ISSN No. 2278-3091

Volume 1, No.3, July – August 2012
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://warse.org/pdfs/ijatcse01132012.pdf

Human Errors in Information Security

Munir Ahmed, Lukman Sharif, Muhammad Kabir & Maha Al-Maimani
London College of Research, School of Computing,
43 West Street, Reading, RG1 1TZ, United Kingdom
m.ahmed@lcrl.org.uk

ABSTRACT

The purpose of the paper is to target audience and stakeholder individuals whom are in charge of securing the assets of their organisations and institutions. This paper starts by providing a brief overview of information security, outlining the main goals and techniques of the discipline. The paper also discusses the role of human factors and how the information security research community has recognised the increasingly crucial role of human behaviour in many security failures. This is followed by a literature review of human errors in information security. Finally, this paper discusses Reason's Generic Error Modelling System (GEMS) as a potential model for explaining human errors in information security [18]. The terms computer security, network security and information security are used interchangeably in this paper.

Key Words: Information Security, Network Security, Computer Security, Human Errors, Human Computer Interaction

1. INFORMATION SECURITY OVERVIEW

In recent years, information security has received much attention from various industry sectors, organisations, enterprises, and governments. In general, this can be attributed to the recent increases in security breaches resulting in major losses for the affected enterprises.

The fundamental concepts and models used to describe security processes are set down in international standards [24]. According to [12], [20] and [9], computer information security has several major principles that it strives to uphold: confidentiality, data integrity and availability. These principles of information security are upheld with the use of three main techniques: prevention, detection and response [13] and [14]. The bedrock on which these principles and techniques are built is the ability to distinguish between authorised and unauthorised users. The process by which this occurs is called user authentication, whether the user logs on to the authentication system from home, work or anywhere in the world.

For organisations and users facing security threats against their assets, there are security policies that govern how the assets are managed and protected. However, this transfers the cost to the users and organisations. Therefore, users and organisations must seek to minimise the impact of information security breaches. Although many effective countermeasures, technologies and solutions exist for many of these breaches and threats, unfortunately in most cases they are not correctly and effectively implemented.

2. HUMAN FACTORS IN INFORMATION SECURITY

Within the computer information security industry, much attention is often focused on technical aspects with some organisations viewing technical solutions as the immediate answer to their information security problems. However, technology alone cannot deal with all information security risks; it is the people in organisations that are the primary line of defence [10] and [11]. Although security technologies such as firewalls, antivirus software, and VPNs are valuable weapons in an organisation's information security armoury, pursuing a purely technological approach presents severe drawbacks.

Information security is ultimately about people. Much of the research into the methods used by hackers and attackers to compromise IT systems illustrates that the human element is always crucial to the majority of successful attacks. Simple configuration mistakes by careless employees can render network ports open, firewalls vulnerable and entire systems completely unprotected. In reality, human error is far more likely to cause serious information security breaches than technical vulnerabilities [7] and [23].

The security research community has recognised that human behaviour has a crucial role in many security failures. In information security literature, humans are often referred to as the weakest link in the security chain. Although human behaviour and resulting errors often facilitate security breaches; the issue is not adequately addressed by many current security models. Information security researchers e.g. [25] and practitioners e.g. [26] have called with increasing frequency for the human factors to be considered in the design and review of security in IT systems.

Human Computer Interaction (HCI) is a fast emerging discipline that already considers the human aspects of computing. The goal of the HCI is to reach an optimal balance between two criteria of system performance: task quality (how good the product is) and cost of achieving that quality (for the user, stakeholder, the computer system) [27]. It has been argued that HCI research should seek to build validated theory and models that can make the knowledge gained through practice more easy to re-use in order to give a better probability of successful design [27].

Information security research has had little penetration into the traditional HCI community. A review concluded that there is little work that moulds technical security issues with a wider HCI perspective, particularly in the areas of theories, models and frameworks [28]. In particular, there is a lack of empirical research in the field of information security and human errors. The results of a study by [1] and [5] reveal limited research in the area of human errors in information security at the organisational level. One possible reason for this could be due to organisational unwillingness to share information and statistics on security. However, research in this area is important because user concern for information privacy has the potential to affect the future of e-commerce.

Information security has traditionally been thought of as a hardware and software problem. However, recent statistics [12] have shown that an overwhelming percentage of information security breaches are caused by human factors such as lack of information assurance knowledge, inadequate training, and a general failure to follow security procedures [2]. Many organisations focus exclusively on technological controls while ignoring the threat of human errors resulting in costly financial losses. Although technical solutions are also very important, unfortunately, they do not address the ignorance or omission of the people using IT systems. IT administrators and information security professionals often spend a lot of time discussing and exchanging ideas about new and emerging security threats; unfortunately these conversations do not educate end users [8].

3. HUMAN ERRORS IN INFORMATION SECURITY

It has been reported that human errors contribute to more than 80% of the accidents in venues, ranging from air transport operations to nuclear power plants [12] and [29]. If we conservatively estimate that human error impact on security practices is two-thirds of that of safety accidents, we are still left with human error involvement in the majority of security incidents.

It is not possible to separate the human from the technology factors. In order to achieve a given task, both elements are indispensable. Today, there are very few professions that can claim to get by without the help of machines. At the same time, machines do not have intuition and intelligence. They require instructions in the form of commands such as setup, start and stop operations. The human worker can receive feedback from the machine, e.g. control parameters, alarms and other data. Only humans can understand such machine data, analyse it and transform it into new machine inputs. Humans are not ready to live in a fully automated society. An attempt by Airbus to develop fully automated airliners was rejected by consumers. Interaction between humans and machines will always exist [4].

Both machines and humans are subject to errors and can influence the quality of a product. Although ultimately every failure can be put down to a human mistake. Our society tends to always search for someone to bear the responsibility of an accident or error. In that sense, humans are under constant pressure and hold the responsibility for the quality of the end product.

The way humans think is very complex. Humans are subject to many influences. In general, these can be divided into two types: internal or external. The internal influences are those defined by the organisation's environment; whilst external ones relate to everyone's private life. Humans are not perfect, and for that reason, workers will always be prone to make errors.

Depending on the nature of the industry, the errors could result in huge losses. As such, potential human errors cannot be ignored in a thorough risk analysis. There could be many different reasons for human errors, including carelessness, inadequate training, lack of supervision, lack of concentration, etc.

4.REASON'S GENERIC ERROR MODELLING SYSTEM

In order to prevent such human errors from occurring in information security contexts, it is important to identify the different types of human errors and inform users of the possible risks and put in place strategies to avoid them. Within the field of human factors, various models and concepts have been developed for understanding and characterizing various types and levels of human error. These models and concepts have been successfully applied in various industries to analyze the causes of accidents [17]. In [18] and [19], Generic Error Modelling System (GEMS) explores the cognitive mechanisms involved in human error as well as the role of organizational and management factors in the creation of error-prone conditions [17]. This model offers a potential framework for explaining human errors in information security.

In [18] GEMS model, mental operations can be in either attentional mode or schematic control mode.

4.1 Attentional Mode

This mode is concerned with the consciousness and the working human memory of the user. This type of mode is slow, requires effort and is difficult to sustain for a prolonged period of time. This mode is typically used by humans for tasks such as goal setting, monitoring progress, recovering from errors/mistakes, etc. In the context of security, a user may use this mode for recalling their system logon details such as username / password.

4.2 Schematic Control Mode

The mode helps to processes familiar information very quickly. It does not require any conscious effort or great mental exertion. This mode is not limited in terms of the amount or duration of the stored information.

Within the various cognitive processing stages, different types and levels of human error may occur.

4.3 Categories of Behaviour to Distinguish Types of Error

In [18] postulates that human errors may be divided into categories of behaviour based upon an individual's level of performance. The errors could be distinguished by both psychological and situational variables.

Skill-based Errors

These types of errors are made with routine, are automatic and unconscious. They occur under schematic control mode. Errors of this type are known as slips, unintended actions, or lapses.

Rule-based Errors

This type of behaviour selects and applies formerly stored rules to the information. For most part it is automatic and unconscious. This type of behaviour occurs when a change is needed to modify the automatic behaviour found at the skill-based level. The user may apply a memorised rule with periodic checks to monitor the progress and outcome of the action.

Knowledge-based Errors

This type of behaviour operates under first principles and occurs under attentional control. Knowledge-based behaviour only occurs after repeated failure and without a pre-existing solution.

In general, the majority of errors are likely to be skill-based, not rule- or knowledge-based.

The National Research Council Computer Science and Telecommunications Board [6], has distinguished between two main types of human error: accidental and deliberate. Accidental causes are non-deliberate and unintentional, e.g. a programming error that causes a system to crash. Whilst deliberate causes are referred to as attacks whereby the perpetrator seeks to cause damage deliberately. In this paper, the term human error encompasses both categories.

In [18], the model reinforces the fact that humans will always be the weakest link in the overall process. Recently, information security researchers have begun focussing on human errors, producing statistics identifying it as a large component of problems in computer security. In the Global Financial Services Industry (GFSI) Security Survey [7], reveal that the majority (86%) of respondents confirm that human error is the leading cause of information systems failure. [15], [3] and [16] cite the National Institute of Standards and Technology, where 65% of the economic loss attributed to information security breaches was caused by human error, whereas only 3% of the loss was attributed to malicious outsiders as shown in table 1. In [3] and [22], found that 41% of security incidents were caused by human error, whereas only 9% were due to wilful crime.

Table 1: Percentage of economic loss due to information security breaches; Adapted from [16]

Percentage of Economic Loss	
Violations (22%)	Errors (65%)
Sabotage ➢ 3% malicious outsiders ➢ 13% dishonest employees ➢ 6% disgruntled employees	Slips and Lapses ➢ Skill based errors mistakes ➢ Rule based errors ➢ Knowledge based errors

Although much of the statistics produced to date focus on human errors in organisational settings, there is no significant research and statistics on human error improvement / mitigation techniques.

Human errors by computer users can cause information security breaches in a variety of ways. These errors could be caused as a result of lack of computer knowledge, technical errors or simply carelessness on the part of the computer users.

We live in the internet age and more and more people have access to a computer. However, the vast majority of people only know the very basics of using a computer; e.g. sending emails, web browsing, word processing, etc. Most users do not know or understand the importance of security measures such as anti-virus software, firewalls, regular updates and patches [21]. Such users quite easily become targets of malicious software and hackers. This type of user error can result in a computer being compromised and used as a launch pad for further attacks on other unprotected systems.

Sometimes even expert programmes who develop and build operating systems and applications can commit serious errors. In most cases, these errors are not intentional but they can create security loopholes in the software that can allow hackers to gain control of affected systems. Although once discovered, it is possible to address such security loopholes through software patches, such patches may not always be applied by the system administrators or end users due to negligence.

Carelessness is perhaps one of the most common and fatal causes of human errors in information security contexts. Carelessness can be linked to many common security breaches, e.g. users writing passwords on sticky notes left on keyboards, users accessing harmful websites despite repeated warnings displayed by their web browsers, workers blatantly ignoring and failing to follow proper security policies and procedures.

The U.S. Department of Homeland Security conducted an interesting experiment aimed at finding out how easy it would be for hackers to corrupt workers in order to gain access to computer systems [8]. This involved secretly dropping computer discs and USB sticks in the car parks of government buildings and private contractors. Almost 60% of those who picked them up, plugged the devices into office computers. Furthermore, if the drive or CD had an official logo, 90% were installed on the employee's computer.

Careless and untrained insiders are an even greater threat to organisations. This includes workers who fall prey to social engineering attacks as well as malicious and disgruntled employees. Businesses lose millions due to security breaches, most of which are linked back to human errors. Regardless of the investments in physical and software security measures, most organisations are vulnerable to some of the most basic security risks. A balanced combination of policies, procedures, training and technology could help to mitigate the risk of human errors for organisations.

5. CONCLUSION

This paper has provided an overview of information security, human factors in information security and a literature review of human errors in information security contexts. This paper has also discussed Reason's Generic Error Modelling System (GEMS) as a potential model for explaining human errors in information security [18].

The future paper will outline the research methodology used in information security human errors research for investigating the causes and remedies of human errors in information security contexts. This will involve asking open-ended questions to information security experts. The responses to open-ended questions will be analysed using grounded theory, leading to the development of a theoretical model.

ACKNOWLEDGEMENT

This research has been funded by London College of Research, UK and has been supervised by Dr Margaret Volante, Middlesex University, London, UK.

REFERENCES

1. Basu, A. and Muylle, S. **Authentication in E-commerce,** Communications of the ACM, 46(12), pp.159–166, 2003.

2. Bean, M. **Human Error at the Center of IT Security Breaches,** Newhorizons.com, February 2008. Online at http://www.newhorizons.com/elevate/network%20defense%20contributed%20article.pdf. Accessed on 20th March 2012

3. Brostoff, A. **Improving password systems effectiveness**, PhD thesis, UCL, UK, unpublished, 2004.

4. Bubb, H. **Human reliability: a key to improved quality in manufacturing**, Human Factors and Ergonomics in Manufacturing, 15(4), pp.353–368; Wiley Periodical, 2005.

5. **Business Software Alliance** (2002). Information Security Governance: Toward a Framework for Action, http://www.bsa.org/country/ Research%20and%20Statistics/~/media/BD05BC8FF0F04CB D9D76460B4BED0E67.ashx. Accessed 29 April 2009.

6. Computer Science and Telecommunications Board-National Research Council (2002). **Cybersecurity Today or Tomorrow: Pay Now or Pay Later.** National Academy Press, Washington, DC.

7. Deloitte (2008). **Global Financial Services Industry (GFSI) Security Survey**. Online at http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/Financial%20Services. Accessed on 15th March 2012.

8. Edwards, C., Kharif, O., and Riley, M. (2011). **Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy**, Bloomberg, June 2011. Online at http://www.bloomberg.com/news/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy.html. Accessed on 13th March 2012.

9. Garfinkel, H. **Studies in ethnomethodology**, Eaglewood Cliffs NJ: Prentice Hall, 1967.

10. Hansche, S. D. **Making Security Awareness Happen**. In H. F. Tipton & M.Krause (Eds.), *Information Security Management Handbook* (4th ed., Vol. 3, pp. 337-351). New York: Auerbach Publications, 2002.

11. Hare, C. **Policy Development**. In H. F. Tipton & M. Krause (Eds.), **Information Security Management Handbook** (4th ed., Vol. 3, pp. 353-383). New York: Auerbach Publications, 2002.

12. Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G., and Williams, T. **Gray Hat Hacking**, The Ethical Hacker’s Handbook, Third Edition, McGraw Hill, 2011.

13. Howard, P. D. **The Security Policy Life Cycle: Functions and Responsibilities**, In H. F. Tipton & M. Krause (Eds.), **Information Security**

Management Handbook (4th ed., Vol. 4, pp. 999). Boca Raton: CRC Press, LLC, 2003.

14. Maiwald, E. **Network Security**, 2nd Edition, McGraw Hill, 2003.

15. McCauley-Bell, P. **Predictive modeling to evaluate human impact on Internet security**. Paper presented at the HFES99, Houston, TX, 1999.

16. NIST (1992). ***1991 Annual Report of the National Computer System Security and Privacy Advisory Board.*** National Institute of Standards and Technology.

17. Reason, J. **Managing the Risks of Organizational Accidents**. Ashgate, Brookfield, 1997.

18. Reason, J. **Human Error,** Cambridge, UK: Cambridge University Press, 1990.

19. Reason, P and Rowan, J (eds), (1981), **Human inquiry: a sourcebook of new paradigm research**, Chichester: John Wiley.

20. Reed, D. **A Balance Introduction to Computer Science** *(3rd edition)*, Pearson Prentice Hall, 2010.

21. Roberts, P (2004). **AOL survey finds home user ignorant to online threats,** ComputerWeekly, April 2010. Online at http://www.computerweekly.com/news/2240058434/AOL-survey-finds-home-user-ignorant-to-online-threats. Accessed on 10th March 2012.

22. Spruit, M. E. M., and Looijen, M. **IT security in Dutch practice**, *Computers and Security*, 15(2), pp. 157–170, 1996.

23. Swanson, M., and Guttman, B. **Generally Accepted Principles and Practices for Securing Information Technology Systems**. Washington D. C.: U.S. Department of Commerce, National Institute of Standards and Technology (NIST), 1996.

24. BSI. (1996). **Information technology — Guidelines for the management of IT Security—** Part 1: Concepts and models for IT Security (BS ISO/IEC TR 13335-1:1996). London: BSI.

25. Whitten, A., and Tygar, J. D. **Why Johnny can't encrypt: a usability evaluation of PGP 5.0**, Paper presented at the 9th USENIX security symposiom, Washington, 1999..

26. Zurko, M. E., and Simon, R. T. **User Centered Security,** Paper presented at the New Security Paradigms Workshop, Lake Arrowhead,CA, pp.17-20, 1996.

27. Dowell, J., & Long, J. (1998). Conception of the cognitive engineering design problem. Ergonomics, 41(2), 126-139.

28. Dhillon, G., and Backhouse, J. **Current directions in IS security research: towards socio-organisational perspectives,** Information Systems Journal, 11, pp.127-153, 2001.

29. Hollnagel, E. **Human Reliability Analysis: Context and Control**, London: Academic Press, 1993.

AUTHOR BIOGRAPHIES

Professor Dr Munir Ahmed is a professional member of the Institution of Engineering and Technology (MIET), United Kingdom (UK). He is completing his DProf - Doctor in Professional Studies (Computer Communications Engineering - Information Security) with Middlesex University, London, UK in October 2012. He has completed partly his EdD - Doctorate in Education (Information Communications Technology) from University of Greenwich, London, UK in 2006. He earned his PhD in Digital Communications Systems Engineering from London Institute of Technology, London, UK in 1997; his MSc in Information Systems Engineering – Computer Networking from South Bank University, London, UK in 1994 and BSc in Electrical Engineering – Electronics and Telecommunications from the University of AJK, Kashmir in 1990. He holds permanent positions as Professor of Computer Networks and Security Engineering, Chairman of Advisory Board and Director of Research at London College of Research, Reading, UK. Since August 2006, he works for Taibah University, Saudi Arabia as Professor of Computer Networks and Communications Engineering on contractual basis. He is a leader of Security Engineering Research Group (SERG) - London, UK. He is also a reviewer of different international journals. He has extensive experience in the commercial sector and has held a variety of high-level positions in the industry, including Chief Executive Officer (CEO), Chief Operations Officer (COO), Training Director and Chief Network Architect in the UK. His current research activities aim to consolidate his skills and extensive commercial experience with various research areas in the field of Computer Networking and Communications Engineering. His particular areas of focus include Wireless Sensor Networks, Routing Protocols, and Information Security. Professor Ahmed has gone to author or co-author 6 books with leading international publishers in Germany and has had above 250 advanced research activities including papers and articles in international journals and conferences; technical manuals, workshops and presentations in industrial milieu.

Lukman Sharif is a professional member of the Institution of Engineering and Technology (IET). He gained his Bachelor's degree from London Metropolitan University in Computer Networking. He has worked in the IP communications industry for over a decade as a Network Architect and Consultant. He is currently a Senior Lecturer in Computer Networking and Information Security at London College of Research, UK. His research interests include IP routing and security in Mobile Ad-Hoc Networks.

Muhammad Kabir received his PhD in Computer Science at the University of Braunschweig, Germany. He is a member of Advisory Board of London College of Research, Reading, UK. He is also an Assistant Professor at the Department of Computer Science, Taibah University in KSA. His research interests include is- sues related to numerical methods, embedded systems and combustion engines.

Ameera Al-Rehili has completed her BSc in Computer Science at Taibah University, al-Madinah, KSA in June 2012. Her area of research interest is Artificial Intelligence, Translating and communication systems.