Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Psychology: A Precious Security Tool

Understanding attackers' motivations can help to improve computer security measures. Using good communication and collaboration may make security objectives easier to achieve. These skills are usually not part of training for security specialists. This document is a reflection about human behaviour regarding computer security. It explains why understanding psychology is as important as mastering technical skills. It shows how some human actions can weaken security regardless of technology in place. It proposes techniqu...

Copyright SANS Institute
Author Retains Full Rights

AD

Psychology:
A precious security tool

Yves Lafrance

GSEC certification
Practical Assignment 1.4b
Option 1

Submitted: 2004-02-2

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Abstract

Security specialists have to master many technologies to help organizations being more secured. People tend to forget an important factor influencing computer security: The human factor. Understanding attackers' motivation can help to improve security measures. Using good communication and collaboration make security objectives may be easier to achieve. These skills are usually not part of training for security specialists. This document is a reflection about human behaviour regarding computer security. It explains why understanding people psychology is as important as mastering technical skills. It shows how some human actions can weaken security regardless of technology in place. It proposes techniques to minimize the effects of unwanted behaviours and turn them into more secure ones.

This paper discuss about external enemies such as hackers as well as those who attack form inside organizations. It also discuss on how a better understanding of employee's psychology can give clues on how to discourage some kind of behaviour, encourage others to stop unwanted actions. We'll also discuss about security awareness programs that help increase security. Finally, will discuss about laying the foundation of a security culture and its effects on the organization. In each section, some 'psycho-security tips' will be given to illustrate how a concept can apply to real situations. They do not pretend to address completely a situation. Reader should consider them as examples to illustrate a point and not instructions on how to secure their organizations. Those ideas should be adapted for use in a larger plan.

© SANS Institute 2004, As part of the Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Content

Abstract i

"Enemy Psychology" 1
Hacker's motivation 1
Hacker's techniques 3
Psycho-security tip – Vulnerabilities 3
Another hacker's technique: Social engineering 4
Psycho-security tip - Discretion - Keeping the information for ourselves 7
Psycho-security tip - Searching help into newsgroups 8
Psycho-security tip - Domain related information 9

The enemy inside 9
Intruders? Insiders? 10

Motives 11
Psycho-security tip - Controls 12
Psycho-security tip - Implementing control 13
Psycho-security tip - Onion strategy 14

"Employee's Psychology" 14
Psycho-security tip - Passwords! – A little help? 15
Psycho-security tip - Oh no!… A virus… again! (or Click-o-maniacs!) 16

Security awareness 17
Security policy 19
Security policy vs. employees: a burden or an ally? 20
Psycho-security tip - Security policy 20

Security culture 22
A longer way 22
A safer way 23

Conclusion 24

References 25

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

"Enemy Psychology"

Computer security is about protecting networks computers and data against unauthorized access or use. But what kind of profit can someone gain in accessing a server? It is important to note that profit definition include but is not restricted to economical benefits. Enounced more candidly, we could ask: Why did 'he' choose my company (or home)? Why this did 'he' choose this specific computer? Answers may lie in the person behind theses action. Understanding the motives, the reason of an attack (past or future) can give system administrators clues on how to harden a system to prevent this technique of attack. Examining each technique, one by one, can be compared as looking at trees in a forest. This approach is very effective and precious to secure an environment.

But, if we stand back a little and examine the forest instead of trees? We will find that the forest is made of different species of trees. Similarly, hackers don't search for the same 'targets'. There motivation will influence the target they choose and the technique they take to approach it.

Hacker's motivation

Trying to understand hackers, is trying to differentiate their motivation. We won't discuss, about 'insiders' or when an attacker act from inside a company or organization. We will talk about those subjects in the next section "The enemy inside".

In an article entitled "Who are the Hackers?" [1], Masha Zager describes hackers based on their motives. Based on her article hackers can be described with three (3) "families" base on their motivations: Casual hackers, Political hackers, Organized crime.

Casual hackers are frequently motivated by curiosity. Hacking computers give them thrill. Sometimes, they hope to use somebody else's subscription on paying sites. Casual hackers form the biggest group. Most of them are not very skilled persons. They use tools created by more experienced people. Their inexperience may cause costly damage to installations. Casual hackers often leave clues on computers they break in.

Acceptance by other hackers and notoriety are important motivations to casual hackers. As described in "Microsoft Windows Security Resource Kit":

> By breaking into a network of a major company or government agency and defacing its Web site, an attacker is virtually guaranteed national and international publicity and enshrined in the electronic hacker community. [2]

Political hackers generally are militant for a cause. They are also called cyber-activists. They use their knowledge to make publicity about the cause they believe in. They also can try to attack site that represent interest against their conviction.

Cyber-terrorists motives can be related to cyber-activists ones. Bill Crowell, CEO of security firm Cylink Corp. and a former deputy director of the National Security Agency declares:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

> Clearly, the vulnerabilities of the nation to cyberattack are growing. Critical national functions like banking, financial services, health, water and communications are increasingly dependent on highly automated systems that connect the many nodes of their operations. [3]

Political hackers target computers either for what they represent or as part of a "disorganization plot". Their knowledge and skills may vary. Experts tend to agree that, as time goes on, this group will become more educated. The treats with political hackers are mostly WEB site defacement and Denial Of Services (DOS). Cyber-terrorists, in particular, may want to achieve DOS over long period of time for critical services as declares Ruth David, former director for science and technology at the CIA:

> In the aftermath of the 9/11 attacks, those adversaries almost certainly observed the immediate effect of service interruptions as well as the prolonged economic impact of infrastructure disruptions. While the weapon used was explosive rather than cyber, it doesn't take much imagination to see that similar effects could be achieved through cyberterrorism. [3]

Organized crime is use to name professional criminals and hackers that breaks into systems to gain financial profit. Secret information, credit card numbers, industrial and international espionage especially interest this group. Spies also belong to this family. Spies' usual goals are to gather information. Sometimes spies could also try to modify victim's information. Members of this family usually want to avoid detection to complete their attacks successfully.

Compared to casual or political hackers, these well organize and methodical people usually utilize a different approach. They select carefully their targets. They take time to gather information before trying to break into systems. They pay great attention to remove traces of their actions. Social engineering is common tools for them.

To these three "families", I would personally add a forth one which can be called **squatters.** These hackers target systems without considering whose property they are. Their attacks are impersonals. They may want to gain access computers to store data (music, movies, passwords, credit card numbers, stolen programs, etc.) sometimes for their own use or to redistribute it. They may also want to break systems to have "zombie systems" to be used in Distributed Denial Of Service (DDoS) attacks.

Worm programmers can be considered as part of this family because their prime objective is to spread a worm's "payload" as widely as possible. Once installed, payload function may have specific target, but on Internet point of view, the distribution of the worm is, most of the time, impersonal.

Like casual hackers, most of squatters use identified vulnerabilities to gain access of target systems.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Hacker's techniques
Hackers like many persons prefer simple techniques to complicated or long ones. Most of them will seek an existing technique or tool instead of developing a new one for each tentative they make.

Two major factors will influence techniques hackers choose to break into systems: Hacker's abilities (or experience) and their motives when selecting a specific target. Considering these two factors, an important proportion of casual attacks and most of squatter attacks are regardless of the organizations that own the systems they target.

The familiar point of these attacks is that they use a known process to exploit a known vulnerability. To identify their target, hackers scan a range of IP addresses to detect systems. They compile information on systems that are susceptible of responding to one or more vulnerabilities they intend to use. Using this information, they will use a known exploit the vulnerability to break into target systems. The difference between a human and a worm attack reside in the fact that worm will try to break in by trying to exploit vulnerability. Il will not scan to find it at first. Most worms spread blindly to any system responding to the vulnerability they use to propagate. This leave virtually no time for the target computer administrator's to react because there is no reconnaissance phase where the vulnerability is identified on a system and the system being attacked.

Psycho-security tip – Vulnerabilities

Suppose a company having several servers linked to the Internet. Usually a company have DNS, mail, web and maybe FTP servers. They want to protect themselves from the majority of the attacks present "in the wild". They first want to take measures against common attacks.

With regard of these attacks, today's challenge is to shorten the time frame between the discovery of a new vulnerability and the moment maintenance is applied.

This scheme will provide clues to system and network administrators to implement a security strategy based on technology. Among these tools, we may find, as example:

- A good software maintenance plan;
- A frequently updated anti virus software;
- Thigh port control on each systems;
- Firewalls to control network access.

They also want to take measures against viruses and worms. Usual anti virus software are helpless against new them until the manufacturer provides a new signature file against their malicious code. During this period, user education is one the best protection.

Technological measures are excellent. However, only relying on them may be a mistake.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Casual hackers and squatters usually look for easy targets. Because they plan to gain access to a large number of computers, they do not take heavy precautions to be undetected. Most of the time, counter measures based on technology are efficient in these cases. When a door is close they simply try to knock at another one. Regularly updated static defense scheme have good success against this kind of attack. If technology fails to block them, regular logs review usually permit to discover traces of the intrusions. Once the "*modus operandi*"[a] has been found, recovery and protection measures are quite straightforward to implement.

As mentioned, these countermeasures are based on technology. They are good, well documented and mandatory to protect informational assets. As sophisticated as they can be, these techniques have limits. Well implemented, they will almost certainly block inexperienced hackers. They may also slow down and block intermediate ones. But what about really determined and experienced ones? Are these measures are not secure enough to block everything? No. They aren't silver bullet.

Hackers who identify specific objectives will not give away so easily. They consider their target as unique because of the organization that own it or because of the data possibly available through it. For this reason, they will choose a less direct approach. They will act as a hunter with his prey. They will progress slowly to reduce probability of being detected. They begin by gathering, accumulate and understand a lot of information about the target. These actions are described as the "reconnaissance phase".

Another hacker's technique: Social engineering

In some circumstances, the reconnaissance phase of the attack operation is driven very discretely. Often, hackers use "social engineering techniques" to gather information. An article on "Subject, Wills & Company" 's web site describe social engineering in theses terms:

> PT Barnum said, "There's a sucker born every minute" - Social engineering attempts to capitalize on this philosophy. Social engineering can be regarded as "people hacking" or the exploitation of the human factor. Basically, it's hacker jargon for soliciting unwitting participation from a person inside a company rather than breaking into the system independently. This is accomplished by persuading "marks" or "targets" to volunteer or assist with delivering information about critical systems, applications or access to such information. Social engineering is a highly developed skill that can best be described as "the art and science of getting people to comply to your wishes".[4]

For many, Social engineering may appear as a mysterious hacker's trick. It is, at the opposite of technical tools, only limited by hacker's imagination. Social engineering techniques take time to master and needs, especially when interacting directly with people, practice and intuition. This technique is efficient because it take victims in a way they do not expect. In most people's mind, hacker master technology… not human

[a] '*Modus operandi*": the particular way in which a person performs a task or action.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

behavior! Efficiency resides in the unexpected… in the surprise. Let's go deeper to understand the technique.

A few days ago, someone asked me information about sniffing. Once the answer given, the person replied that sniffing was too much trouble and it was still easier to stand behind someone and look at the computer screen. That's simple case of social engineering.

The philosophy underneath social engineering presents humans as the weakest link of security measures. Hackers, as most of humans, search for the easiest way to perform a task. Social engineering is a frequently used technique when hackers "feel" that strong technological measures are in place around their target information or computers. One of the most well known social engineer, Kevin Mitnick, wrote about this technique in an article regarding his first visit to RSA's security conferences:

> You could spend a fortune purchasing technology and services from every exhibitor, speaker and sponsor at the RSA Conference, and your network infrastructure could still remain vulnerable to old-fashioned manipulation. [5]

Let's look at some ways hackers might choose to penetrate an organization. First, hackers will document themselves about the target they choose. Not a bit of information is neglected. Advertising, financial reports, newspapers, web sites, competitor's web sites, newsgroups, etc. This amount of information may give them schemes to follow to perform their approach. If not, information could be use by the hacker to learn business environment: language terms used, name of key people, etc.

Another hacker can try to be hired as a janitor or to provide green care. This "position" will provide them plenty of occasions to grab information such as names, job's title, phone numbers and why not… passwords on post-it placed around computer's monitors! If they are lucky enough, they may even have opportunity to gain physical access to servers or unlocked laptops!

One step further is the trashing technique… Yes! Looking at the enterprise's trashes. Some hackers do not hesitate to "purchase" trashes… What can they find in enterprises trashes? Think about it for a second… The question should be… What can't they find? Old company phone books, meeting notes, program listings, network schemas, contracts, material or software bills, old hard disks, etc… And now, environmental concerns helping, paper trashes are sorted and don't smell bad!

I can almost ear you saying… "But we shred confidential papers!" That's exactly what happened in 1979 at the US Embassy in Iran:

> When the "Students Following the Line of the Imam" stormed the U.S. Embassy on November 4, 1979, they gained access to the embassy's extensive files. Before they were taken hostage, embassy officers had tried to destroy as much as possible — often by shredder — but the Iranians managed to recover the shredded items and systematically reassemble them. They then published

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

> facsimiles of the documents in a series that currently numbers over 70 volumes. Most of the shredded materials are CIA cables that relate to clandestine contacts with Iranians. This example describes a nugget of military information provided by one such contact. [6]

You can look at a reassembled page on the same site, at:
http://www.gwu.edu/~nsarchiv/nsa/publications/iran/irdoc.html [7]

"Well… it would probably take plenty of time to reassemble stripes of paper!" **Time!** You just mentioned something very important…. Hackers have plenty of time… system administrators don't. This is an important element to keep in mind to understand hacker's way of thinking. They use time as a weapon; to the limit they have infinite time to set up an attack. They will spend this time gathering knowledge about their target. They will continue as long they are not convinced they can avoid being detected while breaking target's technological defenses. One of hacker's saying is: "Knowledge is power"!

Scary isn't it? Is there something that can be done against that? Is the battle already over? Certainly not! It is unusual to say to IT people something like Scott Culp's "10th immutable law of security":

> **Law #10: Technology is not a panacea.**
>
> […]
>
> Raise the cost and difficulty of attacking security technology, and bad guys will respond by shifting their focus away from the technology and toward the human being at the console. It's vital that you understand your role in maintaining solid security, or you could become the chink in your own systems' armor.
>
> The solution is to recognize two essential points. First, security consists of both technology and policy – that is, it's the combination of the technology and how it's used that ultimately determines how secure your systems are. Second, security is journey, not a destination – it isn't a problem that can be "solved" once and for all; it's a constant series of moves and countermoves between the good guys and the bad guys. The key is to ensure that you have good security awareness and exercise sound judgment. […] Combine great technology with sound judgment, and you'll have rock-solid security. [8]

In short: Do not rely only on security devices. To neutralize such hacker's techniques, one must use their own weapons against them: good old grey matter! If you know what they might want to know and how they can try to know it… then you KNOW! Remember? Knowledge is power! And the good news is that we have more control on information than we might think. In a certain manner, we can possibly reverse the initiative - usually on hacker's side - and give them harder time grabbing it. In fact it's the save strategy as those used with technology… If the target is too difficult to reach, chances increase they will select another one.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Using examples, let's look at strategies we might use to oppose to hacker's techniques. Let's imagine how we can use their weapons against them. In this game, information is the ammunitions. We will use and sometimes transform information to make it work for us against hackers.

Psycho-security tip - Discretion - Keeping the information for ourselves

Let's take the example of a public financial report may, mentioning the installation of 30 new phone cells in city X, and 28 more in city Y to rise quality of service. It may describe its "state-of-art datacenter" located on Old street, Workcity. It may boast the replacement of old MiK-4 computers with 32 HAL 2000 running the latest version of Xunil OS to answer customers on the Internet. Yes… this report will illustrate to customers and investors how the company is dynamic!

This report may interest hackers as well. It will probably give away precious information. They may now check for the vulnerabilities regarding the OS and establish surveillance around the datacenter.

Ok… this example may be simplistic but it shows that an organization may supply needlessly information to spiteful persons. Sometimes, people are not conscious of the information value. They do not realize they also have a certain control over this information before it is published.

We can draw two observations base on this example:

1. A business (neither a person) should not publish an information of any nature unless it is necessary
2. A single person, even a team cannot filter all the information released (printed, electronically or verbally) by the organization. This would be inefficient and over the long run stall the business.

In certain circumstances, this is more difficult. Government organizations must, by example, have publicly opened acquisition process. They may have the obligation to describe in a public document that they want to purchase 16 Bigtel-based servers. But they maybe not have to mention they will install XYZ operating system on it to be configured as eight WEB servers, four firewalls, two WQL database and two "prophecy" servers; all these to be installed at 789 Rstreet!

They may try to break the ordering process into different parts. Release them within different time frames, with different delivery addresses. They may also break orders to have different responsible names related to them. Or on the contrary, always have the same shipping contact, billing contact, delivery address. They can also separate software orders from hardware ones.

These slight changes may help to confuse outsiders. Even non-governmental organization can do the same and mislead hackers by playing a little with addresses

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

and contact names. This may imply little changes in the business habits but they worth the effort. The idea behind this is to complicate hacker's research. Mislead them using every occasion you see.

Sometimes, information disclosure is made by technical personal. Internet is a big database encyclopaedia where we can find almost anything. People should develop habits that help reduce the amount of information leaking from their organization.

Psycho-security tip - Searching help into newsgroups

A system administrator having problem applying a path to a web server can ask for help in specialized newsgroups (mailing lists or forums).

> Hi,
> I have problem applying the new patch #5678 on Cherokee WEB server version 4.3. Every time I apply the patch, the server doesn't start. I tried on our 3 web servers with the same result.
>
> Can somebody help rapidly? It's important because we use the feature describe as vulnerable.
> Thanks
> Johnny.Tabasco@Spicy.com

The administrator may spice up his life acting that way! It's like sending invitation to hackers! This administrator has two choices:

1. Remove all details about the situation. Even if he proceeds like this, chances are a hacker could inference that Spicy's WEB servers are vulnerable.
2. Ask for the information but removing all clues that can lead to the company, the servers or the administrator. How? By using a free email facility (Hotmail, Yahoo!, etc.) It might look like:

   > I have problem applying the new patch #5678 on Cherokee WEB server version 4.3. Every time I apply the patch, the server doesn't start.
   >
   > Can somebody help me?
   > Thanks
   > AppleSauce75@Hotmail.com

This way, it is more difficult to link the situation to a specific installation. Even though, it's important to be careful by looking at the newsgroup, list message or forum. Search for information that may be obtained from the email headers such as sender's IP address. This detail is especially important on mailing lists. By checking email headers, a hacker could find an IP address or a mail server name belonging to the sender even if he uses a free mail service.

To work around this problem, it is possible to use an ISP link (different from the

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

office's one), which uses dynamic IP addresses (dial-up should be fine) to post "public" messages. This way, if an IP address is found in email headers, it won't trace back to the business's IP addresses. For the same reasons, it's also better to create the message by using a WEB page instead of a SMTP client.

Same precautions should apply when you correspond with persons who answer your email or when you correspond with strangers in general.

Information leakage can be possible even if there is no correspondence between people. Let's use another example, but this time concerning technology. This one can show that disclosure of what seems to be harmless information can lead to a security breach.

Psycho-security tip - Domain related information

Every business having a domain name has to supply contact information before having it registered. This information includes, a street address; phone numbers, fax numbers and email for three contacts (administrative, Technical and billing). This information is easily available to anyone on the Internet.

With a single "whois" command, contact names and associated information is accessible to a hacker. He can steal impersonate somebody in the company and contact the 'technical contact' he found (either by phone, fax or email) and gather more information.

But what if we replace, by example, technical contact information by a forge identity? We can assign a real email address, real phone and fax numbers to this identity. We can instruct people answering these fake address or phone to "ring a bell" to security staff. This will act as an alarm for the organization that an attack may me on preparation. Simple, easy, elegant and SAFER!

The objective, as illustrated, is to reverse the process. Usually, hacker take initiative, they choose ways to approach a sitting duck (passive victim). Changing your attitude, you become a flying duck (moving target) and you can mine the ground around to fool or embarrass intruders. Adding such strategies together, you progressively cease being a less accessible duck (target).

To carry on with this strategy: If they cannot know what they want to know… Better, if something they know is not the right information to know… and if they do not know that they do not know? (Well! Did I go to far with that one?) Once again, Knowledge is power…Reducing the knowledge usable against you, will decrease the pressure against you. Okay let's go back to earth!

The enemy inside

"Uh! How can the enemy be inside? I fired the green care person and had the janitor have a background check!" – could you say.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Intruders? Insiders?

First, lets discuss about persons which objective is "to have a foot in the place" (or around it) with malicious intention. Examples of this case could be spies or competitors. They can try several techniques or crafty tricks to successfully gather information. Social engineering is an important component of their "toolkit". Strictly speaking, this kind of attack can be regrouped with external ones. An organization should protect against them in the same way they do for social engineering. The first line of defense against them would be vigilance to keep intruders outside of the organization.

Unauthorized access by insiders is done more frequently that could people could imagined. This situation happens for years now as stated in the "Eighth annual Computer Crime and Security Survey Highlights" from Computer Security Institute (CSI):

> Survey results illustrate that computer crime threats to large corporations and government agencies come from both inside and outside their electronic perimeters, confirming the trend in previous years. Forty-five percent of respondents detected unauthorized access by insiders. [9]

Worst, damages to organizations are more significant when caused by insiders.

> "You can spend a lot of money to protect against the attack from the outside, but once you bring somebody into camp, the threat goes way up because the greatest damage comes from an inside threat," says the FBI's Hendershot [b]. [10]

But what if employees act against their own organization. When we come to this aspect of the question, we must talk about trust. This a small word for a heavy meaning. Developing business requires all kind of competences and skills. Rare are enterprises that don't have to hire. Hiring somebody implies beginning a trust relation with person. As time goes on, this trust relation will develop. Without this trust relationship, an organization cannot grow.

Without trust between co-workers, suspicious climate will poison working relation and slow enterprise evolution. This only shows that trust is necessary. By essence, people have good intentions. People usually want to contribute to enterprise success. But certain circumstances may happen where people can become untrustworthy. The following example shows that such behaviour is damageable for both the person and the organization.

> Among those arrested was a contract employee of the provincial license bureau – the Société de l'Assurance Automobile du Québec [c] – who police allege provided Bandido[d] members with license numbers and addresses from the bureau's database. In previous investigations, the police have alleged that information leaked from the SAAQ was used in such biker-gang hits. Eleven of the 62 people facing charges in the case are accused of conspiring to kill anyone associated

[b]: Harold Hendershot, is section chief of the computer intrusion section of the FBI's cyberdivision

[c] Organization's acronym is SAAQ (note by the author)

[d] Bandido: a biker-gang (note by the author)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

> with the Hells Angels. It is the fourth time, since December 2000 that criminal charges have been filed against people who had access to the SAAQ's databases. [11]

Motives

Why an employee would consciously commits immoral or illegal acts? As we did in the previous section with hackers, let's take a look at motives that can drive individuals on the wrong side of the fence. The point here is not to suspect every employee. It's about finding which factors, mindset or events can make employees turning into "enemies". Once identified, we may try to influences factors we can control to reduce this risk category. It is also important to consider than such situations develop over a certain period of time. This must be kept in mind when planning measures in this domain.

Economical profit often comes in first thoughts. Most of people will choose paths that are ethical and legal. For thousands of reasons, some individuals may think they need or deserve more money than they earn. Accumulated debts, by example, caused by gambling as well as scholar or health charges (or others) may lead to situations were the obsession money overcome ethic or legality.

Personal interests may motivate others. Employees may want to access or worst modify information regarding, a family member. Some others may try to access data about an unpleasant neighbour.

Revenge is another frequent motivation. Some may consider this motive as an extension of personal interests motives. By doing so, an employee may target a superior, the organization itself or somebody outside the organization. We have a tendency to think that revenge targeted against organization or its personal can be considered separately from personal interests revenge. We have this opinion because we think that an organization should have a certain influence on this kind of motivation.

External Pressure on an employee may often influence behaviour. This pressure can come from relatives, organized crime or from spies. As seen with social engineering, A lot of reasons may be use to put pressure on a person. Here a some of those, from a former counterintelligence officer:

> Now CEO and president of California-based Advantage SCI, Elsa Lee spent 20 years as a counterintelligence officer in the U.S. and has seen a variety of ways in which employees give away their employers' secrets.
>
> Seduction and exploitation are popular techniques, says Lee. Having used sex, drugs, money or alcohol to get a hold on someone, a counter-intelligence officer can then move on to blackmail when they want to put more of a squeeze on their supply of information. Social engineering is an established pattern of techniques […] but aggressive surveillance, like all security threats, is always evolving. [12]

To gain access to the desired information, one needs **opportunities** to do so. However, in addition to their state of mind, employee need and use some advantages (compared

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

to external attackers) to be successful. The first advantage is often the job position occupied by the person. It is easier to "steal" information records when it's your job to access this access this information on a day-by-day basis. Ben Smith and Brian Komar in "Microsoft Windows Security Resource Kit" describe the situation this way:

> Attackers who are employees of the organization they're attacking present a unique danger to networks for several reasons. Such attackers have the following in their advantage:
>
> - Higher levels of trust
> - Physical access to network resources
> - Human resources protections [2]

In opposition, the **perceived risk** of proceeding of unauthorised access will also influence the reasoning of an employee. The higher the perception of the risk of being caught, the higher the chances a person renounce to the unauthorized access. It is important here to note the difference between the risk and the perceived risk. The risk represents the chances of being caught. The perceive risk is the chances someone "estimate" of being caught. We will use this difference with the next example.

Psycho-security tip - Controls

Suppose for a moment, two hospitals having the same measures performed to control the work of the persons in charge of patient admissions.

In the first hospital, a daily list of consulted patient records by a single employee is checked against the admission forms signed by the patients. Security staff performs this process and nobody else have knowledge of this control.

In the second hospital, the same control is performed but the control results have to be signed every morning by the personal being checked and countersigned by employee superior.

In which hospital, in your opinion, is more probable to have a person in charge of patient admission risking an unauthorised access to a patient record?

The purpose of this tip was to show that making people aware of controls might be a security tool. We will discuss other aspect of controls in the next tip.

This case shows that perceived risk take importance. It can constitute a barrier to help persons restraint themselves to commit unauthorised accesses. Letting people be aware that controls exists and are applied is a dissuasion tool. It is the application of the old saying: "Fear…is the beginning of wisdom".

We deliberately implied three persons in the case of the second hospital. This measure was present to reduce risks of **collusion**. It is more difficult for tree persons to agree to commit an act than having only two of them. This argument is stronger if persons are close colleagues.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

How can we implement measures to secure from insiders without creating a climate of suspicion through the organization? Let's take a few examples of possible controls.

Psycho-security tip - Implementing control

While implementing defensive measures against insiders, one must keep in mind that insiders may be aware of details of the security strategy. They may have an in-depth understanding of barriers the have to defeat. That being said, it is possible to use this situation positively:

- Implement good internal controls measures. These must be described as general measures. Avoid pointing specific groups or persons in the processes you describe. Show that measures are there to guide more than to find culprit. Controls must be perceived as prevention and not as enquiries.
- Partially disclose some of the controls you implement. Do not necessarily publish an exhaustive list. Even if "security by obscurity is a controversial principle" " (as described in the Wikipedia encyclopedia); [13] a little *aura of mystery* can make potential inside attackers think twice and restrain themselves. On the other end, employees' being aware of surveillance among them is not wrong. Just enough disclosure may increase perceived risk.
- Have audits (both internals and externals) conducted on a regular basis. Let know that audits are sometimes announced…. And sometimes not. Do not disclose audit report to employees unless it is necessary. Partial disclosures will keep alive the *aura of mystery.*
- Have the upper management clearly state and publish than people responsible for security breach will be subject to disciplinary measures. State thoroughly what are theses measures in a confidentiality agreement. Have employee signing the agreement yearly.

We will continue this discussion with the next tip.

As seen in the last "tip", dealing with insiders can look like the carrot and the stick technique. We have discussed about "stick" but what can be carrots? Good management practices regarding employees constitute positive measures as well as mean to measure employee feelings concerning their job. Low-level management play an important role regarding employees. Keeping in touch on a frequent and regular basis with people is a good way to detect persons who can become potential insider risk. Measures can be promptly taken such a change of role in the organization or referring the employee to an "Employee assistant plan" (from human resources department) to help them solve their problem before they develop into security concerns.

Informing employee about security breach consequences and 'keeping an eye on them cannot be taken as solid rock measures against insiders. Defense in-depth measures must be taken to complement 'managing the human factor'. Onion strategy does not rely on a single measure; it consists in having multiple layers of protections completing each other. In the security domain, having both belt and braces does not look too bad after all.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

;o) It is possible that all measures surrounding persons fails. Other measures (controls, IDS, etc.) can take over and signal unauthorized behaviours before they grow.

Psycho-security tip - Onion strategy

If preventive actions fail, organization must have mechanisms in place to prevent, protect or detect unauthorized insiders behaviour. In this domain defense in-depth attitude is a good protection model. Some examples of such measures could be:

- Segmented network architecture. Create different physical networks for each task to perform. Control access between networks with firewalls.
- Use judiciously placed IDS to detect suspect traffic.
- Identify critical information, its location, people requiring access to it
- Have all critical data access logged.
- Have automatic logs analysis to find 'unusual' access. Investigate theses exceptions.

A good reading about implementing this kind of measures could be Dan Houser's "Network security: Submarine Warfare" in August 2003 number of Security Magazine. [14]

"Employee's Psychology"

In the last pages, we discussed about the enemy outside as well as inside an organization. We covered cases where people are consciously acting against organization's assess. This being said, could it be situation where good willing employee can make actions weakening or breaking information security?

Besides all the quality of many employees, force to see that important security breach come from the actions they may do. Kathleen Coe, Regional Education Director, at Symantec Corp agrees:

> However, many of the best Internet firewalls are circumvented not by experienced hackers, but by careless employees. Some of today's largest security breaches can be traced back to individuals who have not been properly trained to both recognize and respond to Internet threats. For example, many employees don't know what types of practices lead to an increased security risk, nor do they understand what to do if a virus or other threat actually infects their computer. Organizations large and small must develop their most useful line of defense: employees.
>
> The need for employee involvement in information security is clear. Ninety percent of large corporations and government agencies detected computer security breaches in the United States in 2001, according to the 2002 Computer Security Institute/FBI Computer Crime and Security Survey. Eighty percent of those organizations acknowledged financial losses due to security breaches. In an effort to better protect themselves from such losses, many organizations have

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

implemented robust, integrated security systems, yet they often fail to plug a major security hole — employees.[15]

Let's first talk about passwords… Passwords! Security staff nightmare, administrators' nightmare…. User nightmare! Many books and security articles discuss about problems related to password usage: If they are trivial, they are said to be weak. If they are complex, they are said to be too difficult to remember. Many other practices related to passwords lead to security breach:

- Writing down a password on a sticky note placed on or near your computer.
- Using a word found in a dictionary. That's right, a dictionary. Any dictionary!
- Using a word from a dictionary followed by 2 numbers.
- Using the names of people, places, pets, or other common items.
- Sharing your password with someone else.
- Using the same password for more than one account, and for an extended period of time.
- Using the default password provided by the vendor. [16]

Some authors says that time have come to change security practice and to replace password usage, biometry being a possible alternative. We won't go into discussing technologic alternative to password, which is beyond the scope of this document. We want to show that strong passwords are reachable (and by extension stronger security) for ordinary people… using a little help.

Most of these actions may be related with misunderstanding of the technology or ignoring impact of lazy practices. Another cause could also reside into failure from security staff to explain what means 'weak and strong passwords' as well as techniques to create good passwords. Next tip discuss about improving password strength.

Psycho-security tip - Passwords! – A little help?

Many users have difficulty dealing with passwords. Some use simple passwords others create complex passwords but have to write them down to remember them.

Simple techniques could be use to help breaking these two habits. Theses techniques have as common point that they have to be explained to promote their usage. They are simple tips, easy to learn and remember.

A first tip would be to use phrases instead of a single word. It is a well-known fact that one of keys strength is key length. Following this principle, the longer are passwords, the safer the protection. In addition, phrases are relatively easy to remember.

A second tip would be to interchange some letters by others keyboard characters that "look alike" in the person's mind. By example, some may find that letter 's' look alike they '5' symbol; or that the '&' symbol may replace the 'e' letter. Using theses substitution, the word 'seventeen' would look like '5&v&nt&&n'.

Another technique would be to mix a date within a word: Using the word 'evening'

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

with let's choose 2004-04-13 that could be the expiration date for the password (your birthday date would be less efficient). We may spread date numbers between letters to give '2e0v0e4n0i4n1g3'.

Theses three techniques show that simple tips can help users create and remember complex passwords. Of courses theses techniques can be mixed to create stronger passwords.

The point of this discussion is to show that you can turn an apparent human weakness into strength. All this by teaching users simple techniques. People, having a different brain, can invent their own password algorithms.

To make all this more easy to remember, a tutor could perform an easy demonstration:

1. At session beginning ask to every present person to key in a password similar to those the usually create. An alternative technique would be to have the instructor key in simple passwords known to be weak.
2. Using a password cracking software show how easy it is to break weak passwords.
3. At this point the instructor could show tips to create safer password.
4. As practical part, the instructor asks every participant to key in a strong password and shows with the same software how stronger are the new passwords.

By helping people to improve themselves, we have better results than by issuing rules. Doing so, we help building pride and self-confidence.

Let's now address another user's and network administrator's nightmare: Viruses!

Psycho-security tip - Oh no!… A virus… again! (or Click-o-maniacs!)

(For the need of this discussion, we will use the "popular" virus definition that includes both viruses and worms). Worms and viruses can spread across the Internet at surprising speed. As time goes on, viruses are more sophisticated. They use more tactics to spread. This requires from virus writers programming skill and knowledge.

But this alone cannot explain their efficacy. Why? Viruses spreading using as email attachment need a 'human intervention' to activate. In many cases, viruses needs that email title or text 'convince' someone to double-click on the attachment. This leads us again to "social engineering techniques".

Virus writers become more efficient in social engineering to convince people to activate their viruses. "MyDoom" worm is a good example of this. The malicious file came as an attachment. The crafted email message was using technical terms to fool the person.

Theses elements are settled up to awake user's curiosity. In our point of view, the

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

social engineering capacity of messages takes big importance in the virus ability to spread. This leads us to try to break the trust relation between virus writers and the email users.

Security staff used to warn users from opening mail (and mail attachments) received from strangers. This measure is obsolete because viruses now use real email addresses from address books on infected computers to send messages. Consequently, users must develop their own judgement abilities to decide to open messages or not.

Pushing this reflection to its limit, well-educated users can be hundred percent efficient and anti virus software would become obsolete. People would know how to react in any circumstances: using email, consulting web sites and downloading programs from any source! This is probably utopia.

A more realistic objective is to educate users to make them understand that anti viruses aren't panacea. User judgement is the only weapon against new viruses until anti virus programs are updated with fresh viruses signature files.

Education about viruses, limits of anti virus software usage and how user may have control over virus propagation is an important weapon. For many organizations, cost of such training sessions might be inferior to the cost for a single virus clean up operation.

We can regroup employee behaviour related problems in two categories:

Problems cause by **ignorance**. In this category, we may find behaviour caused by the fact that employees are not aware that some action may cause problem like:

- Information system misuse,
- Computer used to listen to music or online radio, TV,
- Unauthorized access to Internet WEB sites
- Installation of programs for personal use such as: games, peer-to-peer file exchange, instant messaging
- Mail virus propagation

Employees ignoring correct procedures related to an information system may use it incorrectly. This situation may cause integrity problems within the system. Integrity problems are indeed security problems. Unauthorised use of company resources (computers, Internet access, etc) is another example of resource misuse. A frequent question rise in those cases: Did employee know if "It was authorized or not?"

Security awareness

This brings us to an interesting concept: Security awareness. Sensibility varies from person to person. Security domain makes no exception to this rule. In the same

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

organization it is frequent to encounter people having a high security consciousness mixed with other reckless in the same domain. Security awareness programs aim to progressively raise collective consciousness about security. This concept may sound counter current for some people in a world relying on technology to increase security. Others, like Jack Wiles, agree:

> During my 20 plus years of working in the various fields that I will collectively call 'computer security,' I have never found anything to be more effective than company-wide employee awareness training. Not only is it effective, it may also be the least expensive security countermeasure that any size company can employ.
>
> I'll even make a very bold statement that is certainly my personal opinion simply based on many years of experience. I truly believe that without a good and sound employee awareness program, where every employee is taught the ways that they can help with the overall security of their company, most other more expensive countermeasures will be much less effective. [17]

Because they can rapidly "see results" with technology investment, some people may underestimate "peopleware"[e] power. The principle underlying is stating that a chain is as weak as its weakest link. On the contrary, if you harden each individual link, you harden the whole chain.

Security awareness programs could include many (but is not limited to) topics like:

- Why security is important
- Why each person is important in security matter
- Passwords
- Viruses
- Social Engineering
- Physical security
- Security Policy

This kind of training program should use regularly spaced short - one-topic sessions. It is easier to keep interest level and people involvement high. A SANS' GSEC practical paper by Chelsa Russell identify pitfalls to avoid when implementing a security awareness program. Mrs Russell's paper can be found at http://www.sans.org/rr/papers/47/418.pdf [18]

Security awareness as well as security is not tangible. It is hardly measurable as quantity of probe or virus infected email messages. However, one can feel awareness trough employee attitude when facing day-to-day situations.

Although security awareness is hardly measurable, researches try to develop models usable to measure the global security level within organizations. One of them, performed

[e] Peopleware: Human factor in Information Technology

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

at Stockholm's University, studied the critical success factors required to successfully implement an information security management system.[19] Another one, performed in South Africa, tried to measure security level using a questionnaire.[20] Both research pay attention to employee's motivation and management engagement as important factors influencing security level.

Awareness should be given time to grow and produce benefits. Security awareness is an attitude. It is developed using knowledge and understanding of given situation, problems or procedures. It is important to persevere over a long period with an awareness program. Topic specific sessions should be repeated in the case of new employee, or when dealing with a situation (ex: a virus propagation).

Searching new means to increase security awareness into organizations, a Sweden research project used a computer game to help employees become effective regarding computer security. The author observed, "IT security differs from other learning domains in that respect that every person, regardless of profession, needs to use and rely on it." [21] The research reports an interesting conclusion:

> The conclusion from the experiments is that computer games can be a suitable non-linear teaching method when learning to understand IT security and therefore also a suitable alternative/complement to conventional linear instruction. [21]

Because it is a human-related issue, security awareness is a first step to increase information security into organizations. Teaching security basics to employee is an important step allowing organizations to implement security policy properly:

> Organizations also realized that before they could enforce employee responsibility, they had to ensure that all employees understood information security issues. Employees cannot be held responsible for their actions if they are not aware that information security exists and how their actions can directly or indirectly influence information security. One way to present information security to employees is by means of an information security awareness programme. This information security awareness programme can be used to ensure that the security policy and best practices are implemented and complied with. [22]

Security policy

Security policy is a basic and strategic element to implement security. It is as critical for computer security as blueprints to construct a building. Security forces reflection about many organizational aspects. Among them we have: people attitude, procedures, networks architecture, workstation usage, application development and day-to-day operations.

We will not discuss about security policy's content. We will concentrate on psychological issues involved when talking about security policy. By understanding policies effect on people, we will try to point out ways that may help dealing with security policies. This question is complex:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

> Security policies and procedures affect not only what people do but also how they see themselves, their colleagues and their world. Despite these psychosocial issues, security personnel pay little or no attention to what is known about social psychology. Yet the established principles of human social behavior have much to teach us in our attempts to improve corporate and institutional information security. [23]

Security policy vs. employees: a burden or an ally?

Machines and networks are not affected by policies because they do not have emotions (not yet!). People do have emotions. Most of information security specialists are formed to deal with machines, networks, software and procedures. Dealing with this question maybe difficult because many are not well aware of the "human aspects" of security policies. There is much more in a security policy than a series of rules and directives. The most important part of it may not be written. It is about dealing with people to enforce the policy.

Some may think than having a policy written is the end of a process and once distributed employee must comply to it even if the do not agree with it content. Policies are often associated with rules. Most of people dislike rules. So how can we develop and implement a security policy while making employee acceptance easier?

Psycho-security tip - Security policy

Security policy is necessary in modern enterprises. Traditionally, it is developed and implemented by security staff. Usually security policies are a pain to develop and to implement. How can we reduce pain for both employee and security staff? Maybe employee implication is a key? Elizabeth Ferrarini says about policy creation:

> Policy creation should consist of a representative group of decision makers, technical personnel, and day-to-day users from different levels within the organization. Decision makers should have the power to enforce the policy. Technical personnel should advise on the ramifications of the policy. Likewise, day-to-day users should have a say in how easy or difficult the policy will be to carry out. [24]

A policy developed by such group has more chances to be accepted than imposed directives. Employees who participate in policy elaboration are in good position to explain policy elements to coworkers. This process progressing on a certain period, while the policy is elaborated, will give both time and information to employee to domesticate it. This will contribute to reduce resistance and facilitate policy acceptance. It would also be well advised to consult (or better to involve in the process) syndicates, human resources and legal advisor.

We see more advantage with this technique. Developing security policy with employee involved in day-to-day work has better chance to produce accurate policy elements that will be more easily applicable and measurable.

If managed correctly, security policy elaboration can become a common pride for

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

both management and employee. It will also facilitate, if needed, disciplinary consequences because these were developed based on a consensus and approved by high management. Because peers developed it, social pressure forcing the policy respect will help in its day-to-day application.

Such technique will need winning conditions to be successful. Among those, trust and respect are, on the top of the list. It is important to have the right timing to start this kind of project. Management representative should be receptive to employee ideas and initiatives. Security people should take time to explain security implications of each policy elements. It is important to allow time for people to adapt.

Security policy development is a great occasion for an enterprise to increase security awareness. It can create occasions to discuss about uneasy situations before being confronted to them. Once again, it is possible to turn a potentially problem situation (employee acceptance) into an asset if we understand human behaviour.

Enforcing a security policy is not an easy game. The main reason is because it urges people to change their behaviour. Organizations tend now to implement it using security awareness programs and as a shared objective with employees.

> […] New security policies often conflict with the way employees have done their jobs for years. For example, offices and departments that once operated with full and open information sharing are now being told that they must learn to control information, confront strangers who aren't wearing identification badges and refuse access to sensitive areas to anybody who can't produce identification - even the boss.
>
> Industry experts and corporate trainers are relying more and more on slogans, posters, games, trinkets and rewards to raise awareness about the importance of information security and the ever-changing threats that companies face in cyberspace. And while these small reminders might not be the entire answer to changing employee behavior or to garnering senior management support, experts agree that they are important elements in an overall security program. [25]

The objective here is to gain and keep employee's understanding and collaboration regarding security. An interesting research from at Henley Management College (UK) concludes that 'balance' is a keyword to keep in mind while elaborating and enforcing security policy.

> Finding the right balance will involve reviewing the strategic importance of information security and IT in general. Organisations that seem to be the most at ease with their information security environment are those that understand that over-restrictive controls can be as damaging for business as lax attitude to security. These are the organisations that have also spent time carefully balancing the trade-offs resulting from this equation. Finally, the research presented here also shows that information security cannot be solved by

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

> technology alone, since technology is only one of several components in an organisations defence of its information assets and IT infrastructure. [26]

The same research also reports that organizations that incorporate security in their business' day-to-day practices have a better success enforcing security awareness and policies. On my opinion, it is also important to remember that implementing a security policy is not a overnight operation but is a gradual process.

When persevering with security awareness training, organizations come to a point where security awareness program effects become tangible. Employee's self-confidence about security grows progressively. Enterprises may then collect benefits from investment they made into security awareness. From this moment, it is now possible to talk about a new enterprise culture: Security culture.

Security culture

Security culture is the logical result of a well-driven security awareness program. Once people become aware of threats it is in their nature to react to it. Motivated people want to solve problem if they feel concerned about it.

Building information security culture within an organization may be as simple as making people aware about security matter. Given tools to react, like information, training, time and most people are happy to contribute to solve the problem. Good communication between open-minded security staff, managers and employees is foundation of security culture.

A longer way

Security culture is not a target by itself. It is a state of mind and a way of living. There is no straightforward program leading to "implement security culture". It depends on many elements that contribute to raise awareness, confidence and trust within organization.

> John Butters, Partner in Ernst & Young's Information Security Practice commented: "Security is more than a technical issue; it is a business and, ultimately, a people issue. There are elements of security that are technical and clearly belong in IT, like providing a secure perimeter, and elements that are the responsibility of the business, such as defining who needs access to what. The trick is to get the balance right."
>
> John adds: "Updating rules in technology is easy, changing human behaviour is much more difficult." [27]

It takes longer time to change attitudes but profits from this investment are more durable. Directives may be forgotten. Attitude is a stable asset. Obviously, big challenges are related to important transformation such as adopting a new organizational culture.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

A great deal of flexibility is required from management. It is important that managers do not discourage employee initiatives. On the contrary, they should congratulate good attitudes and innovation.

A great challenge awaits security staff too. Seeing people, many of them not being specialized in security, wanting to assume new roles or wanting bigger security responsibilities may look menacing for some persons. To make place for security initiative, new ideas, security staff may have to redefine their role in the organization.

It is important for security people not to feel threaten by this change of culture. Being aware of this issue from the beginning may help them to face this situation. Even if security staff's roles are promise to changes, the situation should be seen as a benefit. Other persons taking care of simpler tasks they used to perform, security specialist will have time to work on more complex situations. They will be in better position to enhance organization's security this way.

A safer way

One (among many) indicator to measure security culture level in an organization may be the perception of enterprise employees about security staff.

If security staff are perceived as police officers, if they struggle to enforce security policy… maybe security level is not very high. On the other end, if they are invited to participate in projects at their starting phases, if they are perceived as resource people or instructors... security culture is probably well engaged on its way!

Changing the first perception into the second one require tact and understanding. A good place to start is using discussion groups where respect and listening are privileged. As technology, learning communication skills requires training... and patience.

Creating security culture within an organization is a long-term investment. It requires constant efforts to grow and to maintain. Security culture in return, gives enterprises every employee working actively to improve security. It gives enterprise a deeper defense. This process also changes relation between people. Because great trust relationships are required to go through such process, greater respect between employees has good chance to grow. This influence not only security but also the entire organisation.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Conclusion

Understanding enemies' motives can improve security response to attacks. In addition, better human behaviour understanding helps to improve security.

Some authors may recommend an attitude of "a steel hand within a metal glove" to implement security. This technique requires energy to 'enforce' security elements. It requires important efforts to 'disciple the troops'.

What happens if you remove such a security officer? An important part of security measures falls apart because other persons don't believe in them.

We should not neglect tools that can help us improve security. Understanding human behaviour and motivation is this kind of tools. Using this knowledge, we can do a better job implementing technology. We can make allies instead of creating resistance within organization by promoting security culture. This requires energy invested into listening to people. It takes time to create and implement security policy with employee collaboration. It needs efforts invested into security awareness training.

Now… remove the security officer. What happens? Almost nothing happens because other employee's autonomy has grown. Because every security elements are tied together and are taken in charge by several different persons, the enterprise can survive more easily when somebody quits.

After all… security is a matter of surviving. Isn't it?

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

[1] Zager, Masha. " Who Are the Hackers?" Newsfactor Network. September 17, 2002
URL: http://www.newsfactor.com/perl/story/19419.html (Feb. 21, 2004)

[2] Smith, Ben. Komar, Brian. Microsoft Windows Security Resource Kit. Redmond: Microsoft Press 2003 p.22

[3] Verton, Dan. " Outflanking The Cyberterrorist Threat" Computerworld. April 08, 2002
URL:http://www.computerworld.com/industrytopics/financial/story/0,10801,69866,00.html (Feb. 21, 2004)

[4] "Social Engineering" Subject, Wills & Company. 2002
URL: http://www.swc.com/news/articles/socialengineering.htm (Feb. 21, 2004)

[5] Mitnick, Kevin. "My first RSA conference" SecurityFocus. April 30, 2001
URL: http://www.securityfocus.com/news/199 (Feb. 21, 2004)

[6] Byrne, Malcolm. (Edited by) National Security Archive Electronic Briefing Book No.21. November 5, 1999
URL: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB21/ (Feb. 21, 2004)

[7] Bill, James A. IRAN - 1 9 7 7 - 1 9 8 0 (no publication date)
URL: Document: http://www.gwu.edu/~nsarchiv/nsa/publications/iran/iran.html (Feb. 21, 2004)
URL to picture: http://www.gwu.edu/~nsarchiv/nsa/publications/iran/irdoc.html (Feb. 21, 2004)

[8] Culp, Scott. "The Ten Immutable Laws of Security" Microsoft. (October 2000)
URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/10imlaws.asp (Feb. 21, 2004)

[9] "Eighth annual Computer Crime and Security Survey Highlights". Computer Security Institute (CSI). (May 29, 2003)
URL: http://www.gocsi.com/press/20030528.jhtml?_requestid=108932 (Feb. 21,2004)

[10] Duffy, Daintry. " Underground Fears" CSO Magazine. December 2003
URL: http://www.csoonline.com/reùad/120103/underground.html (Feb. 21,2004)

[11] Nathanson Centre. "Study of organized crime and corruption"
URL: http://www.yorku.ca/nathanson/CurrentEvents/April-June02.htm (Feb. 21,2004)

[12] Booth, Nick. The spy within - So who can you trust? SC Magazine. January 2004 URL: http://www.scmagazine.com/features/index.cfm?fuseaction=FeatureDetails&newsUID=682d7fd3-eb00-498d-9abd-5d32215335de&newsType=Features (Feb. 21,2004)

[13] Wikipedia encyclopedia. "Security trough obscurity"
URL: http://en.wikipedia.org/wiki/Security_through_obscurity (Feb. 21, 2004)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

[14] Houser, Dan. "Network Security: Submarine Warfare" Security Magazine. August 2003.
URL: http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss21_art86,00.html (Feb. 21, 2004)

[15] Coe, Kathleen. "Employees: The first line of defense". ITAudit. January 15, 2003.
URL: http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=528 (Feb. 21, 2004)

[16] "Password Protection 101" NERIC.
URL: http://security.neric.org/password.htm (Feb. 21, 2004)

[17] Wiles, Jack. "Security Awareness Training - It's Time To Get Serious" Infosecurity news. Feb. 13, 2002.
URL: **http://www.infosecnews.com/opinion/2002/02/13_02.htm** (Feb 21, 2004)

[18] Russell, Chelsa. "Security Awareness – Implementing an Effective Strategy". SANS GSEC Practical. Oct. 25, 2002.
URL: http://www.sans.org/rr/papers/47/418.pdf (Feb 21, 2004)

[19] Björck, Fredrik. "Implementing Information Security Management Systems - An Empirical Study of Critical Success Factors." June 11, 2003.
URL: http://www.dsv.su.se/~bjorck/files/success-factors.pdf (Feb 21, 2004)

[20] Eloff, JHP. Martins, A. "Measuring Information Security" 2001.
URL: http://philby.ucsd.edu/~cse291_IDVA/papers/rating-position/Martins.pdf (Feb 21, 2004)

[21] Näckros, Kjell. "Empowering Users to become Effective Information Security and Privacy Managers in the Digital world through Computer Games"
URL: http://smg.media.mit.edu/cscw2002-privacy/submissions/kjell.pdf (Feb 21, 2004)

[22] Von Solms, E. Eloff, J.H.P. "Information Security Development Trends" Sept. 2001
URL: http://osprey.unisa.ac.za/saicsit2001/Electronic/paper52.PDF (Feb 21, 2004)

[23] Kabay, M.E. "Psychosocial factors in the implementation of security policy" Network World Fusion. Feb. 16, 2000.
URL: http://www.nwfusion.com/newsletters/sec/0214sec2.html (Feb 21, 2004)

[24] Ferrarini, Elizabeth. "Establishing a Bullet-Proof Security Policy". EarthWeb.com. October 4, 2001.
URL: http://networking.earthweb.com/netsecur/article.php/897881 (Feb 21, 2004)

[25] Verton, Dan. " Companies Aim to Build Security Awareness" November 27, 2000.
URL: http://www.computerworld.com/careertopics/careers/training/story/0,10801,54375,00.html (Feb 21, 2004)

[26] Ezingeard, Jean-Noël. Bowen-Schrir, Monica. "Information Security: A Strategic Issue" 2003.
URL: http://www.dfs.se/upload/images/kretsar/sthlm/HenleyDFs_report.pdf (Feb 21, 2004)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

[27] "Survey Shows: Organizations Need To Develop Information Security Culture" ChannelMinds. Jan. 28, 2004.
URL: http://www.channelminds.com/article.php3?id_article=1582 (Feb 21, 2004)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced