Human Decision Models in Computer Security

Andrew Marturano
University of Illinois at Urbana-Champaign
Coordinated Science Laboratory
martura2@illinois.edu

Mohammad Noureddine
University of Illinois at Urbana-Champaign
Coordinated Science Laboratory
nouredd2@illinois.edu

Masooda N. Bashir
University of Illinois at Urbana-Champaign
Coordinated Science Laboratory
mnb@illinois.edu

ABSTRACT

In this paper, we first discuss the importance of the human aspect of security, and what kind of research has been carried out. We then introduce and discuss the methodology of our systematic review of literature on the subject. We then suggest areas for further research, as well as any limitations we encountered.

Keywords

Digital Security, Privacy, Mental Models, Information Security Awareness, Information Security Misuse

1. INTRODUCTION

The science of security is a topic that has become increasingly important, especially given the rate that technology has progressed over the past 25 years. In order to ensure that the systems that are implemented are truly secure, we have to consider the non-technological piece of the puzzle: the human factor. While a system can be secure from a technical standpoint, humans inevitably make mistakes. They write passwords on notecards next to their workstation or work at home on their personal computer. To err is human, and in order to create a more secure system, we must examine the underlying aspects of human decisions. Therefore, we believe a thorough literature review of the existing research on human decision-making models related to security applications is a necessary and worthwhile step forward. This review will benefit our understanding of how human perceptions of security are made, as well as what the overall findings include. In addition, this review will help us to understand what research and theories have already been used, as well as what patterns have been found.

2. METHODOLOGY

This review of literature examined papers pertaining to human decision-making models in computer security. For the study selection, the following keyword combinations were used: *perceived risk*, *password policy*, *risk decision-making*, *security awareness*, and *security decision-making models*. Since user-based security research falls under many different fields (psychology, computer science, economics, criminology, etc.) different combinations of keywords were used throughout the literature search in order to maximize the number of relevant studies. This allowed for the inclusion of studies that fit the selection criteria, but perhaps had a title that did not include the keywords.

Because of this, “snowball” methods were employed to supplement the results of keyword searches. This refers to examining the references of relevant studies to expand the pool of studies. By using this method, studies that influenced the current pool of knowledge could be included as well.

An initial search of six library databases (ACM, IEEE Xplore, JSTOR, PsycINFO, UIUC Library Database, and Web of Science) yielded 513 potentially eligible papers. In order to further refine the scope of the literature review, specific criteria for inclusion were drafted. The inclusion criteria for papers in this review included the following: must reference concrete experimental data (no conjecture), have a psychological basis of theory in the research model, and must be published between 2000 and the present (2015). These publication dates (2000-2015) were used because current events of the early 2000s spurred much more research on human usability than previous years.

The criteria eligibility screening yielded 58 eligible papers. The candidates were evaluated by relevance, methodology, and nature of their findings. After evaluation, 26 papers had to be disqualified, as they were found to be restating existing information, or not citing experimental data for validation. This left 32 eligible studies on which we conducted this systematic review.

3. BACKGROUND

It has been recognized for some time that humans were an integral part of computer security, and as a result there has been an abundance of research on the subject. Although there have been many studies, and work on modeling human behavior in security, there has been little done in the way of summary and meta-analysis. This study identifies the mental models that are used in existing research, and appraises them by the frequency that they occur. By doing this, further work can be carried out to examine untapped applications of user-centered security.

4. FINDINGS

The preliminary literature search yielded several theories of human decision-making, which appeared in several papers. Table 1 shows the data for theories of decision-making, and the frequency at which they appeared in the included studies. Additional analysis will be carried out as we continue to explore the topic. In the following sections, a brief description of the relevant theories will be provided. The theories will be presented in order of how frequently they appeared in the selected studies.

4.1 General Deterrence Theory

As shown in Table 1, this theory appears in 8 separate studies included in the literature review, establishing it as a major factor in human decision-making models of security. This theory focuses on disincentives or sanctions against committing a criminal act, where

Conference’10, Month 1–2, 2010, City, State, Country.

DOI: 10.475/1234

sanctions are formal punishments for failing to follow established security policy [2].

Table 1. Mental Model Prevalence in Relevant Research

Psychological Theory	Year	Author	Category of Application
General Deterrence Theory	2012	Crossler et al.	Information security, future directions for research
	2009	D'Arcy et al.	Information security misuse
	2009	Herath et al.	Penalties of behavior, perceived effectiveness
	2004	Lee et al.	Computer abuse, social control
	2010	Siponen et al.	Neutralization, information security misuse
	2011	Son et al.	Compliance, motivation
	2010	Tam et al.	Password management, risk perception
	2005	Theoharidou et al.	Information security standards, policy
Theory of Planned Behavior	2009	Beautement et al.	Security compliance budget, security behavior in organizations
	2010	Bulgurcu et al.	Security policy compliance, information security awareness
	2009	Herath et al.	Penalties of behavior, perceived value/effectiveness
	2011	Ifinedo et al.	Behavioral compliance, intrinsic/extrinsic motivation
	2009	Ng et al.	Health care connections, security awareness, email attachments
	2011	Son et al.	Intrinsic/extrinsic motivation, perceived value
Rational Choice Theory	2009	Anderson et al.	Costs/benefits of security, risk perceptions
	2009	Beautement et al.	Security compliance budget, security behavior in organizations
	2010	Bulgurcu et al	Security policy compliance, information security awareness
	2008	Verendel et al.	Bounded rationality, perceptions of risk, decision-making
Protection Motivation Theory	2011	Ifinedo et al.	Intrinsic/extrinsic motivation
	2010	Johnston et al.	Fear appeals, threat appraisal
	2009	Ng et al.	Health care connections, security awareness, email attachments
	2010	Tam et al.	Password management, risk perception

The theory's main aspects are the *Certainty of Sanctions* (probability of being punished) and the *Severity of Sanctions* (degree of punishment associated with the act).

4.2 Theory of Planned Behavior

This theory was referenced the second most times among the studies in the literature search, as shown in Table 1. This theory suggests that intentions are an important factor for predicting behavior. This is most affected by the person's attitude toward the behavior, social factors, and control factors [3]. A person's *Attitude toward Behavior* is the degree to which a person does or does not favor a certain behavior. If he/she perceives the result of a behavior as positive, he/she will shape a positive attitude towards it, and vice versa (negative perception will shape a negative attitude). *Social Factors* are normative beliefs concerning a behavior. In order for a person to adopt a behavior, he or she must first be motivated to comply with its social demands. *Control Factors* mean that a person shapes his/her intentions in regard to a particular behavior based on his or her personal beliefs.

4.3 Rational Choice Theory

This theory did not appear in as many studies (Table 1) as the previous two, but we found that it was mentioned alongside the more prevalent theories, leading us to believe that it is significant. This theory states that an individual determines how s/he will act by balancing the costs and benefits of her/his actions. The individual recognizes alternative courses of action and contemplates the likely outcomes of each course of action. An *outcome* is defined as the state of the world after an action is taken, and a given action can lead to various outcomes [1].

4.4 Protection Motivation Theory

Like Rational Choice Theory, this theory was not as common as a reference compared to the first two (Table 1), but Protection Motivation Theory provides general frameworks of human decision-making that are broadly relevant to the research topic. The theory adds another factor to the already established Theory of Planned Behavior, and asserts that motivation emanates from not only the threat appraisal (Certainty/Severity of Sanction), but from the coping appraisal as well. *Coping Appraisal* is defined as an individual's assessment of his or her ability to cope with a threat [4]. This breaks down into three factors: self-efficacy, response efficacy, and response cost. *Self-Efficacy* is an individual's judgment regarding his or her capabilities to cope with and avert the potential loss or damage arising from a threat. *Response Efficacy* is the compliance with information security policy as being an effective mechanism for detecting threats. *Response Cost* emphasizes the perceived opportunity costs in terms of money, time, or effort extended in adopting the recommended behavior.

5. LIMITATIONS

The keywords used for the literature search covered most of the relevant information, but searching with a more expansive inventory of relevant keywords would yield a larger pool of research. This would also decrease the reliance on snowball methods to increase the pool of knowledge.

Another limitation was the time frame criteria. Through research, we discovered that many of the theories stem from older, non-digital research in a variety of fields. Since our initial criteria could not include research from before the year 2000, we had to leave out some original sources of the theories. A more thorough review that includes older research will be presented as our research progresses further in the coming months.

6. CONCLUSIONS AND FUTURE WORK

The content of this review showcases our overall research findings thus far. This review is a preliminary analysis; it offers one of the first steps in predicting human decision-making behavior in computer security. We are currently in the process of completing a more robust review, as well as examining the relevant theories in greater detail.

7. ACKNOWLEDGMENTS

This material is based upon work supported by the Maryland Procurement Office under Contract No. H98230-14-C-0141

8. REFERENCES

[1] Bulgurcu, B., et al. (2010). "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness." MIS Quarterly **34**(3): 523-548

[2] D'Arcy, J., et al. (2009). "User Awareness of Security Countermeasures and Its Impact on Information Systems

Misuse: A Deterrence Approach." Information Systems Research **20**(1): 79-98.

[3] Ifinedo, P. (2012). "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory." Computers & Security **31**(1): 83-95.

[4] Johnston, A. C. and M. Warkentin (2010). "FEAR APPEALS AND INFORMATION SECURITY BEHAVIORS: AN EMPIRICAL STUDY." MIS Quarterly **34**(3): 549-A544.

[5] Son, J.-Y. (2011). "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies." Information & Management **48**(7): 296-302.