Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS).

Tommy Pollock
tp809@mynsu.nova.edu

Abstract
For several decades, researchers have stated that human error is a significant cause of information security breaches, yet it still remains to be a major issue today. Quantifying the effects of security incidents is often a difficult task because studies often understate or overstate the costs involved. Human error has always been a cause of failure in many industries and professions that is overlooked or ignored as an inevitability. The problem with human error is further exacerbated by the fact that the systems that are set up to keep networks secure are managed by humans. There are several causes of a security breach related human error such as poor situational awareness, lack of training, boredom, and lack of risk perception. Part of the problem is that people who usually make great decisions offline make deplorable decisions online due to incorrect assumptions of how computer transactions operate. Human error can be unintentional because of the incorrect execution of a plan (slips/lapses) or from correctly following an inadequate plan (mistakes). Whether intentional or unintentional, errors can lead to vulnerabilities and security breaches. Regardless, humans remain the weak link in the process of interfacing with the machines they operate and in keeping information secure. These errors can have detrimental effects both physically and socially. Hackers exploit these weaknesses to gain unauthorized entry into computer systems. Security errors and violations, however, are not limited to users. Administrators of systems are also at fault. If there is not an adequate level of awareness, many of the security techniques are likely to be misused or misinterpreted by the users rendering adequate security mechanisms useless. Corporations also play a factor in information security loss, because of the reactive management approaches that they use in security incidents. Undependable user interfaces can also play a role for the security breaches due to flaws in the design. System design and human interaction both play a role in how often human error occurs particularly when there is a slight mismatch between the system design and the person operating it. One major problem with systems design is that they designed for simplicity, which can lead a normally conscious person to make bad security decisions. Human error is a complex and elusive security problem that has generally defied creation of a structured and standardized classification scheme. While Human error may never be completely eliminated from the tasks, they perform due to poor situational awareness, or a lack of adequate training, the first step to make improvements over the status quo is to establish a unified scheme to classify such security errors. With this background, I, intend to develop a tool to gather data and apply the Human Factors Analysis and Classification System (HFACS), a tool developed for aviation accidents, to see if there are any latent organizational conditions that led to the error. HFACS analyzes historical data to find common trends that can identify areas that need to be addressed in an organization to the goal of reducing the frequency of the errors.

Disciplines
Information Security

Introduction

Background

Human error has always been a cause of failure in many industries and professions that is overlooked or ignored as an inevitability, (Wood & Banks, 1993). The problem with human error is further exacerbated by the fact that the systems that are set up to keep networks secure are managed by humans, (Kjaerland, 2006). Part of the problem is that people who usually make great decisions offline make deplorable decisions online due to incorrect assumptions of how computer transactions operate (Bratus, Masone, & Smith, 2008). Quantifying the effects of security incidents is often a difficult task (Acquisti, Friedman, & Telang, 2006), because studies often understate or overstate the costs involved.

Whether intentional or unintentional (Kraemer & Carayon, 2007), errors can lead to vulnerabilities and privacy breaches. These errors can have detrimental effects both physically and socially, (Norman, 1983). The aviation industry has a tool for tracking human factors in incidents (Liu, Chi, & Li, 2013; Shappell et al., 2007; Wiegmann & Shappell, 2001) called the Human Factor Analysis and Classification system (HFACS). This system is in place to track what role human error plays in aviation accidents and incidents (Shappell et al., 2007), and the underlying casual factors in an organization that lead to incidents and accidents. The medical community uses the Theory of Planned Behavior (Beatty & Beatty, 2004), to predict whether medical professionals would routinely violate patient safety guidelines. (Liginlal, Sim, & Khansa, 2009), suggests using a generic error modeling system (GEMS) in reported privacy breach incidents to categorize the types of errors called slips and mistakes. This information can be utilized to creating effective information processing policies in an organization as well as a means to enforce them.

Problem Statement

Human error remains a leading cause of security breaches (BakerHostetler, 2016). Such errors occur either due to lack of awareness (Bratus et al., 2008; Kraemer & Carayon, 2007; Kraemer, Carayon, & Clem, 2009; Safa et al., 2016) or through distraction, fatigue, and boredom (Hopping, 2017; Reason, 1995). Human error can be unintentional because of the incorrect execution of a plan (slips/lapses) or from correctly following an inadequate plan (mistakes) (Beatty & Beatty, 2004; Liginlal et al., 2009; Reason, 1990, 1995). Regardless, humans remain the weak link (Metalidou, Marinagi, Trivellas, Eberhagen, Skourlas, & Giannakopoulos,

2014) in the process of interfacing with the machines they operate and in keeping information secure. Systems users make bad decisions (Bratus et al., 2008) based on incorrect assumptions and lack of proper training. Users tend to have a lack of risk perception (Choi & Levy, 2013; Parsons, Mccormac, Butavicius, & Ferguson, 2010; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014) that can lead to poor security awareness. Hackers take advantage to this lack of awareness (Safa et al., 2016) to breach security. Security errors and violations, however, are not limited to users (Kraemer & Carayon, 2007). Administrators of systems are also at fault.

Human error is a complex and elusive security problem that has generally defied creation of a structured and standardized classification scheme (Shappell et al., 2007). While Human error may never be completely eliminated from the tasks they perform due to poor situational awareness, or a lack of adequate training (Endsley, 1995; Flach, 1995; Puhakainen & Siponen, 2010), the first step to make improvements over the status quo is to establish a unified scheme to classify such security errors.

Research Goal

The goal of this research is to create a methodology for information security using the Human Factors Analysis Classification System. The research is to find out how situational awareness (Endsley, 1995; Flach, 1995), and human error relate to one another in order to develop methods based on HFACS (Liu et al., 2013; Shappell et al., 2007) to help improve information security through the identification of any latent organizational conditions that lead to human error. System design rules based on cognitive engineering (Norman, 1983), and improvements in security behavior compliance, (Herath & Rao, 2009; Puhakainen & Siponen, 2010).

Research Questions

This research will use a design science approach based on (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007) DSRM to design an artifact to address human error as a cause of cyber security breaches. First, how can the human factors analysis and classification system (HFACS) be adapted to find the casual factors leading to an information privacy breach? Secondly, why is human error so easily discounted as a factor in information privacy breaches? Finally, can systems be designed to minimize the effect of privacy breaches caused by human error?

Relevance and Significance

Human error will never be completely eliminated from the tasks that they performed because of poor situational awareness (Endsley, 1995; Flach, 1995), or through the lack of training (Puhakainen & Siponen, 2010). Humans are the weak

link (Metalidou, Marinagi, Trivellas, Eberhagen, Skourlas, & Giannakopoulos, 2014) in the process of interfacing with the machines that they operate and keeping information secure. This damage (hardware or software) can be unintentional because they lack the training or intentional violation of guidelines, (Beatty & Beatty, 2004). Corporations also play a factor in information security loss (Qian, Fang, & Gonzalez, 2012), because of the reactive management approaches that they use in security incidents. Undependable user interfaces (Maxion & Reeder, 2005) can also play a significant role in the human error caused security breaches due to flaws in the design.

Barriers and Issues

The main barriers and issues in performing this research is the short amount of public information available through reporting clearing houses. Human error is also a complex subject to quantify the actual cause and effect of when dealing with information security and information systems. Historical data can be incomplete or not framed in a way that can give definitive answers to research questions. The systems and procedures themselves may play a significant role in the errors.

Review of the Literature

In Norman's (1983), research on cognitive engineering "System design principles can be derived from classes of human error" (p. 254). Norman (1983), bases his research on high level specifications of desired actions known as intention. The intentions are broken down into mistakes and slips that were researched by Liginlal et al. (2009), and Reason (1990). In trying to find the casual factors in an organization that cause human error to occur the use of experimental psychology and human factors engineering the probability of human error can be directly measured, (Wood & Banks, 1993). System design and human interaction both play a role in how often human error occurs particularly when there is a slight mismatch between the system design and the person operating it, (Wood & Banks, 1993). One major problem with systems design is that they are designed for simplicity which can lead a normally privacy conscious person to make bad security decisions, (Bratus et al., 2008). The system design issue can be addressed through the creation of artifacts through design science (Johannesson & Perjons, 2014). A flexible methodology created by Peffers et al.(2007) consists of a six step design science research methodology (DSRM). Peffers et al. (2007) found that there was a serious lack of a DSRM in IS research even with 15 years of prior application of DS in the IS research discipline.

Situation awareness (SA) also plays a key role in human error, (Endsley, 1995; Flach, 1995; Sim, 2010). SA is a factor that played a role in the HFACS studies

(Liu et al., 2013; Shappell et al., 2007). Although SA is mainly looked at in aviation incidents and accidents, SA is applicable to a variety of environments, (Endsley, 1995). SA is used to measure operator performance in an environment, which makes it easily adaptable for measuring information privacy breaches. According to (Siponen, 2000, 2001) If there is not an adequate level of awareness, many of the security techniques are likely to be misused or misinterpreted by the users rendering adequate security mechanisms useless. According to (Endsley & Conners, 2014) Successful SA achievement in cyber environments has proven quite difficult with current systems (p. 8). In the development of a situational awareness model for information security risk management (Webb, Ahmad, Maynard, & Shanks, 2014) found only two scholarly article on SA (Dinev & Hu, 2007; Shaw, Chen, Harris, & Huang, 2009). The importance of SA in an IT environment needs to be addressed in order to reduce it as a factor in human error with users and administrators of systems.

An empirical study by (Liginlal et al., 2009) asks how significant is human error as a cause of privacy breaches? They state that privacy breaches that are caused by human error are often overlooked. The definition of error according to (Reason, 1990) is "the failure to achieve the intended outcome in a planned sequence of mental or physical activities when failure is not due to chance", (p. 7). Some reasons given for ignoring or dismissing human error as a cause of privacy breaches according to (Wood & Banks, 1993) is that human error is viewed as inevitable and that there is not much to be done about it. Human error is also responsible for 65% of data breach incidents according to (Lewis, 2003), which result in economic loss. The definition of privacy and what it means to different people and cultures is often hard to determine (Liginlal et al., 2009), because of differing semantics. Reason (1990) proposed the generic error modeling system (GEMS), that categorized error into slips and mistakes, which can be used to create system design principals, (Norman, 1981, 1983). Human error incidents cross many domains such as aviation (Liu et al., 2013; Shappell et al., 2007), and medical (Beatty & Beatty, 2004; Dekker, 2007; Gawron, Drury, Fairbanks, & Berger, 2006).

The human factors analysis and classification system (HFACS) was developed in 1997 for the U.S. Navy/Marine Corps aviation community by (Shappell et al., 2007; Wiegmann & Shappell, 2001) to address a series of aviation accidents and incidents that were occurring. HFACS is based off Reason's (1990) Swiss cheese model of latent and active failures, breaking human error down into four different levels of failure, (Wiegmann & Shappell, 2001). The four levels are unsafe acts of operators, preconditions for unsafe acts, unsafe supervision, and organizational influences. Under the unsafe acts level on the HFACS model error is further broken down into three categories, decision errors (honest mistakes), skill-based

errors (unconscious thought), and perceptual errors (sensory). HFACS is designed to see if there are any latent organizational conditions that led to the error. As with the privacy issue, cultural differences can have an underlying effect on the cause of the accidents and incidents, as evidenced in the different HFACS studies by Liu et al. (2013) and Shappell et al. (2007) found that the causes of historical accidents differed. According to Liu et al. (2013), Fallible decisions in upper management directly led to pre-conditions of unsafe acts which impaired the performance of pilots' due to a breakdown in supervisory practices. Inversely the Shappell et al. (2007) study found that the casual factors causing the aviation accidents were at the unsafe act level. Over half (56.5%) were skill based errors and over a third (36.7%) were decision errors. Before HFACS was developed human error was a complex and elusive matter that was not well defined without a structured and standardized classification scheme, (Shappell et al., 2007).

According to Johannesson and Perjons (2014) design science is a study of artifacts like many other scientific disciplines. These artifacts are then developed to solve practical problems that people face. In the information systems (IS) perspective these problems involve systems and the people that operate them. Design science utilizes both qualitative and quantitative research methodologies according to Johannesson and Perjons (2014). According to Maher (2011) even though design is a complicated and complex process that includes formulation, synthesis, and analysis, the results can bring value to the processes and design. Some of the values in design sciences according to (Niiniluoto, 2014) are anecdotal conditions for actions. According to Niiniluoto(2014), design science is based the 19th century application of applied arts (industrial design) and design research based off Simon (1996). Some of the world greatest minds, da Vinci and Aristotle employed some sort of design science in their time (Niiniluoto, 2014).

Walls et al (1992) states that there is a need for information systems design theories that are both effective and feasible. Walls et al (1992) broke down the components of an information systems design theory into two categories (pg. 43), the design product, and the design process each of these had multiple sub categories. The systems development life cycle (SDLC) was one of the widely accepted design theories that (Walls, Widmeyer, & El Sawy, 1992) mentioned as an example in their design process development. Even though design science has had a resurgence as a research paradigm in the last few years there seems to be a lack of any ethical components (Myers & Venable, 2014). According to Myers et al (2014), as the build-evaluate cycles have become more complex and elaborate no ethical considerations were included in the work. Ethical considerations are an important aspect in the design and deployment of IS systems because of the effect that they have on human subjects (Mason, 1986). Mason (1986) proposed four ethical principals in the design of information systems as a form of a social

contract. The four principles that Mason (1986) suggested are Privacy, Accuracy, Property, and Accessibility (PAPA). The utilization of these guiding principles will help maintain a person's privacy, ensure that the data that is collected is accurate and authenticated, helps ensure personal property rights, and sets accessibility standards for any personal data collected.

According to (Peffers et al., 2007) design science was first proposed for information systems in the early 1990's by (March & Smith, 1995; Nunamaker Jr. & Chen, 1990; Walls et al., 1992). Peffers et al. (2007) used these sources as a background to create his design science research methodology for information systems. The six step design science methodology developed by (Peffers et al., 2007) was developed to meet three objectives: consistency with prior literature, provides a nominal process model for DS research, and provides a mental model for presenting and evaluating DS research in IS. The six steps are: problem identification and motivation, definition of the objectives for a solution, design and development, demonstration, evaluation, and communication (Peffers et al., 2007). Peffers et al. (2007) DSRM offers researchers the flexibility to follow the steps in the sequence that best fits the approach to solving their research problem. Problem centered approaches would start with step one and follow a nominal sequence and object centered solutions could start with step 2 and build outwards.

Methodology

Overview of research methodology/design:

HFACS is an analytical tool designed originally for the Navy/Marine Corps aviation community for accident and incident investigations by, (Shappell et al., 2007). Figure 1 shows the conceptual model of the HFACS system and the four levels of human error in and organization. HFACS was based on the Swiss cheese model of latent and active failures concept developed by (Reason, 1990). The goal of this research is to create a methodology for information security using HFACS. The research is to find out how SA (Endsley, 1995; Flach, 1995), and human error relate to one another in order to develop methods based on HFACS (Liu et al., 2013; Shappell et al., 2007) to help improve information privacy through identifying any latent organizational conditions that lead to human error.

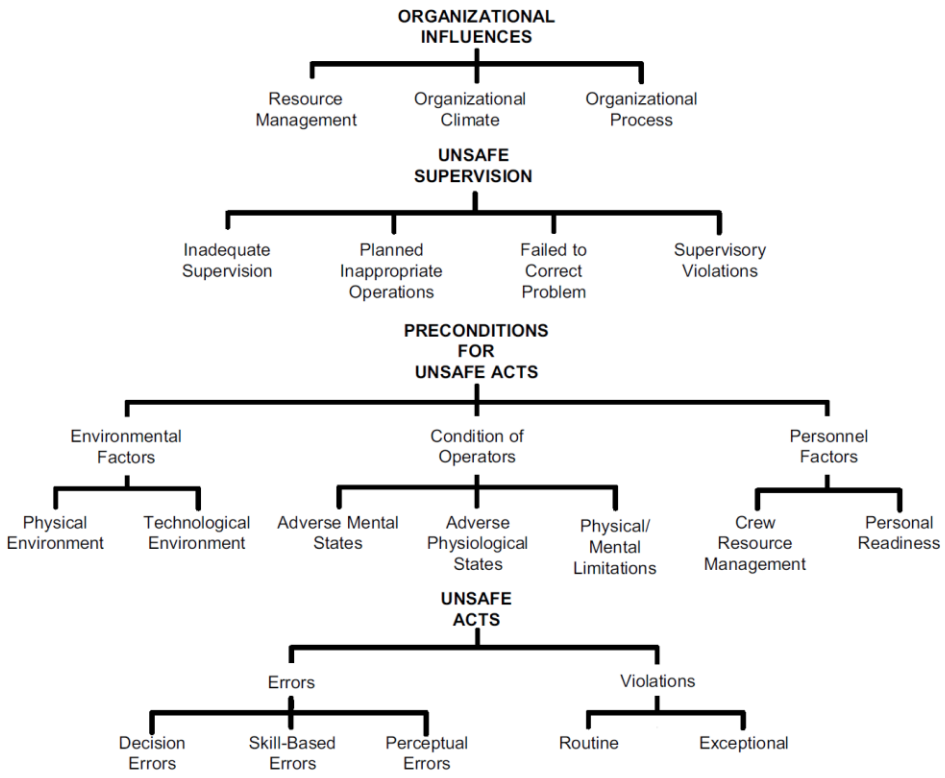

Figure 1. The HFACS framework.

Figure 1 (Shappell et al (2007)

Instrument development and validation:

A survey instrument will be developed for this research based off the HFACS checklists. Ideally the survey will be distributed to a wide variety of industries to gather as much data as possible to possible to see how information privacy is handled due to the varying regulations that govern privacy. Initial data can be gathered from the data breach clearing house to test how the reported data works in the HFACS framework to help design a survey in the correct format to avoid invalidating the testing.in order to help design a survey in the correct format to avoid invalidating the testing.

Proposed sample:

Ideally, we would like a sample size over 100 survey participants so that a valid statistical model can be constructed and that a trend analysis can be formed to see if there are any patterns that emerge from the data gathered from the participants.

The sampling will consist of IT and non-IT staff including managerial and non-managerial employees to obtain a broader sample of differing perspectives. The sample questions will be developed based on the HFACS methodology requirements and processed with the HFACS software after the data has been anonymized.

Data analysis:

All the gathered data will be entered into the standalone HFACS software package obtained from HFACS Inc. This software will provide the necessary analytical processes to classify the data into the four different tiers of the HFACS model. Once the data is processed by the HFACS software we will generate a report based on the results with appropriate tables and figures to illustrate the data being analyzed and the results. Some data may have to be manually analyzed and reformatted to be processed by the HFACS software.

Summary

In summary, this research will be geared toward finding a way to implement the HFACS framework into an information security incident testing procedure. Using lessons learned from historical incidents will provide the needed background in order to help guide us through the steps to make the implementation of the HFACS framework successful.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In *Proceedings of the Twenty-Seventh International Conference on Information Systems* (pp. 1--20). https://doi.org/10.1.1.73.2942

BakerHostetler. (2016). *Is your organization compromise ready? 2016 Data Security Incident Response Report*. Retrieved from http://f.datasrvr.com/fr1/516/11618/BakerHostetler_2016_Data_Security_Incident_Response_Report.pdf

Beatty, P. C. W., & Beatty, S. F. (2004). Anaesthetists' intentions to violate safety guidelines. *Anaesthesia*, *59*(6), 528–540. https://doi.org/10.1111/j.1365-2044.2004.03741.x

Bratus, S., Masone, C., & Smith, S. W. (2008). Why do street-smart people do stupid things online? *IEEE Security and Privacy*, *6*(3), 71–74. https://doi.org/10.1109/MSP.2008.79

Choi, M. S., & Levy, Y. (2013). *Assessing the role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills toward computer misuse intention at government agencies*. *ProQuest Dissertations and Theses*. Doctoral dissertation (UMI Number: 3599848).

Dekker, S. (2007). Doctors are more dangerous than gun owners: A rejoinder to error counting. *Human Factors*, *49*(2), 177–184. https://doi.org/10.1518/001872007X312423

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, *8*(7), 386–408. https://doi.org/Article

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64. https://doi.org/10.1518/001872095779049543

Endsley, M. R., & Conners, E. S. (2014). Cyber defense and situational awareness: Foundations and challenges. *Advances in Information Security*, *62*, 7–27. https://doi.org/10.1007/978-3-319-11391-3

Flach, J. M. (1995). Situation awareness: Proceed with caution. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 149–157. https://doi.org/10.1518/001872095779049480

Gawron, V. J., Drury, C. G., Fairbanks, R. J., & Berger, R. C. (2006). Medical error and human factors engineering: Where are we now? *American Journal of Medical Quality*, *21*(1), 57–67. https://doi.org/10.1177/1062860605283932

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Hopping, C. (2017, June). Bored workers are your biggest security risk. *IT Pro*, 1–2. Retrieved from https://search-proquest-com.ezproxylocal.library.nova.edu/advancedtechaerospace/docview/1907598505/fulltext/2619815E4E3C42EBPQ/1?accountid=6579

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science*. *Springer International Publishing Switzerland*. https://doi.org/10.1007/978-3-319-10632-8

Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers and Security*, *25*(7), 522–538. https://doi.org/10.1016/j.cose.2006.08.004

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, *38*(2), 143–154. https://doi.org/10.1016/j.apergo.2006.03.010

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers and Security*, *28*(7), 509–520. https://doi.org/10.1016/j.cose.2009.04.006

Lewis, J. (2003). Cyber terror: Missing in action. *Knowledge, Technology & Policy*, *16*(2), 34–41. https://doi.org/10.1007/s12130-003-1024-6

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, *28*(3–4), 215–228. https://doi.org/10.1016/j.cose.2008.11.003

Liu, S. Y., Chi, C. F., & Li, W. C. (2013). The application of human factors analysis and classification system (HFACS) to investigate human errors in helicopter accidents. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8020 LNAI*(PART 2), 85–94. https://doi.org/10.1007/978-3-642-39354-9-10

Maher, M. Lou. (2011). Leadership in science and technology:Design science. *SAGE Reference Online*, 113–121. https://doi.org/http://dx.doi.org/10.4135/9781412994231.n13

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, *10*(1), 5. https://doi.org/10.2307/248873

Maxion, R. A., & Reeder, R. W. (2005). Improving user-interface dependability through mitigation of human error. *International Journal of Human Computer Studies*, *63*(1–2), 25–50. https://doi.org/10.1016/j.ijhcs.2005.04.009

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia - Social and Behavioral Sciences*, *147*, 424–428. https://doi.org/10.1016/j.sbspro.2014.07.133

Myers, M. D., & Venable, J. R. (2014). A set of ethical principles for design science research in information systems. *Information Management*, *51*(6), 801–809. https://doi.org/10.1016/j.im.2014.01.002

Niiniluoto, I. (2014). Values in design sciences. *Studies in History and Philosophy of Science Part A*, *46*, 11–15. https://doi.org/10.1016/j.shpsa.2013.11.002

Norman, D. A. (1981). Steps toward a cognitive engineering: Design rules based on analyses of human erros, 378–382.

Norman, D. A. (1983). Design rules based on analyses of human error. *Communications of the ACM*, *26*(4), 254–258. https://doi.org/10.1145/2163.358092

Nunamaker Jr., J. F. F., & Chen, M. (1990). Systems development in information systems research. *System Sciences, 1990., Proceedings of the Twenty-Third Annual Hawaii International Conference on*, *iii*(3), 89–106. https://doi.org/10.1109/HICSS.1990.205401

Parsons, K., Mccormac, A., Butavicius, M., & Ferguson, L. (2010). Human Factors and Information Security : Individual , Culture and Security Environment. *Science And Technology*, (DSTO-TR-2484), 45. https://doi.org/10.14722/ndss.2014.23268

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014).

Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Puhakainen, P. P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757–778. Retrieved from http://dl.acm.org/citation.cfm?id=2017496.2017502

Qian, Y., Fang, Y., & Gonzalez, J. J. (2012). Managing information security risks during new technology adoption. *Computers & Security*, *31*(8), 859–869. https://doi.org/10.1016/j.cose.2012.09.001

Reason, J. T. (1990). *Human error* (First). Cambridge England ; New York: Cambridge University Press.

Reason, J. T. (1995). Safety in the operating theatre — Part 2: Human error and organisational failure. *Current Anaesthesia & Critical Care*, *6*(2), 121–126. https://doi.org/10.1016/S0953-7112(05)80010-9

Safa, N. S., Solms, R. Von, Futcher, L., von Solms, R., Futcher, L., Solms, R. Von, … Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud and Security*, *2016*(2), 15–18. https://doi.org/http://dx.doi.org.library.capella.edu/10.1016/S1361-3723(16)30017-3

Shappell, S. A., Detwiler, C., Holcomb, K., Hackworth, C., Boquet, A., & Wiegmann, D. A. (2007). Human error and commercial aviation accidents: An analysis using the human factors analysis and classification system. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *49*(2), 227–242. https://doi.org/10.1518/001872007X312469

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Sim, I. (2010). *Online information privacy and privacy protective behavior: How does situation awareness matter? ProQuest Dissertations and Theses*. Doctoral dissertation (UMI Number: 3437383).

Simon, H. (1996). *The sciences of the artificial* (3rd ed.). Cambridge, MA: MIT

Press.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Siponen, M. (2001). Five dimensions of information security awareness. *Computers and Society*, *31*(2), 24–29. https://doi.org/10.1145/503345.503348

Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an information system design theory for vigilant EIS. *Information Systems Research*, *3*, 36–59. https://doi.org/10.1287/isre.3.1.36

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, *44*(March 2016), 1–15. https://doi.org/10.1016/j.cose.2014.04.005

Wiegmann, D. A., & Shappell, S. A. (2001). Human error analysis of commercial aviation accidents: application of the Human Factors Analysis and Classification system (HFACS). *Aviation, Space, and Environmental Medicine*, *72*(11), 1006–16. https://doi.org/10.1037/e420582004-001

Wood, C. C., & Banks, W. W. (1993). Human error: An overlooked but significant information security problem. *Computers & Security*, *12*(1), 51–60. https://doi.org/10.1016/0167-4048(93)90012-T