Federation of Business Discipline Journal
Volume 13 2022 3 - 11

A THEORETICAL FRAMEWORK FOR STUDY OF INFORMATION BEHAVIOR BY OPPORTUNISTIC INSIDERS

Vikas Sinha
Bill Randall
University of North Texas,
Denton, Texas 76203

ABSTRACT

As typical computing infrastructure in enterprises become highly complex and distributed, most enterprises have adopted stronger perimeter-based and asset-based network security to lock down access to infrastructure securely and protect their information assets. In the recent decade, a significant amount of research has focused on better-protecting enterprises' infrastructure and their information assets by further enhancing from the traditional data protection, identity and access management, and data privacy approaches to more holistic enterprise security and privacy management strategies. All these advancements help reinforce enterprise perimeter security as well as improve controls for information assets.

Researchers are actively pursuing an area studying the threat to enterprises' data and information from insiders. Insiders are employees with authorized access to enterprises' networks, systems, and data. There is a risk that an insider can intentionally exceed their granted access and opportunistically misuse the information that is available to them through their customary access rights.

This exploratory research undertakes a review of the scholarly publications and extends the understanding by exploring various relevant models and other corresponding theories to propose a conceptual model which could be applied to understand the antecedents to human factors that lead to an opportunistic insider exhibiting such malicious intent in their information behavior.

Keywords:

INTRODUCTION

As typical computing infrastructure in enterprises become highly complex and distributed, most enterprises have adopted stronger perimeter-based and asset-based network security to lock down access to infrastructure securely. In the recent decade, a significant amount of research has been done on better protecting an enterprise infrastructure and information. Organizations are lately leveraging concepts from the "zero-trust architecture" framework (Rose et al., 2020) to secure corporate information and access to that information, and further enhancing from the traditional data protection (Ragavan, 2012), identity and access management, and data privacy (Luther, 2007) approaches to more holistic enterprise security and privacy management strategies. All these advancements help reinforce the enterprise perimeter security as well as improve controls for information assets.

An area that is actively being pursued by researchers is the study of the threat to an enterprises' data and information from insiders. Insiders are employees with authorized access to enterprises' networks, systems, and data. There is a risk that an insider can intentionally exceed their granted access and opportunistically misuse the information that is available to them through their normal permitted access rights.

This paper presents a theoretical and conceptual construct to understand the antecedents to human factors that lead to an opportunistic insider exhibiting malicious behavior with information to which the enterprise has granted them the rights. Theory of Reasoned Action Framework and Social Control Theory are adopted as foundation to propose a theoretical framework that integrates elements from both these theories.

THE MALICIOUS INSIDER

Since the insiders have legitimate and authorized access to the information, it is inherently complex and challenging to detect such misuse of information. This paper focuses on establishing a theoretical framework for understanding the antecedents to opportunistic information behavior by insiders and subsequent abuse of that information with malicious intent. Let's consider a hypothetical situation to understand what opportunistic information behavior and malicious misuse intent could be. Consider a human resources manager at a company. This individual has access to all employee records, including information on compensation, social security numbers, demographics, ethnicity, health-related information, background check reports, immigrant/visa status, performance reviews, ratings and rankings, disciplinary actions, and plenty more. In short, the HR manager has information available to easily profile an employee in any dimension. An individual with malicious intent could leverage this information to take advantage of and benefit from vulnerable employees. The misuse of this information could range from simple manipulation of employee performance ratings in the company records to extreme blackmailing for financial gains with, say, information relating to sexual harassment. While the topic of "to trust or not to trust HR" can be a separate discussion on its own, here we will stay with trying to understand the antecedents to such behaviors that can be severely damaging to any organization and its employees. Such behaviors expose the organizations to the risk of lawsuits and severely tarnish their reputation and standing in the industry.

While the above hypothetical example illustrates malicious insiders' information behavior, another recent real-world example would be the information behavior demonstrated by Edward Snowden (MacAskill & Dance, 2013) which became a matter of national security with the information sharing becoming a discussion item on the global stage. WikiLeaks too has been notorious for making sensitive or private information public, made available to them through anonymous insiders of various corporations or governments. These are examples of the behavior the model proposed in this paper seeks to address.

LITERATURE REVIEW

According to an insider threat study jointly done by the United States Secret Service and Software Engineering Institute CERT program at Carnegie Mellon University (Cappelli et al., 2012), such insider threats require more deliberation than just considering it to be a problem that can be mitigated only by software or hardware enhancements. Researchers have focused primarily on techniques for the detection and control of insider threats (Adams, 2013; Al-Mhiqani et al., 2020; Hasheem, 2018). Some researchers have explored employees' risk-taking behaviors that can emerge as insider threats (Alohali et al., 2018; Johnston et al., 2019). There appears to be an opportunity to understand further why individuals engage in such behaviors by exploring and discovering the antecedents to such behaviors.

Table 1: Literature review map

Focus	**Subtopic**	**Literature Reviewed**	**Key Theory Referred**
Detection threat and violations	Computational techniques, ML, AI, etc	- Velpula & Gudipudi (2009) - Hashem (2018) - Harris (2020) - Sticha & Axelrad (2016)	Integrated Systems Theory
	Biometrics and human body response tracking	- Jenkins et al (2019) - Hashem (2018)	
	Communal/group behavior	- Chen et al (2012) - Johnston et al (2019)	Socioecological Theory, Social Disorganization Theory
Understanding behavior	Employee/social behavior	- Randazzo et al (2005) - Cappelli et al (2012) - Harris (2020) - Ngufor (2020) - Alohali et al (2018)	Social Control Theory
	Modeling and simulation	- Sokolowski et al (2016) - Burns et al (2017)	
	Psychological factors	- Sticha & Axelrad (2016)	
Organizational threat management	Suppressing access controls and heavy hand enforcement	- Yaseen & Panda (2012) - Adams (2013)	Enterprise Risk Management Theory
	Awareness campaigns and improving processes	- Stewart & Jürjens (2017) - Dhillon et al (2020) - Shaw et al (1999)	
	Security best practices	- Harris (2020)	Integrated Systems Theory

A review of the literature on the topic of insider threats (Table 1) from the recent few years illustrates most research focus has been on insider threat detection and prevention and very little on understanding the motivations for someone to engage in morally inappropriate behavior with the information they are privileged to. Some of the leading theories that were leveraged by the researchers to provide theoretical foundation for their work include: Integrated Systems Theory (Harris, 2020), a unified framework considering policy, controls, and risk as integrated elements for understanding the controls required to protect organization's information; Socioecological Theory (Johnston et al., 2019), a framework for observing interaction between personal traits of an individual and the environmental factors; Social Disorganization Theory (Johnston et al., 2019), establishing factors for strength of a society to develop into more resilient communities wherein employees in an organization would say something when they saw something inappropriate happening; Social Control Theory (Wiatrowski, et al., 1981; Ngufor, 2020), foundation to explain delinquent behavior in individuals through their implicit societal norms; Enterprise Risk Management Theory (Adams, 2013), risk-reward equilibrium in corporate executive management decision making as a framework for determining policies and controls for enterprise security; and Grounded Theory (Thompson, 2014), where the researcher is proposing a new emergent theory on insider threat resilience based on their study.

THEORETICAL FRAMEWORK AND CONCEPTUAL MODEL

To understand why someone would engage in information behavior with the intent of malicious use of such information, we need to seek an understanding of factors that influence an individual's ability to understand right from wrong in various situations. These factors could be explicit, such as a desire for a financial gain, or implicit, such as professional jealousy. While there could be factors that can motivate an individual to engage in such risky behavior, there could be also be complementing factors that can provide a reverse motivation, or sort of demotivation, possibly due to the fear of consequences if caught performing the malicious act. There are two theories that emerged as appropriate for use in the current context. These are the theory of reasoned action framework (Ajzen & Fishbein, 1977) and the social control theory (Hirschi, 1974). Both these theories propose constructs that can be adopted to construct the "yin-yang" of motivational factors and demotivational factors that often influence the character and intent of an individual. This section will briefly explain the relevance of these theories and how they are adopted for the current study.

Theory of reasoned action framework (TRA)

Theory of reasoned action framework's (Ajzen & Fishbein, 1977) foundational premise is that any action is always preceded by an intention to actually perform that action. Such intention is rationalized by aggregation of two components – attitude and subjective norms. Attitude refers to the ease with which an individual may be driven towards engaging in a specific behavior, and the subjective norms define their internal sense of approval to engage in that behavior. A typical application of TRA is in the areas of psychological and behavioral sciences, where the objective is often to understand why people do what they do. An example application of TRA would be to understand why students cheat in exams (Simkin & McLeod, 2010).

The concept of attitude and subjective norms is adopted in this study's theoretical framework (Figure 1). Attitude is presented as the "yin-yang" of the motivational and demotivational factors that may influence an individual's risk-reward judgment ability while contemplating a malicious use of information. The subjective norms represent the societal factors, which introduce the fear of repercussions and exclusion from their peer group should they be caught performing the malicious act. The attitude and subjective norm together are assumed to define the information behavior of the individual.

Social control theory (SCT)

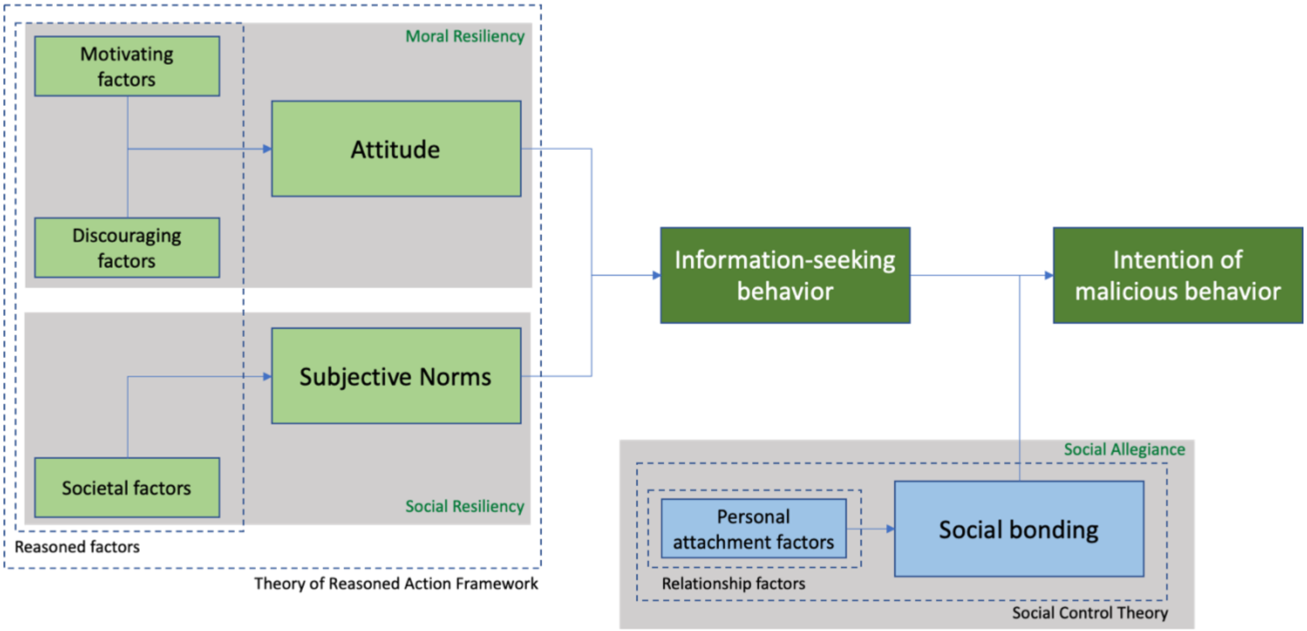
Hirschi's (1974) proposed the social control theory as a viable framework to explain internal means of control, such as their own sense of right or wrong, for any individual. SCT focuses on the strength of an individual's social bonds and presents it as playing an essential role in reducing the likelihood of engaging in malicious activities or criminal behavior. Strength of social bonds is driven by key elements such as the individual's sensitivity to failing in the eyes of a revered individual they respect and worship, their commitment to the norms and conventions of the group they believe they belong to, their level of involvement in group's conventional activities, and their beliefs in the shared values accepted by their group. SCT is often used for understanding the behavior of individuals in the field of criminology and delinquency.

The concept of social bonding resulting from personal attachment is introduced in the theoretical framework (Figure 1), as an influencer to the information behavior to predict the individual's intention of malicious behavior. SCT framework was applied by Ngufor (2020) in the context of insider threat assessment to understand the behavior of individuals attempting to exploit information vulnerabilities and the impact of the strength of supervision on decelerating that behavior.

Theoretical framework

The theoretical framework proposed in this study (Figure 1) is assimilated through the aggregation of concepts from theory of reasoned action and social control theory. The concept of attitude and subjective norms from TRA are applied to reflect an individual's information behavior. Social bonding concept from SCT is used as a mediating influencer to the information behavior.

Figure 1: Theoretical framework

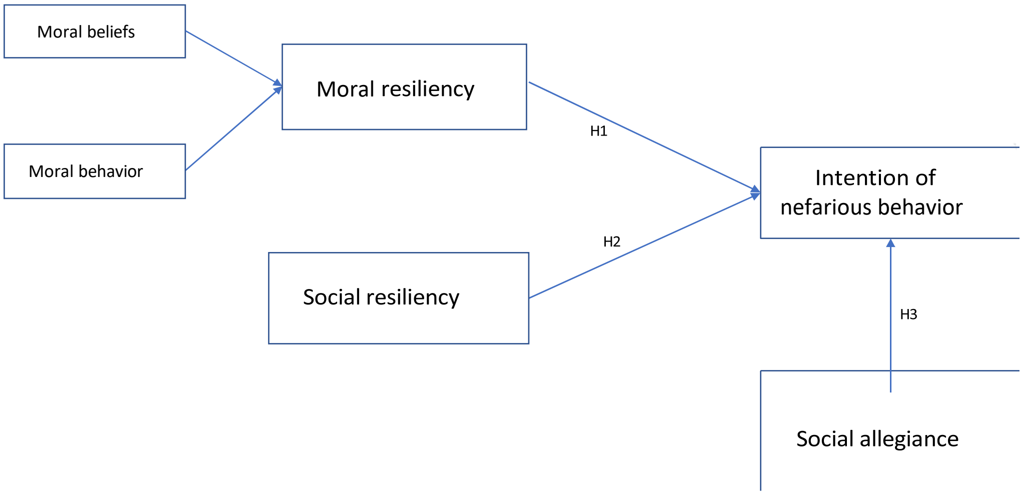


Conceptual model

Following the theoretical framework, a conceptual model was derived to understand the antecedents to the information behavior, which may be considered malicious, unethical, or antisocial, as described in the earlier sections (Figure 2).

The model adopts TRA's attitude factors as representing moral resiliency and subjective norms factors from TRA as representing social resiliency. The combination of moral resiliency and social resiliency are indicators of an individual's information behavior. The social bonding factor from SCT is introduced as a representation of social allegiance, which is presented as having a mediating effect on the intention of malicious behavior with the use of information.

Figure 2: Conceptual model



Moral resiliency is the individual's internal strength to hold up against doing anything wrong with the information they have access to, controlled by their moral beliefs and moral behaviors. Moral belief is how an individual internally deals with opportunistic situations. Would they engage in doing something inappropriate if no one is watching? Are they situationally self-conscious, i.e., know the action they are about to perform is inappropriate? Are they the type who would blame others for their actions, viz., "I must do this because I have no other choice" or "others do it and are never caught, so it must be ok for me to do the same"? The answers to these types of questions would present the antecedents to motivating their behavior to take advantage of the opportunity. Moral behavior reflects their motivation to comply with established norms, their self-efficacy to comply. Does the individual believe that the information is an asset of the company and does not belong to them personally regardless of their access level? Are they the type that will speak up if they see someone else engaging in similar inappropriate behavior? Answers to these types of questions would present the antecedents that drive their moral behavior.

A combination of moral resiliency and social resiliency presents the internal balance, or the "yin- yang" referred to in the earlier section, on how an individual may be likely to behave with information at their disposal.

The model introduces an additional component of social allegiance to describe an individual's decision making to differentiate wrong from right. Individuals often have a revered person, a mentor, a coach, an elderly person in the family, etc., who they look up to. They want to be seen by these people as being on high moral ground, as a person of integrity, as someone trustworthy and responsible. Before knowingly engaging in a malicious act, there is a possibility for the individual to consider if their action would let down any of these people they respect, what would those people think when they find out about the malicious behavior this individual engaged in with the information that was implicitly trusted with the person. This social allegiance, feeling of obligations to others, could be a strong mediating factor to the negate the intent of the individual to engage in any malicious or nefarious behavior with information.

The following hypotheses are proposed to test the model.

H1: Moral resiliency has a positive influence on information behavior

Individuals with positive moral beliefs and positive moral behaviors demonstrate a higher moral resiliency, which will prevent them from engaging in the misuse of the information available to them with any malicious intent. This is their internal mechanism for managing the temptation of taking undue advantage of the information available to them.

H2: Social resiliency has a positive influence on information behavior

Individuals may constrain their intent to misuse information due to perceived ethical expectations from their relevant peer group and the fear of getting isolated, disowned, or ostracized by their group. Such impact of the peer group influences an individual's social resiliency and creates an implicit prejudice towards their choice of actions to be ethical or not.

H3: Social allegiance is a mediating factor in information behavior

Individuals with stronger social allegiance are likely not to want to bring shame to their family, friends, loved ones, and others in the society they relate with. Stronger social allegiance could act as a mediating factor in an individual's decision not to engage in the malicious use of information.

CONCLUSION

The information behavior and intent of individuals can be modeled with the theoretical framework and the conceptual model proposed in this paper. Moral resilience and social resilience help formulate an individual's information attitude and social allegiance moderate the choice of ethical or malicious use of that information.

REFERENCES

Adams, M. (2013). *Employees as a threat: Developing effective performance monitoring systems* (Publication No. 1490996824) [Master's thesis, Utica College]. ProQuest Dissertations and Theses.

Ajzen, I., & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological bulletin*, *84*(5), 888-918.

Al-Mhiqani, M. N., Ahmad, R., Zainal Abidin, Z., Yassin, W., Hassan, A., Abdulkareem, K. H., Ali, N. S., & Yunos, Z. (2020). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. *Applied Sciences*, *10*(15), 5208.

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information and Computer Security*, *26*(3), 306–326.

Burns, A. J., Posey, C., Courtney, J. F., Roberts, T. L., & Nanayakkara, P. (2017). Organizational information security as a complex adaptive system: Insights from three agent-based models. *Information Systems Frontiers, 19*(3), 509–524.

Cappelli, D., Moore, A., & Trzeciak, R. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud)*. Addison-Wesley.

Chen, Y., Nyemba, S., & Malin, B. (2012). Detecting anomalous insiders in collaborative information systems. *IEEE Transactions on Dependable and Secure Computing, 9*(3), 332–344.

Dhillon, G., Talib, Y. Y. A., & Picoto, W. N. (2020). The mediating role of psychological empowerment in information security compliance intentions. *Journal of the Association for Information Systems, 21*(1), 152–174.

Harris, C. D. (2020). *Understanding controls to detect and mitigate malicious privileged user abuse* (Publication No. 2441239943). ProQuest Dissertations and Theses.

Hashem, Y. (2018). *Multi-modal insider threat detection and prevention based on users' behaviors*. ProQuest Dissertations and Theses.

Hirschi, T. (1974). *Causes of delinquency*. University of California Press.

Jenkins, J. L., Proudfoot, J. G., Valacich, J. S., Grimes, G. M., & Nunamaker, J. F. Jr (2019). Sleight of hand: Identifying concealed information by monitoring mouse-cursor movements. *Journal of the Association for Information Systems*, *20*(1), 1–32.

Johnston, A. C., Gangi, P. M. D., Howard, J., & Worrell, J. (2019). It takes a village: Understanding the collective security efficacy of employee groups. *Journal of the Association for Information Systems*, *20*(3), 186–212.

Luther, M. (2007). Identity-based encryption: From identity and access management to enterprise privacy management. *Information Systems Security, 16*(1), 9-14.

MacAskill, E., & Dance, G. (2013, November 1). *NSA files decoded: Edward Snowden's surveillance revelations explained*. The Guardian.

Ngufor, F. A. (2020). *Understanding the perspectives of information security managers on insider threat: A Phenomenology Investigation* (Publication No. 27957983). ProQuest Dissertations and Theses.

Ragavan, H. (2012). *Insider threat mitigation models based on thresholds and dependencies*
(Publication No. 1508837). ProQuest Dissertations and Theses.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector* (TECHNICAL REPORT CMU/SEI-2004-TR-021). Software Engineering Institute, Carnegie Mellon University.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture.

Shaw, E. D., Post, J. M., & Ruby, K. G. (1999). Inside the mind of the insider. *Security Management*, *43*(12), 34–44.

Simkin, M. G., & Mcleod, A. (2010). Why Do College Students Cheat? *Journal of Business Ethics, 94*(3), 441–453.

Sokolowski, J. A., Banks, C. M., & Dover, T. J. (2016). An agent-based approach to modeling insider threat. *Computational and Mathematical Organization Theory, 22*(3), 273–287.

Steele, S., & Wargo, C. (2007). An introduction to insider threat management. *Information Systems Security, 16*(1), 23–33.

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security, 25*(5), 494–534.

Sticha, P. J., & Axelrad, E. T. (2016). Using dynamic models to support inferences of insider threat risk. *Computational and Mathematical Organization Theory, 22*(3), 350–381.

Thompson, E. E. (2014). *Information technology security and human risk: exploring factors of unintended insider threat and organizational resilience* [Doctoral dissertation, Walden University]. ProQuest Dissertations and Theses.

Velpula, V. B., & Gudipudi, D. (2009). Behavior-anomaly-based system for detecting insider attacks and data mining. *International Journal of Recent Trends in Engineering*, *1*(2), 261-266.

Wiatrowski, M. D., Griswold, D. B., & Roberts, M. K. (1981). Social control theory and delinquency. *American Sociological*, *46*, 525–541.

Yaseen, Q., & Panda, B. (2012). Insider threat mitigation: Preventing unauthorized knowledge acquisition. *International Journal of Information Security*, *11*(4), 269–280.

ABOUT THE AUTHOR

Vikas Sinha is a doctoral candidate pursuing his PhD in Information Science with specialization in Data Science at University of North Texas. He has over 25 years of industry experience at companies such as Broadcom, CA Technologies, IBM, and SPSS. Vikas has prior advanced degrees from Northwestern University, Florida Atlantic University, and Sri Venkateswara University.

Bill Randall is a doctoral candidate pursuing his PhD in Information Science with specialization in Data Science at University of North Texas. He has over 38 years of program management, software and engineering leadership experience. Bill has prior advanced degrees from the Air Force Academy, Chapman University, and Georgia College.