Journal of Theoretical and Applied Information Technology
10th January 2013. Vol. 47 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

HUMAN ERRORS IN COMPUTER RELATED ABUSES

[1]AHMAD SALEHI SHAHRAKI, [2]MEHRNAZ NIKMARAM

[1] Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia (UTM),
Johor 81310, Malaysia
[2] Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia (UTM),
Johor 81310, Malaysia
E-mail: [1]ahmad.salehi.sh@gmail.com, [2] mehrnaz_nikmaram@yahoo.com

ABSTRACT

The term "Human error" can simply be defined as an error which made by a human. In fact, Human error is an explanation of malfunctions, unintended consequents from operating a system. There are many factors that cause a person to have an error due to the unwanted error of human. The aim of this paper is to investigate the relationship of human error as one of the factors to computer related abuses. The paper beings by computer-relating to human errors and followed by mechanism mitigate these errors through social and technical perspectives. We present the 25 techniques of computer crime prevention, as a heuristic device that assists. A last section discussing the ways of improving the adoption of security, and conclusion..

Keywords: *Human Errors, computer crime, Social Perspective, Technical Perspective*

1. INTRODUCTION

The Jmaes Reson (1990) distinct the errors from mistakes, errors are distinguished into two types: slips and lapses. Slips are execution failure for example: being attached by the wrong document to an email. Lapses are memory storage failure for example: forgetting logoff computer. Mistakes are resulted of inadequate plan for example replying email that appears to come from a reasonable source [1].

Jens Rasmussen (1986) defined to category of error type related to human performance such as Skill-based: familiar, automatic procedural or subconscious tasks, e.g. typing a password, and Rule-based: tasks approached by pattern matching from a set of internal problem-solving rules e.g. "If my bank sends me a message I will respond." And Knowledge-based: tasks approached by reasoning from first principles, when rules and experience do not apply, e.g. sending sensitive data to a home email address, not realizing that the network connection was less secure than the corporate network [2].

One of contributing factor in accidents and disasters in industries such as aviation, nuclear power, and medicine is human error. "Human error" mechanisms are the same as "human performance" mechanisms; it means that "human error" is part of the human behavior. Many things caused a person to have an error, but that not mean it is the person's fault for that condition is another factor. A person can be fool, distracted, persuaded, distracted and blackmailed but the conditions that increase the errors can be individual and based on the humans characteristics for example when a person's tired, idle, apathetic and uncaring. The study of human errors in the event is relevant to industry accident.

Although several types of human error have been identified and studied [3][4][5], biggest risk to an organization's network security is human error. The errors can be caused as a result of lack of knowledge, ignorance, and experience [6]. The knowledgeable also make poor and incorrect decisions. Therefore, it is critical that designers and operators be aware of human errors problem and build a mechanisms for coping the errors that will occurred [7].

2. COMPUTER RELATED TO HUMAN ERROR

Through the absence of an appropriate guardian, crime occurs. Computer- related crime maybe constituent of three factors of opportunity, motivation and the absence of appropriate guardianship. Opportunity is expanded with the increasing of digital technology. Motivation will depend on the nature of the criminal tendency or greed, revenge, adventure or lust. Therefore, the most control of computer-related crime contains of technical, law enforcement solutions [7].

One of the most subtle sources in data loosing and failure is human operator errors. It happens for many reasons, but the main cause can be mismatch between a human mental and the environment actual state. Sometimes this happens because of poorly designed security's guard. In 2001, the Microsoft suffered 24-hour disorder in Web properties because of human error while configuring name resolution system.

In a brief and simple example we carried out to investigate the importance of this problem, we asked six people to perform software in their systems. All six participant of this experiment were trained on how to install and perform the program and given printed instruction step-by-step. Each participant performed several assessment of the process. We found out even on this simple test with full instruction and in a stress less setting, the participants made fatal errors.

Crime can be reduced by the environment that occurred and altering the opportunity. The most effective solution for reduce the crime is through condition which allow the error to be performed. Therefore the aim of this paper is that find a solution on human errors.

3. MECHANISMS TO MITIGATE HUMAN ERRORS – SOCIAL PERSPECTIVE

These days, many organizations spending large portions of their budgets on defending against technical attacks and do nothing to prevent operation of the human factor. The role of human errors in computer abuse is undeniable, the here are two main approaches for decreasing of the human errors:

a) Teach the user how to do the right thing
b) Prevent the user from doing the wrong thing [8].

Two ways are exist to prevent human error from affecting a system: one way is keep people away from making errors or keep the errors from reaching the system. Both of them require that the possible error be anticipated, so none of them are effective. But people are good in findings an unanticipated ways to make mistakes.

User interface training or design is typically accomplished error avoidance. Before that, the user interface is designed to block possible errors, for instance wizards guide a user through default tasks, or human input be removed automatically. In performance, these approaches tend not to be very successful, so the operators often end up bypassing wizards or he automated some aids to complete the tasks that went unanticipated.

One option is to train users not to make an error, instead of blocking errors at the interface. Training can be achieved by developing the human's mental model of the computer system. In the other hand, that is a major source of errors by preventing the mental-model mismatches. The reason of effectiveness is that it is broad, however: in order to help build mental models, the broadest training must focus on concepts not process. It also must develop with the system to ensure that mental models are up to date.

The best training programs are frequent, extensive, and well designed. It forces operators to be out of their zones. From the technology point of view, it can help achieve these goals. It integrates training periods into a system's normal operation.

People make mistakes when error avoidance fails but preventing the system to receive those mistakes. A good example is that when many e-mail clients configured to batch and delay sending for several minutes it provide a recovery window during which an incorrectly sent message recalled. These buffering strategies influence the human ability to self-detect errors so that they are effective. Psychologists believed 70 to 86 percent of error can be detected immediately, even if they cannot be anticipated.

Preventing of errors has some limitations; it happens because of human faults and can be provide a recovery windows. This cannot work in changeable situations where system change quickly and exposing buffered commands by the time.

In spite of the limitations, both approaches have an important role. Trainings of the humans is a critical element of data managing, it means if a person is unaware of security issues, he is unaware of available protection. In the other hand, the experts have argued against relying on user education. They propose that it is wrong to put responsible on users, when the problem originates from the technical layer. Therefore, the education of user should be considered as a last resort for existing secure applications.

However, should not expect a home user to have received special training. The best way of preventing human error can be by designing at system phase. ‘It is easier to act yourself into a new way of thinking, than to think you into a new way of acting’ Behavioural psychologists said. They should design some features to minimize or eliminate human errors. This approach supports much accident prevention. The other way can be designing out human error, for example: administrator-only modification of software components. Although by practice and training the knowledge base can be increased, it cannot work of memory.

4. MECHANISMS TO MITIGATE HUMAN ERRORS – TECHNICAL PERSPECTIVE

Ronald Clarke (1981) provided the set of 25 techniques crime prevention [9]. The techniques are divided into five categories: reducing the rewards; increasing the effort; increasing the risks removing excuses; and reducing provocation. Table 1 shows the techniques that are applied to activities to prevent computer crime. It shows a range of security related prevention efforts which reduce opportunities for mitigating human error, they are shows in italics.

Table 1: Techniques of Crime Prevention Applied to computer Security (Adapted from R. Verhaaf 2006 [10])

Increase the effort	**Increase the risk**	**Reduce the rewards**	**Reduce provocations**	**Remove excuses**
1. Target Harden ● *firewall* ● *phishing filter* ● *encryption* ● *patch management* ● antivirus software ● robust software development	**6. Extend Guardianship** ● remote tracking of use	**11. Conceal targets** ● security policy through trusted connected systems	**16. Reduce frustrations and stress** ● do not overwhelm the user	**21. Set rules** ● *security policy* ● *usage policy and protocols* ● *implement best practice standards*

2. Control access to facilities ● *authentication* ● *monitoring incoming email* ● access control groups	**7. Assist natural Surveillance** ● informant email address ● expert or community ratings	**12. Remove targets** ● air-gap sensitive systems	**17. Avoid disputes** ● political mediation ● clear policy on acceptable use	**22. Post instructions** ● security policy ● policies on use of portable data devices
3. Screen exits ● *monitoring systems* ● *monitoring outgoing email and webmail* ● IDS (Intrusion Detection Systems)	**8. Reduce anonymity** ● *authentication* ● *digital identification*	**13. Identify property** ● *digital signatures/certificates* ● Registrar of property (control access to data – audit trails)	**18. Reduce emotional Arousal** ● awareness building ● remove provocations	**23. Alert conscience** ● User warnings (ex. IP stamps) ● *awareness campaigns*
4. Deflect offenders ● honeypots	**9. Utilize place managers** ● moderators ● users through awareness building	**14. Disrupt markets** ● *ISPs to provide protection against phishing, viruses and spyware*	**19. Neutralize peer pressure** ● *awareness building*	**24. Assist compliance** ● secure, robust Applications
5. Control tools/weapons ● restrictive or authenticated use of IT ● *authentication* ● *digital identification* ● IP address linked to specific User	**10. Strengthen formal surveillance** ● *monitoring systems* ● *publicly portray security accreditation*	**15. Deny benefits** ● *immediately fix vulnerabilities* ● *encryption* ● *back-ups* ● *limit new vulnerability publicity* ● *computer or data 'kill' technology*	**20. Discourage imitation** ● negative publicity for bad practice	**25. Control drugs and alcohol** ● *ban their consumption by personnel in critical posts (e.g. physical or IT security)*

Note To Table 1: Tactics Which Can Reduce Human Error Are Shown In Italics.

Using firewalls and phishing filters are reduced the chances and so reduces the human errors relating to risky computer use. The other way can be keeping a backup of data, it does not any elimination by accidentally delete, disrupt or steals. The backups are reduced recover the data when they accidentally deleted, and also the damage done by cruel effort to destroying data [11].

Patch updated and automated software loading reduce human error, they remove the activated requirement by users for loading updates. Using the software that manage the incoming and outgoing emails reduce the general misuse of email and encourage good practice. This software will check sensitive attachment data and reduce the possibility of human errors which are loading to data disclosure to the wrong addressee.

In contrast, clear protocol and policies do not make it harder to commit error, or to abuse or misuse data, they just remove any excuses and clarify of doing careless action. They will good practices that reduce human error. Therefore, many existing security efforts contain some designing to mitigate human errors. Some mentioned tactics work with more than one mechanism. For instance, honeypots are used for the tracking and detection of offenders, but a main role of honeypots is to prevent attacks away from more in danger parts of network, and here they are included under technique of preventing offenders.

As the other typologies, the set of techniques that focus on the great deal of information and additional setting security issues is a heuristic device. The given brief explanations and coverage does not do justice to the value of this framework. Moreover, the development of new security tactics is the aim so the set of techniques are view as one component to solve the problem of human errors.

5. DISCUSSIONS ON LIMITATIONS OF EXISTING TECHNICAL SOLUTIONS

Through daily improvement of technology and computers network, we have a long way to solve human errors. Most of the discussed techniques here are far from ubiquitous, and they are difficult to implement appropriately.

In the other hand, since human operator error is not likely to disappear anytime in the reliability of computers systems, so it is important to continue and improve the state of the art in human error acceptance. This should be done both by enhancing and pursuing the present approaches here. And it also achieved by developing innovative new approaches that can deal with human error efficiently, effectively, and at low implementation cost.

6. CONCLUSIONS

Computers technology and networks played a significant role in knowledge and overcoming barriers to economic prosperity and innovation. People can lose their confidence in communications and feel control in computer-related technology with the huge impact of socio-economic activity is one of the characteristics of inadequate security.

One of the implicit aims of designing framework for human error is to minimize the need for training, education and culture relating to the security. Since human awareness of a problem is useful but the best security is that does need a particular cooperation of human users, where possible, the default option should be secure. Explicit action to over the security is offence and based on the definition, the open action is not an error.

REFERENCES

[1] Reason, J. (1990). *Human error*. Cambridge University Press.

[2] Rasmussen. J. (1986). Information Processing and Human-Machine Interaction. North-Holland, New York, 3.

[3] Wallace, B. and Ross, A. (2006). *Beyond human error*. CRC Press.

[4]Roth, E. et al. (1994). *An empirical investigation of operator performance in cognitive demanding simulated emergencies. NUREG/CR-6208, Westinghouse Science and Technology Center*. Report prepared for Nuclear Regulatory Commission.

[5]Senders, J. and Moray, N. (1991). *Human error: Cause, prediction, and reduction*. Lawrence Erlbaum Associates. User education is not the answer to security problems. Alertbox, 2004.

[6] Norman, D. (1988). *The psychology of everyday things*. Basic Books.

[7] Brown, A. B. (2004). Coping with Human Error in IT Systems. 35-41.

[8] Nielsen. J. (2004) User education is not the answer to security problems. Alertbox.

[9] Cheswick's B. keynote at the 1st Symposium on Usable Privacy and Security (SOUPS 2005) proposed 'Windows OK': a stripped down version of the operating system to suit the large number of computer who just need basic Internet access.

[10] Verhaaf. Cyberterrorism. R. (2006) Thesis submitted to the Midlands Centre for Criminology and Criminal Justice, Loughborough University. Loughborough, 2006.

[11] Clarke's first version appeared in the British Journal of Criminology in 1981. For the most recent statement see Cornish, D.B. and R.V. Clarke. Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention in M.J. Smith and D.B. Cornish (Eds.) Theory for Practice in Situational Crime Prevention, Vol. 16 of Crime Prevention Studies. Cullopmpton: Willan Publishing, pp. 41-96, 2003.