterfeit Intelligence Report, in October 2005 alone, there were more than 341 separate incidents involving goods valued at more than U.S. $1 billion, and involving more than 54 separate countries. Not surprisingly, the top 10 brands counterfeited included Adidas, Nike, Louis Vuitton, Microsoft, Chanel, Gucci, Prada, Fendi, Manchester United and Puma.

II. Elements of Securing IP

Many CISOs believe their corporate IP is adequately protected by the standard data security practices they already have in place. However, IP lives in different parts of your network, and it's not always digital—IP also exists in filing cabinets and whiteboards. It is also sometimes subject to a different set of legal protections.

Intellectual property also varies from company to company and industry to industry. A CSO in the entertainment industry, for example, is not necessarily going to look at IP loss and theft in the same way as a CSO at a chemical company—so CSOs will approach protection of their companies' assets differently.

For all these reasons, protecting IP from myriad threats is a daunting prospect. The most common scenario, alas, is that an employee unwittingly shares a trade secret or a confidential idea, or that your business partner forgets about a nondisclosure agreement signed long ago. Just the same, here is a range of protections that you should consider putting in place.

The Basics

Know what you've got: The best way CSOs can protect proprietary information is by educating themselves and their employees about what their organizations hold valuable. If all employees understand what needs to be protected, they can better understand how to protect it, and whom to protect it from. To do that, CSOs must communicate on an ongoing basis with the executives who oversee intellectual capital. So meet with the CEO, COO and representatives from HR, marketing, sales, legal services, production and R&D at least once a quarter. Corporate leadership must work in concert to adequately protect IP.

Identifying what your IP consists of and where it resides is no easy feat because IP can be deceptively chameleon-like and take multiple forms: structured and unstructured, amorphous and concrete, small shreds of things or entire databases, thoughts in someone's head or captured in a document.

Prioritize it: Conduct a risk and cost-benefit analysis. Make a map of your company's assets and determine what information, if lost, would hurt your company the most. Then consider which of those assets are at highest risk of being stolen. Putting those two factors together should help you figure out where to best spend your protective efforts (and money).

Label it: If information is confidential to your company, put a banner or label on it that says so. If your company data is proprietary, put a note to that effect on every log-in screen. This seems trivial, but if you wind up in court trying to prove someone took information they weren't authorized to take, your argument won't stand up if you can't demonstrate that you made it clear that the information was protected.

Lock it up: Physical and digital protection is a must. Lock

the rooms where sensitive data is stored, whether it's the server farm or the musty paper archive room. Keep track of who has the keys. Use passwords and limit employee access to important databases.

Educate employees: As is often the case, humans are often the weakest link in the defensive chain. That's why an IP protection effort that counts on firewalls and copyrights, but doesn't also focus on employee awareness and training, is doomed to fail. Target the awareness campaign to specific groups of employees. At a manufacturing facility, for instance, you'll get employees' attention if you tell them a certain competitor is known to be working on a particular type of manufacturing technology and would love to get their hands on their information. And engineers or scientists will listen more carefully if you point out the danger of anyone learning more about an area to which they've dedicated a great deal of their life.

Networks and data

With increased digitization, more and more corporate IP is now in digital format. This data requires a particular set of controls and protection. Here are some considerations:

Decide on your protection level: Electronic protection of IP is different from protecting many other types of information. Often referred to as the "corporate jewels," IP is so precious it needs to be protected at a data and document level, not just a system level. However, draconian measures will inhibit data sharing, which is anathema in today's collaborative environments. On the other hand, when you have a small amount of ultra-secret, non-shared information to protect from prying eyes, the task is fairly straightforward: encryption or data masking, two- or three-factor authentication and embedded access controls.

These decisions—what to count as IP and how and to what degree to protect it—should flow from your business objectives, according to Evan Falchuk, chief strategy officer for Best Doctors, a global healthcare provider that provides health insurance and health advisory services. Since its business is to ensure people get the right medical care, it pays particular attention to its brand, which people need to trust, in addition to using comprehensive IT security technologies and practices, requiring all new employees to sign a nondisclosure agreement, and enforcing clean desk policies (see "Clean Desk" section below).

Don't boil the ocean: It's nearly impossible to identify all your corporate IP that you need to protect; instead, work to understand what IP is the most valuable 1 or 2 percent and protect it accordingly. It's less important to find and protect every nugget of information than to secure the crown jewels.

Apply a range of technologies: An essential tool is data loss protection (DLP), which helps track, identify and protect confidential and sensitive information for data that is stored, in use or in motion. In addition to DLP, you need to be able to monitor your two biggest communications channels (Web and e-mail) for outbound data and stop it in its tracks if necessary. Identity and access management tools are increasingly useful for ensuring that data doesn't fall into the wrong hands, and using security information and event management software with a solid log management tool can help you identify suspicious behavior and follow it all the way through to remediation of the threat.

Be diligent when doing this, and add your findings to training materials. Because while the reporting features of these tools are getting better, you still need to have highly trained eyes regularly analyzing the output to ensure you are truly protected.

Don't overlook your blind spots: In terms of data, the biggest IP blind spots are on your mobile devices, in cloud services and in SSL traffic. SSL accounts for up to 50 percent of Web traffic, and criminals know that most IT security systems do not inspect it. Most anti-malware security solutions don't look out for man-in-the-middle attacks decrypting the SSL traffic coming into the network. This is also not something that's always covered by DLP. As services such as Gmail move to automatically send all traffic to SSL, this will only become more of an issue.

Understand encryption and apply it judiciously: Encryption is often seen as a quick and dirty way to fix years of security neglect. Sometimes it is considered scary and difficult to understand. While encryption is extremely powerful, it can only protect your data when its requirements are properly defined, and its implementation is properly deployed.

Encryption deployments can be both effective and efficient. The following tips from security consultants Ben Rothke and David Mundhenk helps show that encryption is something to be embraced—not to be intimidated by.

Data that is effectively encrypted is unusable to the party who recovers it if that party lacks the proper decryption key(s) and means to decrypt. Encryption should be seen as a fundamental element of an organization's risk management program; however, while technologies such as firewalls and IDS/IPS are de rigueur, encryption is still lacking in far too many enterprises. According to the PGP 2009 annual study of U.S. enterprise encryption trends, only 25% of U.S. organizations have an encryption strategy in place that is enforced enterprise-wide.

Encryption challenges: The main reason why so few large-scale encryption efforts are successful is that—while many encryption hardware appliances are touted as plug-and-play—getting encryption to work in the enterprise is a significant undertaking. Many companies are simply not willing to commit sufficient time and effort. Effective encryption requires many things, including:

- Attention to detail
- Good design
- Good project management
- Comprehensive documentation
- Responsible ownership

In fact, it may take two or three years to complete all the activities involved within the more-complex encryption deployment scenarios. This is primarily due to internal

political sensitivity, application testing and workflow or database use modifications. Organizations should break their encryption projects into smaller, more manageable portions, while keeping the bigger picture in mind.

If encryption is not done correctly, there can be negative impacts to the performance of applications, systems and people who are supposed to use it. It can also adversely impact existing service level agreements.

Documentation and policies: An effective encryption deployment requires formalized documentation of relevant policies, process and procedures, as well as a formal asset risk management program. This will help to demonstrate that the work was adequately planned and supervised, and also shows that internal controls have been studied, valuated and can be accounted for.

The encryption policies must be endorsed by management and effectively communicated to end-users, business partners and all third-parties that handle sensitive data. If they can't comply with your policies, don't give them access to your data. Also, the policy must be flexible enough to deal not with just merchant data on statically deployed systems, but also laptops, PDAs, mobile devices and more.

Encryption data discovery: Before you can start encrypting data, you need to identify precisely where all relevant, requisite critical data elements are stored. This process should be preceded by having properly defined a formalized set of data classification and retention requirements. Data integrity compliance requirements should drive the criteria defining what is considered to be sensitive data, what constitutes acceptable protections for it, how long it should be retained, and how to securely destroy it when no longer needed.

An enterprise-wide audit of all data repositories should be completed, taking great care to ensure all possible data storage locations have been identified. Note that this process can take a few months in larger organizations.

Encryption types: There is no one size fits all or even one size fits most when it comes to data encryption. The method and type of encryption you decide on must be based on requirements specific to your organization. They should also be based upon industry standards and proven encryption algorithms, as well as robust encryption key lengths. The most successful encryption deployments are when the client drives the projects and brings in external expertise to assist when needed.

There are many different encryption types to consider, each with its own set of advantages and disadvantages. A list of some of the most common are:

1. HOST-BASED ENCRYPTION (AT REST)

This is where data is encrypted at creation, and is the first possible level of data security. Even if the encrypted data is intercepted (either accidentally or maliciously), the encryption renders it unreadable:

- Can increase processing overhead up to 50%
- Requires additional processing power/expense
- Highly secure and well-suited to active data files
- Large-scale data encryption can be unwieldy and impact performance

2. APPLIANCE-BASED ENCRYPTION

The data leaves the host unencrypted, but then goes to dedicated appliance for encryption. After encryption, the data enters network or storage device. This is the quickest to implement but can also be the easiest to bypass:

- Costly
- Not easily scalable
- Good quick fix—for extensive data storage encryption, cost and management complexity of encrypting in-band can increase significantly

3. STORAGE DEVICE ENCRYPTION

- Data transmitted unencrypted to storage device
- Easiest integration into existing backup environments
- Supports in-device key management
- Easy to export encrypted data to tape
- Easy to implement and cost-effective
- Best suited to static and archived data or encrypting large quantities of data for transport
- Large numbers of devices can be managed from single key management platform

4. DATABASE ENCRYPTION

DBMS-based encryption may be vulnerable when encryption keys used to encrypt data are stored in the database table inside the database, and only protected by native DBMS access controls

Users who have access rights to encrypted data often have access rights to the encryption-decryption keys. This creates security vulnerabilities because encrypted text is not separated from means to decrypt it. It also doesn't provide adequate tracking or monitoring of suspicious activities

Key management and administration capabilities come as built-in features of the product

Those who have a need for database encryption should read Cryptography in the Database: The Last Line of Defense, which is an excellent reference.

Key Management: The two most terrifying words to those involved in encryption are key management (KM). Part of the reason is that many technical and security professionals work in their own fiefdoms and never really have to interact to create a solution. In addition, management often doesn't clearly understand the technical consequences of the encryption requirements, and the technical engineers often don't clearly see the impact of the solution on the business.

KM is essentially the generation, distribution, storage, recovery, and eventual destruction (or end-of-life) of encryption keys. Many encryption failures are due to ineffective KM processes. It has often been said that effective KM is as important as protecting the data itself.

Like all of encryption, effective KM policy and design requires significant time and effort. Start your KM effort by asking a lot of questions. Some of them include:

- How many keys do you need?
- Where are keys stored?
- Who has access to keys?
- How will you manage keys?
- How will you protect access to encryption keys?
- How often should keys change?
- What if key is lost or damaged?
- How much key management training will we need?
- How about disaster recovery?

Post Deployment: Your post-deployment plans are almost as important as your pre-deployment plans. A well-designed encryption program should be able to seamlessly integrate new requirements without significant re-engineering of production systems.

Physical Access Controls

Physical security extends beyond controlling who can enter the building, when, and monitoring activity within the building. With digital data, there are many other physical ways that criminals can pilfer data-based corporate IP. Here are some examples of how physical devices can lead to theft, as well as how to combat these threats:

USB STORAGE KEYS AND USB COPIERS

How: Keys transfer electronic files onto plugged-in USB storage devices; copiers transfer data from one USB key to another without a computer.

Why: Low cost; easily concealed; portable; zero configuration; plug and play with any computer.

Mitigation: Disconnect USB ports; confiscate keys and copiers; ban possession or limit to on-site use only; monitor important file activity/transfers.

Comments: Keys quickly turning into a scourge because of their low cost and small form factor. Managing this threat should be a top priority.

MOBILE DEVICES

How: Transfer network files onto local hard drive.

Why: Mobile devices are ubiquitous, and taking them offsite is not unusual or suspicious; massive storage space allows large-scale data theft.

Why not: Likely to leave digital footprints of computer and file use if confiscated.

Mitigation: Monitor file use and activity; many commercial programs classify and encrypt data, block unauthorized file transfers and alert security if important files are tampered with; also consider LoJack-like devices for laptops; adopt laptop check-in and check-out policies and rules of use for laptops outside the office.

Comments: Classic security/productivity clash. As ubiquitous as mobile devices are, they create numerous risks to IP, including losing them. Prepare for policy battles.

LAPTOP APPLICATIONS

How: Transfer IP out of company through e-mail, IM, Web-based remote access, FTP, other applications.

Why: Create immediate access outside company; physical removal not necessary; quick transaction; can make it look like normal online activity.

Why not: Requires an accomplice (knowing or unwitting) person or machine to receive data; likely to leave audit trail.

Mitigation: Use products to inspect and prevent transactions; ban hard-to-control apps like IM; monitor applications and file transfer activity.

Comments: A wide variety of defenses are available. The biggest challenge isn't the mechanics of stopping the crime but the clash of productivity and openness with the need to secure. Some companies will easily ban IM; others will have a user revolt. And you can't ban e-mail, yet surveillance of e-mail is an imperfect option too.

MOBILE DEVICE CAMERAS

How: Take pictures of notes, whiteboards, labs, other sensitive data.

Why: Discreet; can capture handwritten data; portable; concealable; physical removal unnecessary.

Why not: Low image quality; limited storage space.

Mitigation: Ban mobile device cameras from use on premises; where appropriate, search bags upon building entry; employees should report unusual behavior with mobile devices.

Comments: Many companies already ban mobile device cameras, especially in research areas or at sensitive meetings. Searches should start with visitors and extend to employees working in high-risk environments.

WIRELESS ROUTER

How: Scan for and link to unsecured wireless networks and devices for unauthorized access.

Why: Remote snooping; targets hard-to-control ad hoc connections (e.g., at a convention or coffee shop).

Why not: Inefficient; no guarantee that access will yield anything; wireless increasingly encrypted.

Mitigation: Preconfigure all wireless devices to encrypt and hide wireless network connections; bar wireless devices from accessing all networks except trusted ones.

Comments: Wi-Fi threat is most pressing outside the office, where there's less control over user behavior. The key is smart configuration upfront to prevent ad hoc connections.

ANTENNA

How: Intercept wireless microphone transmission or Bluetooth device transmissions.

Why: Audio can be captured from far away; equipment readily accessible at electronics stores; situations that utilize wireless mics (e.g., offsite meetings at hotels) can yield important information

Why not: Requires some knowledge of radio/wireless transmissions; equipment conspicuous.

Mitigation: Encrypt wireless microphones; Bluetooth wireless should have specific security added; suspicious-looking people with antennas should be reported; design/set up lecture rooms to be acoustically secure; use pink noise generators.

Comments: Really two threats. Radio wireless is best mitigated with encryption and isnt changing much. Bluetooth wireless, while it requires more sophisticated equipment to exploit, is increasing because of the amount of Bluetooth wireless being used in PDAs and other gadgets.

DIGITAL AUDIO RECORDER

How: Record audio of conversations with concealed device.

Why: Can capture hours of high-quality audio; easily concealed or stashed bug-style.

Why not: Requires proximity; may have to leave device unattended, which risks detection; some knowledge of acoustics required.

Mitigation: Searches preceding important meetings; bug sweeps in high-risk environments.

Comments: Risk of audio capture increasing because devices are shrinking, approaching bug size. Thus treat them as such.

VOIP TELEPHONE

How: Tap and record data streams from IP-based phone calls; phish using VoIP applications.

Why: New technology not well understood or secured; tapping and recording applications available on Web; users' inherent trust in phone makes a good social engineering target.

Why not: Requires expertise to exploit.

Mitigation: Devote resources to understanding VoIP and how to secure it; block access to and use of tapping and recording applications.

Comments: Threat is escalating rapidly as more VoIP is deployed; CSOs concerned about having to protect against new threats.

PAPER

How: Dumpster- or printer-dive for sensitive documents.

Why: Provides a hard copy without exactly stealing; group printers easily accessible.

Why not: Inefficient unless you know when and where sensitive data is printed or thrown out; dumpster-diving conspicuous behavior; may require knowledge of trash protocols.

Mitigation: Shred all paper trash; require users to enter a personal PIN at a group printer for retrieval; employees should report suspicious "diving" behavior around trash, printers.

Comments: Decidedly low-tech but still common and effective. Shredding policies will require some user training/acceptance.

SPOTTING SCOPE/BINOCULARS

How: Spot information on whiteboards, in notebooks and elsewhere from a distance.

Why: Magnification technology powerful/advanced, allows spotting from long distances; no expertise required; can be used to capture handwritten (as opposed to digitally stored) information.

Why not: Must memorize or capture data in some other way; can look conspicuous.

Mitigation: Move whiteboards, labs, other places with sensitive data out of spaces with long lines of sight, particularly where exposed to outside windows visible to adjacent buildings; use whiteboard shutters; employ clean-desk policy; people on or near premises with binoculars should be reported as suspicious.

Comments: Threat similar to a high-powered camera but this requires much less expertise. Some binoculars can now capture what they see, like a digital camera. Higher threat in urban environments with buildings close together.

ZOOM CAMERA (DIGITAL OR FILM)

How: Capture notes, whiteboards, meetings and other sensitive information from a distance.

Why: Excellent image quality; can capture IP from off premises; digital camera can immediately turn image into electronic file.

Why not: Expensive; requires expertise, beneficial lines of sight; not discreet.

Mitigation: Have employees report suspicious photography in and around site; make meetings and offices with sensitive information unavailable to long lines of sight; implement clean-desk policy; use whiteboard shutters.

Comments: Old-school threat that requires high expertise, so it's rarer than some others. Again, risk increases in urban settings where windows of tightly packed buildings face each other.

IPOD/MP3 PLAYER

How: Transfer files using storage space on portable music players.

Why: Offer more storage than USB keys; ubiquitous and hard to control; nonstandard files can be stored and not seen in menu.

Why not: Personal music players expensive and sometimes require software to be installed for file transfer.

Mitigation: Ban use of music players on work systems; ban installation of music player software on work systems; encrypt sensitive files.

Comments: Again, many workers will balk at an iPod ban. Consider prohibition only in settings where IP theft risk is highest.

BLANK CD/DVD MEDIA

How: Burn data onto blank CDs or DVDs.

Why: Portable; inconspicuous; relatively high-volume storage.

Why not: Time-consuming to burn CDs; requires long periods of access to data.

Mitigation: Disable CD burners; ban CD burning applications.

Comments: Once state-of-the-art IP theft but declining rapidly as better, more efficient methods come along, like USB keys. Still a threat, especially with employees leaving a company who want to burn large amounts of data onto CDs or DVDs to take with them.

Internal Employees

Initially, it may look like most of the threats to your intellectual property are external, but that's typically not the case. No matter what your industry, intellectual property is lost or stolen in the same ways: insecure IT systems, disloyal or careless workers or social engineering. Whatever the reason, employees are the conduit through which IP is most frequently compromised. Here are some ways to fight back.

Careless employees: It's easy for employees to forget the role their work plays in the company at large, and they don't always remember that discussing a project at a cocktail party can put the company at risk. Business lunches and plane trips, in particular, are black holes for intellectual property—employees are talking to one person, while someone else eavesdrops or takes a peek at one of the employee's laptop screen.

Employees need to understand the criticality of their job, how it fits into the larger picture and affects everyone in the company. One way is to personalize it for them, to help them see the personal impact of losing IP.

Sometimes, employees give away crucial information for personal reasons, without knowing it. For example, your industry may employ people with PhDs who, to stay certified, must publish field-related research. Policies need to be enforced that allows them to share their work but not anything they're currently working on that would be of great interest to competitors.

In other cases, engineers might enthusiastically explain a top secret project to a supplier just because the supplier asked about a certain part. Outsiders have no obligation to keep that information secret, particularly if they do business with competitors.

Even with good software and constant auditing, any method by which your company stores or transmits content has the potential to be infiltrated. This is where encryption comes in, as once it's out there, you no longer have control over it.

Social engineering: Another way employees can unwittingly aid in IP loss is through social engineering. Examples include phone calls from people posing as graduate students doing a research project or as ex-employees trying to track down a former boss. CSOs dub that kind of attack a pretext call, and even when employees know what's going on, they sometimes think they can handle it themselves. What they don't realize is that they're dealing with trained intelligence professionals who use even tiny bits of information to construct a picture of what a company is doing.

The people on the other end of these calls are often competitors or someone hired by competitors. Corporate espionage and competitive intelligence probes are the underground fraternities of the business world—knowledge of their existence is implicit, but no one likes to talk about them. They are, however, a big threat to the security of your company's IP. If you and your employees aren't on guard, your rivals could walk away with everything from your marketing plans to your deepest trade secrets.

Disloyal employees: Of course, there are those who will give away IP assets on purpose. Disgruntled employees walk out the door and, despite having signed nondisclosure agreements, find their way to the competition or form their own companies using your trade secrets. It's important to understand what factors contributed to someone taking information elsewhere, and how you could keep it from happening again. This way, at least they see the consequences of breaking the rules.

Legal & Copyright Protection (patents, trade secrets etc)

From a legal standpoint, there are four types of intellectual property. IP registered in one of those categories with state and federal agencies is protected by law, and if infringed upon or otherwise abused, the infringers can be prosecuted.

The four legally-defined categories of intellectual property are:

Patents: When you register your invention with the government—a process that can take more than a year—you gain the legal right to exclude anyone else from manufacturing or marketing it. Patents can also be registered in foreign countries, to help keep international competitors from finding out what your company is doing. Once you hold a patent, others can apply to license your product. Patents can last for 20 years.

Trademarks: A trademark is a name, phrase, sound or symbol used in association with services or products. It often connects a brand with a level of quality on which companies build a reputation. Trademark protection lasts for 10 years after registration and can be renewed "in perpetuity." But trademarks don't have to be registered. If a company creates a symbol or name it wishes to use exclusively, it can simply attach the TM symbol. This gives the company room to prosecute if other companies attempt to use the same symbol for their own purposes.

Copyrights: Copyright laws protect written or artistic expressions fixed in a tangible medium, such as a novel, song or movie. A copyright protects the expression of an idea, but not the idea itself. The owner of a copyrighted work has the right to reproduce it, to make derivative works from it (such as a movie based on a book), or to sell, perform or display the work to the public. You don't need to register your material to hold a copyright, but registration is a prerequisite if you decide to sue for copyright infringement. A copyright lasts for the life of the author plus another 50

years.

Trade secrets: A formula, pattern, device or compilation of data that grants the user an advantage over competitors is a trade secret. It is covered by state, rather than federal, law. To protect the secret, a business must prove that it adds value to the company - that it is, in fact, a secret - and that appropriate measures have been taken within the company to safeguard the secret, such as restricting knowledge to a select handful of executives. Coca-Cola, for example, has managed to keep its formula under wraps for more than 117 years.

Data Destruction and Media Destruction

A critical part of securing intellectual property is the timely elimination of records and data you no longer need. When it comes to selecting ways to destroy data, there are basically three options:

- Overwriting, which is covering up old data with information.
- Degaussing, which erases the magnetic field of the storage media.
- Physical destruction, which employs techniques such as disk shredding.
- Several factors need to be considered when choosing one of these methods:
- Time: Is data destruction something the company does a lot, or does it have a lot of disks to go though?
- Cost. Can the company afford to destroy disks or do they need to be reused, and can it afford specialized destruction hardware?
- Validation and certification: Is data destruction a regulatory compliance requirement? How will you prove to regulators or auditors that you have met the requirements?

Here's a look at some of the advantages and disadvantages of these methods.

Overwriting: One of the most common ways to address data remanence—the residual representation of data that remains on storage media after attempts erase it—is to overwrite the media with new data. Because overwriting can be done by software and can be used selectively on part or all of a storage medium, it's a relatively easy, low-cost option for some applications, experts say. Among the biggest advantages of this method is that a single pass is adequate for data removal, as long as all data storage regions are addressed.

Software can also be configured to clear specific data, files, partitions or just the free space on storage media. Overwriting erases all remnants of deleted data to maintain security, and it's an environmentally friendly option.

On the downside, it takes a long time to overwrite an entire high-capacity drive. This process might not be able to sanitize data from inaccessible regions such as host-protected areas. In addition, there is no security protection during the erasure process, and it is subject to intentional or accidental parameter changes. Overwriting might require a separate license for every hard drive, and the process is ineffective without good quality assurance processes.

Another factor to consider is that overwriting works only when the storage media is not damaged and is still writable. Nor will overwriting work on disks with advanced storage management features. And while cost-effective, overwriting is not free. While cheaper than other methods, you still have to have the headcount to manage it, which adds to the cost.

By following standards created by the Department of Defense and the National Institute of Standards and Technology, CSOs can be pretty sure the overwritten data will be unreadable and unusable. Still, overwriting is by no means foolproof. There are areas where errors might occur and the data might not be fully overwritten.

Degaussing: Degaussing is the removal or reduction of the magnetic field of a storage disk or drive, performed by using a device called a degausser, which is specifically designed for the medium being erased. When applied to magnetic storage media, the process of degaussing can quickly and effectively purge an entire storage medium.

A key advantage to degaussing is that it makes data completely unrecoverable, making this method of destruction particularly appealing for dealing with highly sensitive data. On the negative side, strong degausser products can be expensive and heavy, and they can have especially strong electromagnetic fields that can produce collateral damage to vulnerable equipment nearby.

In addition, degaussing can create irreversible damage to hard drives. It destroys the special servo control data on the drive, which is meant to be permanently embedded. Once the servo is damaged, the drive is unusable, so if you're reusing those media, this may not be the right method. Once disks are rendered inoperable by degaussing, manufacturers may not be able to fix drives or honor replacement warranties and service contracts.

There's also the issue of securing media during the process of degaussing. If there are strict requirements that prevent exit of failed and decommissioned media from the data center, then the organization must assign physical space in the data center to secure the media and equipment for the disk eradication" process.

The effectiveness of degaussing can depend on the density of drives. Because of technology changes in hard drives and the size of them, some degaussing capabilities diminish over time.

Physical destruction: Organizations can physically destroy data in a number of ways, such as disk shredding, melting or any other method that renders physical storage media unusable and unreadable. One of the biggest advantages of this method is that it provides the highest assurance of absolute destruction of the data. There's no likelihood that someone will be able to reconstruct or recover the data from a disk or drive that's been physically destroyed.

On the downside, physical destruction can be a costly way to get rid of data, given the high capital expenses

involved. This makes it fiscally unsustainable as a long-term strategy and also contravenes an organization's green and sustainability programs. Some companies have found a way around those limitations by working with scrap contractors that melt down and reclaim or recycle metals.

In the cloud: Questions persist about how to handle data that's in the hands of cloud computing providers. While a traditionally outsourced data center provider will typically commit to destroying data at the end of a contract and confirm this destruction in writing, that type of policy is rare to nonexistent for SaaS. Cloud services are likely to sharpen their data destruction policies and procedures as adoption of the cloud grows.

"Clean Desk" Practices

Even the most conscientious employees are vulnerable to the occasional lapse in IP safety and could use a regular refresher. Ira Winkler, president of the Internet Security Advisors Group and former National Security Agency analyst, offers his advice for keeping prying eyes at bay by IP theft-proofing your desk.

Realize the likelihood. Yes, it can happen to you. Very few people think they will be victimized by IP thieves. It's important to recognize and remember that intellectual property theft is a real threat.

Log your computer off. Lots of people walk away from their computers and leave sensitive information available for the taking. Winkler has found documents worth billions of dollars to a company on an accessible computer. Log off so that someone else cannot log in to your system while you're away.

Understand that you cannot hide. Don't think you can hide keys or passwords in your paper clip drawer or taped under your keyboard. If you've thought of a place to hide sensitive information, someone else will have thought of it too. And although obvious, don't ever tape passwords to your monitor. Unfortunately, this practice continues today.

Clean your desk off. Don't leave sensitive papers lying around. Information should not be readily available to the passerby, including custodial staff. Ensure that clean desk policies are distributed and followed and that all corporate managers understand that it is their responsibility to verify that clean desk policies are understood and followed.

Shred. Shredders are often available only in the legal department and executive suite, but intellectual property passes through all departments of a business. Have shredders available at desks and be sensitive to trash that is otherwise sensitive, valuable or proprietary.

Lock your desk drawers and file cabinets. Keys and backup keys are vulnerable to theft. Occasionally people will forget their keys and will need to contact someone with a backup. Oftentimes, those backup keys are left in unlocked drawers for easy access. Leaving a drawer of keys unlocked—whether they are primary or only for backup use—is not a good idea. And neither is having one person walking around with a huge key ring. Use a combination key, or put that big key ring in a combination-lock safe.

Policies

Properly designed, communicated and enforced, corporate policies go a long way toward protecting corporate IP. Here are some ideas on what to include in policies that make you less vulnerable to IP theft.

Educate your teams on the right practices for handling this data. Identify the 1% or 2% of your corporate data and documents that are of highest value. Work with the people who have access to this data, including the Board of Directors and engineers. Talk to them about how to handle this data and set good controls for admins. Eliminate admin rights on desktops. Then reinforce the training through mock social engineering attempts and penetration testing. There are many good companies that can help you with this and measure the success of your education efforts over time.

Many companies turn to the experts—lawyers, generally—for help educating staff and getting their commitment to protect IP. Seminars covering IP basics can help organizations immunize themselves against IP leakage.

Protecting ideas: Another IP threat is idea misappropriation, such as when a former employee tries to claim credit for the idea behind a product or service. This can be resolved by instituting a clear-cut idea-submission policy that establishes ownership of ideas once they are shared with the company. By eliminating the implied duty of confidentiality right out of the box, you can avoid claims down the road.

Social media policies. Employees can inadvertently expose IP by over-sharing company activities on social networks when they get excited about something their company is working on, be it a cure for cancer or a new car that runs on curbside trash. By sharing too much about their employer's intellectual property on social networks, they threaten to put it out of business by tipping off a competitor who could then find a way to duplicate the effort or spoil what they can't have by hiring a hacker to penetrate the network or by sneaking a spy into the building.

Then there are hackers controlling legions of botnets that could be programmed to scour a company's defenses and, upon finding a weakness, exploit it to access data on the intellectual property. With the data in hand, the hacker can then sell what they have to the highest bidder, which just might be your biggest competitor.

The vulnerabilities caused by social networking have sparked a debate in the industry about whether companies need to revise their employee computer use policies with more specific language on what is/isn't allowed in the social networking arena. To rein in the urge to share too much, it might be useful to repeat this saying, which has started to appear in the public domain: "Loose Tweets Sink Fleets."

III. Threats & Tactics

TROLLS

IP protections exist in U.S. law for the purpose of ensuring inventors and creators are compensated for their works, encouraging innovation. Unfortunately, these very protections—patents, copyrights and trademarks—are now often used as weapons by companies that exist solely to shake down other companies for licensing fees. What was created to encourage innovation is now routinely used to stifle it.

Under this scheme, a company gathers up rights to one or more patents (most often in high tech) and attempts to extract a fee from "infringing" companies. The problem is that these claims are often made based on groups of patents in which it is unclear exactly what is protected. These companies are usually non-practicing entities that exist only to attempt to extract money from others.

Small companies that get hit with a trollish patent claim may well have to close their doors. Larger companies have suffered severe damage, too. These suits are widely considered a drag on the economy. It is difficult to know what to do about them, other than pay the requested fees, which calls to mind a mafia shakedown. (In most patent defense cases, the defendant countersues the plaintiff; this practice has some chilling effect on frivolous suits. Patent trolls, by contrast, are not doing anything with their patents so there is no way to countersue.)

DEPARTING EMPLOYEES

Any employee who leaves the company under any conditions—layoff, firing, going to a competitor—poses a threat to trade secret leaks. Here are 11 lessons for how to avoid trade secret misappropriation.

1. Create mirror images of hard drives. The security team, working with IT, should always replicate a departing employee's disk drive the day that person leaves for a competitive company. For large companies that may have hundreds of employees coming and going daily, the security team should identify the riskiest departures, usually those with high levels of access to trade secrets and those who are known to be leaving for a competitor. Imaging is important for the defense in a trade secrets case too, so consider doing this for high-profile new employees coming to your company, as well.

2. Don't poke around. This is the first of two cardinal sins companies should not commit. The emotional impulse of someone who feels violated is to immediately start rifling through the suspect's computer looking for the smoking gun. Don't. Think of the computer as a crime scene. Just as you wouldn't go around picking up bullet shells or putting your fingerprints on weapons found at the scene, you don't want to start accessing files, plowing through e-mails or otherwise tainting the evidence. The more you do, the more the defense can argue that the evidence is highly unreliable, even tampered with.

3. Don't redeploy too quickly. You don't want to eliminate the scene of the crime. Viable trade secret cases are rendered moot when a suspect's machine has its drive wiped clean and is redeployed for a new hire. Especially for computers of high-risk employees, IT's inventory efficiency must take a back seat to preserving evidence.

4. Add arriving employee protocols. As part of accepting a job, have employees arriving from a competitor sign a statement affirming they've brought no sensitive documents with them, making sure to include a laundry list of the types of documents and form factors that are verboten. (Work with counsel on this.)

5. Add departing employee protocols. Likewise, when an employee announces he's leaving for a competitor, have a piece of paper ready that shows him what he can and can't take off his computer. Include a statement that images of hard drives are taken as standard operating procedure. If necessary, have a security staffer sit with the person as he collects his personal files, such as pictures of the kids. This will help protect against one of the most common defenses offered by the accused: "I didn't know it was a trade secret." Chaperoning, or at least providing a list, specifies what is a trade secret.

6. Prepare an incident instruction memo. For a company on the receiving end of a trade secrets misappropriation accusation, a quick response is crucial to protect itself from ending up dealing with spoliation motions. CSOs should prepare a form letter or e-mail that's sent to relevant employees immediately upon accusation. The message of the letter is: You have an obligation to preserve evidence, no matter how bad you may think it makes you or us look. Legal precedent establishes that manipulation of evidence is far worse. Specifically, instruct the employee with the following: Do not delete any files from your work computer. Do not transfer any files off your work computer to other computers or devices. Do not throw away or destroy storage media such as CDs or USB keys. Do not install or use hard drive wiping products like Evidence Eliminator. Do not delete personal e-mail accounts or anything in them. It is crucial to expressly mention third-party sources such as Yahoo accounts and home computers as requiring preservation.

7. Understand modern methods of trade secret misappropriation and build defenses against their abuse. CD burning, USB keys, public e-mail accounts and ubiquitous network access—all these make keeping secrets harder than ever. CSOs should consider disabling CD burners and USB drives on computers.

8. Make sure employees understand that on computers, delete doesn't actually mean delete. To be sure, CSOs have lost an edge in preventing trade secret misappropriation because of technology. But they've gained something too. Technology leaves behind more fingerprints than paper. What many fail to fully appreciate is that everything they do on a computer leaves behind some bread crumb that a skilled forensics investigator will find. A good rule of

thumb for employees to understand is that there's no such thing as "delete." Programs that promise to truly delete or eliminate digital files are not perfect either, and in fact, evidence of their presence or use often has a negative effect, making the employee appear as if he has something to hide.

9. Bone up on trade secret misappropriation law. Someone accusing your company of trade secret misappropriation must prove two things. First, he has to prove that what was taken is a trade secret. Second, he must prove that it was taken, which can be more difficult than you think.

On the first point, the defense will often argue that if something is easily observable or reverse-engineered, it's not really a trade secret. On the second point, proving someone took something electronically often relies on cobbling together a forensic time line. But often that's essentially a string of circumstantial evidence. That's why the points on imaging hard drives and communicating the obligation to preserve evidence are crucial.

10. Create a litigation response team. The idea behind a litigation response team is to have a single response to an accusation rather than distinct reactions from different offices. The team should be able to assemble quickly and should include CSO, counsel, HR, a forensics expert, IT and a representative of the company's ISP.

11. Be ethical, no matter what. A trade secret misappropriation case will involve many employees with varying ethics. Some may want to bend or break the rules to protect themselves or the company. Your obligation is to the company, but also to "the right thing." If it appears support is rising for some questionable act, you are duty-bound to assert why it would be wrong and the ramifications, including your declining to participate and possible need to report the incident. It might be a good idea to show them a copy of trade secret misappropriation cases and the results of those cases when evidence was destroyed or manipulated. Have counsel or forensics experts explain why such acts won't work anyway.

COUNTERFEITING

Counterfeiting has been dubbed the crime of the 21st century, and nowhere is the problem more out-of-hand than in China. New Balance sneakers, Callaway golf clubs, Foo Fighters CDs, Viagra tablets, Cisco routers, you name it: China is the world's Wal-Mart for fake goods. The evidence goes beyond the well-known 90 percent software piracy rate in China cited by the Business Software Alliance. For example:

In the U.S., in fiscal year 2004 the Department of Homeland Security seized almost $140 million in goods that violated intellectual property rights; goods from China (and Hong Kong) made up almost 70% of the haul.

In 2003, Brooklyn prosecutors charged six men with importing up to 35 million counterfeit brand cigarettes from China. The smugglers allegedly hid the goods in shipping containers behind kitchen pots.

China's Shenzhen Evening News, a government-owned newspaper, wrote that some 192,000 people died in China in 2001 because they consumed counterfeit medicine.

While there's no easy answer, you can take steps to reduce the chance, or at least the impact, of the heisting of your brand. Here are a few:

Do your due diligence. If you're considering a joint venture, make sure your partner has a clean bill of health. Find out whether the partner is a reputable company, not in financial trouble and not involved in any IP-related violations.

Travel to China. Learn about Chinese culture and people. " This advice is good not only for CSOs but also for lawyers, investigators and anyone involved in fighting counterfeiting.

Budget smartly. Don't assume working in China will be simple and easy. Basic investigations cost between $500 and $1,500. This is higher than elsewhere for a variety of reasons: The country is huge, making transportation more costly; experienced counterfeiters are good at evading detection, making investigations more time-consuming than they used to be.

Protect your IP. If you do business in China, register your trademarks with the Trademark Office there. But even if you don't sell there today, it's a good idea to register trademarks there now if you might do business there in the future.

Consult with U.S. government officials. That includes people in Washington, the U.S. embassy in Beijing and consulates in China. They have IP experts on staff that can help answer questions about legal processes or other protection strategies.

Pursue criminal enforcement when necessary. You may be advised to pursue just administrative enforcement, which is cheaper and easier than a criminal case but usually leads only to seizure of fake products and modest fines. Better advice is to investigate deeply and do a criminal case, experts advise, although it requires more work from lawyers and investigators to make sure the courts properly handle the case.

Look at alternative enforcement strategies. Civil strategies—in which the main objective is compensation—are worth pursuing sometimes, such as sending a trademark infringer warning letters and taking the case to court for damages and injunctions. Civil enforcement can also be cost-effective. If an infringer has assets in a bank account, for instance, you can seize their assets before the case gets started.

Have a notarized, legalized power of attorney available. Experts advise having someone on the ground in China with power of attorney to file court actions or authorize your licensee to file actions on its own behalf. When cases go to court, you'll need this local presence.

Show your presence. If you have manufacturing operations, make sure you have good supervision in place. That may mean assigning some of your people working in China to supervise the action. Supervision also could entail putting counters on machines to know how many pieces are

being produced. It's also important to make sure controls are in place to keep track of how much raw material you've sourced.

Have key people sign a noncompete agreement. Noncompetes are a good way to protect information about your operations when local employees leave the company. They may not be easy to enforce, but at least they get employees who sign them to think twice before they jump ship.

Consider anticounterfeiting technologies for your products. Technologies such as holographic labels and RFID tags are being deployed to prevent counterfeits. Holographic tags can't be removed, burned or scraped from the product, and RFID tags allow product tracking.

Look to industry associations, such as the Quality Brands Protection Committee, for help, which can be better resources for information than paid middlemen, who may work only with select trademark authorities.

OFFSHORING

Different countries have different laws and tolerance levels for IP protection, and this becomes particularly relevant when choosing a services provider. A good resource for evaluating the threat of doing business in different parts of the world is the Corruption Perceptions Index published each year by Transparency International (and made famous by The Economist).

Here are nine practical steps for protecting IP specifically where you're offshoring software work:

Send people to inspect the physical premises where the software will be written. Note whether buildings have basic security check-in procedures and the like. Find out what kind of access people have to key systems.

Look closely at the way networks function, particularly if you plan to use virtual private networks. These are good for cross-facility communications, but make it easier for remote employees to work from home or on notebook computers, which can increase vulnerability.

Protect important information, such as source code, with passwords and access codes, and make sure that these are not widely available, either in the U.S. or at the outsourcing location. Approvals do reduce flexibility, but not as much as they reduce risk.

Demand that the outsourcer have tight human resources screening. Look for employee retention figures, find out if competitors do business with the same companies, and if so, ensure that there is no contact between teams.

Know what risks your own organization can take. Regulated industries such as health care and financial services need to keep closer controls over data and software development than, say, packaged goods companies.

Work to understand the legal system and culture of the country. Negotiate contracts that make the offshore company responsible for the actions of its employees.

Budget for greatly increased telecom costs, as well as for regular visits to the outsourcer.

Make sure any test data being used does not expose real information that could be traceable to real customers.

Always maintain an original copy of source code. This step seems obvious, but in one Y2K outsourcing case, a company was unable to prove a bug had been added to a program because it had not kept its source code.

Companies that don't have the resources to take these steps should think twice about what they are putting at risk by offshoring, whether it's software development or some other function like call centers involving sensitive customer data.

EAVESDROPPING

During the technology boom, one early-morning flight from Austin to San Jose earned the nickname "the nerd bird." Shuttling businesspeople from one high-tech center to another, that flight and others like it became good places for job recruiters. They also became great places for competitive intelligence professionals to overhear discussions among coworkers or to sneak a peek at a fellow passenger's PowerPoint presentation or financial spreadsheet.

Any public place where employees go, snoops can also go: airports, coffee shops, restaurants, and bars near company offices and factories, and, of course, trade shows. An operative working for the competition might corner one of your researchers after a presentation, or pose as a potential customer to try to get a demo of a new product or learn about pricing from your sales team. Or that operative might simply take off his name badge before approaching your booth at a trade show.

Employees must be cautioned about talking about sensitive business in public places, and how to work with the marketing department to make sure the risks of revealing inside information at a trade show don't outweigh the benefits of drumming up business.

Job interviews are another possible leak. Daring competitors may risk sending one of their own employees to a job interview, or they could hire a competitive intelligence firm to do so. Conversely, a competitor might invite one of your employees in for a job interview with no other purpose than gleaning information about your processes, what type of work the person would be assigned to and what kind of experience the company was looking for.

PIECING TOGETHER THE PUZZLE

Criminals and competitors don't always go after the big tuna—they can also effectively string together seemingly innocuous details into a big (and damaging) picture, without doing anything illegal. Such "plain-sight opportunities" include salespeople showing off upcoming products at trade shows, technical organizations describing in great detail their R&D facilities in job listings to attract top-notch scientists, suppliers bragging about sales on their Web sites and publicity departments issuing press releases about new patent filings. Combined, the right details might help a rival reduce your first-to-market advantage, improve the efficiency of its manufacturing facility or focus research in a

profitable direction. It's just a matter of connecting the dots.

Consider this scenario: A professional snoop once had a client who wanted him to find out whether any rivals were working on a certain technology. During his research of public records, he came across nine or 10 people who had been publishing papers on this specialized area since they were grad students together. Suddenly, they all stopped writing about the technology. The snoop did some background work and discovered that they had all moved to a certain part of the country to work for the same company. None of that constituted a trade secret or even, necessarily, strategic information. But he saw a picture forming.

Because they had stopped publishing information about the technology, it became clear that they had recognized that the technology had gotten to a point where it was probably going to be profitable, the snoop surmised. Then, by calling the people on the phone, going to meetings where they were speaking on other topics, and asking them afterward about the research they were no longer speaking publicly about, his firm was able to figure out when the technology would hit the market. This information, he says, gave his client a two-year heads up on the competition's plans.

DUMPSTER DIVERS

In this new age of data protection, where most information is stored digitally and paper shredding is commonplace, you don't need to worry about private information ending up in the garbage, right? Wrong. Sensitive data is sitting on USB drives, in the garbage, in the discarded fax pile and plenty of other places, waiting to be found by criminals. For this reason, good old-fashioned dumpster diving is alive and well.

Recently, a professional snoop went through the dumpsters of a large U.S. bank. Here is what he found:

Wire transfer information: The snoop obtained the wire transfer information of many transactions. Documents included transfer information for transactions between U.S. banks and banks in Jordan, Saudi Arabia, Dubai and Portugal. The documents included the account numbers and Social Security numbers of both the sender and the receiver, and their names.

Check copy: He also found a clear and easily-readable copy of a bank check with all of the important information: Bank account number, routing number and name of the account holder. The account holder's Social Security number and small business ID number were handwritten on the top right of the check.

Bank account transaction history: The dive also turned up the bank account numbers, balances and banking activity for the fundraising account of a prominent politician in the area.

Personal financial statement: He found the personal financial statement of a very wealthy individual listing the person's name, home address, real estate owned and values of the properties, several of the individual's bank account numbers, Social Security number and date of birth.

An entire, intact PC: The experiment even yielded a whole laptop with a tag on the back that said, "Property of [another financial institution]".

SOCIAL ENGINEERING

Social engineering is the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques. Social engineers use well-practiced tactics for eliciting information without asking for it directly or by implying they are someone they aren't. Pertinent information includes lists of employee names, titles and phone extensions, or internal newsletters announcing retirements or promotions.

Such scams might also include "pretext" calls from someone pretending to be a student working on a research project, an employee at a conference who needs some paperwork, or a board member's secretary who needs an address list to mail Christmas cards. The goal is always to gain the trust of one or more of your employees. Most of those calls are not illegal. Lawyers say that while it is against the law to pretend to be someone else, it's not illegal to be dishonest.

Social engineering has proved to be a very successful way for a criminal to "get inside" your organization. For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password, which he can use to log in and snoop around for sensitive data. Another try might be to scam someone out of an access card or code in order to physically get inside a facility, whether to access data, steal assets, or even to harm people.

Criminals will often take weeks and months getting to know a place before even coming in the door or making a phone call. Their preparation might include finding a company phone list or org chart and researching employees on social networking sites like LinkedIn or Facebook. Once a social engineer is ready to strike, knowing the right thing to say, knowing whom to ask for, and having confidence are often all it takes for an unauthorized person to gain access to a facility or sensitive data.

In one penetration test, a social engineering consultancy used current events, public information available on social network sites and a $4 Cisco shirt purchased at a thrift store to prepare for an illegal entry. The shirt helped the consultant convince building reception and other employees that he was a Cisco employee on a technical support visit. Once inside, he was able to give his other team members illegal entry as well. He also managed to drop several malware-laden USBs and hack into the company's network, all within sight of other employees.

John Nolan, founder of the Phoenix Consulting Group, has some amazing stories of what people will tell him over the phone. "I identify myself and say, 'I'm working on a project, and I'm told you're the smartest person when it comes to yellow marker pens. Is this a good time to talk?'" says Nolan, describing his methods. "Fifty out of a hundred people are willing to talk to us with just that kind of information."

The other 50? They ask what Phoenix Consulting Group is. Nolan replies (and this is true) that Phoenix is a research company working on a project for a client he can't name because of a confidentiality agreement. Fifteen people will then usually hang up, but the other 35 start talking. Not a bad hit rate. Nolan starts taking notes that will eventually make their way into two files. The first file is information for his client, and the second is a database of 120,000 past sources, including information about their expertise, how friendly they were, and personal details such as their hobbies or where they went to graduate school.

Social engineering tricks are always evolving, and awareness training has to be kept fresh and up to date. For example, as social networking sites grow and evolve, so do the scams social engineers try to use there; The National Cyber Security Alliance recently launched a "Stop, Think, Connect" campaign to get users to give more thought to their online behavior so they recognize social engineering cons before they get in trouble.

CORPORATE ESPIONAGE AND NATIONS-STATES

Espionage is sometimes sanctioned—or even carried out—by foreign governments, which may think they can boost the country's economy by helping local companies keep tabs on foreign rivals. The U.S. Defense Security Service, the entity with the counterintelligence oversight for corporate America's engagement with the Department of Defense, said in its most recent counterintelligence study that more than 100 countries were active in and engaged in attempts to acquire intellectual property from U.S. entities.

Various countries have vastly different ethical and legal guidelines for information gathering. It's important to be aware of corporate sleuthing tactics that are widely practiced by some countries and governments, including bugs, bribes, theft, even extortion.

No single set of guidelines for protecting IP will work everywhere in the world. The CSO's job is to evaluate the risks for every country the company does business in, and act accordingly. Some procedures, such as reminding people to protect their laptops, will always be the same. But certain countries require more precautions. Executives traveling to Pakistan, for example, might need to register under pseudonyms, have their hotel rooms or work spaces swept for bugs, or even have security guards help protect information.

Suppose you work for a cement manufacturing company, and you and your rivals are bidding on a big contract with the Pakistani government, says Ira Winkler, author of Corporate Espionage, who spent 11 years working with the National Security Agency. The intelligence goal, Winkler says, is to learn what your rivals are bidding so that you can undercut their prices. During the week the government has asked people to come make presentations, you chat up the staff at nice hotels in Islamabad, to find out if there are any guests from cement companies. Better yet, Winkler says, "If you know the name of the person who's the vice president of development for Europe/East Asia for your competitor, you could call up the hotel and ask if Mr. So-and-So is going to be there next week." Once you know who else is bidding, "you go to their customers and ask how much the competitor sold them cement for, saying you're willing to cut them a break."

And if those customers have confidentiality agreements in place? Well, you could always pay the hotel cleaning staff $25 to let you into the executive's room for 10 minutes, where you could hide a microphone or take pictures of documents. The rival would never knoweven, perhaps, after losing the bid.

"Why would it be far-fetched?" Winkler asks. "In America, it's just not done, typically. However, the reality is that throughout the rest of the world, competitive intelligence is just a fact of life. Americans are fairly naive about how things are handled.

Another example is a bank in South America that suspected espionage and hired a security consultancy to sweep the place of bugs. When the loss of information continued, the bank hired a different security team, which found 27 different devices. The entire executive suite was wired for motion and sound. In fact, it's possible that the first team that came in to look for bugs was probably installing them.

One common ruse is to organize professional conferences and invite native scientists who have emigrated to the United States. In other situations, the government might bug hotel rooms or tap phones, as the French are known for doing. Espionage can be a lot cheaper, after all, than investing in research and development, and it's very difficult to defend against when it's backed by a foreign government.