

GEORGE WASHINGTON UNIVERSITY

**INFORMATION: AN
ORGANIZATION'S GREATEST
WEAPON AND WEAKNESS**

A report submitted in partial fulfillment of

EMSE 318.10 Information Operations

BY

DOV YORAN

“Information is power.” Although historic, this statement is as true as ever at the dawn of the new millennium. In today’s fast paced business environment, information is more critical than ever. It can mean the difference between becoming a successful Fortune 500 corporation or another abysmal company lead to ruin, bankruptcy and eventual dismantling. Ensuring the confidentiality, integrity and availability of business information is critical to every enterprise and its operational viability. The sharing of information among various parties in today’s complex business environment is a necessity. The protection, detection and correction of technologies and methodologies used to keep information safe is at the of any business’s decision to defend oneself again Information Warfare attacks from competitors, private citizens and foreign national governments.

Business information can take many different forms. There are almost countless events and bits of information that are meaningful. Knowing a competitors market strategy and beating them to punch, stealing product plans or understanding product weaknesses are all forms of information that give distinct advantages to a business. Even information as simple as knowing the cost of production potentially gives a competitor the ability to set prices below to where a company might not be able to follow. Business information also includes recruiting strategies, organizational structure, internal personal and human resources information, financial data, operating costs, production materials, delivery/distribution processes and schedules, marketing strategies, product enhancements, pricing, competitive information, consumer information, etc. are just a few more examples.

Within the United States, there numerous codified laws that define the legality and the abuse of business information thought of as Intellectual Property. This legislative effort used to combat the misuse and theft of Intellectual Property are outlined by Copyright, Copyright Management – Digital Millennium Copyright Act (DCMA), Bootlegging, Trademark, Trade Secrets, Integrity of Intellectual Property, Misuse of Disseminating Systems, No Electronic Theft Act, and the Economic Espionage Act.¹ Intellectual property and trade secret is formally classified in the eyes of the law if a company takes “reasonable effort” and documents actions taken in protecting such business information.²

Clearly there has to be a methodology of classifying information and making it available for the appropriate audiences. The audience includes internal employees, external competitors, investors, news and media, government officials, potential candidates for employment etc. One example of classification of information is the method that the United States Government employs, via its Top Secret, Secret and Confidential schema. The Top Secret category is defined as information that for which disclosure is given could be “reasonably expected to cause exceptionally grave damage to national security.”³ The Secret category is defined as information that for which disclosure is given could be “reasonably expected to cause serious damage to national security.”⁴ Finally the Confidential classifies information that for which disclosure is

¹ Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice: <http://www.cybercrime.gov/ip.html#VIIIa>; Internet accessed on 10 November 2002.

² United States v. David T. Krumrei, No. 97-9285 (1998)

³ *The White House Office of the Press Secretary*, Executive Order 12958, April, 1995, Classified National Security Information.

⁴ *Ibid.*.

given could be “reasonably expected to cause damage to national security.”⁵ Documents containing information on military weapons, strategic plans, foreign intelligences, domestic and foreign activities and military operations as well as scientific and technologic information are all data pieces kept secret to varying degrees within the above classification schema. Typically the US government classifies information at the paragraph level, indicating the level of clearance needed to access each paragraph. Commercial organizations typically adhere to the principle of least privilege. This ideological follows the logic that employees/resources should only be given access to information that is necessary for functionally performing one’s job. This involves identifying an individual’s responsibility and information needs in accomplishing his or her tasks; then restricting the user’s access to the minimal information needed for completing this task.⁶ Often times this principle can be executed through assigning a user to a classification domain. As each classification is defined, the user’s rights and access are defined as well. Corporations and organizations will usually have a system administrator assign the user privileges upon employment of a new individual. Often times the individual is given access rights equal to other members of his or her organization. In a simple example, a new employee in the marketing department will be given access to the marketing databases and this user will be denied access to the finance and accounting systems. Innate to this ideology is the fact that each individual team is classifying and organizing information to be shared within itself, among its members. When the department compartmentalizes its data, some individuals will receive more

⁵ Ibid..

⁶ David Ferraiolo and Richard Kuhn, “Role-Based Access Controls” (National Institute of Standards and Technology, US Department of Commerce, 1995).

access to information than they actually need, the cost benefit analysis to this method is still very effective.⁷

What are some other methods of leveraging information internally within an organization? Internal departments such as Human Resources need to share salary, bonus and other personal employee information within its organization. How can this information be shared safely and effectively without compromising the integrity of the data? Historically, sensitive information was filed in restricted areas such as records room whereby necessary employees are given access. This is still practiced, for example hospitals often have dedicated rooms for patient records. This is also common practice for legal departments within an companies where by they need to store original legal documentation such as contracts, letters of intent, non-disclosure agreements, stock option plans, employee payment records, etc.

On a more broad sense, organizations have to now share information both internally and externally with business partners, alliances and customers. This is imperative for the future growth of a company. There are many technologies and solutions that can be implemented to help foster a better sense of security.⁸ Agent technologies were developed to enable companies and partnerships to intercommunicate more effectively with a focus on interoperability. Cooperating corporations can pool resources together to for distributed problem solving, sharing of information, etc.⁹ Hiring

⁷ Randall K. Nichols, Daniel J. Ryan, and Julie J.C.H. Ryan, *Defending your digital Assets against Hackers, Crackers, Spies & Thieves* (New York: McGraw-Hill, 2000), 101-103.

⁸ Ravi Sandhu, "The Technology of Trust," *Internet Computing, an IEEE Distributed Systems Online Publication* <http://dsonline.computer.org/0211/f/w6gei.htm>, Internet accessed on 12/08/02

⁹ Csilla Farkas and Michael N. Huhns, "Making Agents Secure on the Semantic Web," *Internet Computing, IEEE Distributed Systems Online* (November/December 2002), Internet, <http://dsonline.computer.org/0212/d/w6age.htm> accessed on 12/05/02.

outside consultants to assist with internal project are a cost effective solution that is common industry practice. Not only do consultants have specialized talents and expertise, they also bring a fresh and unbiased perspective. Companies have to be aware of the internal security risks with these consultants. Often times they are given the same physical and network access the same as most internal employees. There is an inherent danger in that these temporary employees do not have a vested interest and level of trust that permanent employees have. Furthermore, there is also conflict of interest in a consultant accessing information to prolong his or her engagement. It is prudent to keep an open eye on all personnel accessing corporate assets, especially those without a tighter affiliation.¹⁰

One solution for sharing electronic information across an organization or department that has become relatively common practice in the last fifteen years is the employment of server equipment in a classic Client/Server design. This architecture allows for the information to be stored centrally in one location on a server, or several computers in cluster, and shared to all remote client workstations via a network. This is a marvelous solution in that many corporate resources can access the necessary information. For example, one central server can store all the financial data, such as accounts receivable, monthly invoices, division costs and budgets, etc., while the finance team, perhaps located in several cities or countries around the world can access that information as long as they have access to the network. Perhaps the most common method of protecting this information internally is through the use of access control lists, or ACLs. ACLs restrict the usage of employees and users accessing the information by

¹⁰ Kathleen Melymuka, "Know your partner," *Computerworld* (November 2002, Vol. 36) 45-46.

limiting one's ability to access information. These lists are contained on a file, usually located on the server where by each user is associated with a password granting him or her access. If a user attempts to access a specific server where he or she is not listed in the ACL, they are simply not given access. Often times, users are assigned access upon initially logging into the network through his or her machine rather than logging onto individual servers/networks at a time. Upon beginning employment, typically the Information Technology Department sets the appropriate access control of each employee.

There are numerous methods used to share information both internally and externally across an organization. Corporations must take caution when collecting, transporting and sharing information from partners, employees and customers. There are many legal connotations both domestically and internationally that must be considered when using business data.¹¹ One popular method for sharing information is the installation and use of company intranets and internal web sites. These file-sharing systems are great ways of sharing information because web navigation is almost innate to all employees in today's technology environment. Essentially the designer, information architects, must distinctly clarify a number of aspects such as the mission, objective, business needs, customers (internal employees) needs, etc., to help determine the navigational elements, content and functionality.¹²

The Ford intranet/internal Web site consists of over 100,000 pages. This Intranet allows scientist and engineers to share information electronically from various

¹¹ Rebecca S. Eisner and Brad L. Peterson, "United States: Privacy Update: Does Data Privacy Matter To Your Business?" *Mondaq Briefing*, Mayer Brown Rowe & Maw, Gale Group, Inc. (September, 2002).

¹² Louis Rosenfield and Peter Morville, *Information Architecture For The World Wide Web*, United States: O'Reilly, 1998. 11-14.

locations.¹³ Productivity is dramatically improved upon by increased sharing of intellectual capital and information. In fact, Ford shortened its new car production time from 37 to 24 months!¹⁴ These internal web sites can provide other necessary information to business users such as sharing marketing information and other large documents. Appropriately securing Intranets begin with the formation of appropriate policy development, described later. Other technologies such as securing servers can also help insure authenticity and protection of information.¹⁵

Corporations also share information with employees through traditional training classes and educational forums. Aside from the historic classroom environments, new and innovative technologies that allow for distant learning are becoming increasingly popular.¹⁶ For example, a Web cast is an easy medium to share information across numerous remote users. This relatively new technology provides an intimate and an extremely convenient medium for information exchange. The course instructor, or meeting sponsor presents his or her information through a Web broadcast. Each user who accesses this site through a web browser see the information presented by the meeting organizer. The sponsor controls the user's web browsers and present information from a variety of applications and formats such as excel, word, and most commonly PowerPoint. A Web cast is an excellent tool for sharing information;

¹³ Tracy Primich and Ken Varnum, "A Corporate Library Making The Transition to Web Publishing," *Computer Libraries*, (November/December 1999 Vol. 19, No. 10)

http://www.infotoday.com/cilmag/nov99/primich_varnum.htm, Internet accessed on 12/12/02.

¹⁴ "Ford Motor Company: Collaborative Product Development Via Web Technology," *EC.com Journal*, Cardinal Business Media, Inc., (December 1996),

<http://groups.haas.berkeley.edu/citm/publications/briefings/fordbrief.htm>, Internet, accessed on 12/12/02.

¹⁵ Brian Collins, "Designing Secure Intranets," *Manufacturing Engineer*, (December, 1998 Vol. 77, Issue 6): 4.

¹⁶ Claudia Loebbecke, "Electronic Trading in On-Line Delivered Content," paper presented at the 32nd Annual Hawaii International Conference on Systems Science, Kohala Coast, HI, 1998.

especially for meetings conducted where employees are located in many differing locations and regions.

A Web cast is initiated through a third party software tool or outsourcer. These vendors allow personnel to easily create and hold a web conference. Typically, there is also an audio feed by which the presenter can speak through the Internet connection or via a conference bridge where by the participants log into as part of the meeting. The meeting organizer setup a meeting through the vendor, who provides a specific URL location for participants for a certain date and time. At the time of scheduled meeting, participants will come to the desired URL to join the Web cast. Appropriate security measures are implemented by requesting the invitee to enter a username/password to gain access to the meeting. User's can communicate with the coordinator through voice if there is a conference call bridge or usually through an instant messaging/polling system built into the Web cast software application. Some common commercially available applications are PlaceWare and WebEx.

How do organizations protect their information? The first step is to identify the nature and type information requiring protection. Once information assets are identified, a risk assessment can be conducted to determining which applications/information needs protection according to its value within the organization. After determining risk tolerance for identified information, an enterprise can then take the appropriate steps to protect itself.

The most crucial and fundamental protection of a corporation's assets and sensitive information is the proper creation, implementation, education and use of

policies and procedures, coupled with audit practices to ensure policy compliance.

Policies and procedures are the foundation to proper governance of employee conduct, with regard to a variety of subjects such as sexual harassment, appropriate use of corporate resources, PCs, telephones, updating laptops with anti-virus software, Intranets, etc.

Policies are the fundamental corporate laws that bring order to a corporate organization. Policies are guidelines that dictate the appropriate behavior for all corporate employees, essentially its management's instructions indicating how a corporation should be run. These typically include statements of goals, objectives, beliefs, ethics and responsibilities. Within an information security framework, a policy provides, "...the basic guidance we use to decide the value of our information assets, the impact of their exploitation, corruption or destruction, and level of risk we are willing to accept in providing for their protection."¹⁷ Well-defined policies can go along way towards protecting information. Some examples of policies might be requiring employees to employ random alphanumeric passwords, employees logging off their workstations, wearing issued identification badges while on company property, etc. A procedure is the guideline on implementing and practicing a policy. Procedures are, "Specific operational steps that workers must take to achieve goals - - goals which are often outlined in policy."¹⁸ Examples of procedures might be that employees must change their passwords every thirty days; passwords must have at least eight characters with at least one letter and number; employees must log off of from their workstations

¹⁷ David Carothers, "Policies, Standards, Guidelines and Procedures," as part of presentation for EMSE 218 Managing Information Systems, Alexandria, VA., 6-13, February 2002.

¹⁸ Ibid..

upon completion of each business day; employees must wear their identification badges around their neck in a visible manner, etc. Creation of policies and procedures are only the first step in fundamental organizational security. Educational classes and training room sessions must be conducted to guide employees. Although not always intuitive, a fundamental necessity for successful policies is the dissemination of such guidelines throughout the organization, i.e. training.¹⁹ With all the hype about vulnerabilities in technologies and products, managers often forget that employees are the weakest link in an organization's security chain. Being only as good as your weakest link, the education of personnel must be critical to every organization's security effort. Individual employees can provide an incredible amount of security and information protection.

The final step in policy management is the auditing verification that they are being properly followed. Ensuring compliance is the only way to effectively enforce company policies and procedures. Being able to monitor, control and institute remedial actions are all steps that administrators and managers must plan and participate in executing. (Note: Having the authority to follow up on these tactical responses should be policies themselves so that user's and employees the corporation's rights.)²⁰

Following suite with the examples above, auditing policy can be information to check compliance is, routine audits of password files (administrators conducting a monthly review to ensure that employees are indeed changing their passwords and also using appropriate password parameters), administrators can also perform bi-monthly audits of server logs to verify that employees are logging off of work stations on a nightly basis,

¹⁹ Charles Cresson Wood, "The Human Firewall Manifesto," *Computer Security Journal*, (San Francisco: 2002) Vol. 19 Issue 1. 15-18.

²⁰ Scott Barman, *Writing Information Security Policies*, Indiana: NewRiders Publishing, 2002. 157-160.

security guards and other personnel can do random hallway checks, or prevent employees from entering the building and grounds without properly displaying identification badges. Often times, an internal committee can conduct security audits, so the responsibility and burden of execution is shared among other internal organizations. As information security issues and threats gain notoriety, acceptance and practice of security audits will continue to rise as well.²¹

The corporate practice of creating and institutionalizing organizational wide policies and procedures are fundamental to the protection of a company's physical and information-based assets. These steps help corporations protect themselves by keeping the appropriate information internal within its own organization and employees. Standards such as ISO7799 and BS7799 are becoming increasingly popular, allowing organizations to prove to management and partners, the validation of one's security posture through certification. Although preached for years by security managers and industry experts, the creation and implementation of such certifications marks a fundamental change in that information security is now accepted as a management process instead of a technology process.²²

There are numerous technologies, aside from policy creation and enforcement, implemented to help protect, detect and correct the confidentiality, integrity and availability of organizations information. Simple technologies such as paper shredders can also go a long way in protecting corporate information. People often do not realize

²¹ Lawrence Ritcher Quinn and Alan E. Brill, "Risky Business," *Journal of Accountancy*, (June, 2002) 65-70.

²² Queenie, Ng, "Security Is A Management Process," *Asia Computer Weekly*. (October, 2002)

the potential danger of throwing away company data without proper disposal. Biometric access control such as palm scanners, retinal eye scanners, and facial recognition software can all play a pivotal role in security access to both physical and network based information. This practice is commonly employed for areas that require strict access such as Data Centers and hosting environments where customer servers are stored. Other simple techniques are locks and doors, often implemented in record rooms where personnel files are physically stored.

One of the most effective means for protecting and communicating information is through cryptography. In practice since the dawn of civilization, is a continuously growing field; both in Research and Development and in wide spread corporate use.²³ Cryptographic standards such as Pretty Good Protection (PGP) and RSA have helped to bring about more frequent use of cryptography within the corporate environment. Often times these encryption technologies lay the ground work for future mediums of business information exchange through digital bilateral exchanges of credentials.²⁴ These technologies will only become increasingly important as multinational corporations continue to grow and will continue to need to communicate with employees at countless office locations and remote users such as traveling sales representatives. Providing an effective and safe means of communication must be a chief priority for many executives.

Another trend that most corporations are implementing to protect their information is through the implementation of technology devices such as firewalls, host-

²³ H. X. Mel and Doris Baker, *Cryptography Decrypted* (Boston: Addison-Wesley, 2001), 45-46.

²⁴ Marianne Winslett, Tin Yu, Kent S. Seamons, Adam Hess, Jared Jacobson, Ryan Jarvis, Bryan Smith, and Lina Yu, "Negotiating Trust on the Web," *Internet Computing, an IEEE Publication* (November/December 2002 Vol. 6, No. 6): 30-37.

based intrusion detection systems and network-based intrusion detection systems.

According to IDC, the global security market, including products like firewall, anti-virus, authentication software, etc., will explode, tripling by 2005.²⁵ As these technologies evolve, they are becoming increasingly powerful and useful if implemented appropriately. These security product devices can help monitor appropriate usage and enforce policy compliance of corporate resources.²⁶ Being able to properly catch and cease the improper use information of an outside intruder, or an insider employee, is a necessity that every organization will have to enforce. These security devices are almost the norm at most corporations that have access to the Internet and use online resources such as email, FTP, etc. Clearly these technologies are crucial to the protection of corporate networks but they must be implemented in an integrated approach. In fact, a piece meal security approach can be more costly and less secure in that redundant spending is conducted across the organization as point solutions do not scale effectively or even interoperate. Another hazard for point solutions is the increased maintenance and training needed to upkeep these technologies. “Application Integration Security” is the practice of ensuring that security solutions such as firewalls, intrusion detection systems, cryptography, etc. are all brought together in unison.²⁷

As security devices and technologies are deployed at an increasing rate across a corporate networks infrastructure, the threat of overwhelming an IT staff becomes more apparent as the flood of alerts from these devices soon become a knowledge management

²⁵ “Global Security Market to Triple by 2005: IDC,” *Businessline*, (Islamabad, September, 2002)

²⁶ Paul E. Proctor, *The Practical Intrusion Detection Handbook* (New Jersey: Prentice Hall, 2001) 121-126.

²⁷ John R. Vacca, “Securing ‘Open’ Corporate Networks,” *E-Business Advisor Magazine* (August 2000), 33-42.

nightmare. Security event managers (SEM) technology offer corporations the ability to take event information produced by multiple point network devices and correlate them into a single output.²⁸ Furthermore, specialized companies that can implement, manage and monitor security devices and solutions are now flourishing through an outsourcing model dubbed Managed Security Services Providers (MSSPs). Organizations such as Internet Security Systems (ISS), Symantec (through acquisition of Riptech), and IBM Global Services are all market leaders in this growing industry.²⁹ These companies can effectively monitor and manage complex and noisy security devices such as firewalls and Intrusion Detection Systems through an ASP-based model without putting significant stresses on a corporations network.³⁰

How do corporations gain a competitive advantage using Information Warfare? Companies are in fierce competition with one another on a variety of levels. Whether it be for new customers, government and educational funding, media attention, financial assistance, etc., there are a numerous fronts where corporate competition comes into play. Conducted on a global playing field in international communities with Wall Street darlings such as Microsoft, Goldman Sachs, or Wal-Mart competing for market share in the billion dollar market values, or two local grocery stores in Anytown, USA competing for the 25 customers that live on the same block, the competitive arena decides who will

²⁸ Judith Lamont, "Computer Security Meets KM-knowing When To Worry," *Information Today, Inc., Knowledge Asset Media*. (July, 2002, Vol. 11, No. 7) 10-12.

²⁹ J. Pescatore, K. Kavanagh, and R. Steinon, "2H01 Managed Security Service Providers Magic Quadrant," Gartner, Inc., (February, 2002) 2-4.

³⁰ "Safeguarding a Firm's Information Assets," *Bank Technology News*, (New York: September, 2002 Vol.15 Issues. 9) 45-47.

win and who will lose. Gaining any type of information that will give a company a distinct advantage, critical to its success.

There are many types of information that could make or brake individual corporations, propelling them into becoming successful enterprises, remaining in dominant market leader positions, or decaying into slow wind-down with eventual bankruptcy looming on the horizon. One example of a dangerous data capture would be to know a competitor's customer list. This obvious data point would be immensely beneficial in gaining new customers for two reasons. The first reason is that the company knows these particular individuals or corporate entities have already purchased a related product, so they have a business need for a particular product or service that is offered by the organization. Secondly, the company would know exactly who the competition is and could launch a marketing campaign specifically crafted to compare one's own product to the competitor that is already in place. Another example of valuable corporate information is knowing a competitors trade secrets; this could be the cost of production, proprietary methodologies or processes in developing products or delivering services, pricing schemes and structures (if that is not publicly published), etc. Imagine if General Motors knows Toyota's cost of producing a 4-Runner. Let say for example it costs Toyota \$20,000 to make one 4-Runner. General Motors, knowing its own cost of producing a Chevrolet Blazer was only \$15,000, could conceivable reduce its sticker price to \$19,000 driving Toyota out of the Sport Utility Vehicle market. Obviously this is an overly simplified example, but it helps bring context how valuable proprietary information is to global multinational corporations. One example of the effect of information and its role in a local business context is that of two local restaurants

competing in for the high end dining dollars for a small town. For example, one restaurant might plan on hiring a famous French Chef for an upcoming summer as a special attraction. If the competing restaurant discovered this information, they could hire another French Chef and launch their specialized cuisine several months ahead of the other business, effectively ruining the original restaurant's motif. The second restaurant could potentially implement more dubious tricks such as pay off the chef to poison the food, quit his job minutes before the initial launch, steal their supplies, etc. There are countless examples of the importance of information, keeping it secret and how it plays a critical role in the successful outcome of any business, local or global.

Now that we have an idea as to what types of competitive information is out there and how important it is for business to protect, we can focus our attention to the methods implemented in gathering such information. It is not uncommon in many businesses today, especially for large global organizations, to have entire teams dedicated to information gathering on competitive companies, products and services. Even in smaller companies, there is usually a resource or two that has responsibility for gathering, digesting, and presenting this information to the necessary parties. Often times, sales and marketing individuals help contribute to this effort of information gathering. Unless there is a dedicated resource/resources, this function is typically handled by the product manager or product marketing manager. A product manager usually has market wide industry knowledge of competitors simply through years of experience working within a particular field. In life there is no substitute for experience/year's served, and a product manager's knowledge base is no exception. Aside from this general experience factor, there are numerous ways of gathering information on one's competition. A simple and

effective practice of information gathering is plain old research. One has to roll up his or her sleeves and get a little dirty. Perhaps the most common tool is the Internet and World Wide Web. Often times a company's Web site will offer a wealth of knowledge for any cyber visitor. Remember, customers use the Internet to find out about products and companies as well, so it behooves organizations to create informational Web sites that will attract customers. One would be surprised at the level of detail and information displayed to the public domain. Aside from a corporate Web site there are several other sources for information. Research databases (such as Consumer Reports, Gartner, IDC, etc.), financial databases (such as Hoovers or Zach's Investments), search engines and portals (such as Google and Northern Lights), news sites (CNN and The New York Times), communities and news groups chat rooms (such as Adelphi and Yahoo communities), etc. are all feasible suppliers of important data if mined correctly. In fact, research groups mentioned above such as Gartner and IDC have paid subscription services where they can help conduct market research. If the company sought after is publicly traded then there is a wealth load of information available especially if it is on Wall Street or the NASDAQ. Public corporation must submit their earnings and other information filing to the Security Exchange Commission (SEC). One easy way to access this data is through Edgar on line, this web site gives access to SEC filings on all publicly traded corporations. Other investigative methods of conducting research are the old fashioned visits to the public and university libraries, the library of congress, public hearings and courthouse records in city or town municipalities, even newspaper records can be a lucrative avenue of information.

One valuable medium for gathering information on competitive products and companies is attending conferences. There are numerous conferences to attend that would house information specific to a competitor or market. For companies large enough, there are end user conferences such as Networkers for Cisco customers and SecureXchange for Symantec users. There are also industry wide conferences such as RSA and CSI for security focused organizations. Even larger conference forums such as PC Expo and Web Expo are held in the Jacob Javitz Center in New York City, for the technology industry in general. Another great industry source are financial consortiums held by many of the investment houses on Wall Street. Visitors to conferences can roam the exhibit hall collecting information from various facets. Company pamphlets and product/service information is often distributed as such shows. Attendees can approach an organization's representative asking them penetrating questions. Although unreliable and unsubstantiated, interviews with fellow showroom visitors often lead to incredibly insightful discoveries.

Aside from trade show attendance and other company/industry specific events, direct contact through phone and email is another information gathering practice that is employed. Although unethical, one can easily disguise oneself as a potential customer or student to inquiry information on product specifications, pricing, etc. Information brochures can often times be mailed/emailed to a recipient. Although somewhat subjective, other exercises of data harvesting are conducting interviews with customers, sales associates, and even a competitor's former employees. This source of information can be incredibly valuable as these people are "on the front line" and have first hand knowledge of the information presented on products, services, pricing, etc. One must be

careful of the natural bias incorporated in this type of information gathering. An employee and customer will naturally tend to have a positive bias for their company and a negative one for the competition.

Unconventional methods employed for collecting information range from the very cheap and dirty to the very expensive and fringing on the border of unlawfulness. Private investigators or employ tactics such as dumpster diving and shoulder surfing. Dumpster diving is a practice commonly used by private investigators, although a bit extreme for common competitive analysis, if the stake is high enough, and millions of dollars at hand, it will be conducted. This is the practice of rummaging through a corporation's trash in hopes of finding desired information. According to many sources, it is a surprisingly effective method of obtaining information. For example, a few years ago Larry Ellison, famed CEO of Oracle, was publicly embarrassed when it was discovered that he hired private investigators to gather information from Microsoft's garbage. Shoulder surfing and piggybacking are common social engineering attacks. In these examples, an outsider will gain physical access into a corporation past the guards by attempting to blend in with the crowd. This can be done by striking up a conversation while approaching the checkpoint station or by falsifying/making pretend to have corporate identification badges to gain access.

There are deeper penetrations of information gathering that employ more social engineering techniques as well. An example could be a hacker calling help desk personnel disguised as a user having trouble logging into his or her account. A more intrusive example would be for a hacker to actually become hired, either as a salaried employee or even as a member of the janitorial or security staff. These are all great areas

to work in for the potential intruder because these administrative duties have access to many of the offices and hallways throughout an organizations building and grounds. Once inside, the hired hand is then potentially free to gather as much information as possible. Often times these tactics are planned well in advance and are executed over the span of several months, even years. Finally, one can simply break and enter into a competitor's office in hopes of gathering information. Obviously this method transgresses the law, a decision made by both the participating individuals and corporations that hire them. Even in the political arena, one can see were this method of information gathering is not too far fetched, it has been less than 30 years since the infamous Nixon Watergate scandal. Similar to other political environments, the business world employs the use of bribes and kickbacks is another nefarious forms of data collection. From the crooked judicial system scandals of Chicago and Al Capone in the 1930's to modern day politicians and business leaders, gaining access to information, or purchasing of information is not an uncommon practice.

Trends have shown that many times, an insider is responsible for the dissemination of business data as described by the annual CSI report.³¹ (Note: Although survey information has the potential for bias, it does highlight some interesting security hazards.) Often time's organizations are focused on preventing external illegitimate ingressions into one's defenses. However, companies need to realize that once

³¹ Richard Power, "Computer Security Issues & Trends, Vol. VIII", Computers Security Institute, p 7.

successfully penetrated, hackers will use legitimate user rights to gain access to information.³²

One of the most highly publicized methods of capturing corporate trade secrets and business information is through a hacker via the Internet. This strikes fear in every Executive's heart, mostly because these cases can occur from remote locations and often times without being detected, or even worse the media can get hold of the incident creating a public relations nightmare. Hackers can attempt to access remote servers where corporate information is stored. Many hacking techniques, such as Brute Force attempts, buffer overflows and installation of back doors, installation of sniffers, permit a hacker to infringe into corporate networks and servers.

There are numerous other information-gathering techniques. A TEMPEST attacks gathers information from any electronic device that emanates electromagnetic radiation (EMR) such as computers, computer monitors, networks, radios, cables, etc. These EMR pulses can be reconstructed to view the original information.³³ A spy can potentially gather corporate information from a competitor via a TEMPEST attack directed at an organization's facility. In a similar manner, intelligence can also be gathered on physical wire-tapping techniques.

³² Sushil Jajodia, Paul Ammann, and Catherine D. McCollum, "Surviving Information Warfare Attacks," *Computer.Org, an IEEE Publication* (April 1999 Vol. 32, No. 4): 57-63.

³³ Cassi Goodman, "An Introduction to TEMPEST," SANS Institute, (April 18th, 2001) <http://rr.sans.org/encryption/TEMPEST.php>, Internet, accessed on 12/15/02.

Although businesses are exponentially more efficient with the advent and adoption of innovations in technology, they are also at more risk. Inevitably, organizations are exposed to more threats at an equal rate of growth to their efficiencies. As the technology continues to evolve at a torrid pace, in line with Moore's Law, information is becoming more easily accessible by more people. These innovations bring both law abiding and more dubious *Netizens* to the information technology arena. Compounded with the ease of hacking tools available, on the Internet provides a forum to launch blended threats from distributed nodes. Corporations need to share their business data across multiple platforms to a distributed work force, which is globally proliferated, as well as numerous business partners and vendors. Finally, there is simply more individual corporate information available. Companies have digitized much of their data to meet the demands and pressures for sharing of information as well as ease of administration. Compounding all of the environmental factors leads to an ominous outlook for companies trying to keep their data behind closed doors.

Fundamental to this is the diametrically opposed interests of sharing and protecting information is the insurance of information. Business data must be accessible to the appropriate parties, but the information must be accessible in a way that guarantees confidentiality and integrity. There are an abundance of technologies, products, solutions, processes and services that can help protect this information. To complete the cycle of information protection, organization must employ methods of detection and correction with equal vigor as these three core concepts revolve and evolve from each other.

No matter what type of industry a company is competing in, clearly information is the driving force behind company successes and failures. Obtaining and protecting sensitive information on competitors is critical in today's business environment. Access to this information becomes an increasingly valuable asset to protect and share. What is the balance of sharing information between customers and investors versus keeping it out of the hands of competitors? There is no universal silver bullet. As with implementing enterprise specific security solutions, so to is the decision of sharing information and data.