Users as the Biggest Threats to Security of Health Information Systems

Ahmad BakhtiyariShahri
Faculty of Computer Science and Information Systems
UniversitiTeknologi Malaysia (UTM)
Malaysia
bsahmad2@live.utm.my

Zuraini Ismail
Advanced Informatics School
UniversitiTeknologi Malaysia (UTM);
Malaysia
zurainisma@ic.utm.my

Abstract—**There are a lot of researches in the world about attacks on information systems (IS). Although there have been many attempts to classify threats of IS's especially in Health Information Systems (HIS), it is still necessary for all health organization to identify new threats and their sources which threaten security of health care domain. The main aim of this paper is to present a research agenda of threats to HIS and identify issues and human factors that assist the implementation and adoption of health information security within the developing countries. In doing so, the authors try to provide a cohesive completeness identification of all threats about HIS and highlight the role of human in all of them. More than 70 threats to HIS are identified by using a large number of disparate data sources. Then they are classified in 30 subjects and finally categorized in seven areas whichuser's activities are the biggest threat at the core of risks to HIS.**

Keywords-Health Information System;Human Error;Threats

I. INTRODUCTION

The information era has ushered in the field of information technology, with all the benefits, threats and risks of new technology and industrialization in modern society [1].The questions for the society, its governments, its industries, and ultimately, its people are in many ways the same for information technology as they were for other technologies and industries:How does it benefit the society?What are the strengths and weaknesses?What are the impacts on freedom and privacy and on life itself in the technology-driven society? Freedom and dignity provide the most profound rationales with such specific rights, even if these reasonable grounds are often controversial, multi-faceted, and pulling into opposite directions [2].

Healthcare information technology has different potentials to improve the quality of care and efficiency.It is currently one of the important factorsfor major innovations and is used in widespread around the world [3]. Using of ICT in health care domain can reduce medical costs and save human's live.In the health care extended, not only people, particularly patients and their families have an important role, but also health care institutional personnel vendors and others are the parts of any HIS[4]. Therefore an effective information security program must be a combination of human and technological controls to prevent loss of data, accidental or deliberate unauthorized activity, and illegal access to data;in this case itguarantees privacy and security of patients[5].

In recent years data security breaches in health care organizations continue to increase; number of threats in health information systems (HIS) area has increased dramatically [6]. For example, from 2006 to 2007 in hospitals alone, occurred exposing of more than 1.5 million names during data breaches [7]. They were received as theft (stolen laptops, computers, or media), loss or negligence by employees or third parties, malicious insiders, system hacks, web exposure, and virus attacks [8]. So, people in different rolesare often the greatest threat to IS assets [9-12] and the human error is the cause of numerous data breaches [4, 13].

II. THE NECESSITY OF REALIZING ORGANIZATION THREATS

Around 500 B.C., the Chinese general Sun Tzu Wu wrote "The Art of War", a military treatise that emphasizes the importance of knowing yourself as well as the threats you face [14]. To protect the information in your organization, first, you must know yourself that is recognized by the data protection and storage, transmission and processing systems; and second,you must know the threats you face. So, information security must be informed about the different threats to assets in information systems [15].

In addition risk assessment requires an understanding of the sources of threats, threat action and how that sources can be trigged or exploited vulnerability in a health information asset[3].Discussion about privacy and security of ISs has long been a major subject in the social science and business press, but recently there has been controversy about lacking a systematic investigation to identify and categorize various sources of threats to information security and privacy in academic literature [4].

Although there are a lot of researches in developing countrieson the necessity ofidentificationand classification threats to security of electronic medical records[16], the deficiency has been observed due to the lack of specific standards for identifying of threats[17]. In addition, because the first step of process of "threat tree generation" for IS is identifying of threats[١٨] so,classificationof different threats and finding the place of human in creating or preventing of themarethe requirements to discuss health information security issues. In addition, management of E-Health information needs to identify the threats for an effective framework by considering the comprehensive incorporation

of confidentiality, integrity and availability as the core principles of information security. This raises major challenges that require new exhaustively attitudes to users such as a wide variety of policies, ethical, psychological, information and security procedures [5].The next section will be the literature on identification of threats to HIS and showsthat different users of ISs play a significant role to create or to prevent a threat[19].

III. LITERATURETO IDENTIFYING OF THREATS TO HIS AND HIGHLIGHT HUMAN ACTIVITY

The results of CSI/FBI Annual Computer Crime and Security Survey in 2002, ranked the followings as significant threats:Virus, Insider Abuse of Net Access, Laptop, Denial of Service, Unauthorized Access by Insiders, System Penetration, Theft of Proprietary Info, Financial Fraud, Telecom Fraud, Sabotage, Telecom Eavesdropping, andActive Wiretap[20].According to Ref.[21] the most important threats about patients' confidentiality are: Accidental Disclosures, Insider Curiosity for infringers own curiosity or purposes, Insider Subornationdone generally for profit, Uncontrolled Secondary Usage, and Unauthorized Access.

The NIST 800-30 provides a categorization of threat sources in six items: Human Deliberate, Human Unintentional, Technical, Operational, Environmental, and Natural [22]. Recent policy-based studies broadly categorize privacy threats, or source of information security, into two areas:Organizational and Systemic threats. Organizational threatsare categorized into five levels: Accidental Disclosure, Insider Curiosity, DataBreach by Insider, DataBreach by Outsider with physical intrusion and Unauthorized Intrusion of Network System[4].Whitman[9]also offered a classification of threats to IS in twelve items based on three fundamental questions. These questions are as follows: What are the threats to information security? Which of these threats are the most serious? How frequently (per month) are these threats observed? Whitman [9]provided an online survey by asking IT executives to rank the threats to information security, to identify the priority of expenditures and to protect IS against these threats. The findings show that the most critical threat for the IS is Deliberate Software Attacks, which was weighted almost twice as important as the second threat in the list. It means Technical Software Failures or Errors, Acts of Human Error, Failure and Deliberate Acts of Espionage or Trespass also present high-risk threats for HIS[23].

Each organization will need to prioritize the threats it faces, based on the particular security situation in which it operates, its organizational strategy regarding risk, and the exposure levels at which its assets operate [14]. Therefore, another categorization scheme has been done that consists of fourteen general categories that represents clear and present dangers to an organizations people, information, and systems. The results are generally similar to previous studies in which Espionage or Trespass and Software Attacks remain at the top of the list and Human Error or Failure in the third position. After them, there are new options, which are added in the last category namely:Missing Inadequate or Incomplete Organizational Policy or Planning and Missing Inadequate or Incomplete Controls[15].Yeh and Chang identifyfifty fundamental security countermeasures commonly adopted to evaluate the adequacy of IS securityinto seven categories[24].

According to the following list, the significant threats have been classified and ranked by Annual Computer Crime and Security Survey in 2008: Denial of Service, Laptop Theft, Telecom Fraud, Unauthorized Access, Virus, Financial Fraud, Insider Abuse, System Penetration, Sabotage, Theft/Loss of Proprietary Info, Abuse of Wireless Network, Web Site Defacement, Misuse of Web Application, Bots, DNS, Attacks, Instant Messaging Abuse, Password Sniffing, Theft/loss of Customer Data [25].Accidental events and deliberate action threats are also two parameters that can severely damage HIS [26].Moreover ISO/IEC 27002 addresses eleven areas related to information security management [27].In Ref.[16]NarayanaSamy, Ahmad et al.introduced "Threats to Total Hospital Information System (THIS)" and discovered that there are altogether 22 types of threats to THIS. Power failure/loss, Acts of human error or failure, Technological obsolescence, Hardware failures or errors and Software failures or errors respectively are the most critical threat in HIS. In 2011, they also examined their categorization in a hospital of Malaysia to find the most critical threats. Although ranking of threats were changed, but they are still the most important threats. In addition, malware attacks and Network infrastructure failures or errors have been added to the important threats.

Pardue and Patidar represent a preliminary effort at cataloging threats to electronic healthcare data associated with unauthorized access, data loss, and data corruption, which caused by vandalism, loss or corruption of data, due to faulty hardware and software, human error, malware, natural disaster and database attack[28]. In addition Ref. [3] presents a modelof the threat tree which is organized around the goal of an attacker or outcome of a threat, depending on whether the threat is intentional or not. At the top level, or root, of the threat tree, there is threatening health information asset.Kotz[29] also provided a taxonomy consisting of 25 threats to HIS organized around three main categories: identity threats, access threats, and disclosure threats. Threats also are organized by different types such as misuse of patient identities, unauthorized access or modification of PHI, or disclosure of PHI. Each category considers three types of the adversary: Patient himself or herself, Insiders (authorized PHR users, staff of the PHR organization, or staff of other M-Health support systems), and Outsiders (third partiesacting without authorization)[29].

Another study mentions that most people are familiar with common types of computer security breaches that are caused byComputer Viruses, The Internet, Hackers, Worms, and MaliciousSoftware Designed to compromise or

disrupt other computer systems, and the Loss or Theft of laptops containing sensitive data.Security of the computers embedded in sophisticated medical devices, and unauthorized communication may increase susceptibility to security breaches [30].

To sum up for each HIS are proposedsix components including:software, hardware, data, people, procedures, and networks[23].They make it possible to use the information resources in academic medical centers. These six critical components enable information to be input, processed, output, and stored[14]. Each of these IS components has some strengths and weaknesses, as well as characteristics and users. Each component of HIS also has its own security requirements[15]. Thereforefinding an organized classification of threats and a relationship between human error and security of information systemsare required in order to discuss information security issues[31]. The next section will discuss the method for identification threats and role of users to security of HIS.

IV. RESEARCH MTETODOLOGY AND OBJECTIVES

This paper uses the principles of secondary data sourcesincluding the use of different threats catalogs and literature to find a complete model which are shown in Table1. Hence, as opposed to positivist or deductive research, authors did not start from a priori theory or formulized hypotheses but categorized common concepts in diverse categories. By constantly comparing the main characteristics of the data, the categories were extended to a complete set in order to get a plausible representation of the main threats in HIS. Necessary data to develop this categorization has been obtained by searching ACM Digital Library, AISeL, EBSCO, IEEE Xplore, PUBMED, SPRINGER, ELSEVIER, and SCOPUS for articles containing 'threats of health information systems', ' threats to health technology', 'threats to information systems', and 'human error' and the related various spellings as keywords.

In the first output, 30 threats to HISin seven areas were identified. Authors analyzed all gathered articles in much detail in second stage. This in turn, helped to further refine the main themes into several sub items for each threat. To sum up the authors identified about 70 threats for HIS and categorized them as a new tree of threats to HIS.Objectives of this paper can provide a basis for discussion and an applied method that yieldrigorous and interesting results.

TABLE I
NEW CATALOGUE OF THREAT TO HEALTH INFORMATION SYSTEMS

Equipment Malfunctions	1. Network Infrastructure Failures or Errors 1.1. Technical Failure of Network Interface 1.2. Technical Failure of Network Interface 1.3. Abuse of Wireless Network
	2. Maintenance Error 2.1. Hardware 2.2. Software 2.3. Network
	3. Hardware Failures or Errors 3.1. System's Hardware Failures 3.2. Network's Hardware Failures
	4. Technical Failure
	5. Theft of Equipment
Application Error	6. Software Failures or Errors 6.1. Introduction of Damaging or Disruptive Software 6.2. System's Software Failures 6.3. Application Software Failure 6.4. Network's Software Failures 6.4.1. Bugs 6.4.2. Code Problems 6.4.3. Unknown Loopholes
	7. Operational Issues
Misuse of Data	8. Espionage or Trespass
	9. Deliberate Acts of Theft of Data 9.1. Theft/Loss of Customer Data or Proprietary Info 9.2. Unknown Loopholes 9.3. Illegal Confiscation of Information 9.4. Dumping Physical Files with critical information in public
	10. Misuse of System Resources 10.1. Third Party 10.2. Information Extortion
	11. Financial Fraud
	12. User Errors 12.1. User Errors in Using the Software Assets 12.2. Masquerading the User Identity 12.3. Unauthorized Use of a HIS Application 12.4. Accidental Disclosure of Information 12.5. Email Confidential Information to an Incorrect Address 12.6. Accidental Entry Bad Data by Employees
Physical Damage	13. Power Failure/loss 13.1. Power Failure of the Server (ANS) 13.2. Power Failure of the Workstation
	14. Sabotage or Willful Damages
	15. Terrorism
	16. Natural Disasters (Acts of God) 16.1. Flood 16.2. Earthquake 16.3. Lightning 16.4. Electrical Storms 16.5. Tornadoes 16.6. Landslides 16.7. Avalanches
	17. Environmental Threats 17.1. Water Damage 17.2. Fire 17.3. Air-Condition Failure 17.4. Pollution 17.5. Chemicals 17.6. Liquid Leakage

Internal or External Attacks	18. Deviations in Quality of Service 18.1. QoS Deviations from Service Providers 18.2. Deliberate Software Attacks 18.2.1. Nonetheless Purposeful, attempt to circumvent system security 18.2.2. Malicious Attempt to gain unauthorized access 18.2.2.1. Password Sniffing 18.2.2.2. Telecom Eavesdropping 18.2.2.3. Database Attack 18.2.2.4. Denial of Service 18.2.2.5. Web site Defacement 18.2.2.6. Incorrect Display 18.2.2.7. Bots 18.2.2.8. DNS Attacks 18.2.2.9. Malware Attack 18.2.2.9.1. Worm 18.2.2.9.2. Trojan Horses 18.2.2.9.3. Spyware 18.2.2.9.4. Virus 18.2.2.9.5. Adware 18.2.2.9.6. Macros
	19. Communications Interception
	20. Social Engineering Attacks
	21. Unauthorized Access to Information Database
	22. Unauthorized Communication
	23. Communications Infiltration 23.1. Device Reprogramming 23.2. Unauthorized Data Extraction
	24. Misuse of Web Application 24.1. Cross Site Scripts 24.2. Information Leakage 24.3. SQL Injection 24.4. HTTP Response Splitting
Human Interaction	25. Repudiation
	26. Staff Shortage
	27. Compromises to Intellectual Property
	28. Missing, Inadequate or Incomplete Organizational Policy or Planning
	29. Missing, Inadequate or Incomplete Controls
Loss of Data	30. Technological Obsolescence

V. PLACE OF HUMAN IN THREATS TO HIS

In a perfect world, we might consider the prospect of aiming for 100% error-free user behavior. It would eliminate the need for many expensive security controls[26].Unfortunately, that is far from attainable in real life. People cannot avoid or eliminate mistakes, no matter how hard we try.Accidents, mistakes and breaches are caused by many human factors: ignorance, stress, fatigue, negligence, carelessness, complacency, apathy, spite, stupidity, criminal intent or just plain bad design[32]. You can blame individuals for making mistakes. But many will be due either to a failure by managers to provide adequate resources, training and oversight, or to a flaw in the design of systems and processes[33].

Since threat is any action posed by a human or non-human source and can originate internally or externally [13, 16] that threatens the confidentiality, integrity, or availability of information assets [34] so, by understanding the threats and their sources to health information security, the organization can better protect its information assets and strengthen the level of protection of information in health information system. Therefore, management of E-Health information needs to identify the threats and also various users for an effective framework by considering the comprehensive incorporation of confidentiality, integrity and availability to be the core principles of information security. This raises major challenges that require new exhaustively attitudes such as a wide variety of policies, awareness, ethical, psychological, information and security procedures [5, 35]. Hence, authors provide an up-to-date categorize of threats to healthcare assets to prove that the human in different way is one of the important factors in threats to HIS; and not only the technical software or hardware aspects that introduce vulnerabilities into an information systembut primarily, users of the system also pose the greatest and most serious information security risk [36]. It is evident that solely technical solutions are unlikely to prevent security breaches.

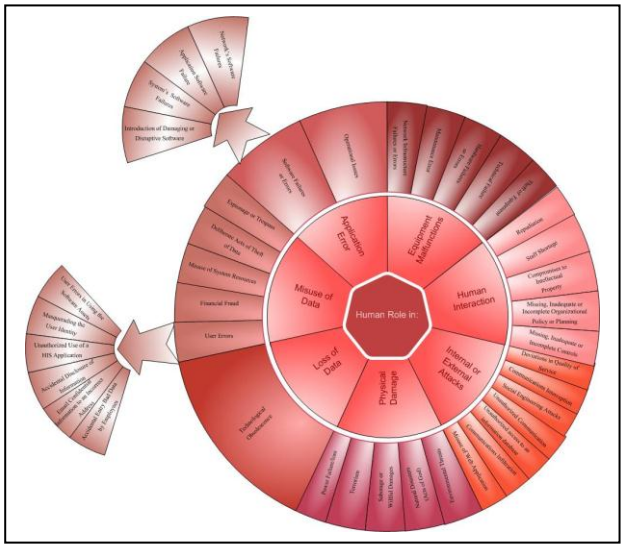

Figure1: Human activity at the core of threats to HIS

Figure1 shows a brief model of role of human in threats to HIS. It is clear that the human activities in role of different HIS's users are at the core of threats to HIS security.

VI. CONCLUSION

This paper presents the categorization of different threats to healthcare information system and also highlights the role of human activity in all of them. Clearing the place of users in different threat would play a significant role as the core of security in HIS. Researchers and system developers may find this effort useful in the advancement of HIS security. Although this study also attempts to shows a clearview of place of human in security of HIS, it is still regarded as a work in progress.

ACKNOWLEDGMENT

The authors express their gratitude to the editor whose comments have helped improve this paper considerably.

REFERENCES

[1] M. Van Eeten, *et al.*, "The State and the Threat of Cascading Failure Across Critical Infrastructure: The Implications of Empiricav Evidence from Media Incident Report," *Public Administration*, vol. 89, pp. 381-400, 2011.

[2] G. Sartor, "Human Rights in the Information Society: Utopias, Dystopias and Human Values," *Philosophical Dimensions of Human Rights*, pp. 293-307, 2011.

[3] J. P. Landry, *et al.*, "A Threat Tree for Health Information Security and Privacy," *Proceedings of the 17th American Conference on Information Systems*, 4-8 August 2011.

[4] A. Appari and M. E. Johnson, "Information Security and Privacy in Healthcare: Current State of Research," *Inter-national Journal of Internet and Enterprise Management*, vol. 6, pp. 279-314, 2010.

[5] C. A. Shoniregun, *et al.*, "Introduction to e-Healthcare Information Security," *Electronic Healthcare Information Security*, vol. 53, pp. 1-27, 2010.

[6] J. W. Brady, "Securing Health Care: Assessing Factors That Affect HIPAA Security Compliance in Academic Medical Centers," 2011, pp. 1-10.

[7] HIMSS, "Kroll-HIMSS Analytics 2008 Report on Security of Patient Data " 2008.

[8] HIMSS, "Kroll-HIMSS Analytics 2010 Report on Security of Patient Data " 2010.

[9] M. E. Whitman, "Enemy at the Gate: Threats to Information Security," *Communications of the ACM*, vol. 46, pp. 91-95, 2003.

[10] J. D'Arcy and A. Hovav, "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures," *Journal of Business Ethics*, vol. 89, pp. 59-71, 2009.

[11] D. Lacey, "Understanding and Transforming Organizational Security Culture," *Information Management & Computer Security*, vol. 18, pp. 4-13, 2010.

[12] J. M. Hagen, "The Contributions of Information Security Culture and Human Relations to the Improvement of Situational Awareness," p. 19, 2012.

[13] G. N. Samy, *et al.*, "Threats to Health Information Security," in *Proceedings of the 5th International Conference on Information Assurance and Security of the IEEE IAS*, ed. Xi'an: IEEE, 8-20 August 2009, pp. 540-543.

[14] M. E. Whitman and H. J. Mattord, "The Enemy Is still at the Gates: Threats to Information Security Revisited," in *Proceedings of the 2010 Information Security Curriculum Development Conference*, Kennesaw, 1-3 October 2010, pp. 95-96.

[15] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Boston: Course Technology Ptr, 2011.

[16] G. Narayana Samy, *et al.*, "Security Threats Categories in Healthcare Information Systems," *Health Informatics Journal*, vol. 16, pp. 201-209, 2010.

[17] M. Ahmadi, *et al.*, "A Review of the Personal Health Records in Selected Countries and Iran," *Journal of Medical Systems*, pp. 1-12, 2010.

[18] A. Yasinsac and H. Pardue, "A Process for Assessing Voting System Risk Using Threat Trees," *Journal of Information Systems Applied Research*, vol. 4, 2010.

[19] S. Alfawaz, *et al.*, "Information Security Culture: A Behaviour Compliance Conceptual Framework," 2010, pp. 47-55.

[20] R. Power, *CSI/FBI Computer Crime and Security Survey: Computer Security Institute*: SCI & FBI, 2002.

[21] T. C. Rindfleisch, "Privacy, Information Technology, and Health Care," *Communications of the ACM*, vol. 40, pp. 92-100, 1997.

[22] G. Stonebumer, *et al.*, "Risk Management Guide for Information Technology Systems," ed: National Institute of Stan-dards and Technology, 2002.

[23] M. E. Whitman, "In Defense of the Realm: Understanding the Threats to Information Security," *International Journal of Information Management*, vol. 24, pp. 43-57, 2004.

[24] Q. J. Yeh and A. J. T. Chang, "Threats and Countermeasures for Information System Security: A Cross-Industry Study," *Information & Management*, vol. 44, pp. 480-491, 2007.

[25] R. Richardson, "CSI Computer Crime and Security Survey," *Computer Security Institute*, pp. 1-30, 2008.

[26] S. Kahn and V. Sheshadri, "Medical Record Privacy and Security in a Digital Environment," *IT Professional*, vol. 10, pp. 46-52, 2008.

[27] R. Gomes and L. V. Lapão, "The Adoption of IT Security Standards in a Healthcare Environment," *Studies in Health Technology and Informatics*, vol. 136, pp. 765-770, 2008.

[28] J. H. Pardue and P. Patidar, "Thrats to Healthcare Date: A Threat Tree for Risk Assessment," *Issues in Information Systems*, 5-8 October 2011.

[29] D. Kotz, "A Threat Taxonomy for mHealth Privacy," in *Proceedings of the 3rd International Conference on Communication Systems and Networks of the IEEE COMS- NETS*, Bangalore, 4-8 January 2011, pp. 1-6.

[30] W. H. Maisel and T. Kohno, "Improving the Security and Privacy of Implantable Medical Devices," *New England Journal of Medicine*, vol. 362, 2010.

[31] S. Kraemer, *et al.*, "Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities," *Computers & Security*, vol. 28, pp. 509-520, 2009.

[32] D. Lacey, *Managing the Human Factor in Information Security: How to win over staff and influence business managers*: John Wiley & Sons, 2009.

[33] T. Asai and S. Fernando, "Human-Related Problems in Information Security in Thai Cross-Cultural Environments," *Contemporary Management Research*, vol. 7, pp. 117-142, 2011.

[34] A. Nematzadeh and L. J. Camp, "Threat Analysis of Online Health Information System," in *Proceedings of the 3rd International Conference on PErvasive Technologies Related to Assistive Environments*, New York, 2010, p. 31.

[35] S. Samsuri, *et al.*, "User-Centered Evaluation of Privacy Models for Protecting Personal Medical Information," *Informatics Engineering and Information Science*, vol. 251, 2011.

[36] M. Boujettif and Y. Wang, "Constructivist Approach to Information Security Awareness in the Middle East," in *International Conference on Broadband, Wireless Computing, Communication and Applications*, Fukuoka, Japan, 4-6 Nov 2010, pp. 192-199.