DPG

Deer Park Group, Inc.

Information Security & Risk Assessment

Larry Runge

One of the most valuable assets of any company is its intellectual properties, also called *information assets*. Some of these are intuitively obvious, such as patents, copyrights, and custom computer code, yet others which are equally valuable are more difficult to define, such as Goodwill, Customer Satisfaction, or esoteric expertise which exists in the skills and knowledge of the employees—expertise which would be expensive and time consuming to replace should it vanish.

Information security is the process of protecting such assets from accidental or intentional misuse by persons inside or outside of an organization. The goal of information security is to keep unauthorized people out of a company's system and to recover from accidental or intentional actions which damages a company's intellectual property. That is, of preventing, detecting, and containing security breaches, and restoring affected data to its previous state should damage occur.

Most companies face a twofold problem when it comes to intellectual properties. One is that they have no idea of what the value of many of these are—or even that some of them exist— and the other is that they are at a loss as to which of these are at risk and what that level of risk might be.

Furthermore, there is value in managing risk, whether it be to obvious assets, such as having your customer database stolen, or whether it be less tangible from a hard dollar standpoint, such as having your company's name dragged through the mud while senior executives are sent to jail.

A survey of 138 companies in 2002 reported that the loss of proprietary information collectively cost them a minimum of $53 billion in 2001 alone. Much of this information was in the form of R&D or financial data. Yet these numbers reflect visible assets alone, and ignore hidden assets, thus the actual loss is considerably greater.

Few companies have a robust and proven method of tracking the loss of proprietary knowledge and other information assets. Without this, such valuable assets can bleed away, like bright colors in strong sunlight, draining the vitality from an organization and causing it to lose market share. Why? Because it is impossible to invent proprietary information assets more quickly than it is to leak, steal or otherwise lose them. Since most managers don't understand that this is happening, they assume business degradation is due to ill winds of fortune.

Yet this is exactly the kind of situation which information security is intended to prevent. The purpose of security assessment and risk analysis is to find and plug the leaks before they occur. The old adage that *it's too late to lock the barn door after the horse has been stolen*, has never been more true than in information security.

There are many different approaches to information security, a few effective, many not. One is the *Spec-*

ter Method, which is to assume what you cannot see cannot exist—and therefore cannot hurt you—and to ignore it altogether. Another is the *Ostrich Process*, which is to bury your head in the sand and hope the threats to your organization will have disappeared when you raise your head to look around. Yet another is the *Tinker Toy Technique*, where you have built some security, but have a lot of loose pieces laying around waiting to trip you up.

Finally, there's the Scientific Approach. In this method, you perform a Security Assessment of your environment and implement a comprehensive security plan, whether it be something developed internally, or an existing security standard such as BS 7799 or ISO 17799.

A *Security Assessment*—also called a *Security Audit*—evaluates your current security environment for integrity and robustness. The purpose is to identify both strengths and weaknesses. These are typically performed by an independent company, unless you have considerable expertise in doing these in-house. Such an audit can run from a few days of discussions, to three weeks or so where security is probed by the auditing team in penetration testing. Obviously, the more time spent, the more detailed the results. Each company has to make a determination just how robust an assessment is appropriate for their firm.

At the *Corrective Action* phase, the company determines what next steps they wish to pursue. This could run the gamut from correcting high risk situations—picking the low hanging fruit—to implementing a full blown security plan such as the *ISO 17799 Security Standard*.

Security should be targeted at potential threats and existing vulnerabilities, specifically areas where a failure could result in excessive or unnecessary expenditure, or loss of confidence in the company. The purpose of the Security Assessment is to determine what these are. Security Risk Analysis is then used to weight these according to damage these could cause and the likelihood of each occurring, versus the costs to prevent such an incident. Armed with this information, management can then make far better judgments and more effective decisions.

Threats to information security can be divided into two broad categories, strategic and tactical. In the former case, threats to your company's information assets may come from competitors seeking to steal clients or products, organized crime (which is quickly becoming computer agile) seeking the credit card information of your customers, the ubiquitous hacker seeking to cause denial of service to your customers and business partners for their own demented reasons, and even foreign governments who may wish to utilize your intellectual properties without the benefit of royalty payments.

Tactical threats are typically aided by laxity or oversight in your own organization. Things such as failing to keep track of holes in the underlying operating systems and firewalls, and ensuring all available fixes are applied and making sure these don't create more problems than they solve. For example, at least one major software vendor is known for providing cures which are worse than the ailment; applying their patches often fixes one problem while introducing a dozen new ones.

Another tactical threat is the management of User-ids. Are the User-ids and passwords of employees removed as soon as the employee leaves, or are they left to smolder in your system for weeks, like a ticking time bomb? Do employees have their passwords written on Post-it notes and stuck to their monitors? Other tactical issues include things such as, are attempted security breaches recognized, investigated and resolved in a timely manner? Are contracts for virus eradication products kept up to date?

These may seem intuitive, but many companies have suffered losses because of these and other oversights. Tactical threats should not be under estimated, for more damage is done by omission than by thieves

Information security is relative, there is no such thing as absolute security. A security policy is a series of trade-offs between security and business requirements. Employees will have a need to access information. Customers and business partners may have a need to exchange data for a business to succeed and thrive. So information security is about balancing risks and rewards, making trade-offs in terms of balancing the requirements of business against the need for confidentiality, integrity, and availability of information. Because your risks, vulnerabilities and business requirements are constantly changing, security is an ongoing process, not something you do once and then put behind you.

One of the areas where a Security Risk Assessment is of high value is in regards to legislation and regulatory controls. The Sarbanes Oxley Act of 2002 is just one of the compliance requirements put on businesses, and the costs of non-compliance could be devastating to both the CEO and CFO. In addition, larger customers often mandate standards which must be adhered to, and failing to do so could cost a company their business. Although different industries have to meet different legal requirements for protecting and reporting data, Risk Analysis enables rapid identification of any such failings.

In the past, mudslinging was usually limited to the political arena. Today, it is commonly directed towards corporations. The press loves to report the latest security bungles. Lets face it, people don't watch or read the news for good news—it is *bad news* that sells the papers and attracts the viewers. But such reporting can erode customer confidence and give shareholders a negative view as to how well your business is run.

Furthermore, we live in a litigious society and there's increasing concern that security breaches could bring about personal injury lawsuits—filed by customers whose personal information has been disclosed. Or perhaps lawsuits based on damage caused by security breaches with business suppliers and partners, or perhaps even class-action lawsuits filed by irate shareholders.

Usually ignored altogether are the intangible risks. Intangible risks can come in many forms, as NASA found out during the Columbia explosion in February 2003. Suddenly the agency came under far more scrutiny, and there was a concern that web sites which had not been kept current might be misinterpreted by the press and public as a general slovenly approach to their operations in general.

A similar scenario was succinctly described when the CEO of a major airline told his management team, "Coffee stains on the flip-down trays means we do our engine maintenance wrong."

Microsoft's reputation suffered a huge blow in August 2003, when security flaws in their XP and 2000 operating systems were exploited by a series of viruses, which shutdown computers by the millions worldwide, causing estimated damages close to the two billion dollar mark.

Another example is that of an American firm specializing in high quality optics and telescopes. In late summer 2003, their orders increase dramatically when the Mars opposition brought the red planet to its closest approach to Earth in 59,619 years. The company's order volume was so tremendous it caused a lag in shipments, which in turn caused dramatically increased call volume to their customer support system. This in turn overwhelmed their phone system, causing delays, busy signals, drop-offs, lost messages, as well as a host

of other problems—proving once again that too much of a good thing can cause unexpected consequences.

All of these instances caused loss or damage to intangible assets, one of which is the consumer's impressions of the organization involved. Interestingly, the first two were generated by problems, but the third was caused by something that would typically be embraced with open arms by any company—dramatically increased sales.

In each case there was risk to intangible assets that none of the organizations were aware of. Yet these three are not alone in this regards, most companies have intangible assets at risk of which they are not aware. That is the purpose of a Security Risk Analysis, to identify risks to both tangible and intangible assets, to place value on these, and to determine the amount of risk associated with each so the company can address potential problems before they can occur and cause damage.

Many security breaches are not accomplished by whiz-brains who would put Alan Turning to shame, but rather something as simple as someone copying a password written down and displayed on another person's desk. When software is installed on mainframes and servers, Test accounts are usually setup to verify that the installation was done correctly. All too often, these accounts are never deleted. In one situation, a government computer hosting secret information was hacked into by teenagers who used the User-id "*Test*" along with the password "*Test*".

Security should be commensurate with its risks. However, determining what level of security is appropriate, what types of controls to apply, and how cost effective all of this will be, can be both complex and daunting. Again, the framework available to help executives with such decision making are Security Assessments and Security Risk Analysis.

Like a chain mail hauberk in medieval times, information security is only as strong as its weakest link. Unfortunately, many companies have not one, but many weak links, This leaves them to rely upon providence and the vagaries of chance, trusting that when an attack comes it will be where their armor is the strongest and not the weakest. Unfortunately, as mentioned earlier, most successful attacks come from people within a company or from former employees and not from hackers—people who know where the weak links are.

A Security Assessment will identify where many of these holes occur. Business management is responsible for deciding what level of security risk the enterprise is willing to accept, while IT management is typically responsible for determining the specific controls and applications employed.

What are some of the benefits of a robust and well-oiled security approach? Lower costs, for one. Intrusions or accidents which compromise a company's information and cause employees to stand idle or for customers denied service to sit and fume while restoration processes are underway, are greatly reduced. It establishes effective corporate governance and compliance with legislation and regulations by demonstrating Due Diligence. Customer confidence is increased in the ability of your firm to handle their sensitive personal and financial information. Embarrassing or devastating public disclosure of security failures in the popular press is avoided or eliminated.

By managing information security risks, damage or loss of intangible information assets is prevented.

The Deer Park Group

(847) 382-5171
www.DeerParkInc.com