Global Information Assurance Certification Paper

Employee Hardening with Social Re-Engineering

By Jon McGee

Global Information Assurance Certification
GIAC Security Essentials Certification (GSEC)
Administrivia Version 2.2
Practical Paper Requirements - Version 1.4
Option 1 - Research on Topics in Information Security
August 18, 2002

Table of Contents

Introduction

What was once an unknown and underutilized subject in many organizations, Social Engineering is rapidly becoming more commonplace due to recent world events and dwindling economic conditions. Frequently associated with Information Technology; Social Engineering is negatively defined and explained by Dictionary.com is a term used among crackers for cracking techniques that rely on manipulation and weaknesses of Wetware (referring to the central nervous system of human beings) for information exploitation. **(1)** From a positive perspective, Merriam-Webster describes Social Engineering as Risk Management of human beings in accordance with their place and function in society. **(2)** Based on the above descriptions, Social Engineering can take many different forms both good and bad and is not necessarily centered on the Information Technology environment. For example, when a prospective employee applies for employment with a company, it is the hope of the organization to hire a compatible and dedicated team player equivalent to a member of an organizational family. Unfortunately for most hiring firms, recruitment is not an easy and inexpensive task. There is the initial financial risk associated with the hiring process, but there is also a security risk which can carry a far greater price to the point of business failure in the event of compromise and/or exploitation. Employees are an organization's greatest asset yet they also serve as the greatest weakness or liability. This paper examines the value of information handling and employee hardening along with the ethics and motivations of people in the organizational infrastructure. In addition, employee vulnerability to Social Engineering is examined as well as the resulting need for organizations to maintain employee hardening in the form of Social Re-engineering to preserve the security and integrity of their operations. How do economic conditions challenge companies already contributing a great deal of time, effort and money towards the process of hiring, training and retaining great employees? What environmental factors contribute to loyal, ethical behavior or dishonest, immoral behavior in employees? Maintaining successful, security conscious employees is a full-time, long-term challenge requiring consistent Social Re-engineering and worthy of further review.

Reengineering as defined by dictionary.com is the examination and modification of a system or entity to reconstitute it in a new form and the subsequent maintenance and implementation of the new form. **(3)** In bluntly comparing Social Engineering to Social Re-engineering for the purpose of this paper; consider Social Engineering as being defined as a perceived or actual influence from either an inside or outside source to change existing behavior. (Example: an individual or organization you do not work for offering a bribe to encourage information sharing or your supervisor offering a day off to the salesperson who produces the highest volume of sales.) Social Re-engineering on the other hand is maintenance of perceived or actual influence from an established condition or source. (Example: Preservation efforts from an individual or organization you currently work for such as Employers reminding employees to lock doors to reduce the chance of burglary.)

Organizational Infrastructure

Returning to the previous recruitment example, employers target their candidates carefully in an effort to contain costs. After candidate interviewing and hiring, the reengineering process already begins for the first time during the orientation process. Because orientation in itself can be a challenge for employers, it is not unusual for hiring preferences to be given to young, recent college graduates or relatives of existing employees. **(4)** These individuals are known as "energetic clean slates" which helps in most cases to ease the reengineering process. History has shown that new-hires in this category more easily learn company policies and procedures as well as adapt to what is commonly referred to as a company's culture. Employees previously working for other organizations have already been exposed to different procedures and cultural guidelines. As a result, extra effort may be required to help these "seasoned" employees unlearn what they have learned as this previous education could counter the current objectives of the organization. **(5)** Additional training costs for the position may be minimal or substantial based on the previous experience of a new hire.

The interviewing and orientation processes are not guarantees for a successful employee. In many cases background checks, disclosure contracts, and probationary periods of 6, 9 and even 12 months are utilized to further evaluate and monitor new hires based on their job performance. Job Performance is diverse and open to various organizational interpretations. It can however be defined as how well the new-hire fits into the company culture, how well they follow policies and procedures, and how strong and loyal their work ethic is towards the company's bottom line or success. Probationary reviews serve as an excellent way to eliminate new-hires with questionable performance or backgrounds without excessive company liability or exposure. **(6)**

Information Handling

Exposure or risk can take many forms. In addition to the management of financial risks briefly discussed earlier there is a higher risk level associated with securing information. Information is defined by dictionary.com as a collection of facts or data. It is knowledge created by people as a result of study, experience, or instruction to be utilized by people. **(7)** Be it related to new technology, financial results, marketing strategies, a new product or formula, etc.; how confidential information is secured and handled primarily through people determines its desirable or undesirable effects. People are the critical "Human" element as they decide how information is created, isolated, stored, used, protected, and exposed or shared with other individuals. At the same time however, people or employees can serve as a vulnerability or even present themselves as a threat to an organization through informational carelessness or malicious behavior based on their overall objectives.

Each aspect of people handling information can be classified into three groups or motives:

1) Individuals contributing to the advantage of their own organization: These individuals are generally perceived positively. Guided by strong morals and high ethical standards; they range from "White Hat" Security personal to employees motivated to correctly understand and handle information appropriately. The overall objective of these individuals is to preserve the well-being of their associates or their primary employer.

2) Individuals contributing to the advantage of a competitor: Often viewed negatively with questionable intentions; these outsiders (and in many cases insiders) manipulate others and/or infiltrate computer systems. Their objective is to access other entities (be it individuals or organizations) with the intent to defraud or gain a competitive advantage for themselves, another individual or organization.

3) Individuals vulnerable to impersonation or manipulation resulting from Social Engineering: A commonality exists between group 3 with groups 1 and 2 respectively. This similarity centers on the overall objective of people to benefit their own self-interests. This pursuit of personal well-being is based on being faced with a decision or problem that has some exposure to influence and exploitation. Individuals are then forced into making a choice between taking a perceived ethical or immoral approach to achieve an end result.

From a Chief Executive Officer who built a multi-billion dollar company from scratch to a new-hire, Contract Employee performing housekeeping duties; everyone to exposed to handling information, Social Engineering and Social Re-Engineering whether intentionally or inadvertently. For unsuccessful new-hires failing probation, initial obvious threats to the organization (be them minor or major) are immediately reduced. Under a best-case scenario for new-hires passing probation, the initial reengineering process is completed. The successful employee has adapted to and is making a positive contribution to the organization by performing their new job well. Most importantly to the organization and regardless of the job description, the employee is seen as having reached a new level of responsibility as potential high-risk threat variables have been minimized with the brief passage of time. What many organizations consider to be initial high-risk threats pertaining to Social Engineering can be explained using these Coca Cola verses Pepsi examples:

1) Individuals working for Coca Cola intentionally applying for positions with a competitor: in this case Pepsi with the intent to gain access in a short amount of time to proprietary or personal information such as Pepsi's secret product formula in turn giving Coca Cola a business advantage.

2) Established individuals working for Coca Cola with an objective of eventually working for Pepsi: Should the individual gain access to new technology developed by Coca Cola, hiring preferences may be granted to the individual by Pepsi in favor of obtaining information or experience with Coca Cola's new technology. **(8)**

Employee Hardening

Although the employee has gained some organizational trust and respect with the passing of probation, the challenge now facing the organization is not only to maintain the existing level of loyalty displayed by the employee, but to continue the development process in this area in order strengthen the employee's devotion to the organization for the long-term. This ongoing Social Re-engineering process involves hardening

employees against the vulnerabilities of carelessness and Social Engineering. The more responsibility an employee earns, the more vulnerable they are to the organization.

Salary

There are many approaches to employee hardening with the most common method being money or compensation. Highly paid employees tend to show more loyalty to an organization than those who view themselves as underpaid. Depending on market conditions, successful growth industries can empower participating organizations to generate above-average levels of revenue. **(9)** In turn these companies can share their wealth by supporting higher salaries and other benefits such as stock participation to retain their employees. This can lead to a false sense of security for employers as although it may be true that higher paid employees in a specific industry tend to stay loyal to that industry, it does not mean they will stay loyal to the firm within the industry. In the late 1990s, more jobs were available than people to fill them. Also cases of perceived growth potential with Initial Public Offering (IPO) companies in the Software Development field alone had such an effect that many employees were actually leaving secure, well-paying jobs. These transitions were occurring in favor of risky startups offering potentially higher paying jobs with higher status. Industry leader Microsoft Corporation, one of America's most admired Corporations was forced to raise their employee salaries when faced with the threat of losing key people along with the development and security knowledge they possessed to startup companies. Social Re-Engineering in the form of salary increases was needed to maintain or rekindle employee interest in the company. **(10)** What made this scenario unique was that startup organizations (with little or no money) would not necessarily provide a high salary with a job offer. Instead, additional perks or benefits from stock options to "potential" future earnings percentages were used to entice key personnel throughout the industry. During this period, people had career choices-more than what had been previously available. For the employee passing probation example used earlier, it was very easy to take this type of chance as risk was deemed very low. The Stock Market was considered a Bull (growth) market and it seemed that everyone was becoming millionaires overnight. And with more career choices, loyalty towards one's own organization can quickly become a low priority. This Social Engineering strategy of startups offering fringe benefits enabled these new entrants to the industry to develop their employee skill set in almost any field quickly. This enabled new market entrants to catch up to that of the industry veterans; in a sense, exploiting the information vulnerabilities of veteran companies who once considered themselves secure where retaining employees was concerned. This trend was short-lived however as the ending of the dot-com boom caused a downturn in the Stock Market, loss of revenue, and the end of potential growth opportunities for most start-up companies. Addressing the challenge of maintaining workforce personnel or even a business as a dot com startup became difficult and in many cases futile. At the same time, with a sharp reduction in job opportunities; massive layoffs have resulted in a surplus of employees either out of work or those settling for new positions with a sharp salary decrease. For large corporations like Microsoft who are still making a profit as well as carrying massive financial reserves, the tables have turned. Unlike startup companies, organizations of large magnitude have "staying power" with the ability to endure a drop in revenue

resulting from a slow economy. Microsoft employees who may have once questioned their loyalty and thought about working for a startup company may now have a rekindled appreciation for their existing employer. In this example of changing economic conditions, Social Engineering has played a role in influencing not only employees but employers into rethinking their motives. In a sense, perspectives have been redefined.

Training

Another critical element of employee hardening focuses on employee training. Unlike the orientation process discussed earlier, effective training can cover a wider range of subjects. This next step in the re-engineering process should initially serve as detailed, in-depth instruction explaining what is considered appropriate and inappropriate employee behavior within the organization. Today's cultural melting pot brings with it a level of diversity that has never before existed. Each person brings with them different views on behavior in the workplace. What one employee considers ethical conduct may be considered offensive by another. The same idea holds true with securing the organization. According to Sharon Gaudin's article on "how to Thwart Social Engineers," **(11)**; with established training courses designed to reengineer employee views on what type of information the organization values, employees can start to take this matter seriously in areas including:

> **1) Knowing what the Organization views as malicious behavior:** With thorough training, employees would no longer have the option of denying responsibility for their actions due to a lack of knowledge. One act of successfully denying responsibility due to a then unknown gap in policy resulted from an individual logging into a company computer system and randomly deleting network files. During a court appearance where the company that incurred the damage attempted to unsuccessfully collect restitution; the judgment ruled in favor of the malicious user because he stated that he was unaware that unauthorized acts on a computer were not allowed. As a result, many organizations today require a Security note posted at the time of login with wording similar to:
>
> SECURITY NOTIFICATION: "You are entering an Official United States Government System, which may be used only for authorized purposes. The Government may monitor and audit the usage of this system, and all persons are hereby notified that the use of this system constitutes consent to such monitoring and auditing. Unauthorized attempts to upload information and/or change information on this web site is strictly prohibited and are subject to criminal prosecution under the Computer Fraud and Abuse Act of 1986, the National Information Infrastructure Protection Act and Title 18 U.S.C. Sec. 1001 and 1030."
>
> **2) Learning what and how data must be secured verses shared with the public:** Unfortunately, common sense cannot be relied upon for securing information in the workplace. Organizations must explain to employees in detail what confidential, proprietary or personal information is. In addition, employers must encourage employees with any doubt to contact appropriate security personnel. Access to both hard copy and electronic data must also be controlled and allocated to only certain individuals on a "need to know" basis. Some examples include access to new product designs being accessible to only engineering personnel, access to employee salary information being restricted to Human Resource personnel, and data related to internal or external investigations being limited to security personnel. Common methods for controlling access to restricted information include Identification Badges, combination locks, keys, sealed packages passwords, escorts, with new technology development in voice, eye, and facial recognition.

3) Understanding some of the Social Engineering Tactics used for manipulation and exploitation: Organizations can give employees a thorough appreciation as to why information handling must be taken seriously by sharing real-life examples like the following by Sarah Granger of the Computer Crime Research Center:

"One morning a few years back, a group of strangers walked into a large shipping firm and walked out with access to the firm's entire corporate network. How did they do it? By obtaining small amounts of access, bit by bit, from a number of different employees in that firm. First, they did research about the company for two days before even attempting to set foot on the premises. For example, they learned key employees' names by calling HR. Next, they pretended to lose their key to the front door, and a man let them in. Then they "lost" their identity badges when entering the third floor secured area, smiled, and a friendly employee opened the door for them.

The strangers knew the CFO was out of town, so they were able to enter his office and obtain financial data off his unlocked computer. They dug through the corporate trash, finding all kinds of useful documents. They asked a janitor for a garbage pail in which to place their contents and carried all of this data out of the building in their hands. The strangers had studied the CFO's voice, so they were able to phone, pretending to be the CFO, in a rush, desperately in need of his network password. From there, they used regular technical hacking tools to gain super-user access into the system.

In this case, the strangers were network consultants performing a security audit for the CFO without any other employees' knowledge. They were never given any privileged information from the CFO but were able to obtain all the access they wanted through social engineering." **(12)**

4) Who to report potential security vulnerabilities to or ask questions without fear of repercussions: In order to aggressively enforce policy, organizations must have access to at least one expert in this field with a primary role of creating, updating, and defining the grey areas of the Security Policy. The integrity of the reporting individual(s) and the security policy can be tested if questionable acts involve high-ranking personnel within the organization. A Commerce Daily newspaper reporter Robert Conlin in his March 12, 2001 article "Oracle Lawsuit Alleges Software Bugs, Insider Trading" provides a high-profile example:

A San Diego, California law firm Milberg Weiss Bershad Hynes & Lerachfiled a class action lawsuit against Oracle Corporation late Friday, alleging that the software giant issued misleading statements about its third-quarter prospects and that its much-touted US$1 billion in cost savings was achieved through job cuts rather than through implementing its own 11i software.**(13)**

The suit alleges that Oracle chief executive officer Larry Ellison is aware that the company's 11i software is "fraught with massive technical problems, including giant gaps in its CRM modules, and required expensive systems integration work to implement." The firm also alleged that Ellison knew that his company would fall short of third-quarter expectations -- and cut his losses by dumping a large chunk of company stock before it nose-dived following an earnings statement revision earlier this month.

"Ellison dumped almost US$900 million worth of his own Oracle stock at artificially inflated prices of as much as $32 a share, in what appears to be the largest insider trading in the history of the financial market," the law firm alleged in its complaint. The firm said Ellison had not sold any shares for the previous five years prior to his sell-off in January according to a Daily News article by Martin Stone. **(14)**

Although this case is still pending, this example shows how easy it can be to disregard moral values in favor of taking advantage of an opportunity.

5) Understanding the penalties for violating the policies discussed: In 1994, a case involved a former employee for the Intel Corporation who copied without authorization computer files relating to the design and testing of the then unreleased Merced microprocessor (now known as the Itanium). At the time, the employee knew that it was a trade secret belonging to Intel Corporation. He copied that trade secret information with intent to convert it to his own economic benefit by using it at his then new employment. Punishment for this type of crime was recorded as 10 years and a fine of $250,000 when the law was written according to a press release from the U.S. Department of Justice.**(15)** Through plea-bargaining, the sentence was reduced to probation. However, as crimes of this nature have been on the rise; the legal system has aggressively worked to reduce the number of lenient sentences issued. **(16)** According to an article by Sharon Gaudin, a well-known hacker Keith Rhodes states that Industrial espionage or idea theft is the biggest corporate security threat today. As recent as Thursday July 11th 2002, an article by Mike McKee states that the California Supreme Court ruled unanimously that the theft of trade secrets worth more than $50,000 can trigger a state statute requiring a minimum county jail sentence as a condition of probation. **(17)**

Work Environment

A more personal aspect of employee hardening deals with the actual work conditions an employee is exposed to. Recent events involving internet access has created to potential for legal repercussions based on a memorandum by Jenifer & Block.**(18)** This atmosphere must be monitored and re-engineered as necessary by both the employee and management but articles by Mark Reutter and the FAA serve as reminders of using caution to avoid an invasion of privacy.**(19)(20)** From an employee perspective, it is important for the employee to recognize not only the significance of their job as it relates to information handling, but they need to enjoy the job they are performing. It is irrelevant if the employee is a Chief Executive Officer or one who mows the lawn, all workers have the potential for accessing information. And what they do with that information can make or break an organization. Also, failing to acknowledge or address the critical element of job happiness or enjoyment can hinder a worker's ability to perform the job. It can also encourage carelessness with other work related duties including not caring about the security and well-being of their organization. On the other hand, enjoying the job can lead to personal happiness and an overall better attitude while working, especially in the area of protecting the organization by taking and complying with security measures. An employee displaying a positive attitude about their job can also affect other employees in a positive manner as well. This trend can build upon itself to the point that overall employee moral can improve benefiting the organization as a whole according to the Positive Attitude Institute.**(21)** Management can be a deciding factor as to whether or not an employee experiences overall job satisfaction. As I mentioned earlier in the overview of this paper: "Employees are an organization's greatest asset yet they also serve as the greatest weakness or liability." Wise Managers realize that losing knowledge to competitors and retraining employees can be very expensive and as a result; try to develop enjoyable work environments. A supporting article by Michael Kanellos shows how this can happen to highly admired companies. Some aspects with developing enjoyable work environments can include opportunities to:

1) Develop the position in the form of Managerial or Technical training.
2) Work with the latest tools or equipment improving efficiency.
3) Receive recognition from a rewards program.

4) Be promoted for a job well-done.
5) Receive pay raises and/or bonuses.
6) Be offered additional vacation or sabbatical time off from work.
7) Get help in developing an effective work/life balance.

These are just a few of the examples that can be used by Management to make positive contributions to employee job wellness which in turn provides an employee sense of accomplishment. However, huge organizational challenges face Managers on a daily basis. Today's diverse cultural and religious workforce brings with it a level vast level of diversity. Different people brings with them different skills and methods of performing their jobs. Not understanding the unique differences people bring can be a huge challenge for organizations and their employees. Mistakes are common for example with the belief that if someone succeeds in one type of job, they will succeed in another job that is completely unrelated. It is not uncommon to have a top sales representative become a marketing manager or an extremely efficient assistant be promoted to run a new department. Unfortunately being good at one thing does not always equate to being good at another and organizations spent millions each year unsuccessfully promoting employees into positions they are doomed to fail at. Other misconceptions include:

1) Creative people put in a position that only requires manual dexterity
2) A people oriented person placed in an isolated back room
3) Someone who requires order being put in a position that requires flexibility
4) Management positions given to those lacking people skills
5) A detailed oriented job being given to someone who avoids details

Managers understanding employee behavior in addition to perceptions can lower employee frustration, predict their actions, and improve loyalty. Whether factual or perceived, negative ideas or feelings are dangerous as they can influence all types of employee behavior from new-hires to seasoned veterans. For example with salaries and promotions, if one employee mistakenly has access to viewing salary information; they can feel a sense of department or company betrayal especially if they feel they are more educated, productive and/or work harder than the higher-paid, promoted employee. Also, rumors can impact an organization in the form of perception. If one employee leaves a successful project unsecured, another employee can essential steal as well as receive credit for the project from management. Employee reaction to feelings such as these can vary. Some simply leave the organization in favor of working elsewhere for they deem to be an acceptable level of compensation. Remember that during a growth economy, this was not hard to do. On the opposite extreme, other employees may become angry and choose to take out their aggression on the offending employee or the organization itself. With an economic slow-down forcing salary cuts, layoffs, and resulting low moral; organizations are vulnerable to malicious acts performed by their own employees. In fact, 70% of the risk exposure and losses to many organizations is a result of exploitation by existing employees, not outsiders. Extreme cases involving hostile events are becoming regular stories with the media. In 1997, the Intel Corporation fired an employee who managed an automated

manufacturing system called Workstream. Upon termination, the employee's computer was confiscated however, the employee was able to log into the system from his home computer. The next day, at 2:15 a.m., the employee deleted a number of files, which shut down Workstream. This slowed, but didn't quite stop, the manufacturing process but cost Intel $20,000 to restore service**.(23)** This along with many other malicious events could have prevented if established termination procedures had been followed. Although termination details of this previous example are not available, assuming the employee termination was justified, the employee's negative reaction could have been associated with his level of values. It takes a very strong individual to admit defeat or failure. It is even more challenging for an employee making a business mistake to persevere and make corrections. Mistakes are a tradeoff for taking chances by pushing the envelope of innovation and many organizations not only recognize but reward this type of behavior. At the same time, exposing employees to business mistakes and teaching them how to recover helps to make these circumstances less personal. The employee's focus could then shift from the cost of the mistake to what can be learned from the mistake.

Ethics

Merriam-Webster defines Ethics as the study of the general nature of morals and specific moral choices made by exhibiting goodness or correctness of character and behavior.**(24)** Although this definition does little to truly explain the concept of ethical behavior, the following example (author unknown) serves to show that ethics can be interpreted differently based on one's own perspective.

> **Ethics and Soda**
> "Clearly, I'm being set up. There's no other explanation for it. Heading into our vending machine room, I see that there is a Coke sitting there, in the machine's dispensing bay, completely unattended. There is no one in the room. It seems to have been empty for at least a few minutes. So, conundrum. An ethical one, at that. And being (generally) an ethical person, one that gets right to the heart of who I am. The question is this: Do I take the Coke or not?
>
> However, that's the boiled down version. The real question is much thornier. Cokes from the vending machine cost $1 each. By taking the Coke, I would thus save myself one dollar. But do I want a Coke? If I don't want it, then I am not saving myself the buck, but instead burdening myself with merchandise I have no desire for.
>
> And even if I want it, I must take into the account that the Coke is not actually free. Someone paid for it, someone who was not me. If this someone was one of my co-workers, I lose my moral footing, as I have just stolen from those who support me in my daily work. If, on the other hand, this Coke fell from the machine after dispensing another Coke that was paid for by my co-worker, this Coke would still have been paid for by the vending company.
>
> However, as I have lost $30 in the last two years to machines supplied by this same company, taking the Coke would put me morally into the black, as I am recouping losses from a morally corrupt company that does not fix their broken machines. (Our "wheel of death" food machine has doors that don't open, yet those rows have food in them and there are no warnings on the machine.)
>
> One must also consider karma. If the Coke is an agent of karma, is it rewarding me for a past good deed? Or is it setting me up to take the fall? Will leaving the Coke allow for another, truly

thirsty person, to have some refreshment that they can't afford otherwise? Or will it continue to be left behind until it spoils? (Okay, yeah, that last isn't terribly likely.)

Taking all this into account, the question becomes: Do I take the coke that may save me a dollar (if I want it) and repay me for lost coinage, and reward me karmically, yet may steal a dollar from an innocent co-worker and set me up for a karmic onslaught, or do I leave the Coke, allowing either the original owner to retrieve it, or some poor soul more needy than myself to have it, and thus avoid karmic retribution, but perhaps rejecting a karmic prize, and thus angering the gods who reward for good deeds?
And just how do you answer that? (For the record, I took the coke.)" **(25)**

The individual in the above example obviously put a great deal of thought and considerable rationalization to justify taking the Coke. With several opinions about this example collected from co-workers, the initial perception of this person was positive as he did take the time to consider the possible benefits and repercussions of his actions instead of initially following an old saying: "Finders-keepers, losers-weepers;" but he did still take the soda. This fact serves as a reminder mentioned earlier in this paper that the overall objective of people is to benefit their own self-interests or personal well-being especially when it comes to making ethical decisions.

This subject of ethical behavior centers on responding to an issue or condition by making what is deemed as the right choice. But what one individual considers a just or right decision may be considered inappropriate by another person. In addition, difference perspectives can influence how an issue is addressed like the following example:

"Chain Letter" Dilemma
Background:
The attorneys general for the state of Deseret and its neighbors are out to fight chain letters and pyramid schemes. They have suggested legislation outlawing them, and have provided for stiff penalties. It seems obvious that a person who sent chain letters to five friends is less of a criminal than someone who sent out thousands of such letters. The penalties are therefore much higher if the number of letters or communications is higher, and penalties are especially severe for "Mass Operators" who mail out more than a thousand letters.

The views of Joseph Blow
Joe is a chain letter recipient who remailed his letter.
"I got this chain letter from a friend. It said that it was legal since it was not being sent by the U.S. postal service and was not "really" a chain letter. All I did was post ONE copy to a bulletin board. I didn't know that it was illegal. When you sign up for the bulletin board, they don't tell you that chain letters are illegal. Besides, I'm not even located IN the state of Deseret. How am I supposed to know that my posting from East Dakota would violate the law in some other state?"

The views of the State of Deseret Attorney General:
When Mr. Blow signed up for the bulletin board, they didn't tell him Fraud, extortion, and murder were illegal either. It isn't their job to tell him such facts. Mr. Blow distributed a chain letter to 29,000 machines, total readers unknown. He knew that the mailing list had readers in other states (and even other countries) because he had seen postings (messages) from them. Pyramid schemes are a threat to society at large, and massive schemes clearly cause much more damage. The fact that he used a computer to mail thousands of copies does not change the fact that he admits to having mailed them. We recommend that he be extradited and tried on the offense, and - if found guilty - be given 10 years in prison.

Computer Administrator View:
Letters like this are a waste of everyone's time. They cause a flood of letters that interferes with normal usage of the system. We just delete them every time we see them. Why not? They are illegal anyway, and besides, they are being sent over MY system, using MY disks, and over network connections that I pay for. I have every right to keep this sort of stuff off of my system.

No, we don't keep a record of each nuisance of this sort. It would involve too much paperwork.
Civil Libertarian View:
Even though each individual node (mainframe computer) in the network is privately owned, USENET news is treated by everyone as a public forum. If an administrator censors a message on his/her machine he/she has also censored it on the machines that depend on his/her machine for news. A system administrator has no right to censor anybody's mail on sites other than his/her own, and clearly has no right to practice censorship of a public forum without giving people some way to protest the action. This censorship is being done anonymously, without records, without recourse, based on the personal standards of the site administrator. In this case it was an arguably illegal message, but the site administrator could just as easily be deleting messages that did not agree with his/her political or religious views, and nobody would be the wiser.**(26)**

Is it an ethical decision to punish Joseph Blow for allegedly making a mistake? If so; How? There seems to be a different response each time the question is asked increasing the challenge of resolving such an issue.

Management must set a Good Example!

The point of this previous example is to show that in some cases what initially appears as a small, trivial issue can quickly turn into a complex choice. This can create a challenge with high-stakes; issues for employees who are expected to conform to organizational and ethical guidelines and yet still push the envelope of effort and innovation. If workers violate organizational guidelines, they face potential disciplinary, terminatory, and even legal action. Recent headlines involving high-profile Chief Executive Officers of Enron and MCI-WorldCom show that several one-time perceived reliable companies are using questionable tactics for their own self interests. The end results have left top managers with large severance packages while the vast majority of workers have had to absorb major financial losses. These, in addition to several other cases now coming to light lead many employees to question their loyalties to their organizations.

These examples are some of the aspects of Social Engineering brought on by society itself. Perceptions and expectations of customers, employees and investors have grown steadily over the past 8 years. Unfortunately, everything from employee workload to company earnings and economic growth reaches a saturation point and there is no where to go but down. In hindsight, had some of these organizations admitted to their losses slowly and gradually, have started to take the necessary steps to address their issues from layoffs to personal salary cuts themselves, the business community might have been Socially Re-engineered into thinking that gradual losses are ok as long as Management is taking the steps to address and correct the circumstances. This however is hindsight, but the examples show that no one is immune to Social Engineering.

Despite the negative perceptions of some Chief Executive Officers, one particularly positive example shows some of the potential benefits of making good ethical decisions that many consider to be above and beyond the call of duty. Take the case of Aaron Feuerstein, CEO of Malden Mills in Massachusetts. In 1995, a fire virtually destroyed his textile factories bring his entire business to a halt. With a tragedy such as this, CEOs have several to choose from where determining the future of his business and his now jobless workers are concerned. The first would be to simply close the business and leave after all Feuerstein was worth several million dollars and at his then age of 69, money would certainly not be an issue for him. His employees however would be unemployed and be forced to look for work elsewhere. The next two options would be in support of rebuilding his factory with two sub-possibilities pertaining to his jobless workers. Feuerstein could lay off his employees, they would receive unemployment and be forced to look for work; or in displaying unusual loyalty to his 2,400 workers he continued paying them for 90 days at a cost of nearly $1.5 million per week while the factories were being rebuilt. He also gave generously to support charities that helped the families of nine critically injured workers who have since recovered which brought his company and himself personally into bankruptcy.

According to an article titled "Ethics is the Bottom Line" by Eileen Brill, "after receiving the Lincoln Award for Ethics and Excellence in Business; Feuerstein affirmed the Lincoln Center's motto that "good ethics is good business." He credited his employees for their hard work during and after the fire, stating, "my people are my best asset." Feuerstein described how after he made the decision to rebuild, his workers thanked him profusely and promised "we will pay you back tenfold." At the same plant which never manufactured more than 130,000 yards a week of Polartec fabric, a mere one month and 10 days after the fire the workers began producing 200,000 yards a week." **(28)**

With employee loyalty of this magnitude, it is not difficult to fathom what this did for the long-term Security and integrity of Feuerstein's operations. Now and in the future, Feuerstein can expect his people to pay extra-close attention to any internal and external factors that may jeopardize the business; perhaps even offering ideas on how to improve security in the facility. Although Feuerstein's generosity does not guarantee a secure Mill, it does reduce the chances of compromise as Feuerstein's employees offer to return their loyalty and generosity by going the extra mile. This story has made recent news as Malden Mills has just recently pulled out of bankruptcy. Perhaps wise CEOs from other organizations can learn from this example.

Conclusion

Re-engineering was defined earlier as the examination and modification of a system or entity to reconstitute it in a new form and the subsequent maintenance and implementation of the new form. For the purpose of this paper, this definition is associated with organizations maintaining the loyalty of their workforce via Social Re-engineering. This re-engineering method helps to sustain a hardened work

environment where Security is concerned which contributes to the integrity and even the survivability of the organization.

The emphasis of this paper was to take a different approach to addressing and understanding the value of Social Engineering. Be it negative or positive to an individual or organization, the aspects of Social Engineering must be monitored, controlled and maintained by an organization in the form of Social Re-Engineering. As opposed to evaluating how passwords can be cracked and permissions changed on a computer network, the importance of people (the "Human Element") in an organization is brought to light. That workers or Managers can portray themselves as honest, friendly individuals willing to go the extra mile for an individual or organization in a job interview, until their needs are met and all other aspects can become expendable. Acknowledging the loyalty of employees in an organization could be considered the most powerful security tool available. Stronger than ID Badges, stronger than money, an employee's love or desire for an organization's success can override these aspects in terms of security. Strong employee loyalty resulting from honest, caring Management, training in work and personal ethics, and simply enjoying the job can increase one's own motivation towards cautious information handling and self employee hardening. Because these circumstances are not realistic for everyone, Social Re-Engineering can also serve as a reminder to help keep personal values in their proper perspective. By learning from any one of the negative and/or following any of the positive examples of this paper; individuals, organizations, and even industries can only benefit from the lessons learned.

Bibliography

1) Dictionary.com = Social Engineering

2) Merriam-Webster = Social Engineering

3) Dictionary.com = Reengineering

4) Tracey, William R. "Human Resources Management & Development Handbook." Irwin/McGraw-Hill Companies, 1999. Case #7, pages 145-159.

5) Tracey, William R. "Human Resources Management & Development Handbook." Irwin/McGraw-Hill Companies, 1999. Case #11, pages 196-214.

6) Tracey, William R. "Human Resources Management & Development Handbook." Irwin/McGraw-Hill Companies, 1999. Case #4, pages 59-71.

7) Dictionary.com = Information

8) Author Unknown. "Coke/Pepsi - Technology Analysis and Discussion." Tufts University, 19, March 1997
URL: www.tufts.edu/as/ issues/mar97/coke.html

9) Khirallah, Diane Rezendes, “Shrinking Paychecks In Silicon Valley” Informationweek.com, 15, March 2002.
URL: http://www.informationweek.com/story/IWK20020315S0033

10) Davis, Jim. "Microsoft Boosts Salaries to Keep Talent in a Hot Job Market." News.com, 6 March 2000.
URL: http://news.com.com/2100-1001-237605.html?legacy=cnet

11) Gaudin, Sharon. "How to Thwart the Social Engineers." Internet.com, 10, May 2002.
URL: http://itmanagement.earthweb.com/secu/article/0,,11953_1041161,00.html

12) Granger, Sarah. "Social Engineering Fundamental, Part 1: Hacker Tactics." Computer Crime Research Center; www.crime-research.org, 5, July 2001.
URL: http://www.crime-research.org/eng/library/Razum.htm

13) Conlin, Robert. "Oracle Lawsuit Alleges Software Bugs, Insider Trading." Commerce Times Daily; www.crmdaily.com. 12, March 2001.
URL: http://www.newsfactor.com/perl/story/8102.html

14) Stone, Martin. "Oracle Named in Class-Action Lawsuit." ComputerUser.com, 16, March 2001.
URL: http://www.computeruser.com/news/01/03/16/news6.html

15) United States Attorney Press Release, "Silicon Valley Man Pleads Guilty to Economic Espionage Act Violation Related to Intel Trade Secrets." U.S. Department of Justice, 14, September 2001.
URL: http://www.cybercrime.gov/owplea.htm

16) Gaudin, Sharon. "The Fed's Top Hacker Speaks."
Internet.com, 10, May 2002.
URL: http://itmanagement.earthweb.com/secu/article/0,,11953_1040041,00.html

17) McKee, Mike, "California High Court: Theft of Trade Secrets Triggers Jail Time."
Law.com 15, July 2002.
URL:http://store.law.com/search_resultscontent.asp?lsrchtype=site&lsrchmode=quick&lscope=1&lcnttyp=All&lqry=Theft+of+Trade+Secrets+Triggers+Jail+Time&x=16&y=9

18) Jennifer & Block, Civil Liability for an Alleged Hostile Work Environment Related to Patron or Employee Internet Use." American Library Association, 2002, Article Date: 13, November 1998.
URL: http://www.ala.org/alaorg/oif/work_jb.html

19) Reutter, Mark. "Implications of Monitoring Employee Behavior Need to be Reviewed." University of Illinois, www.news.uiuc,edu, 1 February, 2002.
URL: http://www.news.uiuc.edu/biztips/02/02privacy.html

20) Federal Aviation Administration. "Administrators Policy Statement of Model Work Environment." Federal Aviation Administration, September 1997.
URL: http://www.faa.gov/acr/mwe/

21) Fermano, Joe. "Your Attitude is Your Life."
Positive Attitude Institute, 4, March 2000.
URL: http://www.positiveinstitute.com/

22) Kanellos, Michael. "Former Intel Employee Admits to Computer Fraud."
News.com 29, June 2000.
URL: http://news.com.com/2100-1001-242634.html?legacy=cnet

23) Mark, Roy. "U.S. TO Triple Information Security Spending."
Internet.com, 13, March 2002.
URL: http://www.esecurityplanet.com/trends/article/0,,10751_991391,00.html

24) Merriam-Webster = Ethics

25) Author Unknown, "Ethics and Soda."
Ethics.org, 25, March 2002.
URL: http://www.onefreeradical.com/osmosis/2002/0525.html

26) Halleck, John Chain Letter Dilemma
University of Notre Dame 29, January 1998
URL: http://www.nd.edu/~rbarger/chain-cse.html
Additional References:
http://www.nd.edu/~rbarger/cases.html

27) Author Unknown. "If Only CEO Meant Chief Ethical Officer."
Businessweek 13, June 2002.
URL: http://uk.news.yahoo.com/020613/244/d131k.html

28) Brill, Eileen "Ethics is the Bottom Line."
Jewish News of Greater Phoenix. 5 August 2002.
URL: http://www.jewishaz.com/jewishnews/970131/ethics.html