Human Factors in Cybersecurity, Vol. 53, 2022, 29–35
https://doi.org/10.54941/ahfe1002198

A Closer Look at Insider Threat Research

Ivan Kong and Masooda Bashir

University of Illinois at Urbana-Champaign, Urbana, IL 61820, USA

ABSTRACT

Insider threats are a danger to organizations everywhere and can suffer greatly when a security incident occurs. Organizations suffer from individuals who expose the organization to risk or harm in some ways. This includes insiders who intentionally, or unintentionally, cause actions that bring harm or significantly increase risk to the organization. Insider security breaches have been identified by organizations as a pressing problem with no simple solution. This paper presents preliminary results of a systematic literature review of published, scholarly articles on insider threat research from 2010 to 2020. In this paper, we present an overview of topics researched in these articles, describe the methodologies used to conduct the studies, and summarize the main recommendations that are noted in the literature. For example, preliminary observations indicate machine learning, and the development of theoretical models is a prevalent practice in the literature while a common recommendation for organizations is to implement an insider threat detection program. While additional research is ongoing, we believe these early insights can provide some guidance for new researchers in the field and organizations.

Keywords: Insider threat, Human aspects

INTRODUCTION

Insider threats affect every business sector and all areas of the economy with close to 75% of the incidents going undetected or unreported according to the National Insider Threat Task Force (Maasberg et al., 2020). A 2015 survey estimated the overall cost to remediate a successful insider attack costed organizations an average of $445,000 (Trzeciak, n.d.). One of the most salient insider attacks was Stuxnet, where an insider deployed malware to sabotage the Iranian nuclear weapons program (Zetter, n.d.). In a survey reported by Trzeciak in 2017, 27% of all cybercrimes were committed by insiders (Homoliak et al., 2019). There is overwhelming evidence that insider incidents are occurring.

Any member of an organization who has access to organizational assets and sensitive information may potentially pose threats to those organizations. The topic of insider threats has been studied from technical and behavioral aspects. Timely detection and prediction of insider threats can prevent such things as financial loss and reputation loss. In addition, insider threat poses a serious dilemma to organizations because they often focus security efforts on external threats and not on internal threats. Insiders are trusted and granted permission to organizational resources for them to do their jobs.

Therefore, insider threat risk is often downplayed even though it may pose serious security threats.

Fortunately, in the past ten years, the topic of insider threat has gained much interest from various types of organizations which has led to increased research and educational programs. However, there still seems to be a lot of debate on a common definition or approach in studying insider threat. For example, the Cybersecurity and Infrastructure Security Agency (CISA) defines an insider as a person who has knowledge and or access to their organization's resources. An insider threat is the potential of the insider to bring harm to the organization's resources ("Insider Threat Mitigation Guide," n.d.). On the other hand, the National Institute of Standards and Technology (NIST) defines an insider as anyone who has access to an organization's resources and an insider threat as an entity with access to an organization's resources that can harm them wittingly or unwittingly (Paulsen and Byers, 2019).

Furthermore, there are many approaches that can be studied regarding insider threat. For example, researchers employ machine learning classification algorithms to predict if an individual will be an insider threat. Researchers also use statistical equations to identify and predict when a user will most likely commit an insider incident. Information flows are also studied to detect anomalous behavior, indicating a potential threat. However, this paper will focus on the human behavior and psychological factors that is often being studied as part of the insider threat literature.

Despite the disconnect between the research and practice of insider threat mitigations, insider threat continues to be a serious security vulnerability and no organization is immune to it. For example, Aldrich Ames committed espionage and worked as a double-agent for the Soviet Union during the 1980s while he was working for the Central Intelligence Agency. About 30 years later, Chelsea Manning was convicted in 2013 of espionage for leaking classified documents to WikkiLeaks. In 2013, Edward Snowden leaked classified information about United States surveillance programs spying on American citizens. CBS reported in 2019 Snowden considered himself a whistleblower because he believed the surveillance programs were illegal. More recently, in 2021, the Department of Justice arrested John Rowe for espionage for attempting to sell classified information to an undercover FBI agent. The suspect had a history of security violations at his former places of employment and expressed pro-Russian sentiments ("Former Defense Contractor Arrested for Attempted Espionage," 2021). These examples represent only a very small number of insider threat incidents. While the insiders' motivation varies, the outcome is still detrimental to an organization.

In addition to increased insider incidents, there is an increase in research publications related to insider threat in the past decade. However, to the best of our knowledge there are no review papers published that focus on the research trends and human aspects of insider threats. Therefore, to fill this gap we examined the insider threat literature that has been published in the past decade to draw insights regarding human behavior and psychological aspects that influence insider threat. In this paper we will focus our

report on the topics that are studied, research methodology that is used, and recommendations that are included in these papers.

BACKGROUND INFORMATION

Insider threat definitions have varied throughout the literature. Mundie, Perl, and Huth conducted a literature review and revealed 42 different definitions for *insider* and *insider threat* (Mundie et al., 2013). Kandias and colleagues stated there is not a common definition for an insider (Kandias et al., 2010). An insider, for the purposes of this literature review, is defined as an individual who is a part of an organization that has knowledge of their organization's resources. An insider threat is defined as an individual who has access to their organization's resources who carries out operations, either purposefully or accidently, that causes harm to the organization. These definitions are the same as CISA and NIST definitions for insider and insider threats since they are the established, industry-standard for defining the two terms.

What we call 'insider threats' is nothing new. For centuries, organizations were not at risk from information computing technologies (ICT). Organizations suffered from a different type of insider, who had to physically access the organizational asset to commit their crime. In the modern era, insiders access organizational assets with ease using ICTs and can cause destruction with a click of a mouse button.

Additionally, insider threat research is not a new area and has been studied extensively. One area of research is studying technical solutions to detecting insider attacks. Researchers in this area employ or devise computer hardware and software solutions to identify and deter insider attacks. Another area is researching the human aspect of insider threats. These researchers study and observe how individuals operate within their organizations and attempt to discern what traits or behaviors would identify an insider as a threat to their organization. The researchers employ a variety of different methodologies in their research such as questionnaires, surveys, and experiments.

In 1983, Quinn researched insider threats to nuclear information and nuclear facilities and how to identify insiders (Quinn, 1983). Barnes researched how to integrate computer systems to produce controlled access authorizations to individuals with a need-to-know access (Barnes, 1985). Goldman and colleagues developed a sophisticated computer program that can detect if single or multiple insiders can attack a facility or information system (Goldman et al., 1985). Butts and colleagues developed a multidisciplined insider threat detection framework to demonstrate the likelihood of an individual being a malicious insider (Butts et al., 2006). Chinchani and colleagues developed a model to predict insiders via a risk-based approach (Chinchani et al., 2005). Markham and Payne developed a hardware firewall solution to prevent insider attacks because they argued software solutions are not adequate enough to prevent insider attacks (Markham and Payne, 2001). There has been a broad spectrum of methodologies to study and combat insider threats and the research is on-going, if not actively growing, in the modern day.

Table 1. Paper and study methodology.

Study Methodology	Number of Papers
Survey	2
Experiment	6
Machine learning	24
Case study	2

METHODOLOGY

Literature Searches

To identify the relevant literature for this review, the following steps were carried out to ensure that a systematic approach was followed for the review:

- Step 1: Identify relevant search terms, keywords, and databases
- Step 2: Specify inclusion and exclusion criteria for publications
- Step 3: Search the databases for relevant literature
- Step 4: Identify and select the relevant literature

The literature review started with a search of all scholarly, peer-reviewed articles on insider threats from 2010 to 2020. The databases searched for articles included Engineering Village, Scopus, Web of Science, IEEE Xplore, APA PsychArticles, Ebscohost, SocINDEX, and ACM Digital Library. Selecting a wide range of databases ensures broad, inclusive review of the literature.

The literature review excluded: papers not from a peer-reviewed journal, papers published before 2010 and after 2020, papers in languages other than English, book chapters, editorials.

The literature publications that were eligible for inclusion were: all peer-reviewed journal articles and conference proceedings.

The following search phrases were used to identify relevant papers:

- "insider threat*" AND "human factor*"
- "insider threat*" AND "psychology"
- "insider threat*" AND "human behavior"
- "insider threat*" AND "unintentional"
- "insider threat*" AND "organizational factors"

A total of 96 articles were found across all databases and once 44 duplicates were removed, 52 unique articles remained. These 52 were the focus of this literature review. Table 1 provides count of the different types of study methodologies used by researchers.

PRELIMINARY REVIEW OF THE SELECTED LITERATURE

The past 10 years has seen significant interest in insider threat research. This literature review produced a wide variety of research topics and conclusions on insider threats. As shown in the word cloud below (Figure 1) that development of theoretical models were common topics in the literature selected for this study. In addition, position papers were another common type of paper in our review.

Figure 1: Word cloud of topics in the literature.

Table 2. Number of papers making organizational recommendations.

Category	Number of papers making this recommendation
Management culture	7
Cyber-technical improvements	4
Training	1
Awareness	4

Once all articles were collected, the first step was classifying them into categories: learning-based algorithms and human aspects. Learning-based algorithms included any type of machine-learning or classification-based research. These papers were focused on differentiating between potential insiders from non-insiders. The human aspect papers dealt with studying the individual and what personal attributes may be relevant to identifying a person as an insider. This category included human aspects concerning behavior, cognition, personality. There were 28 papers in the learning-based algorithms category and 24 human aspects papers.

Numerous papers recommended best practices for organizations to follow (Table 2). Guidance included changes to management culture, cyber-technical technology improvements, training, and awareness. Organizations can institute real-time location-based systems to support insider threat prevention (Choi and Zage, 2012). Organizational leaders, information security professionals, and end-users should all fully participate in the security management process (Guo, 2013). Organizations should also have an insider threat assessment (Mazzarolo and Jurcut, 2019) and insider threat risk reduction programs (Pereira and Santos, 2015).

CONCLUSION

In this paper we reported our initial review of the literature which included an overview of the topics that are studied in insider thereat publications, research methodology utilized in the studies and recommendations made in these papers. As mentioned above, our preliminary literature review reveals that machine learning is a common approach and predictive modeling is heavily discussed. Methodologies such as experiments followed by surveys are often the methodology for these studies. In addition, recommendation to organizations were mostly about training and awareness programs that are focused on recognizing vulnerabilities that increase the risk of committing errors that endanger the organization. Many studies stated that training and awareness programs cannot eliminate the risk associated with insider threats and that organizations must have a comprehensive mitigation strategy that include more effective safeguards to produce fail-safe measures that prevent insider threat.

ACKNOWLEDGMENT

The authors would like to acknowledge Min Cheong Kim for her content and style editing.

REFERENCES

Barnes, L.D., 1985. INTEGRATED SYSTEMS APPROACH TO MEET THE INSIDER THREAT. Nuclear materials management 14, 628–632.

Butts, J., Mills, R., Peterson, G., 2006. A multidiscipline approach to mitigating the insider threat, in: International Conference on I-Warfare and Security, ICIW 2006, March 15, 2006 - March 16, 2006, International Conference on I-Warfare and Security, ICIW 2006. Academic Conferences and Publishing International Limited, Eastern Shore, United states, pp. 29–36.

Chinchani, R., Iyer, A., Ngo, H.Q., Upadhyaya, S., 2005. Towards a theory of insider threat assessment, in: 2005 International Conference on Dependable Systems and Networks (DSN'05). Presented at the 2005 International Conference on Dependable Systems and Networks (DSN'05), pp. 108–117. https://doi.org/10.1109/DSN.2005.94

Choi, S., Zage, D., 2012. Addressing insider threat using "where you are" as fourth factor authentication, in: 2012 IEEE International Carnahan Conference on Security Technology (ICCST). Presented at the 2012 IEEE International Carnahan Conference on Security Technology (ICCST), pp. 147–153. https://doi.org/10.1109/CCST.2012.6393550

Former Defense Contractor Arrested for Attempted Espionage [WWW Document], 2021. URL https://www.justice.gov/opa/pr/former-defense-contractor-arrested-attempted-espionage (accessed 2.8.22).

Goldman, L.A., McDaniel, T.L., Stoddard, J.A., James, J.W., 1985. INSIDER THREAT VULNERABILITY ANALYSIS - MAIT UPDATE. Nuclear materials management 14, 633–635.

Guo, K., 2013. Revisiting the Human Factor in Organizational Information Security Management. ISACA Journal 6, 37–41.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., Ochoa, M., 2019. Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. ACM Comput. Surv. 52, 1–40. https://doi.org/10.1145/3303771

Insider Threat Mitigation Guide, n.d. 133.

Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D., 2010. An Insider Threat Prediction Model, in: Katsikas, S., Lopez, J., Soriano, M. (Eds.), Trust, Privacy and Security in Digital Business, Lecture Notes in Computer Science. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 26–37. https://doi.org/10.1007/978-3-642-15152-1_3

Maasberg, M., Zhang, X., Ko, M., Miller, S.R., Beebe, N.L., 2020. An Analysis of Motive and Observable Behavioral Indicators Associated With Insider Cyber-Sabotage and Other Attacks. IEEE Engineering Management Review 48, 151–165. https://doi.org/10.1109/EMR.2020.2989108

Markham, T., Payne, C., 2001. Security at the network edge: a distributed firewall architecture, in: Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01. Presented at the Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01, pp. 279–286 vol.1. https://doi.org/10.1109/DISCEX.2001.932222

Mazzarolo, G., Jurcut, A.D., 2019. Insider threats in Cyber Security: The enemy within the gates. 8. https://doi.org/arxiv.org/abs/1911.09575

Mundie, D.A., Perl, S., Huth, C.L., 2013. Toward an Ontology for Insider Threat Research: Varieties of Insider Threat Definitions, in: 2013 Third Workshop on Socio-Technical Aspects in Security and Trust. Presented at the 2013 Third Workshop on Socio-Technical Aspects in Security and Trust, pp. 26–36. https://doi.org/10.1109/STAST.2013.14

Paulsen, C., Byers, R., 2019. Glossary of key information security terms (No. NIST IR 7298r3). National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.7298r3

Pereira, T., Santos, H., 2015. Insider Threats: The Major Challenge to Security Risk Management, in: Tryfonas, T., Askoxylakis, I. (Eds.), Human Aspects of Information Security, Privacy, and Trust, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 654–663. https://doi.org/10.1007/978-3-319-20376-8_58

Quinn, E.A., 1983. INSIDER THREAT - NRC's PERSPECTIVE. Nuclear materials management 12, 85–86.

Trzeciak, R., n.d. Analytic Approaches to Detect Insider Threats 50.

Zetter, K., n.d. An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Wired.