International Institute for Applied
Knowledge Management

Refereed Paper Proceedings - KM Conference 2016 – Lisbon, Portugal
A Publication of the International Institute for Applied Knowledge Management

Exploring the motivation behind cybersecurity insider threat and proposed research agenda

[Research-in-Progress]

Angel L. Hueca, Nova Southeastern University, USA, ah1676@nova.edu

Karla Clarke, Nova Southeastern University, USA, kc1127@nova.edu

Yair Levy, Nova Southeastern University, USA, levy@nova.edu

Abstract

Cyber exploitation and malicious activities have become more sophisticated. Insider threat is one of the most significant cybersecurity threat vector, while posing a great concern to corporations and governments. An overview of the fundamental motivating forces and motivation theory are discussed. Such overview is provided to identify motivations that lead trusted employees to become insider threats in the context of cybersecurity. A research agenda with two sequential experimental research studies are outlined to address the challenge of insider threat mitigation with a prototype development. The first proposed study will classify data intake feeds, as recognized and weighted by cybersecurity experts, in an effort to establish predictive analytics of novel correlations of activities that may lead to cybersecurity incidents. It will also develop approach to identify how user activities can be compared against an established baseline, the user's network cybersecurity pulse, with visualization of simulated users' activities. Additionally, the second study will explain the process of assessing the usability of a developed visualization prototype that intends to present correlated suspicious activities requiring immediate action. Successfully developing the proposed prototype via feeds aggregation and an advanced visualization from the proposed research could assist in the mitigation of malicious insider threat.

Keywords: Insider threat, malicious insider detection, cybersecurity, motivation, cybersecurity simulation, data visualization in cybersecurity, proposed experimental research in cybersecurity.

Introduction

The advent of the information age over the last 30 years has produced many technological innovations that assist society in communication, consumerism, innovation, and information gathering along with information decimation through the Internet. As the Internet continues to grow rapidly, illegal cybercrime has become a new channel for those seeking to break the law (Wang, 2007; Donner, Marcum, Jennings, Higgins, & Banfield, 2014). According to Gray and Hovav (2014), "we live in internet time where change appears endemic and things happen much more quickly than other fields" (p. 337). Cyber exploitation and malicious activities have become more targeted and sophisticated (Choo, 2011). Advances in technology have increased the need for expert analysis, since the nature of cybercrime is rooted in information systems (Gottschalk, Filstad, Glomseth, & Solli-Saether, 2011).

Donner et al. (2014) define Cybercrime as "any form of online deviance utilizing technology" (p. 166). Cybercrime can be challenging to prove since procuring digital evidence may be extremely difficult (Wang, 2007; Donner, Marcum, Jennings, Higgins, & Banfield, 2014). Linking patterns in behavior is a major task when investigating motivation (Dweck & Leggett, 1988; Pfleeger & Caputo, 2012). Malicious insiders have found methods to abuse, manipulate, and often profit from technology, regardless of the damages such actions may cause (Claycomb, Legg, & Gollmann (2013). It is the intent of this paper to provide the theoretical foundation for understanding the motivations that may lead trusted employees on a path to malicious behavior. This will set the premise for better understanding the data scheme needed for detecting malicious insider threat. Further, this work will extend into providing an outline for two distinct work-in-progress experiments that will approach the challenge faced when detecting malicious activities.

The insider threat is recognized as one of the most significant problems and of great concern to both corporations and governments alike (Agrafiotis, Legg, Goldsmith, & Creese, 2014). Insider threats are minimally addressed by current information security practices, yet these insiders pose the greatest threats to organizations through various malicious activities (Punithavathani, Sujatha, & Jain, 2015). Many insider attacks emerge from the misuse of access privileges granted by organizations to their trusted internal employees, contractors, or third-party service providers (Ballesteros, Batten, Pan, & Li, 2015). The malicious acts that are carried out by these trusted insiders include, but are not limited to the theft of intellectual property, disclosure of national security information, fraud, and sabotage (Lindauer, Glasser, Rosen, & Wallnau, 2013).

Given such difficulty and gap in the research, the research problem that this work will aim to address is the challenge faced when mitigating malicious cybersecurity insider threat (Nostro, Ceccarelli, Bondavalli, & Brancati, 2014). This challenge is significant as it is difficult to deal with, since insiders have more information than an external hacker (Hunker & Probst, 2008). Malicious activity or criminality refers to stable differences across entities in their inclination to commit malicious or criminal acts (Birkbeck & LaFree, 1993). According to

Hirschi and Gottfredson (1987), criminality alone does not suffice for criminal activity; for a malicious or criminal act to occur, situational encouragement in the way of motivation and opportunity must exist. Coleman (1992) argued that personal monetary gains play a major role in motivating behavior in some cultures. Birkbeck and LaFree (1993) provided a connection between motivation, opportunity, and crime, concluding that motivation in the context of crime involves willingness to commit such crime and is contingent upon opportunity. Osgood, Wilson, O'Malley, Bachman, and Johnston (1996) later applied the conclusions of Birkbeck and LaFree (1993), by finding that unstructured socializing activities resulted in more deviant behaviors. Though money, time, as well as other factors may be a driving force behind malicious activity, understanding the motivating factors that influence trusted individuals to perform malicious acts and presenting patterns in a clearly decipherable interface will aid in mitigating malicious insider threat.

The overall impact of a malicious attack depends on the motivation behind the attack (Hunker & Probst, 2008). Osgood et al. (1996) illustrated several researchers that have investigated the relationship between deviant behavior and the way that people spend their time. They indicated how crime is dependent on opportunity, in accordance with Briar and Piliavin's (1965) idea of situational motivation, which stated that the motivation for delinquency is implanted in the situation rather than the person (Osgood at al., 1996). According to Coleman (1987), in 1939, Edwin Southerland defined the concept of white-collar crime as "a crime committed by a person of respectability and high social status in the course of occupation" (p. 407). Applying this concept to the technologies and integrated computational devices available today, a new paradigm emerges as a people and organizational issue; that of insider misuse of information systems in the form of delinquent behavior in the workplace (Theoharidou et al., 2005). Therefore, the central aim of this work-in-progress is to outline a research agenda for two proposed complementary experimental research studies that will curve the path for the development of a prototype for detection and alerting of insider threat in organizational settings. The next section will provide some preliminary theoretical foundation by discussing motivational factors and theory, followed by the proposed research agenda, and finally, concluding with discussions of the intendant contribution of the proposed research agenda.

Theoretical framework

The theoretical foundation applied to this stream of research is the theory of motivation. Motivation is a classical construct and refers to the key influencers on behavior though other options are present (Tolman, 1938). When faced with a problematic situation, given consideration of possible outcomes and consequences, motivation drives the particular behavior that is selected and performed through alternate means are available (Foote, 1951). Current literature acknowledges three streams of research as the foundation for the study of motivation. Kanfer (1990) identified the three streams of motivation theory research as:

1. Need-motive-value research, or person based determinants of behavior;

2. Cognitive choice research, or expectancy-value formulations;
3. Self-regulation-metacognition research, which focus on target cognition-behavior relations such as goal setting, and cybernetic control theories.

In order to understand motivation within the context of information systems (IS) security theory development, all three research streams, their constructs, and theories should be analyzed. As presented by Atkinson and Birch (1970), motivation is not directly observable – what is observed is an intricate course of behaviors and the results of such behaviors. Dweck and Leggett (1988) concluded that motivational processes that affect behavior were the result of personality variables. Kanfer (1990) indicated that motivational processes can only be inferred by the analysis of the streams of behavior, that are derived from congenital traits and environmental factors, which are "observed through their effects on personality, beliefs, knowledge, abilities, and skills" (p. 78). Consequently, Wang and Lin (2007) observed motivational factors on collaborative learning finding that collective efficacy had a positive effect on discussion behavior.

Turner (1987), in his seminal work, presented the exchange theoretic model of motivation, which highlighted the importance of marginal utility/satisfaction and profit/loss. The augmentation of satisfaction is supported by research that suggests that self-efficacy, an individual's beliefs in their ability to achieve designated goals or performance, is the greatest motivational factor in an individual's choice of activities, effort, persistence, and performance (Wang & Lin, 2007). The fundamental motivating force in classical utilitarian theory is the desire to augment satisfaction, and to circumvent deprival or retribution in social transactions (Turner, 1987). In contrast, Kanfer (1990) indicated that the dependent variables most common in motivation research are direction of behavior, intensity/action/effort, and the persistence of specific behaviors over time. In workplace setting, motivation can be ascribed to what an individual does (direction), an individual's work ethic (intensity), and the duration of an individual's work time frame (persistence) (Kanfer 1990). Thus, motivation can be ascribed from many aspects of the individual, which may be complex to fully understand.

Proposed Experimental Research and Procedures

In his classical work, Edwin H. Sutherland (1940) integrated sociology and business to better understand white-collar crime. To understand organizational deviance Vaughan (1999) applied sociological theory to assess that organizational deviance is routine nonconformity. Like cybercrime, white-collar crime may be inconspicuous and very difficult to substantiate (Gottschalk, Filstad, Glomseth, & Saether, 2011). Similarly, future research will aim to apply sociological theories like the theory of motivation when assessing insider threat mitigation. Theoharidou, Kokolakis, Karyda, and Kiountouzis (2005) applied sociological perspectives to understand the approach followed by ISO177799 when dealing with insider threat, since the social environment plays a critical role in the formation of motivation. Pfleeger and Caputo (2012) argued that incorporating an understanding of human behavior into cybersecurity technologies would aid in better development, design, and use of such tools. To better facilitate design and development of insider threat mitigation technologies, this literary analysis interprets the motivational factors that lead individuals toward malicious behavior.

A significant impediment to insider threat research programs is the lack of data to analyze (Lindauer, Glasser, Rosen, & Wallnau, 2013). In order for the data to be useful it must contain a comprehensive account of human behavior from within the monitored environment (Glasser & Lindauer, 2013). According to Lindauer et al. (2013), researchers in the insider threat domain have two options, either collect real data or use synthetic data. With mature synthetic data, a researcher can flexibly control and economically generate data sets with the desired characteristics, size, quality, and necessary measurable properties (Lindauer et al. (2013). As noted by Glasser and Lindauer (2013), because they are not real, the data sets are complete, and free from privacy restrictions or limitations. U.S. law emphasizes that the workplace and its resources are the property of the employer, furthermore, the employer is generally free to dictate permissible use of company property as the employer sees fit (Abril, Levin, & Del Riego, 2012). According to Grizalis, Strarou, Kandias, and Stregiopoulos (2014), when dealing with employee monitoring, the organization should establish a legal, affordable and effective monitoring solution that is acceptable to all stakeholders. Any data collected as a result of monitoring should be secured and should be solely for the purposes of protecting and optimizing resources Grizalis et al. (2014).

For the purposes of this experimental study, synthetic data will be used. The proposed AI-InCyThR™ will perform similar to network based Security Information and Event Management (SIEM) solutions, establishing an assumed baseline representing the cybersecurity pulse. The user's network cybersecurity pulse will serve as an established baseline from which the AI-InCyThR™ will test and compare against. The AI-InCyThR™ will analyze the synthetic data, system logs, and behavioral data for analysis. Through the use of data mining and predictive analytics, the collected data will be refined and any Type I (false positives) along with Type II (false negatives) errors, as well as correlations will be identified. Once the data has been scrubbed, the recognized feeds, weights, as well as alpha and beta correlations will be measured against the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This procedure will create a set of evidence and/or correlations as precursors to malicious cybersecurity insider threat events.

First Proposed Experimental Research

Punithavathani et al. (2015) found "the fact that the term "Insider" is in and of itself elusive that makes this issue and its many dimensions truly more difficult to understand" (p. 435). The first proposed experimental research will be conducted as a developmental study in three phases. As indicated by Ellis and Levy (2009) "developmental research attempts to answer the question: How can researchers build a 'thing' to address the problem?" (p. 326). The first proposed experimental study will develop and validate a prototype for an analytics-based malicious cybersecurity insider threat in real-time identification system.

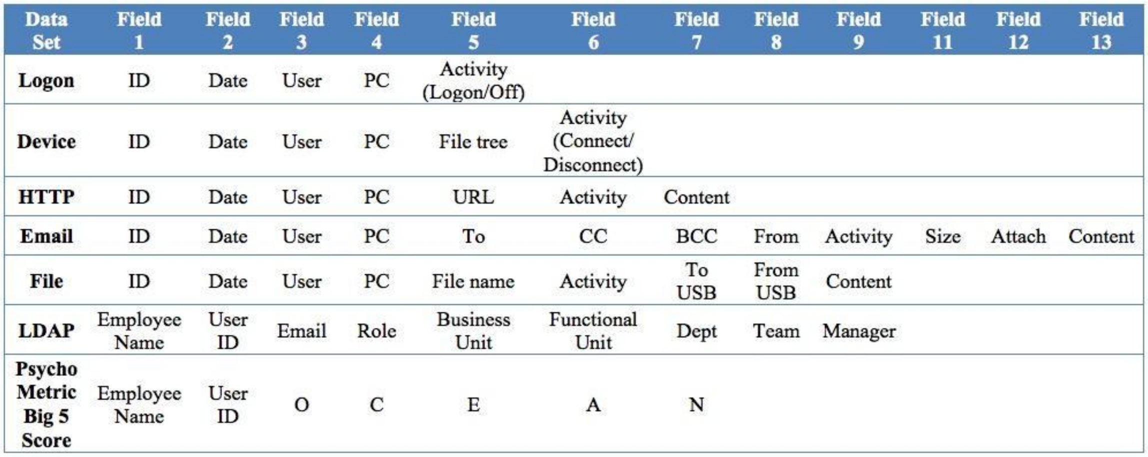
Phase one will develop benchmarking instruments known as feeds; for thorough understanding of the insider threat phenomenon a depth of exploration and analysis of the existing literature was performed. From the literature, trends and recurring themes were identified for the formulation of human-centric and techno-social feeds. Human-centric feeds are feeds that relate to individual behavioral indicators either produced by the individual employee or recorded by human resource professional, colleague, or supervisor. These include but are not limited to: stress, disengagement, anger management, personal issues, and financial difficulties. On the other hand, techno-social feeds, are feeds produced by actor activities, which register the employee's behavior and habits on the organizational network.

When comprehensive lists of feeds have been identified, a panel of information systems security experts from both industry and academia will be solicited to participate in two Delphi method evaluations of the recognized feeds validation. Once the experts have classified the most important feeds needed to identify insider threats, the experts will perform a second evaluation using the Delphi method to assign the feeds weight allocations in order of importance and unit of measure. Feeds will be collected from several sources to include, Operating system registry entries, firewall traffic, email, and network enabled mobile device activity, Web content filtering, network bandwidth usage, as well as other readily available system logs.

Phase two of this study will include the development of the Analytics-based Identifying Insider Cybersecurity Threat in Real-time (AI-InCyThR™) System. The AI-InCyThR™ system will apply determined feeds against a data set of simulated user activity available from Carnegie Mellon University's (CMU) Computer Emergency Response Team (CERT), which the authors have obtained. The data sets provide both simulated background data and data from simulated malicious actors. It is these simulated data sets that this study will utilize as the foundation for the prototype development. The data sets and fields as illustrated in Table 1.

Similar to network based SIEM solutions, the proposed AI-InCyThR™ prototype system will perform passive listening for a short timeframe establish the user's network cybersecurity pulse. The user's network cybersecurity pulse will serve as an established baseline from which the AI-InCyThR™ will test and compare against. The AI-InCyThR™ will collect simulated data, system logs, and behavioral data for analysis. Through the use of Splunk, Hadoop, and Big Data analytics tools, the collected data will be refined and any Type I (false positives) along with Type II (false negatives) errors, as well as correlations will be identified. Once the data has been scrubbed the recognized feeds, weights, and correlations will be measured against the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Risk Management Framework (RMF). This procedure will create a set of evidence and/or correlations (linear & non-linear) as precursors to malicious events.

Table 1: Simulated user activity data set



Data Set	Field 1	Field 2	Field 3	Field 4	Field 5	Field 6	Field 7	Field 8	Field 9	Field 11	Field 12	Field 13
Logon	ID	Date	User	PC	Activity (Logon/Off)							
Device	ID	Date	User	PC	File tree	Activity (Connect/ Disconnect)						
HTTP	ID	Date	User	PC	URL	Activity	Content					
Email	ID	Date	User	PC	To	CC	BCC	From	Activity	Size	Attach	Content
File	ID	Date	User	PC	File name	Activity	To USB	From USB	Content			
LDAP	Employee Name	User ID	Email	Role	Business Unit	Functional Unit	Dept	Team	Manager			
Psycho Metric Big 5 Score	Employee Name	User ID	O	C	E	A	N					

Phase three of the first proposed experimental research will begin the analysis of the evidence and/or correlations against the cybersecurity pulse, and the development of the correlation hierarchical bundling visualizations will occur; with correlations established through real-time data visualization and chord diagrams as seen in Figure 1.

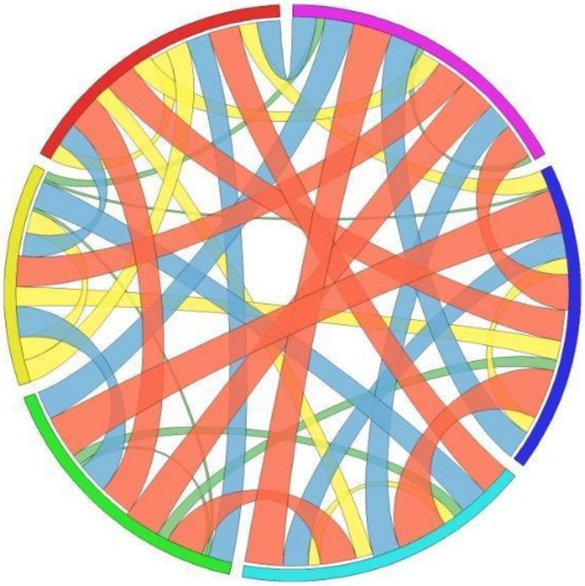


Figure 1: Proposed Correlation Hierarchical Bundling Visualization for AI-InCyThR™

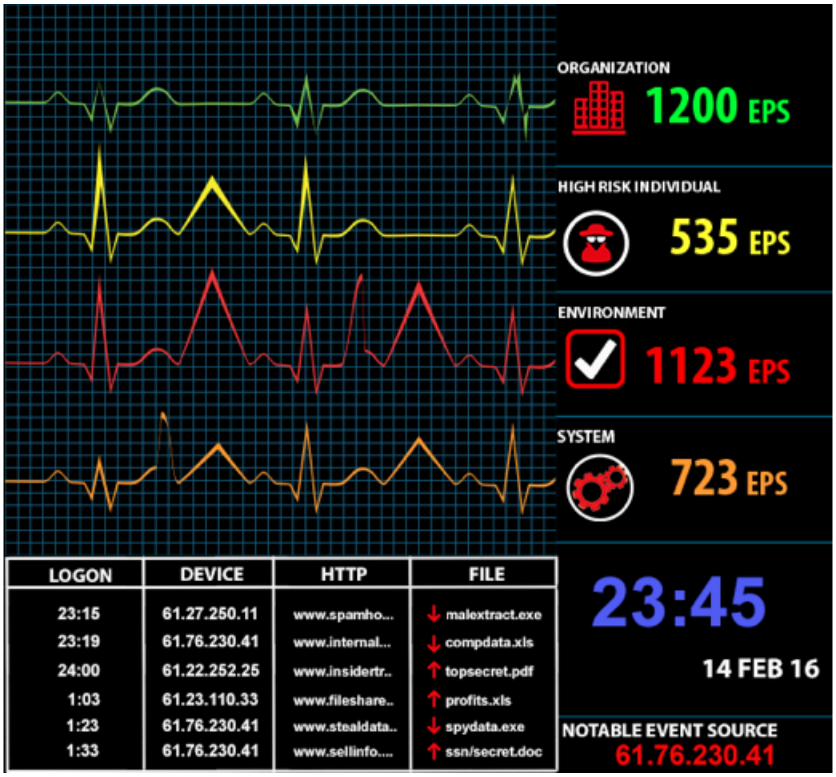
The study continues with an analysis of the findings for overall detection accuracy of predicted malicious events with and without correlations visualizations, as well as the composition of a comparative report, conclusions, and recommendations.

Second Proposed Experimental Research

As insiders become more elusive there is also an increased number of false alerts desensitizing analysts that may result in them ignoring all alerts (He, Zhang, Ma, & Guan, 2015). Thus, the consecutive extension of this work will propose a second experimental research that will develop visualization prototype that will simplify and decrease efforts of cybersecurity analysts attempting to react to trivial alerts. Therefore, the second study will approach this challenge from a perspective that has been minimally assessed to enrich the analytic process through a novel simplified visualization. Attempting to effectively explore data containing complex or multidimensional data sophisticated visualization techniques are needed, using information visualization technologies will aid in improved data analysis especially in areas like fraud or malicious detection (Keim, 2002). Examples of simplified visualizations exist in other industries where false alerts minimization is critical, such as within healthcare and aviation. Within healthcare, visualizations are often used to provide practitioners critical information such as vital signs during emergency medical situations to make lifesaving decisions (Harries, Zacharaih, Kapur, Jahn, & Enarson, 2009). Within aviation, Pilots use a Heads Up Display (HUD) continually references external visual cues and make decisions in the event of abnormal changes (Dopping-Hepenstal, 1981). A simplified executive insider-threat pulse dashboard visualization within the domain of cybersecurity may be utilized to expedite the comprehension of cybersecurity alerts allowing for quick decisions during critical attacks.

Riveiro (2014) argued that there is a lack of appropriate cognitive support for operators to comprehend system outcomes. The proposed second designed experimental research study will assess the ability to identify anomalous and potentially malicious activities utilizing a newly developed added module for the AI-InCyThR™ prototype, called Quality User Insider ChecKing visualization (QUICK.v™) module. Using human-computer interaction (HCI) methods and visualization techniques an added module prototype will be developed then tested utilizing information security professionals. This prototype intends to obtain data from SIEM applications and big data analytics tools to drive the information necessary to generating the cybersecurity vital signs on the proposed front-end executive dashboard. Pfleeger, Predd, Hunker, and Bulford (2010) identified four points that would assist with understanding risky insider actions: the organization, the individual, the information technology (IT) system, and the environment (p. 173). These points are utilized for framing the four vital signs depicted within Figure 2. The vital lines will be developed based on a trend chart depicting events per second within each area over a defined period of time. The developed prototype will include customizable fields indicating potentially high-risk activities that may require investigation. This will aid in resolving the problem faced today where potentially useful data continues to be collected and stored, and resources become paralyzed by the overwhelming quantity of what becomes meaningless data, unless this can be better visualized (Keim, 2002).

The research methodology for the second proposed experimental study within this proposed stream of research will develop and validate an executive insider-threat pulse dashboard prototype using a visualization (noted as QUICK.v™) that will aid in identifying anomalous activities of suspicious cybersecurity insiders. Within the initial phase of the second proposed experimental research, a preliminary add module for the prototype will be developed for analysis of the visualizations of complex data correlations. Identical data will be presented using varying types of visualizations identified as plausible within HCI research. The next phase of second proposed experimental study will assess the effectiveness of the developed executive insider-threat pulse dashboard visualization prototype using a group of 30 subject matter experts (SMEs). Recommendations of the SMEs will then be integrated to refine the prototype. The final phase of second proposed experimental study will assess the types of correlations (linear & non-linear) that allow for effective detection of anomalous insider-threat activities under the simulated environment. After the experiments are completed, revisions to the prototype will be made and recommendations for improvements will be provided.



LOGON	DEVICE	HTTP	FILE
23:15	61.27.250.11	www.spamho...	↓ malextract.exe
23:19	61.76.230.41	www.internal...	↓ compdata.xls
24:00	61.22.252.25	www.insidertr..	↑ topsecret.pdf
1:03	61.23.110.33	www.fileshare..	↑ profits.xls
1:23	61.76.230.41	www.stealdata..	↓ spydata.exe
1:33	61.76.230.41	www.sellinfo....	↑ ssn/secret.doc

Figure 2: Proposed Quality User Insider ChecKing visualization (QUICK.v™) interface

Conclusion

This research agenda outlines two proposed experimental research studies in progress aimed at mitigating malicious cybersecurity insider threat. The first experiment will encompass three phases, the first phase comprises of identifying valid benchmarking feeds. The second phase includes the development of the Analytics-based Identifying Insider Cybersecurity Threat in Real-time (AI-InCyThR™) System, and within the third phase correlation analysis and correlation hierarchical bundling visualization will be produced. The second experimental study will entail developing the Quality User Insider ChecKing visualization (QUICK.v™) module for simplified identification of anomalous and potentially malicious activities. The development of these prototypes and the results of the experiments should provide some initial steps to address the challenge of mitigating malicious cybersecurity insider threat. This stream of research is expected to provide additional insights for understanding the motivation that drives malicious behavior, therefore, aiding in establishing tools for prompt detection of suspicious activities. Overall, both studies will holistically address the issue of malicious cybersecurity insider threat. By enhancing the backend to intrinsically utilize more of the big data already being collected, this proposed line of research is aimed to increase precision when identifying suspicious activities that leads to malicious cyber threats. Then applying a front end with enhanced usability and simplified visualization metrics. Identifying and counteracting malicious cybersecurity insiders can be streamlined. Theses proposed works would allow cybersecurity practitioners to significantly mitigate malicious cybersecurity insider threat.

Acknowledgements

We would like to thank the anonymous reviewers for their time and positive comments.

References

Agrafiotis, I., Legg, P., Goldsmith, M., & Creese, S. (2014). Towards a user and role-based sequential behavioural analysis tool for insider threat detection. *Journal of Internet Services and Information Security (JISIS)*, *4*(November), 127–137.

Atkinson, J. W., & Birch, D. (1970). The dynamics of action. New York: Wiley.

Sánchez Abril, P., Levin, A., & Del Riego, A. (2012). Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee. *American Business Law Journal*, *49*(1), 63–124. doi:10.1111/j.1744-1714.2011.01127.x

Ballesteros, S., Batten, L., Pan, L., & Li, G. (2015). Segregation-of-duties conflicts in the insider threat landscape An overview and case study. *2015 International Conference on Education Reform and Modern Management*, 367–370.

Birkbeck, C., & LaFree, G. (1993). The situational analysis of crime and deviance. *Annual Review of Sociology, 19*, 113-137.

Briar, S., & Piliavin, I. (1965). Delinquency, Situational Inducements, and Commitment to Conformity. *Social Problems*, *13*(1), 35–45. doi:10.1017/CBO9781107415324.004

Choo, K. R. (2011). The cyber threat landscape: Challenges and future research Directions. *Computers & Security, 30*, 719-731.

Claycomb, W. R., Legg, P. A., & Gollmann, D. (n.d.). Guest editorial: Emerging trends in research for insider threat detection, 1–5.

Coleman, J. (1987). Toward an integrated theory of white-collar crime. *American Journal of Sociology, 93*(2), 406-439.

Coleman, J. W. (1992). Crime and money: Motivation and Opportunity in a monetarized economy. *American Behavioral Scientist, 35*(6), 827-836.

Donner, C., Marcum, C., Jennings, W., Higgins, G., & Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior, 34*, 165-172. doi:10.1016/j.chb.2014.01.040

Dopping-Hepenstal, L. (1981). Head-up displays. The integrity of flight information. *IEE Proceedings F Radar and Signal Processing, 128*(7), 440.

Dweck, C. S., & Leggett, E. L. (1988). A social cognitive approach to motivation and personality. *Psychological Review, 95*(2), 256-273.

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology, 6,* 323-337.

Foote, N. N. (1951). Identification as the basis for a theory of motivation. American *Sociological Review, 16*(1), 14.

Glasser, J., & Lindauer, B. (2013). Bridging the gap: A pragmatic approach to generating insider threat data. *2013 IEEE Security and Privacy Workshops*, 98–104. doi:10.1109/SPW.2013.37

Gottschalk, P. (2016). Knowledge management in private investigations of white-collar crime. *Information Resources Management Journal, 29*(1), 1-14.

Gottschalk, P., Filstad, C., Glomseth, R., & Solli-Saether, H. (2011). Information management for investigation and prevention of white-collar crime. *International Journal of Information Management, 31*(3), 226-233.

Gray, P., & Hovav, A. (2014). Using scenarios to understand the frontiers of IS. *Information Systems Frontiers*, *16*(3), 337–345. doi:10.1007/s10796-014-9514-5

Gritzalis, D., Stavrou, V., Kandias, M., & Stergiopoulos, G. (2014). Insider threat: Enhancing BPM through social media. *2014 6th International Conference on New Technologies, Mobility and Security - Proceedings of NTMS 2014 Conference and Workshops*. doi:10.1109/NTMS.2014.6814027

Harries, A. D., Zachariah, R., Kapur, A., Jahn, A., & Enarson, D. A. (2009). The vital signs of chronic disease management. *Transactions of the Royal Society of Tropical Medicine and Hygiene, 103*(6), 537-540.

He, G. F., Zhang, T., Ma, Y. Y., & Guan, X. J. (2015). A novel and practical method for network security situation prediction. *Applied Mechanics and Materials, 701-702*, 907-910.

Hirschi, T., & Gottfredson, M. (1987). Causes of white-collar crime. *Criminology, 25*(4), 949-974.

Hunker, J., & Probst, C. (2008). Insiders and insider threats an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2*(1), 4-27.

Kanfer, R. (1990). Motivation Theory and Industrial and Organizational Psychology. In M. D. Dunnette & L. Hough (Eds.), *Hand book of industrial and organizational psychology* (pp. 75–170). Palo Alto, CA: Consulting Psychologists Press.

Keim, D. (2002). Information visualization and visual data mining. *Visualization and computer graphics, IEEE Transactions on visualization and computer graphics, 8*(1), 1-8. doi:10.1109/2945.981847

Lindauer, B., Glasser, J., Rosen, M., & Wallnau, K. (2013). Generating test data for insider threat detectors. *Journal of Mobile Networks, Ubiquitous Computing and Dependable Applications*, *5*(2), 80–94.

Nostro, N., Ceccarelli, A., Bondavalli, A., & Brancati, F. (2014). Insider threat assessment: A model-based methodology. In *Proceedings of the 2nd International Workshop on Dependability Issues in Cloud Computing, (DISCCO'13, September 30 2013, Braga, Portugal)* (pp. 3–12).

Osgood, D. W., Wilson, J. K., O'malley, P. M., Bachman, J. G., & Johnston, L. D. (1996). Routine activities and individual deviant behavior. *American Sociological Review, 61*(4), 635.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597-611.

Pfleeger, S., Predd, J., Hunker, J., & Bulford, C. (2010). Insiders behaving badly: Addressing bad actors and their actions. IEEE Transactions on Information Forensics and Security, 5(1), 169-179.

Punithavathani, D. S., Sujatha, K., & Jain, J. M. (2015). Surveillance of anomaly and misuse in critical networks to counter insider threats using computational intelligence. *Cluster Computing*, *18*(1), 435–451. doi:10.1007/s10586-014-0403-y

Riveiro, M. (2014). Evaluation of Normal Model Visualization for Anomaly Detection in Maritime Traffic. *ACM Transactions on Interactive Intelligent Systems, 4*(1), 1-24.

Sood, A. K., Zeadally, S., Member, S., IEEE, & Bansal, R. (2015). Exploiting trust: Stealthy attacks through socioware and insider threats. *IEEE Systems Journal*, 1–12.

Sutherland, E. H. (1940). White-collar criminality. *American Sociological Review, 5*(1),1.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24*(6), 472-484.

Tolman, E. C. (1938). The physiological review. *Psychological Review, 45*(1), 1-39.

Turner, J. (1987). Toward a sociological theory of motivation. *American Sociological Review, 52*(1), 15-27.

Vaughan, D. (1999). The dark side of organizations: Mistake, misconduct, and disaster. *Annual Review of Sociology, 25*, 271-305.

Wang, S. (2007). Measures of retaining digital evidence to prosecute computer-based cyber-crimes. *Computer Standards & Interfaces, 29*(2), 216-223.

Wang, S., & Lin, S. S. (2007). The effects of group composition of self-efficacy and collective efficacy on computer-supported collaborative learning. *Computers in Human Behavior, 23*(5), 2256-2268.

Authors Biography

Angel L. Hueca is a Senior Cybersecurity Specialist in VariQ Corporation's federal contracting division, based out of Washington, D.C., USA. He holds a Bachelor of Science in Computer Information Technology, and a dual MBA and Master of Science in Cybersecurity from the University of Maryland University College. Angel is currently ABD and pursuing his PhD in Information Systems with a focus in Information Security from Nova Southeastern University. Angel holds several industry certifications including CISSP, CISA, as well as CEH, and is a member of AIS, IEEE, ACM, ASIS, The Honor Society of Phi Kappa Phi (ΦΚΦ), and Upsilon Pi Epsilon (ΥΠΕ): International Honor Society for the Computing and Information Disciplines.

Karla Clarke is an Associate in KPMG LLP's Cyber practice and a Ph.D. student in Information Systems at Nova Southeastern University. She holds a Bachelor of Arts in Anthropology from the University of Florida, and a Master of Science in Information Systems from Boston University. She is a member of the Information Protection practice at KPMG focused on the areas of identity and access management, privileged user management, logging monitoring and analytics. Prior to joining KPMG Karla work for another international consulting firm focused on infrastructure security and specializing in project management and security strategy implementation. Karla is a member of ACM, IEEE, and ISACA.

Dr. Yair Levy is a Professor of Information Systems and Cybersecurity at the College of Engineering and Computing, at Nova Southeastern University, the Director of the Center for e-Learning Security Research (CeLSR), and chair of the Information Security Faculty Group at the college along with serving as the director of the Ph.D. program in Information Assurance. He joined the university in 2003, was promoted to an Associate Professor in 2007, and to full Professor in 2012. During the mid to late 1990s, Dr. Levy assisted NASA to develop e-learning platforms as well as manage Internet and Web infrastructures. He earned his undergraduate degree in Aerospace Engineering from the Technion (Israel Institute of Technology). He received his Masters of Business Administration (MBA) with Management Information Systems (MIS) concentration and Ph.D. in MIS from Florida International University. He heads the Levy CyLab, which conducts innovative research from the human-centric lens of four key research areas Cybersecurity, User-authentication, Privacy, and Skills (CUPS), as well as their interconnections. He authored over 60 articles, three book chapters, one book, and his publications have been cited for over 1,400 times by other scholarly research. Dr. Levy has been an active member of the US Secret Service (USSS)'s - Miami Electronic Crimes Task Force (MECTF) and The South Florida Cybercrime Working Group (SFCWG). He was trained by the Federal Bureau of Investigation (FBI) on various topics, and actively serves as a member on of the FBI/InfraGard, and consults the FBI/Cyber Task Force (CTF). Dr. Levy serves on the national Joint Task Force of Cybersecurity Education, as well as other national initiatives related to cybersecurity workforce, education, and research. He is also a frequent invited keynote speaker at national and international meetings, as well as regular media interviews as a Subject Matter Expert (SME) on cybersecurity topics. Find out more about Dr. Levy and his research lab via: http://cec.nova.edu/~levyy/