International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 5 –NOVEMBER 2014.

# THE HUMAN INFRASTRUCTURE AND SOCIAL ENGINEERING: SOME IMPLICATIONS

Dr. D.V.Ramana Murthy

*Professor & Head, Dept. of Business Administration, KBN College, Vijayawada, A.P., India*

**Abstract— Information Security Management System (ISMS) defines to setup a solid security framework and regulates systematic way which information technology can use resources. But technical advancements of ISMS do not always guarantee to secure overall organizational environment. Human factors play a significant role for information security.**

**In particular, human characteristics behaviour impacts information security and ultimately associated risks. There are reported studies on Social Attacks, Social Manipulation and Social Engineering which throws a threat to human factor involvement and ethical orientation in managing information security and management system in organisations .This paper explores the human factors and their influence of social attacks, social manipulation and social engineering on the effectiveness of information security management system in organisations.**

**Index Terms— Human Infrastructure, information security and management System. Social Engineering, Social Manipulation, Shoulder Surfing, Dumpster Diving, Phishing, Baiting.**

## I. INTRODUCTION

In a general sense, the term information system (IS) refers to a system of people, data records and activities that process the data and information in an organization, and it includes the organization’s manual and automated processes. It is hard to accept that nowadays, organizations get along without having an astute and decisive information system. Providing a reliable and coherence information System requires a solid security framework that ensures confidentiality, integrity, availability, and authenticity of the critical organizational assets Increasingly, information security incidents result from interactions among people who work across organizations in dealing with ISMS. This has major implications for the role of human factors and challenging their roles in the process of information security.

Technology is quite an essential part relating to securing information assets but people are responsible for design, implementation and operation of these technological tools. Technology evolved enormously in terms of its advancement, but IS incidents still happen and this can be translated to the failure of ISMS.

As result, the ISMS guidelines and standards face a serious credibility threat. Recent studies concluded various technical, non-technical, and regulatory related issues for the failure of ISMS. It has been noted that 92% of large organizations admitted, they had information security incidents, which increased 72% over time IS has a risk and have adverse consequences on organizational operations and assets. Security systems do not depend solely on preventing technical problems, but rather, they also depend on humans who use the systems and behave in “a certain way” in the system environment. The real challenges are from non-technical forces, i.e., human and organizational issues. Therefore it is necessary to understand and address the issues relating to human factors.

Human factors can be divided into two categories, driving and restraining forces, whilst driving forces promotes goals as objective and expectation from the information security and restraining forces deemed as obstacles as a consequence of ineffective ISMS.

Social Engineering in the context of Information Systems is the art and science of manipulating people so that they give up confidential information. This type of attack is a confidence trick for purpose of vital information gathering. It is a term that describes non- technical and social attack that relies on human interaction and tricking people break normal security procedures. White collar criminals use social engineering tactics because; it is comparatively easier than other attacks. It is one of the most successful social attacks, because its victims innately want to trust other people and are naturally helpful. The victims of social attacks are tricked into releasing information that they do not realize that the same information will be used to attack a computer network. Social engineers rely on the fact that people are not aware of value of the information the possess and are careless about protecting it.

Security is all about knowing whom to trust and what to trust; knowing when and when not to take person at their word; when to trust that person you are communicating with; when to trust a web site whether legitimate or not; when to trust that the person on the phone is a legitimate person or not; when providing the information is a good idea or not.

## II. Types of Social Attacks

The social engineering attacks can be broken in to two types:

1. Human Based: Human based social engineering needs interaction with humans; it means person-to person contact and then retrieving the desired information, People use human based social engineering techniques in different ways.

a) Impersonation: In this type of social-engineering attack, the hacker pretends to be an employee or valid user on the system. A hacker can gain physical access by pretending to be an employee, coordinator, or inspecting authority.

b) Posing as an Important User: In this type of attack, the hacker pretends to be a VIP or high level manager who has the authority to use computer systems or files. Most of the time, low level employees do not ask any questions of someone who appears in this position.

c) Being a Third Party: In this attack the hacker pretends to have permission from an authorised person to use the computer system. It works when the authorised person is unavailable for some time.

d) Desktop Support: Calling tech support for assistance is a classic social engineering technique.

e) Help desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.

f) Shoulder Surfing: Shoulder surfing is the technique of gathering passwords by watching over a person's shoulder while they login to the system. A hacker can watch a valid user login and then use that password to gain access to the system.

g) Dumpster Diving: Dumpster diving involves looking in the trash for information written on pieces of paper or computer printouts. The hacker can often find passwords, filenames or other pieces of confidential information.

2. Computer Based: Computer based social engineering users computer software that attempts to retrieve the desired information.

a) Phishing: Phishing involves false emails, chats, or websites designed to impersonate real systems with the goal of capturing sensitive data. A message might come from a bank or other well known institution with the need to " Verify" your login information. It will usually be a mocked-up login page with all the right logos to look legitimate.

b) Baiting: Baiting involves dangling something you want to entice you to take an action the criminal desires. It can be in the form of a device like USB drive etc., when downloaded the person or company's computer is infected with malicious software allowing the criminal to advance in to your system.

c) Online Scams: Emails sent by scammers may have attachments that include malicious code inside the attachment. Those attachments can include key loggers to computer users passwords, virus, Trojans,or warms. Sometimes pop-up windows can also be used in social engineering attacks. Pop-up windows that advertise special offers may tempt users to unintentionally install malicious software.

d) Social networking: We know that nowadays people are using social networking sites such as face book, Twitter, Orkut, LinkedIn, etc.,. it is to be noted that social networks are the world's largest human identification database. Confidential information if uploaded and shared can be tampered causing the damage to the user both reputational and/or financial.

## III. Defending Human Factor against Social Engineering Attacks

No matter how tight your network security or well considered your security policy, the human element at your organization remains vulnerable to hackers. But there are steps you can take to tighten your security against social engineering attacks.

No matter how much expertise and money you put in to your network security and preventing data theft- firewalls, security appliances, encryption, etc.,- the human element remains vulnerable to hackers who apply social engineering techniques.

1. Educating the Human Factor: Our first mitigation is security through education. If people are not educate to the type of attacks being used then they cannot possibly defend against them.
2. Being aware of the information that is being released: People should have complete control on the information that they possess and under no circumstances should share this with anybody unwarrantedly.
3. Determine which of your assets are most valuable to criminals: An independent assessment is the best tool determines which of your assets criminals are most likely to target. Be careful with that data.
4. Design a Security Policy with good Awareness Training: A fool proof design of a security policy is needed fro protecting your data assets. Then back it up with good awareness training.
5. Updating the Software: A lot of information given out would not be damaging if the organisation keeps its software up top date. Staying on top of patches and keeping the software up dated can mitigate a lot of risk.
6. Employees should have a sense of ownership and belongingness when it comes to security: Security programmes are failing miserably because employees do not own them as they are not their personal. Orgainisation need to inculcate the need to feel a sense of ownership when it comes to security.
7. Check for the person with whom we are a parting with the information: Make sure that whether the person on the opposite side really deserves the information that they are asking about.

8. Watch for questions that don't fit the pretext: When an employee is on the phone with somebody asking for vital information and when pressurized

by the person on the other side, think twice before making a decision to part with the vital information. The employee should be careful by not being carried away by the stories being told by the opposite person on the phone.

9. Be yourself and Stick to your guns: when an employee gets a feeling that someone is phishing for information that they should not reveal, they should stick to their guns of security and confidentiality.

## IV. CONCLUSION

Information Security management is not only with your security oriented and highly configured systems, but with your people assets. Hardware and Software prove to be useless without Livewire your people at work, IS professionals. They should clearly understand the possibilities of all sorts social engineering attacks and need to protect themselves very effectively and in turn protect the organisation's data assets from the onslaught of social engineering attacks.

## V. REFERENCES

[1] D'Arcy J, Hovav A &Galletta DF (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research 20(1): 79–98.

[2] Islam, S., & Dong, W. (2008). Human factors in software security risk management. Proceedings of the first international workshop on Leadership and management in software architecture (LMSA2008). Leipzig, Germany, ACM.

[3] Lacy, D. (2009). Managing the Human Factor in Information Security, How to win over staff and influence business managers, Chichester, John Wiley & Sons Ltd.

[4] Lee SM, Lee S &Yoo S (2004) An integrative model of computer abuse based on social control and general deterrence theories. Information & Management 41(6): 707–718.

[5] Lim, J.S., Ahmad, A., Chang, S., & Maynard, S. (2010). "Embedding Information Security Culture Emerging Concerns and Challenges". PACIS 2010.

[6] http://www.webopedia.com/TERM/S/social_engineering.html

[7] http://en.wikipedia.org/wiki/Social_engineering_(security)

[8] http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

[9] http://blog.backupify.com/2013/06/24/5-types-of-social-engineering-attacks/

[10] http://lifehacker.com/5933296/how-can-i-protect-against-hackers-who-use-sneaky-social-engineering-techniques-to-get-into-my-accounts