International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 1 Issue 1 ǁ May. 2013 ǁ PP.26-35

Human Errors In Computer Related Abuses

LeylaRoohi[1], ParisaGerami[2], RezzaMoieni[3]
[1,2,3] UniversitiTeknology Malaysia (UTM) Malaysia

***Abstract*—**This is a survey paper about impact of human error on computer crimes. Model of human error and human factor will review in this paper and impact of these errors with different case study and model will be reviewed. Micro ergonomic frame work that is a conceptual model will describe completely too.
***Keywords*—**Human error, Computer crime,Conceptual model

I. Introduction

Computer crime is an unfortunate artifact of today's wired and global society, as individuals involved in criminal behavior have embraced technology as a method for improving or extending their criminal tradecraft.

According to the Computer Security Institute, these are the types of computer crime and other losses like: 20% physical security problems (e.g., natural disasters, power problems), 10% insider attacks conducted for the purpose of profiting from computer crime, 9% disgruntled employees seeking revenge, 4% Viruses, outsider attacks 1-3%, but 55% of computer crimes and lossesbelongs to human errors. That is a large amount that should be considered. For example the Western Union was attacked by an attribution of human error in autumn 2000 when a hacker entered one of Western Union's computer servers electronically with no permission. In this attack about 15,700 customer credit card numbers were stolen. The incident happened after the system was taken down for regular maintenance, and a file containing the credit card information had unintentionally been left unprotected when the system was returned to operation[1]. HSG48 (1999) provides one classification of types of human failure as human errors and violations. In these classification two main categories: skill based errors and mistakes are known for human errors.National Research Council Computer Science and Telecommunications Board (2002) put the errors caused by human in the category of accidental causes.

Moreover, the field of human factors has developed models and concepts for understanding and characterizing varying types and levels of human error, which have been used successfully in various industries to analyze causes of accidents [8]. These taxonomies not only explore the cognitive mechanisms involved in human error [7], but also emphasize the role of organizational and management factors in the creation of error-prone conditions [8].

Many approaches and models are introduced for describing and evaluating the role of human error and human factors in incidents, and for addressing the source of human factors and error. Following is a survey of these models and case studies that have used these models and also human errors and computer crimes categories.

II. HUMAN ERROR MODELS

Accidents can occur through people's involvement with their work, it is estimated that up to 80% of accidents may be attributed, at least in part, to the actions or omissions of people (Health and Safety Guidance 48, 2003). Figure 1 is the human failure classification according to (HSG).

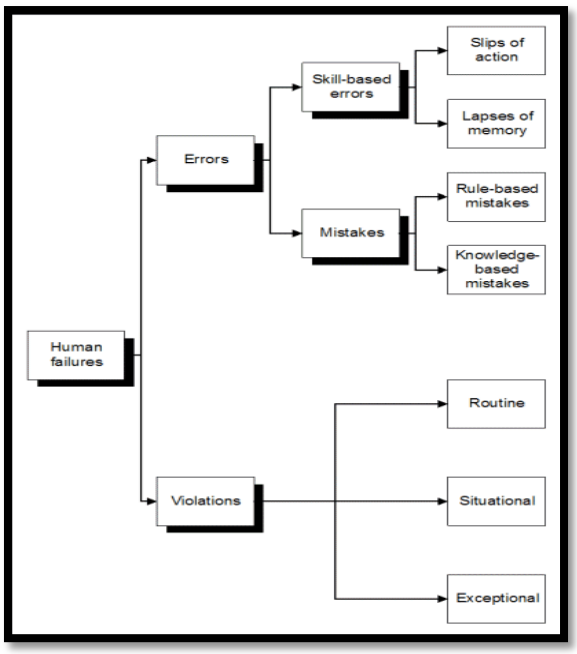

Figure 1: Human Failures Classification

Slips and lapses: describe failures occurring on the level of action course (mistakes in attention and thus fallible perception of the environment or mistakes on recall ofaction sequences). [10] considers the following scenario to be a typical“ slip:”„My office phone rang. I picked up the receiver and bellowed ‚Come in’ at it.”In contrast, failures in planning of actions are referred to as „mistakes“. Although the proper action is carried out correctly, the preceding cognitive steps have processed erroneously.

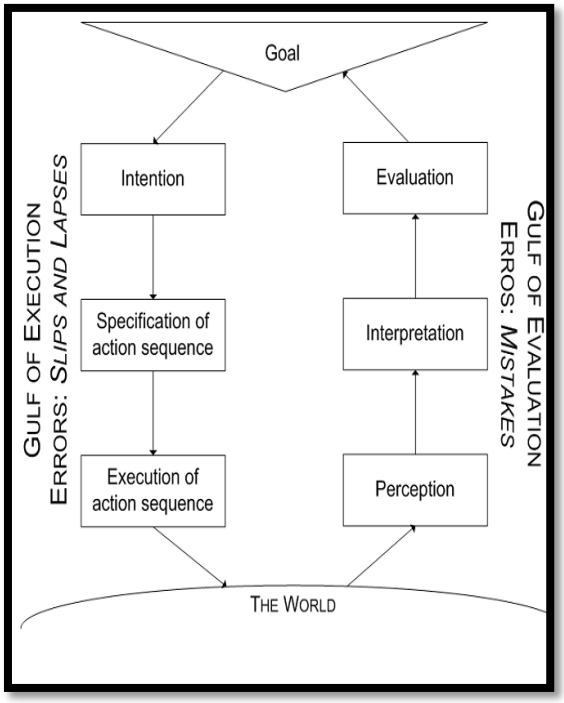

Figure 2: Planning and course of action [2]

*A. **Skill-based behavior***

It is identified as amount of all actions running semi- or fully-automatic as the needed skills to their execution are available and internalized by the operator. Performing this behavior, cognitive resources can be freed for more demanding operations (e.g. problem solving).

B. Rule-based behavior

Describes actions based on externally prescribed rules. The operator does not need any knowledge in order to be able to execute them. As emergency plans have to be completed step by step in a dangerous situation, they perfectly fit into this category.

C. Knowledge-based behaviour

Knowledge based behavior is referred to as generation of action plans based on implicit and explicit knowledge about the system and process. Especially in new and unknown situations, the operator has to be able to generate actions referring to his existent knowledge in order to eliminate difficulties. Thus, this cluster of actions requires most cognitive resources.

[8] tries to classify the already known error types (slips, lapses, mistakes) to the possible operators' actions described in the model of [6]. At this juncture, slips and lapses are assigned to the "skill-based behavior".[10] describes slips as mistakes on execution of activities running semi- or fully-automatic, i.e. actions that do not have to be controlled consciously.

In contrast, "rule-based behavior" and "knowledge-based behavior" in [6] can, following the classification of [8], be described as mistakes: If execution of actions depends on rules (rule-based behavior) or knowledge (knowledge-based behavior), mistakes in planning processes can occur.

Hereby, common biases like heuristics, known from cognitive and psychological science, play an important role. The classification of mistakes according to [8] is demonstrated in Figure 3.

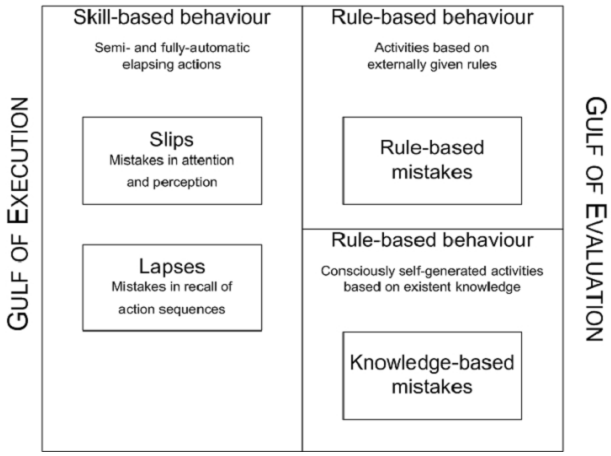

Figure 3: Classification of mistakes[8]

III. COMPUTER CRIME CLASSIFICATION

Computer crime has been defined as any offences that utilize computer or anything which is involved to a computer.. Computer crime has defined by department of justice to any violation of the criminal law that engages the knowledge of information technology for its perpetration, investigation, or prosecution. Other definition is to perceiving opportunities to invade computer systems to achieve criminal ends or use computers as instruments of crime [12]. There are several classes of activities which may also harm information systems and supporting technology. These activities may result in criminal charges depending upon the circumstances and impact on information systems. Currently, these activities fall within classes of viruses, worms, Trojan horse, time bomb, logic bomb, and trapdoors. Logic bombs are software attacks that triggered by a predetermined event. The most common logic bombs occur when information technology employees are laid off from employment. Then, for example, billing systems go awry when an employee id number is no longer on the payroll database.

There are other types of computer crime such as traditional crimes that happen on computers contain fraud, theft, harassment and child pornography. Computer fraud consists of crimes such as online auction fraud, financial and telecommunications fraud, credit card fraud. Harassment and cyber talking, child pornography crimes contain both the sending media which exploits children and also to commit sexual crimes against minors.

Computer crime can be classified by the type of activity which occurs. Four basic categories for computer crime are theft, fraud, copyright, infringement, and attacks.

D. Theft

Theft in computer crime may refer to remove physical object such as hardware or remove or edit information from other person computer without authorization also altering computer input or output without authorization, destroying or misusing. Theft crimes include monetary, service and data theft and privacy.

E. ***Computer Fraud***

Computer fraud is a subset of computer crime and it uses electronic resources to submit fraudulent or misrepresented information as a means of deception, it also refers to as Internet fraud. Unauthorized Access is an important and crucial form of computer crimes and computer fraud. It causes to electronic intrusion, or gaining access to resources via a computer resource without permission.

F. ***Phishing***

Phishing defines as a form of online identity theft that sends fake emails to recipients or use a fake website to trick them and stole financial data such as credit card and numbers or username and password.

G. ***Denaial of Service***

The aim of this kind of attack is to interrupt a legitimate user from having access to the service. The intruder can execute this method in a lot of ways such as limit or prevent access by overloading available resources or modify the configuration of the services, destroy the available connection to data physically.

IV. BRRIEF HISTORY OF COMPUTER CRIME

Every field of study and expertise develops a common body of knowledge that distinguishes professionals from amateurs.
1One element of that body of knowledge is a shared history of
significant events that have shaped the development of the field

Table1: A brief history of computer crime

Year	Location	Description
1968	Olympia, WA	A pistol toting intruder shot an IBM 1401 two times
1970	University of Wisconsin	Bomb kills one and injures three people and destroys $16 million of computer data stored on site
1970	New York University	Radical students place fire-bombs on top of Atomic Energy Commission computer in attempt to free a jailed Black Panther
1972	Johannesburg	South Africa: municipal computer dented by four bullets fired through a window
1972	New York	A person with a sharp instrument attacked magnetic core in Honeywell computer which caused $589,000 of damage.
1973	Melbourne, Australia	American firm‘s computer was shot by antiwar protesters with double-barreled shotgun.
1974	Charlotte, NC	Charlotte Liberty Mutual Life Insurance Company computer was attacked by a frustrated operator.
1977	Rome	Four terrorists pour gasoline on university computer in Rome and burned it.
1978	Vandenberg Air Force Base, California	A peace activist destroys an unused IBM 3031 using a hammer, a crowbar, a bolt cutter and a cordless power drill as a protest against the NAVSTAR satellite navigation system, claiming it gives the US a first-strike capability
1994	New York City	Levin masterminded a major conspiracy in which the gang

		illegally transferred $12M in assets from Citibank to a number of international bank accounts. The crime was spotted after the first $400,000 was stolen in July 1994 and Citibank cooperated with the FBI and Interpol to track down the criminals.
1993	U.S.A	when four executives of a Value Rent-a-Car franchise in Florida were charged with defrauding at least 47,000 customers using a salami technique
1988	U.S.A	The infamous Jerusalem virus (also known as the Friday the 13th virus) of 1988 was a time bomb. It duplicated itself every Friday and on the 13th of the month, causing system slowdown; however, on every Friday the 13th after May 13, 1988, it also corrupted all available disks on the infected systems.
2000	U.S.A	e-mail users opened messages from familiar correspondents with the subject line ―I love you; many then opened the attachment, LOVE-LETTER-FOR-YOU.txt.vbs which infected the user‘s e-mail address book and initiated mass mailing of itself to all the contacts.
2004	U.S.A	the Department of Justice (DOJ) indicted 19 of the leaders of Shadowcrew.122
2005	U.S.A	According to industry security experts, the biggest security vulnerability facing computer users and networks is email with concealed Trojan Horse software—destructive programs that masquerade as benign applications and embedded links to ostensibly innocent websites that download malicious code. While firewall architecture blocks direct attacks, email provides a vulnerable route into an organization‘sinternal network through which attackers can destroy or steal information.

V. DIFFERENT APPROACHES

There are various existing approaches for describing and evaluating the role of human errorand human factors in incidents, and for addressing the source of human factors and error. Some of them are Swiss Cheese model of defense, Micro ergonomic approach, Macro ergonomic approach, Human and Organization Factors(HOF), Error Management and Tripod approach , but among them macro ergonomic has attracted more attention for evaluating the role of human errors in incidents[2].

1) Micro ergonomic Framework

To identify and describe the work system elements contributing to human errors that may cause CIS vulnerabilities [2]. This conceptual framework provides a basis for understanding the various linkages of human

and organizational factorsto human error contributing to security (Figure 4). It is a synthesis of various frameworks describing work systems elements (e.g. the macro ergonomic framework) and humanerror (e.g. human error taxonomies). According to the macroergonomic work system modeldeveloped by Smith and [2], a work system may be conceptualized as having five elements: the individual, task, tools and technologies, environment and the organization. The interplay of these elements may create conditions that contribute to human error and violations. These errors may result in security vulnerabilities and sometimes result in security breaches, if the vulnerability is exploited. This framework used the work system model as a guide to define specific categories of elements that may contribute to human errors and violations.The middle section of the framework describes the various dimensions of human errors and violations. Within various cognitive processing stages, different types and levels of human error may occur. Perhaps the most widely known and accepted human error taxonomy is the skillrule- knowledge (SRK) framework of [4]. This framework postulates that errors may be divided into categories based upon an individual's level of performance.

The errors are distinguished by both psychological and situational variables that together define an 'activity space' on to which the three performance levels are mapped. The three performance levels are: (1) skill-based level errors, which are made with routine, highly practiced tasks in a predominantly automatic capacity with occasional consciouschecks on progress. It is thought that in this activity space people perform very well most of the time; (2) rulesbased performance level occurs when a change is needed to modify the automatic behavior found at the skill-based level. At this point the person may apply a memorized or documented rule, with periodic checks to monitor the progress and outcome of the actions; and (3) knowledgebased performance is an activity space met only after repeated failure and without a pre-existing solution. Errors have been categorized as either mistakes or slips and lapses [8][5]. Using [4]'s SRK model of human performance, mistakes can be further categorized into rule-based mistakes and knowledge-based mistakes. Mistakes occur when the action was intended, but turned out to be inappropriate. In contrast, slips and lapses occur when the action (or lack of action) was unintended. For example, a mistake includes applying a security-related patch to the wrong piece of software. A slip or lapse includes forgetting to apply the security-related patch to the appropriate piece of software.

Violations to the human error taxonomy have been added in [12]. Errors and violations are unsafe acts that are assumed to contribute to security vulnerabilities and security breaches. However, violations do not necessarily lead to security vulnerabilities and breaches. [11] proposed the notion of ''safe violations'', which do not systematically lead to undesired events. Rather, when they are coupled with a valid mental model, they can ensure or even increase the security level of the CIS system. Without a correct mental model of a task and of future system states, violations can lead to accidents, or in the case of CIS, vulnerabilities and breaches. The right side of the framework characterizes the resultants of human errors and violations in the CIS organizational context. Vulnerabilities are weaknesses in a system allowing an unauthorized action [13]. Computer and information vulnerabilities may be thought of as ''near misses'' or the accidents ''waiting to happen''. Security breaches are vulnerabilitiesthat have been exploited by an attacker. A security breach is an unauthorized result, which is an unauthorized consequence of an event resulting from an unsanctioned action (i.e. human error) by a user of the system [13].

VI. COUNTER MEASURES

For reducing human error, two main approaches have been proposed. First teach the user to do their job right second prevent them from doing wrong thing. These approaches also have some limitation. Training of human always remains a important part of data management because if the user neglect about security issue, they might mistakenly deteriorate protection.

This approach underpins many efforts in ergonomics where design can significantly influence human behavior (office chairs) or accident prevention. Designing-out human error can also reduce risks due to deliberate deception. For instance, administrator-only modification and execution of critical software components, and cut down versions of operating systems can help minimize security breaches.

Many countermeasures have been considered in order to reduce human error. In the first one, it is better to remove the source of human error and eliminate the hazards; it means that it is impossible an error happens by a good design in the first place. Control the chances of an error by physical means, it means to plan a good controls in order to prevent error or hazards. Supervision the control and monitoring the errors.

2) Case studies

Three case studies have been described in order to illustrate the act of human error in cyber security breaches.

a) Using social engineering to exploit the personal security; case study (1)

Using social engineering to exploit the personal security and gain sensitive information about people through deception, manipulation and influence. It trick employee to reveal data about their computer systems.

This kind of attack is difficult to detect and is non-technical and it depends onhuman interaction with social engineer .The social engineer targets are large organization and financial and bank institutes.

Kevin Mitnick is a famous hacker and he accessed a lot of computer systems of technology companies like Motorola, Nokia and sun. He attempts to steal the source code ofStarTAC from Motorola and show them how social engineering can be effective. He used a mobile phone and registered to a fake name and call Motorola. He pretended to be from R&D company and passed all steps to reach developer assistant .he could convince the assistance that her boss which

was in a vacation was supposed to give him the phone's source code.She tried to send the file through the ftp server address that he provided but the internal security restricts her action. Before he could protest, she spoke to security to find the problem. She get the information of a proxy server outside of the company's firewall, which was used to send the source code. It wasOnly after four calls demanding different versions of the source code so the con was discovered. The Motorola employee discovered that the phone number he had left her was fake when she tried to call him back to inform him that she had to rush off to a meeting.

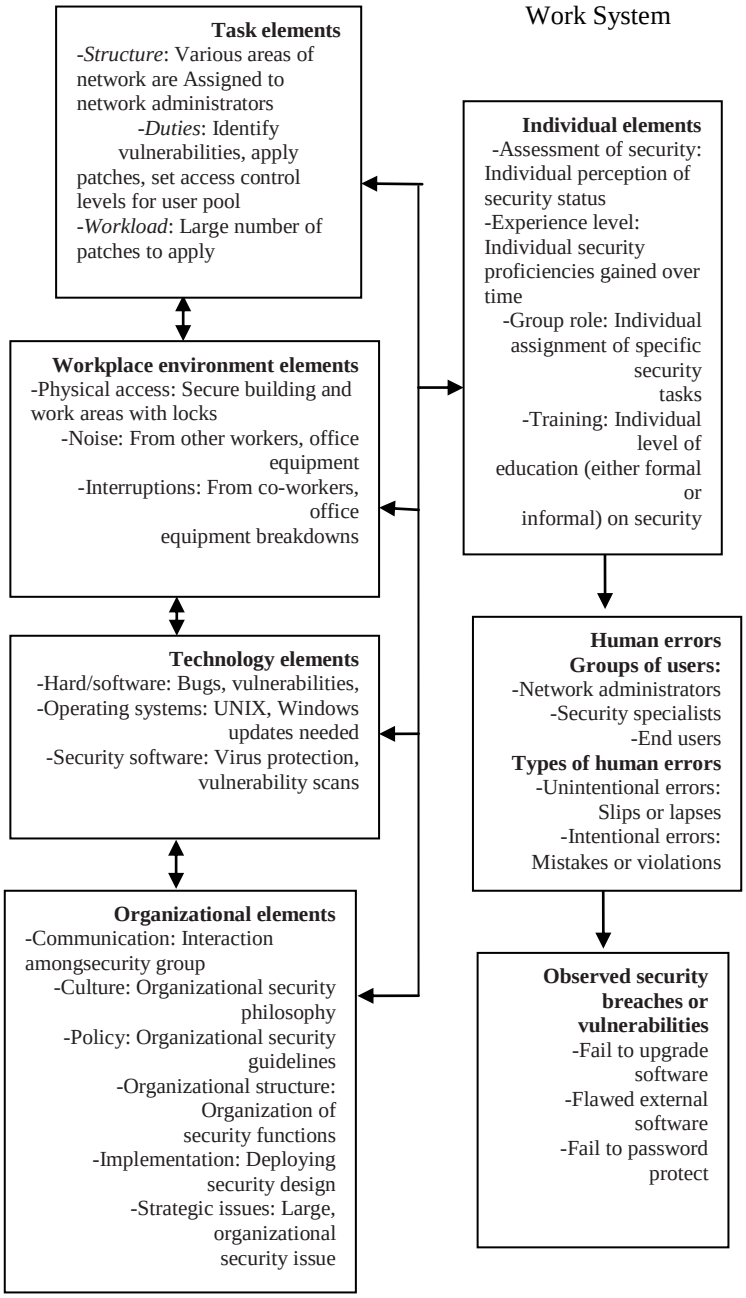

Figure 4: Macroergonomic conceptual framework of security in computer and information systems.

Other type of social engineering scenarios exists that the person deceive the employee of an organization like developing a personal relationship with a user or IT team member with the intent of extracting confidential information from that person that can be used to break into the network.

Counter measures case study1The risk of social engineering is also undervalued in employee training programmers or corporate security policies. Establishing policies is the first step in preventing this type of attack also organizations should avoid posting managerial charts or lists of key people and shred any documents that are discarded that may contain sensitive data. More important step is to make them aware the employee of the danger of social engineering and train them. They should be suspicious about unrequested emails and phone calls and also never be afraid to question the credentials of someone posing to work for their organization.

b) ***Phishing Attacks in e-Commerce; case study (2)***

Phishing is a form of social engineering, where a person tries to get users to provide personal, financial or computer account information. Phishes try to get account information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication, typically email or instant messaging.

Phishes establish a fake site selling goods and wait for a search engine to index them. A user types a query into a search engine and ends up at a real-looking site selling those goods. The site allows users to order goods and pay via credit card, but keeps all their personal details and never sends the goods. Man-in-the-middle is another type of attack; the victim received a email that the link directed them to a fake URL.

Phishing technique tricks the human and taking advantages of them and the most common one are using human vulnerabilities.

i. Requesting personal details for harmless reasons such as a system upgrade or a credit card that has expired. The message is boring, safe and legitimate and appears to be trying to be helpful.
ii. Inviting the recipient to does something that will benefit them for example join a credit card protection service.
iii. Creating a concern that a person's bank account or card is being targeted and that the customer needs to take action quickly.
iv. Using seasonal or national events to take advantage of peoples' emotions for example sending a charity related message.

i) Counter measures for case study(2)

Advice given to those who suspect they have received a phishing communication involves either ignoring it, not following the link or not supplying personal or financial information. Other advice is to check credit card and bank statements immediately after receipt and to look for unexpected charges, even small ones. Using authentication mode and every time the customer want to login it generate a random number and send to their phone.

3) ***Accidental Data Disclosure by an Employee; case study***

In this scenario the neglect of employee can provide such problem. For example an employee of a building society downloaded a database to his laptop so he could work at home. . The data included 11 million customers' name, addresses and account numbers. The laptop was later stolen from his home. The employee did not inform the company about the data on the laptop until returning from a three week holiday. So after three month the company informed the customer. In its investigation, the FSA concluded that the company had failed to assess the risks associated with its customer information, failed to implement procedures and training to manage its risk so they fine the company 1 million.

i. Reassured customers that there was no loss of money due to the laptop theft and passwords and account balances were not lost.
ii. Using the incorrect email address, attaching the wrong file, or transmission over insecure channels.
iii. Loss of portable data devices, it also contains the loss or theft of laptops, USB memory devices, CD-ROMs and DVDs, PDAs and mobile phones.
iv. Allowing access to data by losing hard copies of sensitive reports, failing to password-protect or log-off a computer, and circumventing or failing to use firewalls

i) Countermeasures case study (3)

System-based solutions to data escape can be grouped into three categories. User should compliance to policy and rules is required and it is optional, requiring some effort by the user and also requires proactively on the part of the user.

4) ***Technical countermeasures***

Firewalls and phishing filters reduce the chances and consequences of human error relating to risky computer use. Keeping a backup of data does not make data any more difficult to accidentally delete, steal or

otherwise disrupt. Yet backups reduce the damage done when data is accidentally deleted, and they reduce the damage done by more malicious efforts todestroy data. Automated software loading and patch updates reduce human error by removing the requirement that users manually activate that software and load updates. Software thatmonitors incoming and outgoing email works by different mechanisms. It will reduce general misuse of email and thereby encourage good practice. It will also check sensitive dataattachments thus reducing the possibility of human error leading to data disclosure to the wrong recipient. Clear policies and protocols for security policies, in contrast, do not make it harder for employees to commit error, or to misuse or abuse data, but they remove any excuses for so doing and clarify the consequences (the costs to the employee) of negligent actions. As such they will promote good practice which reduces human error. In fact, many existing cyber security efforts contain at least some orientation towards designing-out human error. Table 2 shows the tactics that can reduce human errors.

VII. Conclusion

An implicit aim of designing-out human error, therefore, is to minimize the need for education, training, and a culture relating to security. This is because the best security is that which does not require a particular cooperation on the part of human users, although human awareness of a problem is a useful additional barrier.

For this purpose, in this paper we have rewired some human errors and computer crime classification and then relationship between human error and cyber security breaches. More over conceptual frame works for evaluating human error that work in qualitative form rewired and macro ergonomic framework described more detailed. Last but not least some social and technical counter measures offered for overcoming breaches that caused by human errors.

Table 2: Tactics which can reduce human error

Increase the effort	Increase the risk	Reduce the rewards	Reduce provocations	Remove excuses
1.Target Harden • firewall • phishing filter • encryption • patch management	5. Reduce anonymity • authentication • digital identification	7. Identify property • digital signatures/certificates	10. Neutralize peer pressure • awareness building	11. Set rules • security policy • usage policy and protocols • implement best practice Standards
2. Control access to facilities • authentication • monitoring incoming email	6. Strengthen formal Surveillance • monitoring systems • publicly portray security accreditation	8. Disrupt markets • ISPs to provide protection against phishing, viruses and spyware		12. Alert conscience • awareness campaigns
3. Screen exits • monitoring systems • monitoring outgoing email and webmail		9. Deny benefits • immediately fix vulnerabilities • encryption • back-ups • limit new vulnerability publicity • computer or data 'kill' technology		13. Control drugs and alcohol • ban their consumption by personnel in critical posts (e.g. physical or IT security)
4. Control tools/weapons • authentication • digital identification				

REFERENCES

[1] Stokes, J., 2000. Stock Watch. Denver Rocky Mountain News, September 12, 2000.

[2] Carayon, P., Kraemer, S., 2002. Macroergonomics in WWDU: What about computer and information security. In: Cakir, G. (Ed.), Proceedings of the Sixth International Scientific Conference on Work With Display Units—WWDU 2002—World Wide Work. ERGONOMIC Institute fur Arbeits- und SozialforschungForschungsgesellschaftmbH, Berlin, Germany, pp. 87–89.

[3] Carayon, P., Smith, M.J., 2000. Work organization and ergonomics. Appl. Ergon. 31, 649–662.

[4] Smith, M.J., Carayon-Sainfort, P., 1989. A Balance Theory of Job Design for Stress Reduction.Int. J. Ind. Ergo. 4, 67–79.

[5] Rasmussen, J., 1982. Human errors: ATaxonomy for Describing Human Malfunction in Industrial Installations. J. Occ. Acc. 4, 311–333.

[6] Rasmussen, J., 1997. Risk management in a dynamic society: a modeling problem. Saf. Sci. 27 (2/3), 183–213.

[7] Rasmussen, J., Pejtersen, A.M., Goodstein, L.P., 1994. Cognitive Systems Engineering.Wiley, New York.

[8] Reason, J., 1990. Human Error. Cambridge University Press, New York.

[9] Reason, J., 1997. Managing the Risks of Organizational Accidents.Ashgate, Brookfield.

[10] Norman, D.A., 1983. Design rules based on analyses of human error. Common. ACM 26 (4), 254–258.

[11] Besnard, D., Greathead, D., 2003. A cognitive approach to safe violations.Cogn.Techn. Work 5 (4), 272–282.

[12] Wickens, C.D., Lee, J., Liu, Y., Gordon-Becker, S.E., 2004. An Introduction to Human Factors Engineering, second ed. Pearson Education, New York.

[13] Howard, J.D., Meunier, P., 2002. Using a ‘‘Common Language’’ for computer security incident information. In: Bosworth, S., Kabay, M.E. (Eds.), Computer Security Handbook, fourth ed. Wiley, New York, pp. 3.1–3.22.

[14] Human factors working group complementary white paper CostisKoumpis,GrahamFraell,AndrewMay,Johnmalley,MartinMaguire,Vaiasderalia

[15] CCPS, Guidelines for Preventing Human Error in Process Safety (1994)

[16] American Chemistry Council, formerly called the Chemical Manufacturers Association or CMA, (1990) A Manager’s Guide to Reducing Human Errors

[17] J. Moraal, Human Factors in Loss Prevention, paper from International conference on Hazard Identification and Risk Analysis, Human Factors and Human Reliability in Process Safety (1992)

[18] Holdsworth, and Smith, “Human and Organization Factors in the Safety of Offshore Platforms”, a paperpresented at the 1996 International Workshop on Human Factors in Offshore Operations