Intellectual Property and Beyond: Why Protecting It Is Everyone's Business

Introduction

The U.S. Department of Commerce estimates that the theft of intellectual property costs businesses more than US$250 billion and results in the loss of 750,000 jobs in the United States every year. In fiscal 2006, U.S. Immigration and Customs Enforcement recorded an 83-percent increase in intellectual-property-related crime, including 14,675 separate seizures of counterfeit goods worth more than $155 million. On a global scale, the International Chamber of Commerce puts the cost of lost intellectual property at more than $600 billion annually.

Loss of an organization's intellectual property can damage employees, partners, customers, and other institutional stakeholders. Theft or nullification of these assets may reduce or even erase profits, disrupt operations, undermine competitiveness, compromise hard-won reputations, and invite litigation or regulatory sanctions.

Many companies have focused on protecting against external threats by employing both physical and data security solutions to create secure business environments and protect their assets. However, in today's threat environment, companies must look beyond traditional border defenses such as access badges and network firewalls. They need to adopt more comprehensive security plans that integrate aspects of the corporate culture itself and encourage employees to take personal ownership of the security process. As companies begin to regard their intellectual property as more than simply a "trove of secrets", they are taking more holistic views. By considering the entire ecosystem of trust relationships both inside and outside the organization, a company can do a better job of protecting its most important assets: the innate qualities that make the business unique, viable, and valuable.

What Is Intellectual Property?

Christopher Burgess, a former national security executive and currently a senior advisor to the Cisco chief security officer, sums up the challenge of safeguarding a company's intellectual property portfolio: "It's identifying what you need to protect, determining who would benefit from taking it, understanding the vectors that can be used to compromise it, and then developing a defense commensurate with the value of the property."

Exactly what is intellectual property? These assets have traditionally been defined as trademarks, copyrights, patents, and trade secrets for which a person or organization can claim exclusive ownership. But in today's business world, that definition has expanded to include virtually any nonmaterial asset—whether "owned" in a strictly legal sense or not—that distinguishes a business and enables it to thrive and prosper. Cisco refers to these as "information assets".

Information assets encompass traditional intellectual property in addition to other nonmaterial assets and incorporate many areas within a business, including:

- Patented inventions that distinguish a company's products. But also the company's "human capital": employees who possess the inventive skills, technical knowledge, and institutional memory that give the organization its stature in the marketplace.

- Customer lists and client files. But also the sales tools, marketing materials, and advertising plans that enable the business to find and retain customers and clients.
- Sales figures and budget projections that, if revealed, could compromise competitiveness. But also other sensitive financials that could affect the business's credit rating, mergers/acquisitions, stock price, or private capital infusions.
- Design documents and plans for future products and services. But also all the R&D results, test data, and market studies that go into producing a successful product.
- Banking information that could make the business vulnerable to thievery. But also the business processes, proprietary practices, and supply chain innovations that help a company achieve and maintain profitability.

Those are just some of the forms that information assets can take. Every organization will have its own inventory of valued assets.

In addition to protecting the wide variety of information assets intrinsic to its business, a company must also take responsibility for safeguarding the assets that have been placed in its care by customers, clients, and partners, and in the case of governmental organizations, by the public at large. These external information assets range from partners' business data and matters of national defense to customer credit card numbers and citizens' identity, tax, and health records. Companies are now in effect stewards of their customers' sensitive information, and if adequate care is not exercised in protecting this data, adverse consequences could befall their customers and result in a huge negative impact to the company.

The Threat Spectrum

The threat spectrum consists of the ways in which an organization's information assets can be stolen or nullified, as well as the motives. This spectrum has expanded significantly with the emergence of global markets and the increasing complicity of governments in industrial espionage and manipulation of the competitive arena in favor of their domestic industries.

The attack vectors that threaten information assets fall into four general categories:

1. Organized crime. This category includes professional counterfeiters, hackers, and others who operate as part of illegal schemes, conspiracies, or criminal networks. Stolen information assets can continue to generate revenue over time.
2. Unscrupulous competitors. Competitors may employ illegal techniques ranging from industrial espionage to patent-infringing reverse engineering to gain unfair advantages in the marketplace. Even joint ventures and sanctioned partnerships have resulted in covert intellectual property theft.
3. State entities. Countries sometimes use their powers of eminent domain to seize or nationalize intellectual property. They may also employ their own intelligence-gathering organizations to uncover valuable assets that can benefit domestic industries.
4. Individuals. There are many instances of current and former employees stealing and selling corporate intellectual property, sometimes gathering this proprietary information for another entity. Competitors have also placed agents in businesses for the express purpose of gathering proprietary information.

Richard Power, a security expert who has served as editorial director for the Computer Security Institute (CSI) and director of global security intelligence for Deloitte Touche Tohmatsu, notes that

information technology has broadened and strengthened these primary vectors of attack. “Industrial Age espionage was conducted principally by compromising insiders,—bribing them, seducing them, hiring them away, and threatening them,” says Power. “But Information Age espionage looks very different.” Now, hacking into a company’s computer network or stealing laptops or PDAs can be an even more effective means of gaining access to coveted secrets.

Globalization has added to the threat spectrum by multiplying the sources of attacks. “If you own a tractor company in the American Midwest, you may be competing with a similar company somewhere in Asia or Europe,” says Power. “Or if you own a small engineering company that designs a part for a particular manufacturing process, someone in Taiwan or Ukraine may be starting up a company that uses that same process. Countries have different values, different laws, and different business practices. But the world has grown smaller and everyone is in everyone else’s business.”

Evaluating the Consequences

Companies should assess the level of worth of their intellectual property when considering how to protect it. What would it cost in terms of revenue, productivity, market share, or well-being if an asset were lost? Just as people put locks on their doors but place only their most valued possessions in a safe, a company should accord the greatest protection to the information assets that are most important to the business.

When evaluating information assets, the business should take their full value into account. This isn’t always simple. If a competitor were to steal a trade secret that enables it to improve a product or produce it more cheaply, that might cost the victimized company market share. However, the competitor would also gain financial advantage by not incurring the R&D expenses necessary to produce that intellectual property. The company that developed the property would be forced to compete against its own investment, which would in effect multiply its loss. Unfortunately, many organizations come to a full appreciation of the importance and vulnerability of their information assets only after having been compromised. For example, Cisco security expert Burgess recalls that it was only after a large U.S. corporation discovered that trade secrets worth at least $100 million had been stolen and sold to a foreign company that it began to change its culture to more effectively protect its information assets.

Sharing information about the latest security threats with other organizations can be an important step toward protecting information assets, even though many companies are reluctant to do so. “It seems that too often in the industry we are driven to keep quiet,” says John N. Stewart, vice president and chief security officer at Cisco. “Instead of collaborating and learning from one another, we frequently suffer in silence. However, in order to solve a problem mutually, you have to talk about it. So, within the guidelines of our human resources and legal organizations, we will discuss what has happened to us so that we and others can learn from our experiences.”

Dimensions of Protection

The most effective way to protect information assets is to carefully inventory what must be protected and identify how those assets relate to the people and processes that make up the business’ intricate skein of trust relationships. For instance, securing a data network involves not only defending its borders, but also understanding how employees, suppliers, partners, vendors, application service providers, and others interact with the network and access the various information resources.

Which technology will work best for safeguarding a network greatly depends on the network

infrastructure and the nature of the organization it serves. “Any new functionality either reintroduces old vulnerabilities or introduces new ones,” says Nasrin Rezai, director of global information security at Cisco. “But what is ‘disruptive’ technology for one company may be very much business as usual for another. We at Cisco are aggressive in deploying new technology in our infrastructure. The protection of information is very much tied to an organization’s culture and appetite for risk.”

So to effectively defend its information assets, a company needs to weigh its business plans, its IT strategy, its risk tolerance, and its corporate culture. However, globalization and its variants—including outsourcing or out-tasking work that may involve sensitive information—must also be taken into account. “All third-party vendors that perform a function for Cisco such as a commerce platform or call-center operation have different levels of access into the infrastructure,” says Rezai. “To protect our assets, we have each vendor sign a network connectivity agreement that sets forth the behaviors we expect. However, what could be legally binding or socially acceptable in the U.S. may not be so in another country. We consult closely with legal and human resources staff in many regions of the world to make sure we are aware of the local regulations and cultural norms.”

“A large part of shielding information assets is to get out there and protect your ownership wherever you do business,” says Burgess. “If you have a patent and you haven’t protected it in the region where you want to grow your market, then somebody else may take advantage. Litigation after the fact is really not a solution. Many times you cannot get adequate satisfaction through the courts.”

Besides diverse legal considerations, there are also cultural aspects to consider when protecting information assets in an increasingly global business environment. For example, employees in cultures with a high degree of social interaction may need to be cautioned about being discreet when they engage in friendly discussions with industry colleagues or family members.

In locations where many employees work from home, telecommuters not only need secure computer connections to the corporate network, but they also must have the means to secure information in diverse forms—including messages on cell phones or paperwork in home offices. And their computers may not be as secure as they think. In November 2006, Cisco sponsored a survey of more than 2000 remote workers in 10 countries, conducted by an independent research firm. The survey found that many teleworkers are putting their companies’ assets at considerable risk. Risky behavior included sharing their PCs with non-employees at home and “hijacking” neighbors’ wireless networks for Internet connections. Often the workers assumed that corporate IT would provide protection in all cases.

Globalization also underscores the importance of partnerships between government agencies and the private sector. Public-private cooperation is critical because it enables the exchange of information and resources that could be vital to the protection of both corporate and national assets. Moreover, it is government entities that administer the legal system and conduct the intelligence gathering that often leads to the prosecution of intellectual property crimes. For example, U.S. Immigration and Customs Enforcement, the largest investigative arm of the Department of Homeland Security, has explicitly targeted intellectual property rights violations as one of its primary concerns.

Government agencies are increasingly working with their counterparts in other nations to curb activities such as counterfeiting and piracy. In 2006 the Immigration and Customs Enforcement agency joined with the People’s Republic of China in their first joint undercover law enforcement operation, resulting in the destruction of a counterfeit DVD ring in China. Governments have other remedies at their disposal as well. In at least one case where the malefactors were not brought to justice, the U.S. government agreed to use customs regulations to punish the foreign firm that

infringed the intellectual property of a domestic company.

Public-private cooperation also extends to operational and technical levels. For example, the Partnership for Critical Infrastructure Security brings together owners of infrastructure and federal agencies in the U.S. to address R&D, information sharing, and internal governance issues. And various information-sharing and analysis centers (ISACs) provide forums where industry and government can combine forces to combat evolving threats, such as spyware.

“I’m a firm believer in staying in touch with local, state and provincial, and even national law enforcement,” says Cisco CSO Stewart. “If someone is trying to harm your business and you need information about how to think about it, law enforcement teams have a large and growing amount of experience in all the various scenarios. Knowing who they are, making sure they know who you are, and working closely with them is absolutely invaluable to our efforts.”

A Pervasive Security Culture

Like security in general, protection of information assets is the business of every employee. One of the main duties of a company’s chief security officer is to construct and maintain a security culture within the organization that places a high value on information assets and their preservation. Employees must feel a sense of ownership when it comes to enforcing a set of security principles.

"Security is about risk tolerance, an individual's actions and responsibilities, and applied technology," says Stewart. "At Cisco, we are all accountable for our individual actions and are rewarded for leadership behavior that helps protect our customers, partners, and suppliers. Not surprisingly, awareness and education are vital."

No organization can expect employees to safeguard information assets if they have never been educated as to what these information assets are and how to protect them. “Don’t leave it up to the employee to interpret how to protect your information,” says Burgess. “Tell them how you expect them to do it.” A large part of establishing a proactive security culture is to encourage and reward compliance, rather than to deal with noncompliance after it has resulted in loss.

To help employees internalize the security culture, the Cisco Corporate Security Programs Organization (CSPO) uses companywide awareness training and education to promote and reinforce behavioral changes that protect the confidentiality, integrity, and availability of Cisco information assets. Mia Bradway Winter, information and security awareness manager for CSPO, employs communications techniques she learned working in the public relations field to get the message across. As part of the awareness campaign, CSPO developed a 3-minute video for executive-level managers highlighting how vulnerable information assets can be. “We used short vignettes to dramatize how easy it is for outsiders to eavesdrop on a cell phone conversation, steal a laptop from bathroom stall, and otherwise target unsuspecting employees,” says Winter.

Any communication regarding information asset protection needs to be tailored to the recipients, especially within a globally based organization. Cultural distinctions are important where information assets and security are concerned. “We can’t apply a homogeneous communications style from one business culture to the next within the enterprise,” says Stewart. “For example, the way you communicate with an employee in Japan should be different than in Germany, though the messages are the same.”

The CSO’s job requires that he or she have access to top-level corporate management. As Burgess puts it, “The CSO should not be a stranger to the boardroom. Lack of interaction between the CSO and other executives makes your enterprise more vulnerable.” This especially comes into

play as the CSO seeks to align the company's security structure with corporate business objectives. The CSO should have a broad enough skill set and level of experience to understand the needs of each business unit, while demonstrating the flexibility needed to set rules that the rest of the company is comfortable following.

Brad Boston, senior vice president of the Cisco Global Government Solutions Group and former Cisco chief information officer for Cisco, points out the risk-management aspect of the job: "The CSO helps the company decide which risks it is willing to take, which risks are too expensive to mediate, and which risks are too important to ignore." But experts agree that sensitivity to risk should never be allowed to jeopardize the company's ability to respond to changing market conditions and take advantage of the latest technologies.

Creating a security culture capable of protecting information assets also requires an intimate understanding of the data lifecycle—what it is, where it goes, who touches it, and where it ultimately resides. This is a multidimensional process that goes beyond IT infrastructure to include people, policies, and processes. So the security organization must query and partner with all the relevant stakeholders to make sure the whole needs spectrum is addressed and met.

Finally, the security outlook must always face toward the future. "We may be solving the problem today, but are we also looking at future challenges and opportunities?" asks Rezai. "Business environments are very dynamic, so security must follow suit."

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-418387-00 7/07

