On The Anatomy of Human Hacking

Abstract: Human hacking is a non technical kind of intrusion that relies heavily on human manipulation. Its impact is continuously giving serious concern in the Information technology arena which has often been undermined due to the ease with which this technique is widely used to infiltrate networks through unsuspecting individuals that are undeniably considered the *"weakest link"* in the security circle. Security awareness that brings about behavioral change, reduces employees' vulnerability, and protects against threats exploiting employees' vulnerability having a positive impact overall on risks related to information assets. Strategies for developing and implementing a successful information security awareness program are presented in this paper which also provides an introduction to the subject of human hacking while discussing the various counter-measures available to minimize the likelihood of such occurrences which have financial, reputation, psychological, and legal ramifications.

1. Introduction

National security has always being an important factor for most governments but, since the World Trade Center bombing the US Government, the European union and other governments re-prioritized national security.

The need for security is not only obvious in every organization, but also to the individual.

The Federal Trade Commission (FTC) reported in 2005 that "more than 1 million consumer fraud and identity theft complaints that have been filed with federal, state, and local law enforcement agencies and private organizations" [1]. According to a survey released on April 2, 2006 by the US Department of Justice [2] "An estimated 3.6 million or 3.1% of American households became victims of identity theft in 2004." It is safe to infer now, more than ever, individuals are at a high risk of having their personal identifiable information compromised and then used by criminals. Victims of these crimes could be left with bad credit ratings, debt, higher interest rates (due to bad credit ratings) and possibly criminal charges pressed against them until they are able to prove their innocence which takes time and money.

Whether it's securing a company's assets, abiding by the law, or guarding an individual's privacy, it has become evident to organizations and individuals that in order to protect confidential information, all necessary precautions must be taken. For organizations, these safety measures include a sound password policy, which places password requirements on access to electronic records or systems that house sensitive data. In addition, only authorized individuals should be allowed access to an environment where sensitive information or systems are located.

When transmitting sensitive data / information within or across networks, data should be encrypted to prevent unauthorized individuals having access to the information should there be interception of the data / information in transit. To further secure confidential / sensitive information, technologies such as IDS/IPS, firewalls etc can be used as part of the defense in depth strategy to make intrusion difficult, but not impossible.

Whether at home or work, sensitive electronic data can be and should be protected by using at least basic authentication mechanisms. However, even with all of these precautions and controls in place, organizations and individuals are still at risk for having their information stolen. Granger [3] points out that "by merely trying to prevent infiltration on a technical level and ignoring the physical-social level, we are leaving ourselves wide open to attack." As Hollows [4] further explains "Many security systems and technologies have been deployed to prevent intruders from accessing high value systems, however, an organization simply cannot patch against social engineering." Social engineering facilitates human hacking.

While confidentiality, integrity and availability represent those aspects of information assets that are being protected; people, process and technology describe how this protection occurs. People, processes and technology play an equally important role in information security. However, technologies, such as firewalls, often receive more than the required attention while people and

processes are given marginal attention if not completely overlooked. While firewalls and other technology components assist in providing required baseline protection, they can be rendered useless if a user either deliberately or accidentally misuses their access or fails to protect resources within their control. One danger that cannot be mitigated by technology is human hacking which unfortunately is consistently on the increase. Due to ease of implementing human hacking attacks, it is considered the single greatest threat to enterprise security.

This paper begins by defining human hacking. It will then describe some of the human hacking techniques and mitigating controls. This paper offers a strategy for developing and implementing an effective security awareness program that is dynamically reviewed and updated in order to better address the ever changing approaches used by human hackers. This should be considered as a guide to effectively addressing the issue of human hacking which can no longer be ignored.

Social engineering is a part of human hacking that can be broken down into human based and technology based techniques. Human Based: Refers to person-to-person interaction which could be over the phone or in person. Technology Based: Refers to using computing software that attempts to retrieve the desired information from an individual e.g. phishing attacks.

The hacking and cracking concepts are often misrepresented and used interchangeably by many within and outside the industry. For simplicity it can be stated that, “hackers build things, crackers break them” [25].

“A hacker is someone who thinks outside the box. It's someone who discards conventional wisdom, and does something else instead. It's someone who looks at the edge and wonders what's beyond. It's someone who sees a set of rules and wonders what happens if you don't follow them. A hacker is someone who experiments with the limitations of systems for intellectual curiosity” [26], while a cracker is someone who breaks into a computer system, often a corporate network with the intention of taking advantage of the system.

The holistic approach to security awareness presented in this paper is the by far best mitigating control for addressing attacks by human hackers. An awareness program should be a breathing / living document that should be reviewed on an on going basis. The phrase “human hacking” is used to draw attention to the severity of this non technical means of hacking. “Amateurs hack systems, Professionals hack people”, Schneier [10].

2 What is Social Engineering?

There are various definitions of human social engineering. However, one thing common to all the various definitions is that social engineers prey on the trusting nature of human beings. “Social Engineering is the human side of breaking into a corporate network”, Gaudin [5]. It is a way of obtaining unauthorized confidential information from a trusting individual through non technical means by building inappropriate trust relationships with information custodians. It is basically an art and science of manipulating individuals into providing sensitive information. Social engineers would normally use the telephone or the Internet as a vehicle for perpetrating their acts.

Social Engineers use different means to achieve their ultimate goal (impersonation, intimidation, phishing, shoulder surfing) , which is to gain unauthorized access to systems or confidential data in order to perpetrate fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network [6]. According to [23], there are four broad categories of human hacking attacks: technical, ego, sympathy and intimation attacks. Psychological techniques are applied in each case.

Human hackers exploit not just the trusting nature of human beings through social engineering but also their lack of security awareness through techniques such as identity theft and dumpster diving.

2.1 What is the Motivation?

Like every crime, there is an underlining motive for such anti-social behavior. Some of the motives include the following:

- **Financial Returns:** For very many reasons, an individual might be financially pressured to get involved with human hacking. For example, family pressure.
- **Revenge:** For personal reasons, an individual might decide to target a friend, colleague, an organization, ex-employer to satisfy their egocentric desires.
- **Self - interest:** An individual might have a vested interest in having access to a system or information in order to modify records for personal gain or to favor a friend, family or colleague.

2.2 Human Hacking Techniques

The techniques that the human hacker employs largely depend on the knowledge, experience and competence of the individual hacker. These techniques include:

- **Shoulder Surfing:** This entails looking over the shoulder of an unsuspecting user as s/he types in their username and password on the system.
- **Phishing:** "Phishing is the most common form of social engineering online and most notably includes email spoofs" [3]. Webopedia defines Phishing "as the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering confidential/ sensitive information that is normally used for identity theft." The email directs the user to a web site that looks very legitimate and they are asked to update personal information, such as social security number, bank account number, credit card number etc that the legitimate organization may be allowed to keep as customer's records. The web site is bogus. Phishing can be considered a form of impersonation except that instead of the intruder masquerading as an authorized individual, the social engineering attack comes via email or other online mechanism.
- **Dumpster Diving:** This technique looks quite crude; however, it is one of the most significant categories of human hacking attack. SearchSecurity.com revealed that "social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it." [7]. Most employees would probably not think twice before throwing away a company phone directory. In the hands of a hacker though, this information could be used for footprinting. Footprinting is the art of gathering information about a predetermined target prior to attack in order to determine viability of such an attack. Dumpsters are attractive to human hackers because are usually left in unprotected areas. Individuals are as vulnerable to dumpster diving as corporate users because most people throw away papers containing their confidential information without shredding the papers .Even if the dumpster diver is unable to use the information found in the trash immediately, it can be used for footprinting.
- **Impersonation:** Impersonation is arguably the greatest technique used by social engineers to deceive people, such as posing as an employee of the same organization. "Most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who "forgot" his / her badge." [8]. In particular, a social engineer finds that pretending to be an employee in the Information Technology (IT) department is typically a useful guise. A simple phone call requesting an employee's password is usually an easy way to get access to information. Once an employee learns that the call is originating from the IT department, he or she will usually disclose the password willingly and without question, especially after that employee has been told, what seems to be, a legitimate reason for the request. Just as humans have a natural tendency to be helpful and trust others, as mentioned earlier, they also have a tendency to protect themselves and fear of getting in trouble. That is why the use of impersonating authority also works very well for social

engineers. “People are highly likely, in the right situation, to be highly responsive to assertions of authority, even when the person who purports to be in the position of authority is not physically present.” [9] .For example, a Help Desk employee, low in the company’s hierarchy, would most likely be intimidated if a person calls in claiming to be the Vice President of Sales and is demanding that his/her password be reset so that s/he may log into the system immediately. In this case, the Help Desk employee might be fearful of the aftermath if s/he did not abide by the request, and may not authenticate the caller. The phone is not only frequently used in the workplace to conduct social engineering attacks it is also a means of obtaining confidential information from people at home. It is common for people to receive calls at home from credit card companies regarding their account. Therefore, people are often not apprehensive about divulging information about their account to someone over the phone who claims to be representing their credit card company. Almost always, the goal of the social engineering attack aimed at the individual at home is to acquire that person’s credit card number, social security number, and/or bank account number. In many cases, the social engineer is able to get this information by offering something of value to the cardholder or by using fear that his/her account is in jeopardy.

- **Hybrid Model:** This is a combination of any of the techniques mentioned above which could result in the executution of a more sophisticated attack e.g. dumpster diving to collect initial data followed by a targeted spearphishing attack.

2.3 Consequences of Successful Human Hacking Attacks

Like any successful security breach, there are consequences of successful human hacking attacks on management, employees, and the organization. The consequences can include the following:

- Loss of public confidence
- Decline in the market share and value of the company’s stock (if publicly traded)
- Negative media publicity
- Fines and other regulatory consequences
- Possible legal proceedings / settlements
- Increase in surveillance and interference from relevant regulatory authorities

3 How to Prevent Human Hacking

Human hacking attacks are among the easiest attacks to commit but are some of the hardest threats to guard against because of the human component. The natural human tendency to take people at their word continues to leave us vulnerable to social engineering attack. As Granger [6] eloquently puts it, “Security is all about trust. Trust in protection and authenticity. Generally agreed upon as the weakest link in the security chain, the natural human willingness to accept someone at his or her word leaves many of us vulnerable to attack.” The best control against this attack is education by training people to be aware of the value of the information assets at their disposal as well create awareness of human hacking techniques, which makes it easy for them to diagnose a social engineer.

Training and awareness to reduce the risk of successful human hacking attacks has become imperative in order for an organization or individual to defend against it. Therefore, a security awareness training program should be provided for all employees of an organization. This training should emphasize the various human hacking techniques as well as how to foil such attacks.

Once people are aware of human hacking attacks, they become conscious of their existence and are able to use best judgment as a defense mechanism. In a situation where an email is received from a company requesting that an individual update his or her account information, an individual that knows about phishing attacks is most unlikely to consent to providing such updates. The

person would either go to the company's web site via another browser window or call the company to verify if the email was legitimate.

Awareness would also allow people to be more careful of what goes into the trash. Once people are cognizant of the value of the information they possess, they will be more careful of how they handle it. Furthermore, when people are mindful that human hackers are willing to go through their trash for valuable information, then they will take necessary precautions when it comes to trash disposal. This should include using a shredder to dispose papers containing confidential / sensitive information.

For a very long time, even security professionals have been under the impression that technology is a "one stop" fix for security breaches of corporate networks. Security entails people, processes and technology.

Technology is a small component of the security picture. People are the biggest component of the "triad" and are unfortunately the most vulnerable being susceptible to human hacking attacks [24].

4 Building an Effective Information Security Awareness Program

Effective security awareness results in a situation where behavior becomes secure and intuitive, such that employees have an automatic reflex for handling information in a secure manner. Hence, for any security awareness program to be successful there must be a paradigm shift from *ad hoc secure behaviour* to a *continuous secure behavior* and, as much as possible, the threat originating from the internal network should be reduced to the very minimum. The business is expected to pre-define its maximum level of acceptable risks as a result of threat exposure.

Below are clearly outlined key steps for building an effective security awareness program:

- **Establish a Security Policy**: A sound security policy is the foundation of any successful security program. Before developing a security awareness program, it is critical to first document all of the high level goals, objectives and requirements of the security program in a security policy document. The policy should be written in a clear and concise manner, and should accurately reflect the organization's overall position on security. Once the policy is created, it is important that users are made aware of the policy's existence and contents. Users will also be made aware of the consequences of non-compliance with the documented policy.
- **Identify Current Training Needs**: The next step in developing a security awareness program is to identify the current training needs within the organization. This is an important step that is often overlooked or rushed. All too often, programs are built based on assumptions, rather than the needs of the users or business. By taking the time to measure the current level of security knowledge across the organization, it becomes easier to determine and prioritize specific needs for awareness training. Below are some factors that help in identifying training needs:
    - User learning styles and preferences for receiving information
    - Topics of specific interest or concern
    - The current level of receptiveness or resistance to security awareness
    - Previous education attempts that were successful or unsuccessful
    - Pre-existing vehicles of training that it may be possible to leverage (there is no need to re-invent the wheel).
    - Possible allies that can assist with gaining acceptance of the program.

By engaging in thorough background work it becomes easier to develop a security awareness program that makes the best use of available resources and has a high potential for success.

Below are additional avenues for identifying an organization's current training needs:

- Interview employees of different level, job function and tenure.
- Send out a survey or quiz to general users on fundamental security topics
- Research the current level of security exposure or violations within the organization e.g. number of laptops stolen the previous year, audit action items etc.
- Perform system, application and network level audits.
- Engage in face-to-face meetings with various units / departments.
- Walk around each regional office and assess the current level of physical security while paying attention to unlocked offices, desks and cabinets, as well as, unsecured workstations, information and media.

- **Obtain Senior Management Support:** Support of senior management is required for any successful awareness program. Unfortunately, an awareness program can be tough to sell. Not only is security viewed as an obstacle to business objectives, security awareness tends to be an undervalued and overlooked component of security while technical controls, such as firewalls and anti- virus scanners, get implemented. There are two main objectives that should be considered in securing the support of senior level management. The first objective is money. Implementing this type of program could be expensive. Depending on the size and type of the target audience(s), a decent size budget would be required to get started. A security awareness programme may take up to 20% of the organization's security budget the first year it is set up. Once a certain level of security awareness has been reached, the security awareness budget might be decreased to 10 – 15% of the security budget [14]. The second but no less important objective is to cultivate security advocates. It is critical to find supporters that do not just lend financial support, but who through their actions can lead others to value and participate in the program. Employees are much more likely to participate in training and awareness opportunities if their manager has reinforced its importance. In order to secure the support of senior level management, it is necessary to help them understand that security awareness is a vital element in protecting the organization information assets. Obtaining necessary support is made easier by providing the results of findings and applicable legislation that support the development of security awareness programs and industry statistics in support of an awareness program.
- **Determine Audiences:** The next major step in developing a security awareness program is to determine its audiences. Not every organization requires the same degree or type of information security awareness training. An awareness program that distinguishes between groups of people, and presents only information that is relevant to that particular audience will have the best results. In order to prevent the messages of the program from being ignored or watered-down it is critical to segment the audience and ensure people only receive the information they need. Some of the most common methods of user community education include:
  - Level of awareness
  - Level of technical skill
  - Job Level/Category
  - Specific job function
  - Technology, System or Application Used

The method that is used for segmenting the user community is not important as long as it works for the organization. One approach that has worked well in large organizations is to the hybrid

approach which is a combination of two or more of the methods above. These audiences can be broken down further as required by specific communication, but should be sufficient to identify key messages. These audiences are defined as follows:

- Senior Management: Top–Level Management
- Management: Middle-management and others in a leadership role
- Technical Custodians: Anyone who has extraordinary access, knowledge and skill pertaining to the corporate network, systems and/or procedures.
- End Users: Anyone who is authorized to use the organization's information systems. End users subsume the three categories above.

- **Define Key Messages:** Before defining individual key messages for each audience, it is important to first establish a single core message or mission statement. This core message may already be written as part of the security policy, but should be considered during this step. All other key messages should support and map back to this mission statement. Here is an example: It is the mission of the information security program to protect the confidentiality, integrity, and availability of the corporation's information assets.

The next step is to establish high–level key messages for each audience. In order to do so, the organization's security policy along with any of, or a combination of, the following International baseline documents related to security awareness should be reviewed, and the core messages that pertain to different audiences determined. The baseline standards include the COBIT *Control Objectives* [13]; *ISO 13335 Section 3, Guidelines for the Management of IT Security*, ISO/IEC 17799 *Code of Practice for Information Security Management* [15] *and* the Information Security Forum's *Standard of Good Practice-Standard for Information Security* [16].

These messages should not only be mapped to the organization's mission statement and security policy but should provide a foundation for additional messages. The following are suggested examples of high-level key messages based on audiences:

Senior Management

- Provide senior management level oversight and guidance on security processes
- Promote alignment of security initiatives with business priorities
- Ensure compliance with enterprise and business unit security policies and standards.

Management

- Develop internal processes and measures to ensure understanding of and compliance with the security policy and standards.
- Examine and address potential security risks in all new and existing processes.

Technical Custodian

- Implement the policies, standards and procedures that management sets.
- Ensure compliance with the security policy and standards by establishing appropriate procedures, access and requirements for end users.

End User

- Protect the confidentiality, integrity and availability of the organization's information assets
- Follow the specific end user responsibilities outlined in the organization's security policy and standards.

After determining high–level messages for each audience, it is time to determine specific messages and educational / training needs. In doing so, it is helpful to re-examine all the components of the security programs as well as recent security related events that may produce opportunities for education.

Some security topics that may be considered include the following:

- Passwords
- Physical Security – at the work facility, outside of the work facility
- Social Engineering
- Viruses, Hoaxes and Spam
- Email and Internet Usage
- Unauthorized Software
- Access Control – principle of least privilege, separation of duties, and back-up procedures
- Working from home
- Laptop Security
- Tele-commuting
- PDA Security
- Desktop Security
- Business Continuity and Disaster Recovery

This particular step should be an on-going process, but should be performed as an initial step in establishing the baseline awareness. The components listed above should always be under evaluation to determine any new educational needs. The security program should be flexible and capable of re-prioritizing the contents and messages as needed. It should create communications that are appropriate for each audience, written at a level that each audience understands.

- **Define Available Communication Vehicles:** The next step in developing security awareness programs is to define the available communication vehicles. In addition, it is important to become aware of any procedures, guidelines or requirements linked to any of these vehicles. Understanding the "rules" in advance will help to plan effort accordingly. Some common communication vehicles include:
  - Broadcast email
  - Targeted email
  - Broadcast Voicemail
  - Company newsletter
  - Human Resources
  - Internal Communications
  - Departmental newsletter
  - Intranet
  - CBT package covering security
  - Printed Materials – posters, bulletin boards and brochures
  - Face-to-Face meetings, presentations, training and security conference / Fair
  - Library-videos, books, interactive presentations
  - Reminders – Login banners, marketing paraphernalia (mugs, pens, mouse pads, key chains, sticky notes, T-shirts, Umbrellas, etc)

In choosing the appropriate communication vehicles, it is important to consider the audience and remember that different people learn in different ways. It is a good idea to use multiple vehicles for any given message so that it can reach the broadest group of individuals within any given audience. It is also a good idea to fully research all available vehicles and determine any limitations or scenarios in which they cannot be used or would not be effective.

Co-ownership of the security awareness program, or at very least partnerships with, the Human Resources and Internal Communications departments of the organization should be considered if the available contribution to the cost of the program from the security budget is not be sufficient to give the program satisfactory reach.

- **Develop a Strategy For Implementation**: The final step in developing a successful security awareness program is to develop a framework for consistent and effective delivery of company messages. Without this necessary step, communication may come across as disorganized and haphazard. In order to develop an appropriate strategy, the target audience, key messages, and available communication vehicle must be considered as well as determining ways to package the program into repeatable processes. As part of this step, a clear marketing strategy should be defined. The marketing component might include: a logo, slogan, common look-and-feel and templates. This would enable the Security Awareness team to deliver consistent and clear messages, but would also enable the audiences to develop an understanding of what to expect. In addition, the audiences will be able to provide more valuable feedback on the information that they receive. An information security awareness program consists of two major objectives: to increase awareness and facilitate understanding through training. The overall framework should be developed with this in mind.
- **Awareness Strategy:** Learning is a continuum; it starts with awareness, builds to training, and evolves into education (NIST SP 800-16). Security awareness differs from security training in purpose, approach, and results. Awareness has the following characteristics:

    - It is intended to focus attention on security and to change attitudes. Awareness sets the stage for training by changing individual perceptions and the organizational culture so that security is recognized as critical. Security failures can keep individuals from successfully completing their work and can threaten organizational survival. “Awareness activities are intended to allow individuals to recognize Information Technology (IT) security concerns and respond accordingly” (NIST 800-16).
    - Learning tends to be short-term, immediate, and specific.
    - Learners are information recipients.
    - It reaches broad audiences with attractive, attention-getting techniques

The ultimate goal of a security awareness program is to bring about behavioral change which makes users aware of the need to protect the organization’s information assets. The following is a list of repeatable (on a yearly basis) practices that should constitute part of an organization’s awareness strategy:

- New Hire Security Package
- Monthly Newsletter
- Security CBT – Which feeds back on “weaknesses”
- Quarterly lunch & learn presentations
- Posters
- Annual Security conference / fair
- Incentive programs – to recognize security related achievements

- Games, Puzzles and Contests

An effective Security awareness program:

- Should be repetitive
- Should have multiple communication methods repeating a message
- Should target messages to audiences (e.g. general Security Awareness to everyone, Information Security planning for managers, etc.)
- Should have executive support (e.g. with people and budget dollars)
- Should be behavior focused (not technology focused)
- Should generate metrics which are used for measuring success rate

- **Training Strategy:** The goal of training and education is to facilitate a more fundamental change in user behavior by instilling in users a deeper level of understanding of how they can protect the organization's information assets. The following should be a repeatable part of the training and education strategy:

  - Basic End User training course
  - Technical (external security focused) training courses for systems and network administrators
  - Advanced Information Security training – This training is for security practitioners and security auditors.
  - Quarterly Education Package - This vehicle should focus on one topic each quarter that has been identified as a specific area of weakness. It should have the ability to deliver specific messages for each audience concerning the chosen topic. It should strive to provide a more thorough level of information than regular awareness materials.

- **Ability to Measure**: Measurement is the final aspect of a security awareness program that needs to be addressed. It is critical that a baseline of current user understanding is established at the beginning of the program in order to be able to determine its successes and failures. Baselines should also be defined before implementation of any new strategies or content. Measuring education and awareness is not always straightforward so some degree of creativity is required. Ideally an external CBT package would be purchased with total employee participation mandated by the Board.

Effective security awareness should result in a positive behavioral and cultural change across the organization. Culture is defined as the predominating, shared attitudes, values, goals, behaviors, and practices that characterize the functioning of a group or organization. The following beliefs, behaviors, capabilities, and actions consistently indicate that an organization is addressing security as a governance and management concern, toward building and reinforcing a security-conscious culture:

- Security is enacted at an enterprise level. Executive-level leaders understand their accountability and responsibility with respect to the security of the organization, to their stakeholders; to the communities they serve including the Internet community, and for the protection of critical national infrastructures.
- Security is treated as a business requirement. It is considered a cost of doing business, not a discretionary or negotiable budget-line item. Business units and staff don't get to

decide unilaterally how much security they want. Adequate and sustained funding and allocation of security resources is required.

- Security is considered during normal strategic and operational planning cycles. Security has achievable, measurable objectives that directly align with enterprise objectives. Determining how much security is enough equates to how much risk exposure an organization can tolerate.
- All function and business unit leaders within the organization understand how security serves as a business enabler (versus an inhibitor). They view security as one of their responsibilities and understand that their performance with respect to security is measured as part of their overall performance.
- Security is integrated into enterprise functions and processes, including risk management, human resources (hiring and firing), audit/compliance, disaster recovery, business continuity, asset management, change control, applications development, and IT operations. Security is actively considered as part of new-project initiation, ongoing project management, and during all phases of any software development life cycle.

All personnel who have access to digital assets and enterprise networks understand their individual responsibilities with respect to protecting and preserving the organization's security. Rewards, recognition, and consequences with respect to security policy compliance are consistently applied and reinforced.

Characteristics of Security Training

- It is more formal than awareness. The purpose of training is to **build knowledge and skills** to facilitate job performance.
- Training takes longer and involves producing skills and competency for those involved in functional specialties other than IT security (e.g., management, systems design, and acquisition).
- It is provided selectively based on individual's roles (job functions) and needs.

5 Benefits of Information Security Awareness and Training Programs

The benefits of well implemented security awareness / training programs include protection from the consequences mentioned in section 2.3 above.

According to Privacy Rights Clearing House **[18]**, 74% of data losses are as a result of employee deceit or "human" error. In recent surveys of 126 companies conducted by Palisade Systems networks **[19],** it was found that over 54% of data losses or breaches suffered were due to employee (human) error. Some of recent breaches include:

- **Nuclear Regulatory Commission**: Social engineering techniques used to obtain license to purchase nuclear materials **[19]**
- **Pfizer**: Pfizer employees' personal data taken from laptop using file sharing software **[19].**
- **Xbox**: Xbox customer service got tricked into helping hackers hijack live services network account **[21]**.
- **Legacy Health Systems**: Personal data for 747 patients possibly stolen by former employee **[22].**

According to Ponemon Institute [20], the average cost of security breach clean-up is $4.8 million.

Given below are some of the benefits of a well implemented security awareness and training program:

Providing better protection for assets:

- Helping employees recognize and respond appropriately to real and potential security concerns.
- Providing fresh, updated information to keep staff current on new risks and what to do about them.
- Making employees, contractors, and business partners aware that the data on their computers and mobile devices (PDAs, thumb drives, smart phones, etc.) is valuable and vulnerable.

Improving employee morale:

- Providing information that is personally useful to staff such as how to avoid scams, fraud, phishing, and ID theft, how to protect home PCs and use email and the Internet safely, lets employees know that the organization cares about them. Building good computing habits at home is as important as building these habits at work. Secure computing habits will transfer across environments.
- Rewarding good security behavior and those who stand up for security. Recognition for doing something well.

Financial Savings:

- Reducing the number and extent of information security breaches. The sooner a breach is identified, the lower the cost of such a breach.
- Reducing systems' costs by allowing control measures to be designed into systems rather than adding them to installed systems. (It is significantly more expensive to retrofit a control than to design it into an application or system.)
- Providing savings through coordination and measurement of all security awareness, training, and educational activities while reducing duplication of effort.

Protection of organization's reputation and brand:

- Showing customers that the organization cares about protecting their information. The goodwill that Johnson and Johnson received when management made a decision to protect customers by pulling Tylenol off the shelves when some packages were found to contain poison provides a strong endorsement for this approach.
- Preventing the negative press that can result from security breaches.

Protection of customer information and corporate information:

- Building a culture of security competence. Motivate employees, contractors, and consultants to improve their behavior and incorporate security concerns into their decision making.

Reducing the potential for fines and mandatory audits:

- Improving overall compliance with the organization's information security policies, procedures, standards, and checklists.

Reducing the potential for lawsuits against the organization:

- Demonstrating a corporate concern for security and a process for ensuring that the workforce will provide adequate protection for information assets entrusted to its care.

Reducing the organization executives' exposure to prosecution:

- Ensuring that the executives understand that they are legally responsible for the integrity of the organization's information assets.
- Demonstrating management's commitment to secure information resources.
- Allowing the organization to comply with regulations that require information security awareness and privacy training (such as the Federal Information Security Management Act, the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act)

Facilitating disciplinary or legal action:

- Documenting the requirements and individual's acknowledgment of the organization's security policies. [17]

6. Conclusions

The state of Information Security is consistently growing more complex. New viruses, vulnerabilities and security breaches are reported every day. McAffe Security reports, for example, that on average 500 new viruses are discovered each month. With the acceleration of technology and compromises [12], it is becoming even more apparent that users lack the appropriate level of security awareness and training. Many users have little to no understanding of their responsibility to protect information assets. It is critical that businesses understand the value of a security awareness program and make a commitment to closing the awareness gap. A well designed and maintained security awareness program can have a great impact on strengthening the security awareness of employees.

In addition to training and awareness programs, security measures against human hacking should be documented in organizations' corporate policies, standards and procedures. Documentation will help support these programs not only by increasing awareness, but by providing a consistent manner in which employees should act. The employee will know that by acting in a predefined manner, s/he does not have to fear any possible repercussions emanating from refusing to be intimidated by a social engineer.

In this context it should be noted that social engineering attacks are quite difficult to mitigate by using a poorly implemented awareness program. Schneier [10] reminds us that social engineering a.k.a "Socio-technical attacks are really all about the human aspect, i.e. trust." Kevin Mitnick, renowned and reformed hacker, in his book "the art of deception" [11] also concludes that people inherently want to be helpful and therefore are easily duped because they assume a level of trust in order to avoid conflict.

Organizations can protect their confidential information by using a layered security "defense in depth" strategy which should incorporate relevant and timely security awareness training. While training people to be aware of the various human hacking techniques is essential to preventing successful human hacking attacks, the approaches to these techniques evolve over time. A holistic approach to awareness is the only reliable way to mitigate human hacking threats because the more people are conscious of the risk / impact of human hacking attacks, the less the likelihood of successful human hacking attacks. It is important to understand that security awareness cannot be organized independently from other security management processes. The security policy and security organization are critical to the success of a security awareness program.

7. References

[1] Federal Trade Commission Fraud Report for 2006 http://www.ftc.gov/opa/2006/01/topten.shtm, Visited March, 2007

[2] Lemos, Robert. (2006). Survey: Identity Theft Hits Three Percent. Security Focus http//www.securityfocus.com/print/brief/177

[3] Granger, Sarah (2006); Social Engineering Reloaded http://www.securityfocus.com/print/infocus/1860 , Visited March, 2007

[4] Hollow, Phil. (2005). Hackers are Real Time. Are You*?* Sarbanes-Oxley Compliance Journal http://www.sox.com/Feature/detail.cfm?ArticleID=623 , Visited March, 2007

[5] Gaudin, Sharon (2002); Social Engineering: The Human side Hacking http://itmanagement.earthweb.com/secu/article.php/1860 , Visited March, 2007

[6] Granger, Sarah (2001); Social Engineering Fundamentals, Part 1: Hacker Tactics http://www.securityfocus.com/print/infocus/1527, Visited March, 2007

[7] Social Engineering (2005); http://www.searchsecurity.techtarget.com/sDefinition/0,sid14_gci531120,00.html

[8] Palmer, C.C (2001); Ethical Hacking: IBM Systems Journal, Vol 40, Issue 3 Pages 769 – 780. ISSN: 0018-8670.June1, 2001. http://www.research.ibm.com/journal/sj/403/palmer.html, Visited March, 2007

[9] Rusch, Jonathan J (1999); The Social Engineering of Internet Fraud. INET '99 Proceedings, http://www.isoc.org/inet99/proceedings/3g/3g_2.htm, Visited March, 2007

[10] Schneier, Bruce; "Secrets & Lies: Digital Security in a Networked World*"*. John Wiley & Sons, 2000. ISBN: 0-471-25311-1

[11] Mitnick, Kevin: "The art of Deception: Controlling the human elements of security" John Wiley & Sons, 2002.ISBN: 978-0-471-23712-9

[12] McAfee Security Report: http://us.mcafee.com/VirusInfo/ Visited May, 2007

[13] COBIT Control Objectives: http://www.isaca.org Visited April, 2007

[14] McBride, Patrick; "How to Spend a Dollar on Security", Computerworld, 9 November 2000

[15] ISO 13335 Section 3, Guidelines for Management of IT Security http://www.iso.org

[16] Information Security Forum's Standard of Good Practice- Standard for Information Security http://www.securityforum.org/assests/pdf/sec_stan.pdf

[17] Benefits of Security Awareness and Privacy Training: http://www.nativeintelligence.com , Visited July, 2007

[18] Privacy Rights Clearing House: http://www.privacyrights.org/chronDatabreaches.htm

[19] Rocket ready Newsletter: http://www.rocketready.com/newsletter.html Visited July, 2007

[20] Ponemon Institute: http://www.ponemon.org Visited July, 2007

[21] XBOX http://news.com.com/2008-1029_3-6170894.html Visited July, 2007

[22] http://etiolated.org Visited July, 2007

[23] Turner, T; "Social Engineering – Can Organizations Win the Battle? " http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_Can_Organizations_Win.pdf

[24] Hall, M (2005); "Secure the people".Computerworld.

http://www.computerworld.com /securitytopics/security/story/0,10801,100448,00.html

[25] Raymond, Eric: How to become a hacker FAQ http://www.tuxedo.org Visited October, 2007

[26] Schneier, Bruce: http://www.schneier.com/blog/archives/2006/09/what_is_a_hacke.html

Visited October, 2007

Biographical Notes:

Dr. P.O. Okenyi, CISSP, CISM, is currently a Senior Information Security Consultant with HSBC.com's Information Security group. Prior to joining HSBC, he worked with Credit Suisse Asset Management New York (CSAM NY) Information Technology Risk team, Credit Suisse First Boston New York (CSFB). Peter has also worked as a Security Consultant for eFortresses based in Atlanta, Ga. eFortresses is an Information Technology Risk Management firm headquartered in Atlanta. Peter has also served as an independent consultant to PepsiCo's Information Security Group (ISG) in Dallas, TX. Peter holds a Masters of Science (MSc) in Information Technology with emphasis in e – Commerce from the University of Bradford (UK). He recently completed his PhD in Information Security Risk Management at Brunel University, UK. Peter is a member of the Information System Security Association (ISSA).

Dr. T.J. Owens, CEng, CMath, is Senior Lecturer Communications in ECE, School of Engineering and Design, Brunel University, UK. He was the Project Coordinator of the European Commission FP6 IST Integrated Project INSTINCT (http://dea.brunel.ac.uk/instinct/) on Broadcast and telecommunications networks convergence. He is the author of more than 40 refereed articles in journals. His current research and teaching interests are focused on Wireless Communications Security and Network Security which he teaches in London, Athens, Esslingen, and Thessaloniki.