CHAPTER 6 Social Engineering

LEARNING OUTCOMES

By the end of this chapter, you should be able to:

1. Understand the social engineering concept;
2. Identify the social engineering types and methods;
3. Determine the prevention method from social engineering attacks;
4. Differentiate the data classification and marking; and
5. Identify the relationship between layer of responsibility, data classification and social engineering.

INTRODUCTION

Before we begin, let us look at one article taken from the internet.

Social Engineering: The Human Side Of Hacking

May 10, 2002
By Sharon Gaudin

A woman calls a company help desk and says she's forgotten her password. In a panic, she adds that if she misses the deadline on a big advertising project her boss might even fire her. The help desk worker feels sorry for her and quickly resets the password -- unwittingly giving a hacker clear entrance into the corporate network.

Meanwhile, a man is in back of the building loading the company's paper recycling bins into the back of a truck. Inside the bins are lists of employee titles and phone numbers, marketing plans and the latest company financials. All free for the taking.

Hackers, and possibly even corporate competitors, are breeching companies' network security every day. The latest survey by the Computer Security Institute and the FBI shows that 90% of the 503 companies contacted reported break-ins within the last year.

What may come as a surprise, according to industry analysts and security experts, is that not every hacker is sitting alone with his computer hacking his way into a corporate VPN or running a program to crack executives' passwords.

Sometimes all they have to do is call up and ask.

"There's always the technical way to break into a network but sometimes it's easier to go through the people in the company. You just fool them into giving up their own security," says Keith A. Rhodes, chief technologist at the U.S. General Accounting Office, which has a Congressional mandate to test the network security at 24 different government agencies and departments. "Companies train their people to be helpful, but they rarely train them to be part of the security process. We use the social connection between people, their desire to be helpful. We call it social engineering.

"It works every time," Rhodes says, adding that he performs 10 penetration tests a year on agencies such as the IRS and the Department of Agriculture. "Very few companies are worried about this. Every one of them should be."

Source: http://itmanagement.earthweb.com/secu/article.php/1040881

Have you ever experienced the same situation as below? From the article above, state your opinions on the issue. Summarise your article and share it in the LMS Forum.

In the realm of computers, the act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information. Social engineering is successful because its victims innately want to trust other people and are naturally helpful. The victims of social engineering are tricked into releasing information and did not realise that it will be used to attack a computer network.

As a security professional in today's ever-changing world, it is important to be familiar with Social Engineering techniques and the counter-measures available to reduce the likelihood of success. By having this knowledge, one can ensure appropriate the preventative, detective and corrective measures are implemented to protect the staff and assets of an organisation.

6.1 SOCIAL ENGINEERING CONCEPT

Wikipedia defined ***Social Engineering*** as ***'The practice of obtaining confidential information by manipulation of legitimate users'***. A social engineer will commonly use the telephone or Internet to trick a person into revealing sensitive information or getting them to do something that is against typical policies.

By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. It is generally agreed upon that "users are the weak link" in security and this principle is what makes social engineering possible."

Social engineering attacks are usually conducted by outsiders who use a variety of psychological tricks to get the computer user to give them the information they need to access a computer or network. It depends on convincing an authorised user to perform an unauthorised action. Therefore, social engineering is a term that describes any attempt to convince an authorised user to disclose secure data or allow unauthorised access.

Social engineering consists of four phases that called ***Social Engineering Cycle***. The phases are Information Gathering, Relationship Development, Exploitation and Execution as shown in Figure 6.1.

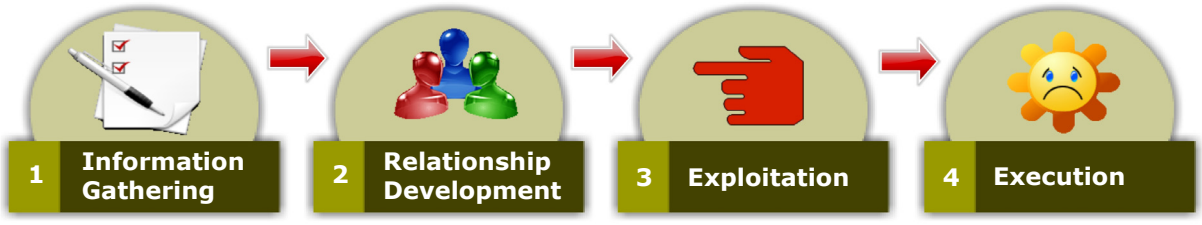


Figure 6.1: Social Engineering Cycle

Each social engineering attack is unique with certain possibility. It might involve multiple phases or cycle and may incorporate the use of other more traditional attack techniques to achieve the desired end result.

Table 6.1 describes the details from the cycle in Figure 6.1.

Table 6.1: Social Engineering Cycle Descriptions

Social Engineering Cycle	Descriptions
Information Gathering	• A variety of techniques can be used by an aggressor to gather information about the target(s). • Once gathered, this information can then be used to build a relationship with either the target or someone important to the success of the attack. • Information that might be gathered includes, but is not limited to a phone list, birth dates, an organisation's organisational chart etc.
Developing Relationship	• An aggressor may freely exploit the willingness of a target to be trusting in order to develop rapport with them. • While developing this relationship, the aggressor will position himself into a position of trust which he will then exploit.
Exploitation	• The target may then be manipulated by the 'trusted' aggressor to reveal information (e.g. passwords) or perform an action (e.g. creating an account or reversing telephone charges) that would not normally occur. • This action could be the end of the attack or the beginning of the next stage.
Execution	• Once the target has completed the task requested by the aggressor, the cycle is complete.

The goal of social engineers is to trick people into giving them what they want such as giving up a password or running a Trojan horse on a secure system. Social engineers prey on qualities of human nature such as described in Figure 6.2.

Figure 6.2: How social engineers prey on qualities of human nature

Social engineering is the most difficult form of attack to defense against because the user who actually takes the action is an authorized user and it cannot be defended with hardware and software alone. There are no documented signatures for such attacks or systems to log the activity associated with social engineering. This means that even if it can be determined that a social engineering attack occurred, it is very unlikely that the crime can be traced back to the perpetrator in such a way that they can be prosecuted

in a court of law.

The best and successful defense against this type of attack is security awareness training that will require effective information security architecture, starting with policies and standards and following through with a vulnerability assessment process. Make sure each person in your organisation is aware of the security implications of not maintaining security. Publish simple guidelines on matters such as physical control and care of passwords. Show employees how easy it is to take advantage of trusting people.

6.1.1 Aspects of Psychology in Social Engineering

Three key aspects of social psychology will help you to understand the methods used by social engineers. These key aspects are described in Figure 6.3.

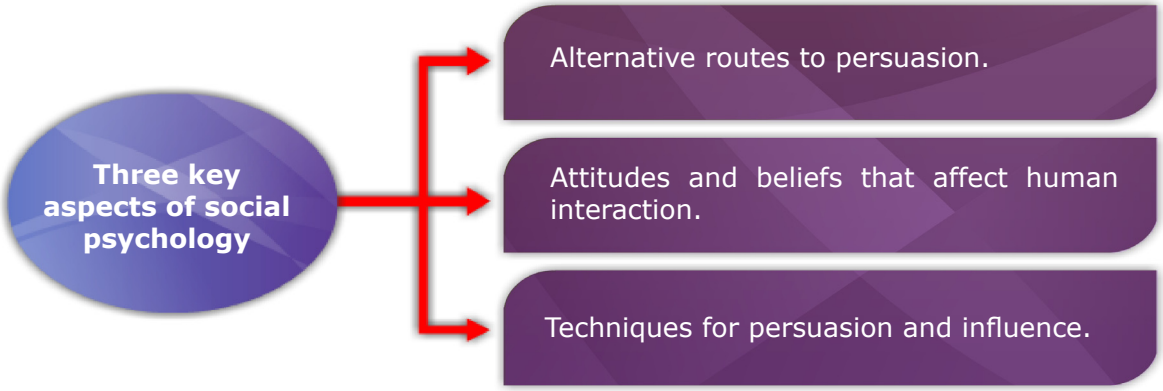


Figure 6.3: The three key aspects of social psychology

In the concept of alternative routes, there are two methods which are the direct route and the secondary route. In the direct route social engineers may simply ask the target for the information. This does not work very often but it is always worth a try. If that fails, they will prepare a systematic approach to obtain what they want. They are willing to invest time in the relationship and gain the pseudo relationship with the intended victim. They will prepare logical arguments that will work on the victim to get him or her to act.

In the secondary or indirect method, social engineers will make the prospective victim more susceptible by making some statement at the outset that triggers a strong emotion such as excitement or fear. Because social engineers are willing to spend time to get to know the mark, or they may be a fellow employee, they can contrive a situation that plays on the background of the victim.

In the typical interaction, our attitudes and beliefs about a request for service begin with the basic belief that all parties are who they say they are. In the social engineering interaction, only the victim maintains this notion. Effective social engineers rely on the knowledge that the victim will seldom question their identity.

6.1.2 Common Types of Social Engineering

Social engineering can be divided into two types which are human-based and technology-based social engineering. Human-based refers to a person-to-person interaction used to obtain the desired action. Technology-based means having an electronic interface to attempt to achieve the desired outcome.

6.1.2.1 Human-based Social Engineering

Human-based forms of social engineering can be categorised to impersonation and important user, third party authorisation, in person, dumpster diving and shoulder surfing.

1. Impersonation and Important User

Impersonation and important user are often used in combination with one another. Impersonation generally means creating some sort of character and playing out the role. Some common roles that may be played in impersonation attacks include a repairman, IT support, a manager, a trusted third party, or a fellow employee. Most of these roles fall under the category of someone with authority, which leads us to ingratiation.

Important user means that by pretending to be a senior manager of an organisation with an important deadline, the aggressor could pressure the Helpdesk operator into disclosing useful information, such as the type of remote access software used, how to configure it, the telephone numbers to the remote access server to dial and the appropriate credentials to log in to the server. Upon obtaining this information, the aggressor could then set up remote access to the organisation's network. The aggressor could then call back hours later to explain that he had forgotten his account password and request that it be reset.

Example of ***Impersonation and Important User*** Scenario
Taken from the book wrote by Katie Hafner and John Markoff, titled Cyberpunk

The authors describe the actions of one Susan Hadley (AKA Susan Thunder). Using an easily accessible military computer directory, she was able to obtain the name of the individual in charge. She used her basic knowledge of military systems and terminology as she called a military base to find out the name of the commanding officer of the secret compartmentalised information facility. She sweet-talked her way into obtaining the name of the major's secretary and then hung up.

Using this information, she changed tactics. She switched from being nonchalant to authoritative. Her "boss," the major, was having problems accessing the system and she wanted to know why. Using threats, she got the access and, according to her, was in the system within 20 minutes. Pretending to be someone else or simply schmoozing are typical examples of how social engineers work to obtain the information they need. They will often contact the help desk and drop the names of other employees. Once they have what they need to gain further access, they will attack a more vulnerable person that someone who has information but not necessarily the clout to challenge anyone of "authority."

2. Third-party Authorisation

The typical third-party authorisation is when the social engineer drops the name of a higher-up who has the authority to grant access. This is because of most social engineers are internal to the organisation and can find this out very easily.

Example of ***Third-party Authorisation*** Scenario

It is usually something like, "Ms. Alia says it's okay" or "Before she went on vacation, Ms. Alia said I should call you to get this information." The social engineer may well have called the authorising office to establish if it would be unavailable to corroborate the request.

3. In Person

Social engineers may enter a building pretending to be employees, visitors, or service personnel.

Example of ***In Person*** Scenario

They may be dressed in a uniform or become part of the contract cleaning crew. A few years ago in an office in New York, the cleaning crew arrived just before lunch and began to go into the offices to empty the trash containers and dust. Most employees offered to get out of the way and left their offices for a few minutes. Later in the afternoon the employees noticed that the trash cart was still in the lobby. After some checking done, they realise that the "cleaning crew" had cleaned the offices of wallets, purses and briefcases.

4. Dumpster Diving and Shoulder Surfing

Dumpster diving, also known as trashing is another popular method of social engineering. A huge amount of information can be collected through company dumpsters.

The LAN Times listed the following items as potential security leaks in our trash:

- Company phone books;
- Organisational charts;
- Memos;
- Company policy manuals;
- Calendars of meeting;
- Events and vacations;
- System manuals;

- Printouts of sensitive data or login names and passwords;
- Printouts of source code;
- Disks and tape;
- Company letterhead and memo forms; and
- Outdated hardware.

These sources can provide a rich vein of information for the hacker. Phone books can give the hackers names and numbers of people to target and impersonate. Organisational charts contain information about people who are in positions of authority within the organisation. Memos provide small tidbits of useful information for creating authenticity.

Policy manuals show hackers how secure or insecure the company really is. Calendars are great that they may tell attackers which employees are out of town at a particular time. System manuals, sensitive data, and other sources of technical information may give hackers the exact keys they need to unlock the network. Finally, outdated hardware, particularly hard drives, can be restored to provide all sorts of useful information.

Example of ***Dumpster Diving and Shoulder Surfing*** Scenario

The shoulder surfer will look over someone's shoulder to gain passwords or pin numbers. A few years ago, one of the news magazine shows did a piece on phone card fraud. During one sequence, the reporter was given a new phone calling card and told to use it at Melaka International Trade Centre in Malacca. While she made the call, the undercover police officer counted at least five people surfing her pin number. One even turned to the cameraman to make sure he got the number too. Within minutes the stolen card numbers were being used to make international phone calls.

6.1.2.2 Technology-based Social Engineering

1. Pop-Up Windows

A window appears on the screen informing the user that the host connection has been interrupted and that the network connection needs to be re-authenticated. The pop-up program then e-mails the intruder with the access information.

In another scam, a message claiming to be from eBay Inc. asks victims to sumit their password and other personal information to a Web site.

The e-mail typically arrives shortly after the victim's credit card has expired, so they don't suspect the site is phony. These are called phishing scams and have been around for years but have in recent months become more numerous and sophisticated.

2. Mail Attachment

Programs and executables can be hidden in e-mail attachments. Vince Gallo was the first to show the vulnerability of governments and corporations to information warfare via e-mail through his simulated Bunratty attack.

The first step to exploiting this vulnerability is to write a program that could be the "inside agent" to which the social engineer would send the covert messages. This program could be written to do anything, from sending copies of documents on the user's computer to spying on other computers on the network. It could be placed in the machine either with human assistance (e.g., a collaborator inside the company) or by placing it on a Web site for download, hidden within innocent-looking software (a Trojan horse).

Once the malicious Trojan software is inside the target machine, it does nothing until the attacker contacts it by sending an email message to the compromised machine; the special message class allows it to be forwarded directly to the hidden folders without ever being seen by the user.

3. Web Sites

A trick used to get an unwitting user to disclose potentially sensitive data, such as the password he or she uses at work.

For example, a website may promote a fictitious competition or promotion, which requires a user to enter in a contact email address and password. The password entered may very well be similar to the password used by the individual at work.

This newer trend in spam and identity theft is called "brand spoofing." In an attempt to scam users into disclosing private information, attackers phish or brand spoof, which means they send e-mails falsely claiming to be from a legitimate enterprise. Government, financial institutions, and online auctions/pay services are common targets of brand spoofing. The attacker sends an HTML e-mail input from within an e-mail or an e-mail providing a link to a deceptive replica of an existing Web page.

6.1.3 Personality Traits That Lead to Social Engineering

Social engineering can be successful when certain personality traits can be exploited. Table 6.2 lists down examples of personality traits that lead to social engineering.

Table 6.2: Examples of Personality Traits That Lead to Social Engineering

Personality Traits	Description
Responsibility Distribution	• The targets are made to believe that they are not solely responsible for their actions. • Social engineers will create situations with many factors that dilute personal responsibility for decision making.
Chance for Ingratiation	• Victims are led to believe that compliance with the request will enhance their chances of receiving benefit. • This includes gaining advantage over a competitor, getting in good with management, or giving assistance to an unknown yet sultry-sounding female although often it's a computer modulated male voice over the phone.
Trust Relationship	• Social engineers spend time developing a relationship with their intended victims. • Through a series of small interactions, a relationship is established. In many instances, victims actually recognise the voice of the social engineer because of all the time they have spent talking.
Guilt	• Most individuals attempt to avoid the guilt trip if possible. • Well social engineers aren't above stopping to lie about their situation. • The social engineer tries to make the victim believe that not granting the request will lead to significant consequences for the requestor.

6.1.4 Security Breaches That Lead to Social Engineering Exploits

Some potential security breaches are so tedious that they hardly seem to be of concern. With all the attack that has to fight each day and the deadlines to be met, sometimes the most obvious threat is overlooked. Let us look at Figure 6.4 which displays several types of security breaches.

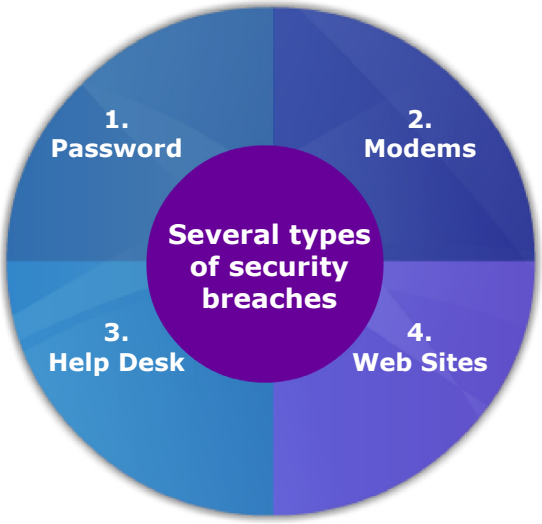


Figure 6.4: Several types of security breaches

From Figure 6.4, each of the types is explained in details as shown:

1. Password

The number one access point for social engineers is the good old-fashioned password. In spite of all the awareness programs and reminder cards, there is still has employee-generated passwords are too short or too easy to guess. System-generated passwords are too long, and employees have to write them down to remember them.

Even today, some systems do not require passwords to be changed. It can find from most often in e-mail systems and Internet accounts. Hence, an assessment of the password length and interval for change standards is recommended.

2. Modems

Every company has more modems than they know about. Employees and contractors will add a modem to a system and then install products such as pcAnywhere or Carbon Copy to improve their remote access time. From the installation made, some of the information can be obtained such as the password used to access the modem and the services used by the organisation.

Therefore, it is recommended that war dialers be used at least twice a year to check on modems to identify any changes to the modem configurations.

3. Help Desk

Help desk is the main place where the social engineers can get the information regarding the responsibility of each employee in the organisation. Hence, put in place processes that can assist the help desk employee in verifying who is on the other end of the phone call.

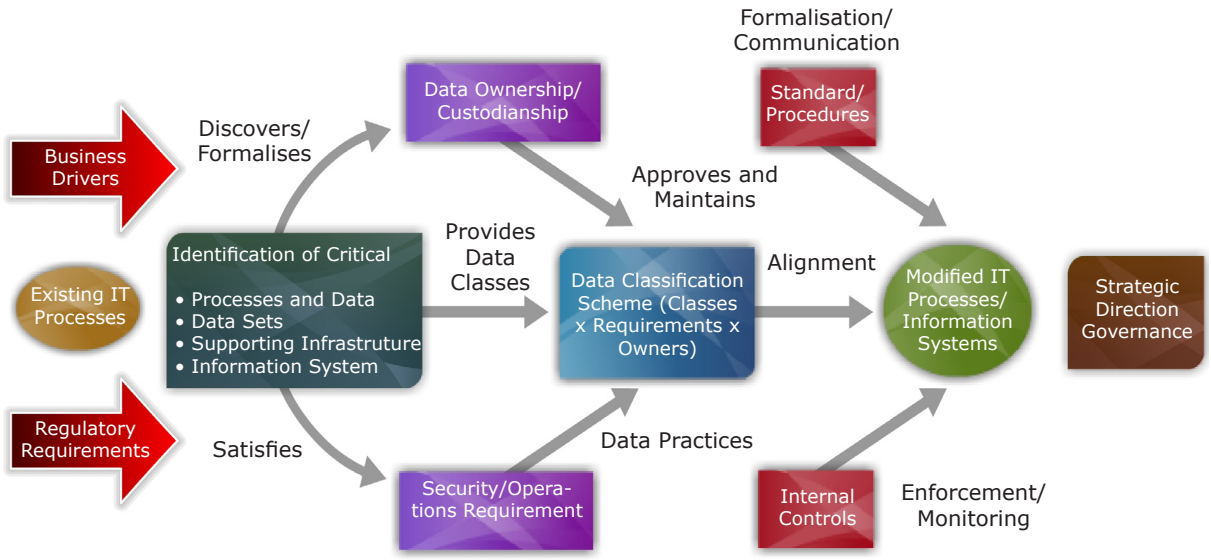
4. Web Sites

There are two problems identified from web sites which are the dummy site that gathers information and the legal site that gives away too much information. Many hackers use the information they gather from the enterprise Web site to launch attacks on the network. Thus, make sure that the information available will not compromise the information resources of the enterprise.

(a) What are the main types of Social Engineering?
(b) Determine the human nature that can be used for social engineering attack.
(c) What is the most effective countermeasure to social engineering?

6.2 DATA CLASSIFICATION AND MARKING

Observe the diagram below.



The diagram represents an example of data classification. From the diagram, can you elaborate on the process of data classification? Look for similar examples from the internet and share your findings in the LMS Forum.

Data classification entails analysing the data of your organisation retains, determining its importance and value, and then assigning it to a category. The implementation and regimented use of a data classification program is a mark of a truly professional information security program. Data classification systems provide users with a way to stratify sensitive information and apply appropriate safeguards to data with varying levels sensitivity in a consistent manner.

6.2.1 Pre-Requisites for Access to Classified Information

There are two pre-requisites (see Figure 6.5) for access to classified information which are security clearance and a need to know.

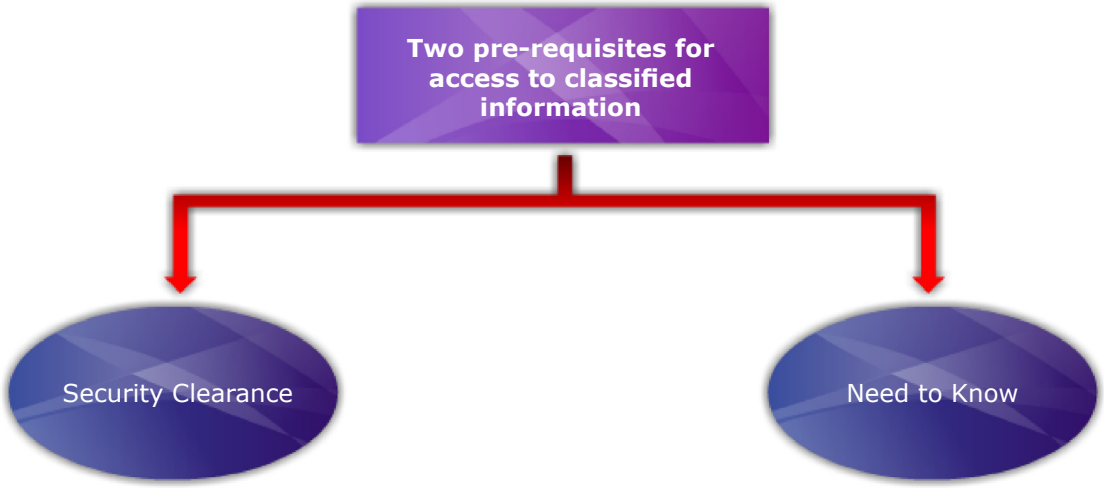


Figure 6.5: The two pre-requisites for access to classified information

1. Security Clearance

In an organisation using a data classification program, the fundamental requirement for anyone to be given access to classified information is that they must have a valid security clearance. In some organisations, determining security clearance is an extremely rigid process that requires completion of rigorous background investigations, polygraph tests and the execution of secrecy agreements. In other organisations, security clearance may be granted automatically upon employment and acceptance of a standard nondisclosure agreement.

First requirement for access to classified information is security clearance. Security clearances are normally granted in various levels that specify the maximum sensitivity level of information that a user is authorised to access. They may also grant special

access to various "compartments" that house extremely sensitive data that is limited to a select subgroup of cleared individuals.

Security clearances should be granted only to those individuals who absolutely need them for the performance of their regularly assigned functions. Furthermore, the clearance status of organisation affiliates should be reviewed on a regular basis. If an individual no longer requires access to classified data for his or her job, that access should be revoked until such time as it is needed again.

2. Need to Know

The second requirement for access to classified information is a valid need to know what classified information is needed to complete a designated job function. Whereas a security clearance offers access to broad categories of classified information, the need-to-know narrows the scope of that access down to specific data needed to complete tasks.

Normally, the process of enforcing security clearance requirements will take place at the centralised location of an organisation such as security office. That office is responsible for granting, maintaining, and revoking clearance. On the other hand, the need-to-know aspect is normally enforced by specific individuals charged with the custody of specific pieces of classified data. When asked for access to information, these custodians must ascertain the individual's identity and after validating his or her clearance, determine whether that person has a valid need to know the information in question. If the need to know cannot be established, they must deny access until such time as it is established in the future.

6.2.2 Classification System

There are two main types of classification systems as shown in Figure 6.6.

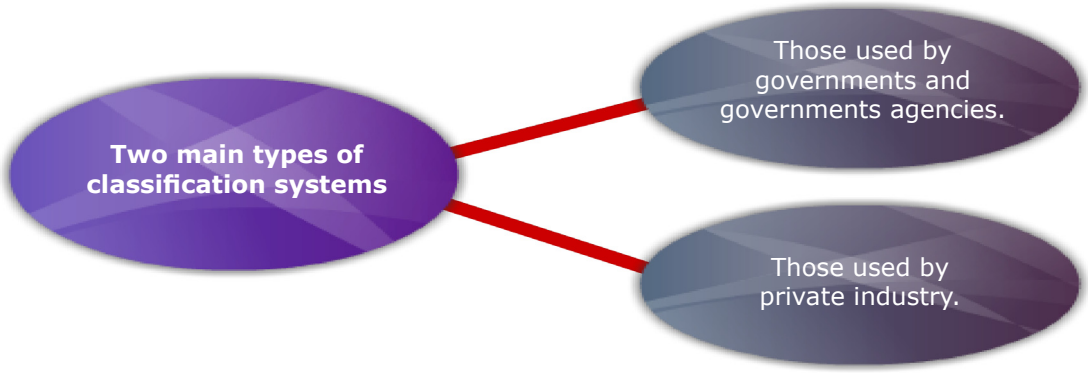


Figure 6.6: The two main types of classification systems

In most cases, the world's governments use classification systems that are much more

restrictive than those used by private industry. They also tend to have a good deal more bureaucracy and administrative overhead behind them.

The following will discuss each type of classification system and explore the benefits and drawbacks of each.

1. Government and Military Classification System

Most of the governments or government's agencies use what known as a mandatory access control system. In this system, each piece of classified data is assigned a specific level and everyone who handles that information is responsible for treating it with the appropriate security safeguards.

The five levels of classified information used by the most governments and their description is shown in Table 6.3.

Table 6.3: Military Data Classification

Classification	Description	Example: The U.S Government
Unclassified	Data that is not sensitive or classified.	Information that is not protected by any classification safeguards and may be freely distributed.
Sensitive But Unclassified (SBU)	Data that could cause harm if disclosed.	Also referred to as For Official Use Only (FOUO). Information for which disclosure would not necessarily cause damage to national security but which the government has some obligation to protect. Examples of information that may fall into this category are personal tax records, proprietary corporate information disclosed to government regulators and details of contract negotiations.
Confidential	Data for internal use that is exempt from the Freedom of Information Act.	Information that if disclosed to unauthorised individuals would cause *damage* to the national security of the United States.
Secret	Data that could cause serious damage to national security.	Information that if compromised would cause serious *damage* to the national security of United States.
Top Secret	Data that could cause grave damage to national security.	Information that if it falls into the wrong hands would cause *exceptionally grave damage* to the national security of the United States.

2. Industry Classification Systems

Industry classification systems are often much less complicated than their government counterparts but still have the same system levels and access controls. Normally, industry uses what known as commercial data classification as describe in Table 6.4.

Table 6.4: Commercial Data Classification

Classification	Description	Examples
Public	Data not covered elsewhere.	Press release, white paper.
Sensitive	Information that could affect business and public confidence if improperly disclosed.	Business strategy, profit plans.
Private	Personal information that could negatively affect personnel if disclosed.	Personal data such as employees' salaries or performance review.
Confidential	Corporate information that could negatively affect the organisation if disclosed.	Audit reports, operating plan.

For example, Table 6.5 describes some of the data classifications commonly found in industry.

Table 6.5: Common Data Classification in Industry

Classification	Description
Trade Secret	Information that consists of the crown jewels of many organisations. This data is normally not protected by formal property systems such as patents and copyrights because the inventors do not wish to risk the public disclosure and eventual release into the public domain that these systems entail. Rather, they have decided to protect the data as a trade secret by using internal controls designed to prevent unauthorised disclosure.
Company Confidential/ Proprietary	Information that consists of data that the business does not wish to see released into the public domain but that is much less sensitive than trade secret information.
Unclassified	Information that like its government counterpart, the company deems does not require classification protection.

However, no matter which system is used, it's important that the organisation should apply it and label information appropriately. This is critical in the event the organisation must later take legal action to enforce the intellectual property rights.

SELF-CHECK

(a) What is the government security classification applies to materials that if compromised would cause serious damage to national security?
(b) What is the classification label is often applied to highly sensitive corporate secrets that the company does not want publicly disclosed?

6.3 LAYERS OF RESPONSIBILITIES

Files and data may contain important and valuable information. This important information should be the focus of the security efforts. But somebody should responsible for ensuring the security of your organisation's information. Therefore, there is a need to assign different layers of responsibility to each piece of important information.

Each file, or data element, should have at least three different responsible parties assigned. The three layers of responsibility represent different requirements and actions for each group. Figure 6.7 shows the most common layers, where each layer has specific expectations to support the organisation's security policy.

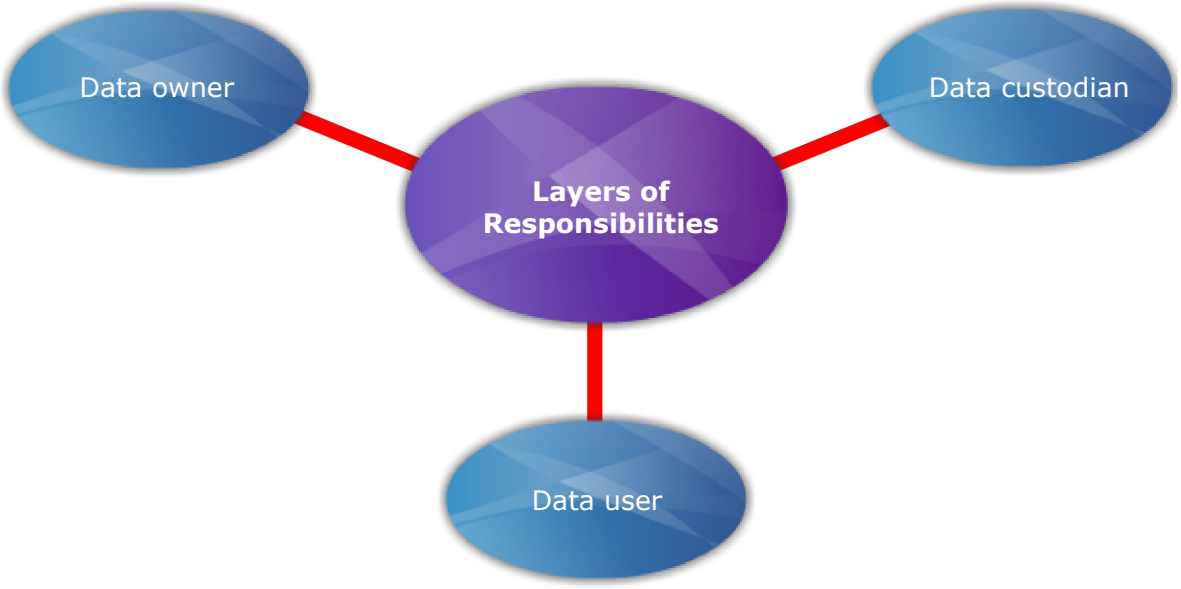


Figure 6.7: Layers of responsibilities

6.3.1 Data Owner

The data owner accepts the ultimate responsibility for the protection of the data. The data owner is generally a member of upper management and acts as the representative of the organisation in this duty. It is the owner who sets the classification level of the data and delegates the day-to-day responsibility of maintenance to the data custodian. If a security violation occurs, it is the data owner who bears the brunt of any negligence issues.

Figure 6.8 displays the responsibility of data owner.

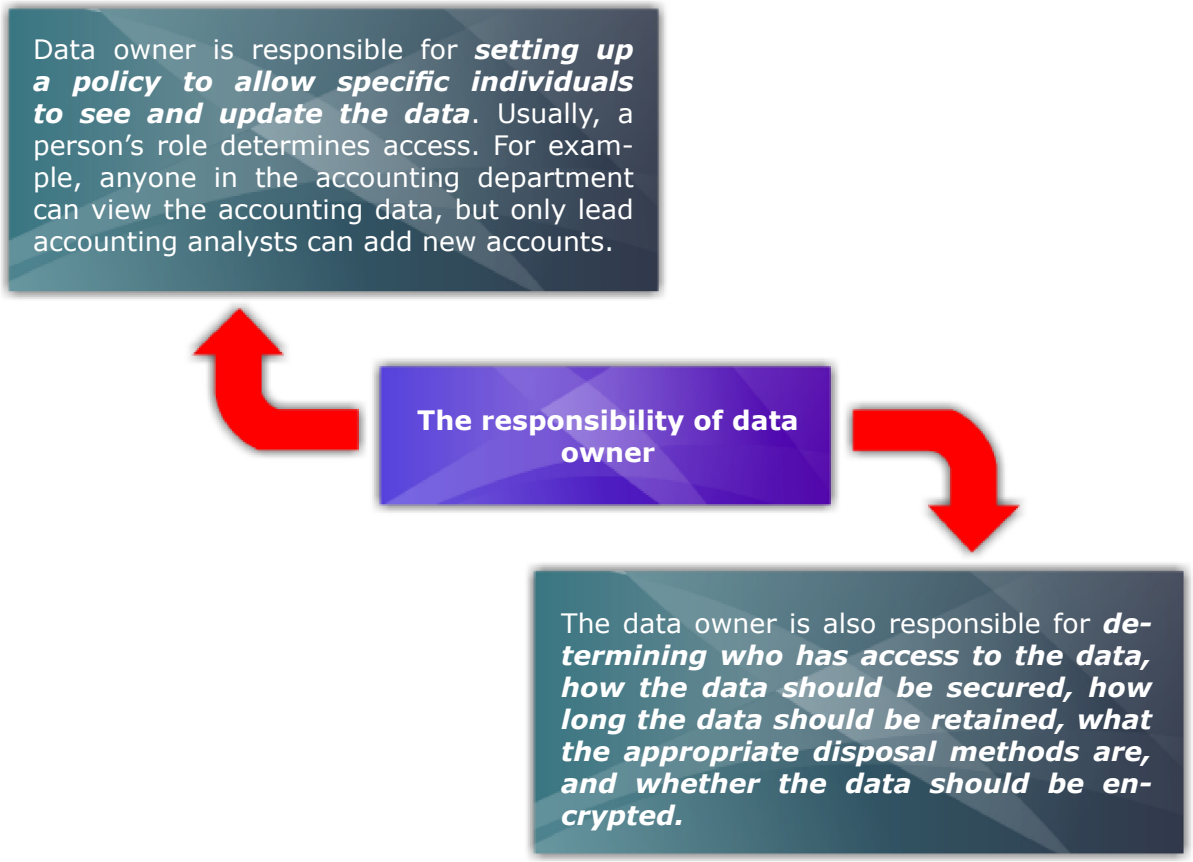


Figure 6.8: The responsibility of data owner

6.3.2 Data Custodian

The data owner assigns the data custodian to enforce security policies according to the data classification set by the data owner.

The custodian is often a member of the IT department and follows specific procedures to secure and protect assigned data. This includes implementing and maintaining appropriate controls, taking backups, and validating the integrity of the data.

6.3.3 Data User

The users of data are the ones who access the data on a day-to-day basis. They are charged with the responsibility of following the security policy as they access data. You would expect to see more formal procedures that address important data, and users are held accountable for their use of data and adherence to these procedures. In addition to a commitment to follow security procedures, users must be aware of how important security procedures are to the health of their organisation.

All too often, users use shortcuts to bypass weak security controls because they lack an understanding of the importance of the controls. An organisation's security staff must continually keep data users aware of the need for security, as well as the specific security policy and procedures.

Let us look at one news article taken from the internet.

BBC News: Net firms start storing user data

Details of user e-mails and net phone calls will be stored by internet service providers (ISPs) from Monday under an EU directive.

The plans were drawn up in the wake of the London bombings in 2005.

ISPs and telecoms firms have resisted the proposals while some countries in the EU are contesting the directive.

Jim Killock, executive director of the Open Rights Group, said it was a "crazy directive" with potentially dangerous repercussions for citizens.

All ISPs in the European Union will have to store the records for a year. An EU directive which requires telecoms firms to hold on to telephone records for 12 months is already in force.

The data stored does not include the content of e-mails or a recording of a net phone call, but is used to determine connections between individuals.

Authorities can get access to the stored records with a warrant.

Governments across the EU have now started to implement the directive into their own national legislation.

The UK Home Office, responsible for matters of policing and national security, said the measure had "effective safeguards" in place.

ISPs across Europe have complained about the extra costs involved in maintaining the records. The UK government has agreed to reimburse ISPs for the cost of retaining the data.

Mr Killock said the directive was passed only by "stretching the law".

The EU passed it by "saying it was a commercial matter and not a police matter", he explained.

"Because of that they got it through on a simple vote, rather than needing unanimity, which is required for policing matters," he said.

Source: http://news.bbc.co.uk/2/hi/technology/7985339.htm

From the article above, highlight the key points taken by the government in data user. Do a research and find similar issues using the Internet.

SUMMARY

1. A social engineer with enough time, patience, and resolve will eventually exploit some weakness in the control environment of an enterprise.
2. Employee awareness and acceptance of safeguard measures will become the first line of defense in this battle against the attackers.
3. The best defense against social engineering requires that employees be tested and that the bar of acceptance be raised regularly.
4. Security professionals can begin this process by making available to all personnel a broad range of supporting documentation.
5. Many employees respond positively to anecdotes relating to social engineering attacks and hoaxes. Keep the message fresh and accurate.
6. The detail of the consequences of successful attacks also should be included.
7. Do not discuss these attacks in terms of how security was circumvented, but on their impact to the business or mission of the enterprise.
8. These attacks can lead to a loss of customer confidence, market share, and jobs.
9. Employees at all levels of the enterprise need to understand and believe that they are important to the overall protection strategy.

10. Without all employees being part of the team, the enterprise, its assets, and its employees will be open to attack from external and internal social engineers.
11. With training and support, the impact of these kinds of attacks can be minimised.

GLOSSARY

Data Classification System	A system that provides a structured methodology for applying protection schemes to information of various sensitivities in a consistent manner.
Data Custodian	Generally an IT person who is assigned by the data owner to enforce security policies according to the data classification set by the data owner.
Dumpster Diving	Searching through rubbish thrown away to obtain potentially useful information that should have been disposed of more securely (e.g. shredding).
Mandatory Access Control	A system-enforced access control mechanism that assigns a security label which defines the security clearance to each subject and object.
Need to Know	A condition when a subject requires access to an object to complete a task.
Shoulder Surfing	Looking over the shoulder of an individual as he types in his access code and password/PIN on a keypad for the purpose of committing this to memory so it can be reproduced.
Social Engineering	Any attempt to convince an authorised user to disclose secure data or allow unauthorised access.

DISCUSSION QUESTION

You have received a phone call from a person who introduce that he is a bank officer from Bank of Malaysia. He claimed that he need to ask you some of information needed for upgrading some of bank services for you.

(a) As a customer of that bank, would you provide the information needed by the officer? If yes, what kind of information will you provide? What is the best reason should be provided to the officer if you do not want to give the information requested?

(b) From you knowledge, is there any bank policies that you know about giving information to the bank? If yes, what kind of situation that is safe to give the information requested?

(c) What are the precautions should you take if you face this scenario?

Write a brief report for your finding based on the scenario above. In the report, you should address all the possible answer and your justification for the solution provided.

REFERENCES

Carol Woodbury (2007). *The Importance of Data Classification and Ownership*. http://www.skyviewpartners.com/pdf/Data_Classification_Ownership.pdf [cited 1/4/09]

Charles P. Pleeger (2003). *Security in Computing*. New Jersey, United States: Prentice Hall.

Malcolm Allen (2007). *Social Engineering: A Means to Violate A Computer System*. SANS Institute: Reading Room SANS.

Michael G. Solomon & Mike Chapple (2005). *Information Security Illuminated*. Sudbury, Massachusetts: Jones and Bartlett Publishers.

Sarah Granger (2002). *Social Engineering Fundamentals, Part I: Hacker Tactics*. http://www.securityfocus.com/print/infocus/1527 [cited 1/4/09].

Thomas R. Peltier (2006). *Social Engineering: Concepts and Solutions*. Information

Security and Risk Management.

No Authors (2002). *Social Engineering*, http://labmice.techtarget.com/security/socialengineering.htm [cited 1/4/09].