

How workplace satisfaction affects insider threat detection as a vital variable for the mitigation of malicious cyber insiders

Karla Clarke, Middle Georgia State University, USA, karla.clarke@mga.edu

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

Laurie Dringus, Nova Southeastern University, USA, laurie@nova.edu

Shonda Brown, Middle Georgia State University, USA, shonda.brown@mga.edu

Abstract

Insider threat mitigation is a growing challenge within organizations. The development of a novel alert visualization dashboard for the identification of potentially malicious cyber insider threats was identified as necessary to alleviate this challenge. This research developed a cyber insider threat dashboard visualization prototype for detecting potentially malicious cyber insider activities QUICK.v™. This study utilized Subject Matter Experts (SMEs) by applying the Delphi Method to identify the most critical cyber visualization variables and ranking. This paper contains the detailed results of a survey based experimental research study that identified the critical cybersecurity variables also referred to as cybersecurity vital signs. The identified vital signs will aid cybersecurity analysts with triage for potentially malicious insider threats. From a total of 45 analytic variables assessed by 42 cybersecurity SMEs, the top six variables were identified using a comprehensive data collection process. The results indicated that workplace satisfaction is one of the top critical cyber visualization variables that should be measured and visualized to aid cybersecurity analysts in the detection of potentially malicious cyber insider threat activities. The process of the data collection to identify and rank critical cyber visualization variables are described.

Keywords: Anomaly detection, cybersecurity, vital signs, intrusion detection, insider threat, visualization.

Introduction

Financial and intellectual property damages continue to rise as a result of insider threats (Cole, 2015; Gorg, Kang, Liu, & Stasko, 2013; Inibhunu et al., 2016; Pfleeger & Stolfo, 2009). The purpose of this study is to address the prevalent challenge within the cybersecurity industry when detecting potentially malicious insider cyber threats and enabling the visualization of threats as they occur. A cyber visualization prototype was developed using Subject Matter Experts (SMEs) validated critical cyber visualization variables and techniques QUICK.v™ (Clarke & Levy, 2017; Hueca, Clarke, & Levy, 2016). This study achieved five goals using a three-phased approach. The first research goal was to identify, using SMEs, the critical cyber visualization variables. The second research goal was to identify, using SMEs, the rank order of the critical

cyber visualization variables that the developed prototype should include, which may aid in identifying potentially malicious cyber insiders. The third research goal was to identify, using SMEs, the most valid presentation of complex data correlations using the identified critical visualization variables over multiple visualization techniques. The fourth research goal was to apply SMEs' identified critical visualization variables, in rank order, and techniques to develop QUICK.v™. The fifth research goal was to conduct an experimental study using SMEs to assess the perceived effectiveness using self-reported value and satisfaction of the QUICK.v™ prototype when mitigating malicious cyber insiders.

The first phase used the Dephi method SMEs to identify and rank the critical cyber visualization variables that should be displayed when using applications to detect potentially malicious insider cyber threats (Levy, 2008; Levy & Ellis, 2011). The second phase used the Delphi method SMEs to identify visualization techniques that are most valid to present complex cyber data correlations and the top six critical cyber visualization variables. The third phase involved SMEs identifying the perceived effectiveness of the developed prototype QUICK.v™. The conceptual design of the study is depicted in Figure 1.

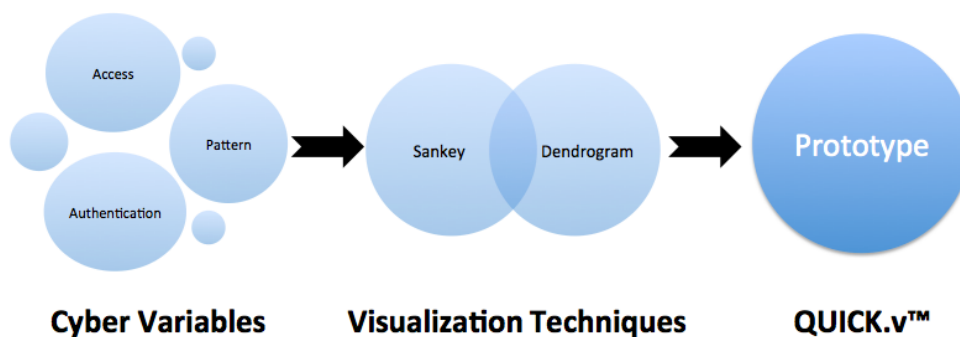


Figure 1. Conceptual Design for QUICK.v™

Methodology

Data Collection Process

Developmental research was conducted in three phases to develop and validate the prototype that will aid in identifying anomalous activities of malicious cyber insiders. Anomalous activities refer to identified correlations denoted as moments, a moment is a mean or standard deviation of the correlations (Qayyum, Islam, & Jamil, 2005). If an event occurs above or below an identified moment the activity is deemed to be anomalous (Jyothsna, Prasad, & Prasad, 2011). Parsing through unknown activities to determine normal versus anomalous activities can be difficult for cyber analysts (Shneiderman, 1996; Shneiderman & Plaisant, 2015; Shneiderman, Plaisant, Cohen, & Jacobs, 2010). Thus, a goal for this research was to identify the critical cyber visualization variables that should be displayed when using applications to detect potentially malicious insider cyber threats. A malicious insider is an insider who has malicious intent and acts against the best interests of the organization (Pfleeger, Predd, & Hunker, 2010; Santos et al., 2012). This study evaluated cyber visualization variables presented by at least 30 cyber analysts that were used to develop the QUICK.v™ prototype. The unit of analysis for this study was the

individual cyber analysts. The selected group of SMEs also included cyber analytics as well as cyber forensics professionals. These SMEs were solicited specifically as the sample population for this study.

In phase one, the critical cyber visualization variables are identified and ranked. Casey (2007) denoted analytics based on attack types, providing a comprehensive list of analytic indicators. These analytic indicators provided a foundation as the initial list of critical cyber visualization variables within this research. For phase one of this study as noted before, the goal for the SMEs was to identify the critical cyber visualization variables that should be displayed when using applications to detect potentially malicious insider cyber threats. A survey was distributed via email to collect responses. A total of 42 SMEs responded by completing survey instrument one. The survey consisted of questions concerning the identification of potentially malicious cyber insiders by identifying relevant cyber visualization variables. The first research question (RQ1) was: what are SMEs' identified critical cyber visualization variables that should be displayed when using applications to detect potentially malicious insider cyber threats? SMEs were asked to select the relevant analytic variable within each identified category that they deem to be most important when trying to identify potentially malicious insider threats. The categories of analytic variables individually assessed include: System, Social, Health, Human Resources, Financial, Security, and Criminal. Based on this data collection process using SMEs and applying the Delphi method the critical cyber visualization variables were identified from the consensus and ranked.

The goal for phase two was to identify the visualization techniques that are most valid to present the cyber visualization variables. Additionally, the goal of this phase was to identify the visualization techniques that are most valid to present complex cyber data correlations. In phase two, 31 web-based survey responses were collected from SMEs. The survey consisted of questions concerning the identification of visualization techniques to present the identified critical cyber visualization variables and to present complex cyber data correlations. The data collected was converted to Excel for initial analysis, answers to each survey question were parsed to identify the count of each variable selected by the SMEs. That data was collected to address the second research question (RQ2): what SMEs' identified visualization techniques are most valid to present complex cyber data correlations? That RQ2 is relevant to the pre-designated critical cyber visualization variables that are applied within the developed cyber visualization prototype QUICK.v™. SMEs were presented with three options of visualization techniques identified for presenting each of the six critical cyber visualization variables. This procedure was performed in order to address the third research question (RQ3): what SMEs' identified visualization techniques are most valid to present top six critical cyber visualization variables? Answer to that RQ3 was needed in order to detect potentially malicious cyber insider activities that are applied within the developed cyber visualization prototype QUICK.v™.

Based on the data analysis results from phase one, since six critical cyber visualization variables were identified, survey two was modified to add six critical cyber visualization variables instead of the initially proposed five. SMEs had to select a visualization technique for each of the critical cyber visualization variables, allowing for the identification of which visualization techniques are most valid to present each of the six identified critical cyber visualization variables.

The goal of phase three was for the SMEs to identify the perceived effectiveness (i.e. satisfaction & value/importance) (Levy, 2006) of the developed prototype QUICK.v™. A total of 26 SMEs completed the survey in phase three. The survey consisted of questions to identify the level of satisfaction and the value for each of the top six critical cyber visualization variables and presentation technique (Levy, 2006). This was done to address the forth research question (RQ4): what is the SMEs' perceived effectiveness (i.e. satisfaction & value/importance) of QUICK.v™? After viewing the developed prototype QUICK.v™ SMEs' were presented a 7-point Likert-type rating scale for satisfaction and in parallel another 7-point Likert-type rating scale for value to assess both satisfaction and value/importance for each stated item. The satisfaction and value/importance of each item was calculated to then determine the perceived effectiveness using the LeVIS index (Levy, 2006). An additional level of analysis was performed on QUICK.v™ to assess the usability. Since obtaining a system usability scale score also provided a very useful metric for the overall prototype usability (Bangor, Kortum, & Miller, 2008). The system usability scale score of identified statements were calculated.

Data Analysis

In all three phases of this study, prior to data analysis, pre-analysis data screening was performed on the data collected from the SMEs. While qualitative data analysis was utilized on the datasets in phase one and two. In phase three, the perceived effectiveness of QUICK.v™ was quantified based on research analysis as indicated below. Within phase one, answers to each survey question were parsed to identify the count of each variable selected by the SMEs. Since the SMEs were asked to select at most two analytic variables for each category, the variables were weighted based on their selection for analysis. If the SME did not deem a variable as critical, they did not have to select a variable within that category. Thus, some variables were not selected and had a count of zero. The count or number of responses pertaining to the particular variable represents the total instances that an analytic variable was selected as a response for variable one and variable two within each category. If the variable was selected as variable one or variable two, this selection was then weighted to obtain the weighted average ranking for that variable.

In phase two, since the SMEs were asked to select one option for each visualization technique presented, the responses were not weighted prior to determining the final allocations. Also, within the survey instrument all questions were marked as requiring a response. As a result, the SMEs had to select a visualization technique for each of the critical cyber visualization variables. Based on the count (n) of all SMEs, the average for each visualization technique was identified. The average was calculated for all data collected for each of the six critical cyber visualization variables. In phase three, data analysis was performed based on the LeVIS index (Levy, 2006) and the system usability scale quartiles. Based on Levy (2006), the aggregation for satisfaction was performed by determining the mean satisfaction characteristic: \bar{S}_{a1} , $\dots \bar{S}_{a11}$, \bar{S}_{b1} , $\dots \bar{S}_{b7}$, \bar{S}_{c1} , and \bar{S}_{c2} . The equation that was used to compute the mean satisfaction for each item across all SMEs is:

$$\bar{S}_{a1} = \left(\frac{1}{n}\right) \cdot \left(\sum_{i=1}^n (A_{1_SAT_i})\right)$$

Here, $A_{1_SAT_i}$ is the satisfaction score rated by SME i for cyber visualization variable A_1 , and n the number of SMEs who participated in the assessment of that variable. The aggregated value score noted as $\bar{V}_{a1}, \dots, \bar{V}_{a11}, \bar{V}_{b1} \dots \bar{V}_{b7}, \bar{V}_{c1}, \dots, \bar{V}_{c2}$. The equation that was used to calculate the mean value is:

$$\bar{V}_{a1} = \left(\frac{1}{n}\right) \cdot \left(\sum_{i=1}^n (A_{1_VAL_i})\right)$$

The $A_{1_VAL_i}$ is the characteristic value score rated by SME i for cyber visualization variable A_1 , and n the number of SMEs who participated in the assessment of that variable (Levy, 2006, p. 184-185). The overall perceived effectiveness was calculated using the LeVIS index formula below:

$$\left(\frac{1}{n}\right) \cdot (V_0 \cdot S_0) \rightarrow 0 \leq LeVIS \leq 1$$

Then, an analysis was performed on modified system usability scale statements that were extracted for analysis. A raw system usability scale score was calculated based solely on the extracted five system usability items within the survey instrument. The system usability scale score was calculated by creating a sum from the items rather than a mean score, this allows for analysis of the same variance as performed by Bangor et al. (2008).

Results

From phase one, the ranking of variables, a corresponding weight was applied to each variable. The weight was used to identify the top six most critical variables. The identified critical cyber visualization variables were: workplace satisfaction, change in violation patterns, audit log modification, changes in data access patterns, and privilege change. In phase two, once the SMEs identified and validated the top six critical cyber visualization variables, a comprehensive review of literature was performed to identify how each variable should be visualized.

The results for each critical cyber visualization variable are as follows. For workplace satisfaction, when presented with the options of a line graph, bar graph, and calendar style view, SMEs identified the line graph as the most valid visualization technique. When presented with an area chart, radar plot, and streamgraph for change in violation pattern, SMEs identified the area chart as the most valid visualization technique. For audit log modification, when presented with a line graph, fisheye distortion, and bar graph, SMEs identified the line graph as the most valid visualization technique. For the critical cyber visualization variable, change in violation pattern when presented with a stacked column graph, a stacked bar graph, and a streamgraph, SMEs identified the stacked column graph as the most valid visualization technique. For data exfiltration, when presented with a line graph, column graph, and fisheye distortion, SMEs identified the line graph as the most valid visualization technique. When presented with a line graph, stacked bars, and stacked columns for the critical cyber visualization variable, privilege change, SMEs identified the line graph as the most valid visualization technique. The visualization techniques used to present complex cyber data correlations were parallel coordinates, chord diagram, and hierarchical bundling. SMEs identified parallel coordinates as

the most valid visualization technique. This is depicted in Table 1. In phase three, the perceived effectiveness for the top six critical cyber visualization variables and the additional items presented to the SME's are summarized in Table 2.

Table 1. Visualization Technique Rankings (N= 31)

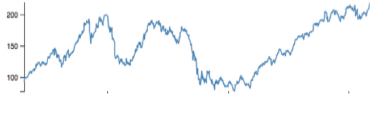
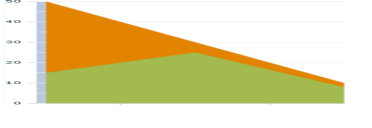
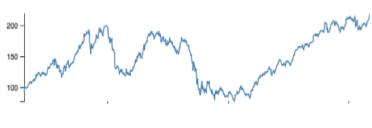
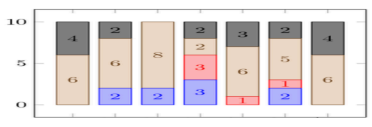
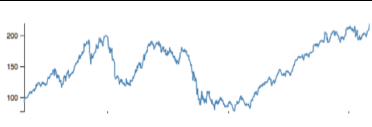
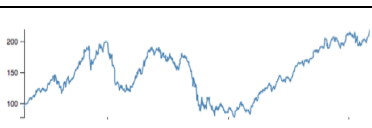
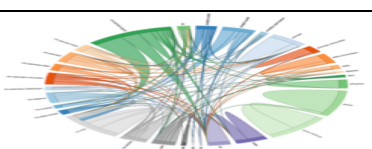
Cyber Visualization Variable	Visualization Technique	N	%	Final cyber visualization
Workplace Satisfaction	Line Graph	16	52%	
	Bar Graph	13	42%	
	Calendar View	2	6%	
Change in Violation Pattern	Area Chart	18	58%	
	Radar Plot	9	29%	
	Streamgraph	4	13%	
Audit Log Modification	Line Graph	18	58%	
	Fisheye Distortion	8	26%	
	Bar Graph	5	16%	
Change in Data Access Pattern	Stacked Column Graph	18	58%	
	Stacked Bar Graph	12	39%	
	Streamgrap	1	3%	
Data Exfiltration	Line Graph	18	58%	
	Column Graph	9	29%	
	Fisheye Distortion	4	13%	
Privilege Change	Line Graph	16	52%	
	Stacked Bars	14	45%	
	Stacked Columns	1	3%	
Complex Data Correlations	Parallel Coordinates	15	48%	
	Chord Diagram	14	45%	
	Hierarchical Bundling	2	6%	

Table 2: LeVIS Index Results for Perceived Effectiveness Summary

Item	Perceived Effectiveness?
Variable 1: Workplace Satisfaction	Yes
Variable 2: Change in Violation Patterns	Yes
Variable 3: Audit Log Modification	Yes
Variable 4: Changes in Data Access Patterns	Yes
Variable 5: Data Exfiltration	Yes
Variable 6: Privilege Change	Yes
Complex Cyber Data Correlations	Yes
Type of Variables Presented	Yes
Interest in Variables Presented	Yes
Organization of Variables Presented	No
Complexity Based on Variables Presented	No
Various Variables Were Well Integrated	No
Relevance of Variables to Insider Threat Detection	Yes
Quality of Visualizations	Yes
Organization of Visualizations Presented	No
Consistency of Visualizations Presented	Yes
Ability to Quickly Decipher Potential Insider Threats	No
Confidence quickly Deciphering Potential Insider Threats	Yes
Ability to Make Actionable Decisions Based on Information Depicted	No
Ease of Use of Information Depicted	Yes
Overall, how would you rate your level of satisfaction/value of QUICK.v™ when identifying potentially malicious cyber insiders?	No

Five system usability scale statements were selected for analysis: Ease of use of information depicted, various variables were well integrated, complexity based on variables presented, confidence quickly deciphering potential insider threats, and consistency of visualizations presented. From the five items analyzed to determine the system usability scale scores, 13 of the 25 participants had a system usability scale score above 70, which is deemed as acceptable. The sample average system usability scale score was 66.9%. Thus, the overall perceived usability of QUICK.v™ based on the five modified system usability scale items fell within quartile two, which is deemed as satisfied based on the system usability scale score by quartile, adjective rating, and acceptability (Bangor et al., 2008). Table 3 depicts the results of this analysis.

Table 3. System Usability Scale Score by Quartile, Adjective Rating, and Acceptability (N=25)

Participant	Inflated Score (adjusted to a range of 0-100)	SUS Quartile	Adjective
p1	54.3	1	Ok
p2	85.7	4	Best Imaginable
p3	22.9	1	Worst Imaginable
p4	65.7	2	Good
p5	80.0	4	Excellent
p6	85.7	4	Best Imaginable
p7	88.6	4	Best Imaginable
p8	100.0	4	Best Imaginable
p9	22.9	1	Worst Imaginable
p10	65.7	2	Good
p11	54.3	1	Good
p12	60.0	1	Good
p13	31.4	1	Poor
p14	74.3	3	Excellent
p15	74.3	3	Excellent
p16	77.2	3	Excellent
p17	82.9	4	Excellent
p18	82.9	4	Excellent
p19	54.3	1	Good
p20	37.2	1	Poor
p21	68.6	2	Good
p22	82.9	4	Excellent
p23	54.3	1	Good
p24	82.9	4	Excellent
p25	82.9	4	Excellent

Overall, the results of the study designated the top six critical cyber visualization variables: workplace satisfaction, change in violation patterns, audit log modification, changes in data access patterns, data exfiltration, and privilege change. The most valid visualization technique to present the top six critical cyber visualization variables as: line graph, area chart, line graph, stacked column graph, line graph, and line graph (denoted in the order that each variable was

previously listed). The results also identified parallel coordinates as the most valid to present complex cyber data correlations relevant to the pre-designated critical cyber visualization variables. Overall, QUICK.v™ was not implied to be effective based on the SMEs' overall perceived effectiveness rating (i.e. satisfaction & value/importance (Levy, 2006)) when mitigating potentially malicious cyber insider threats. However, each of the identified individual critical cyber visualization variables was found to be effective as depicted in Figure 2. Each variable that was rated over 0.5, in the context of this study, was identified as effective.

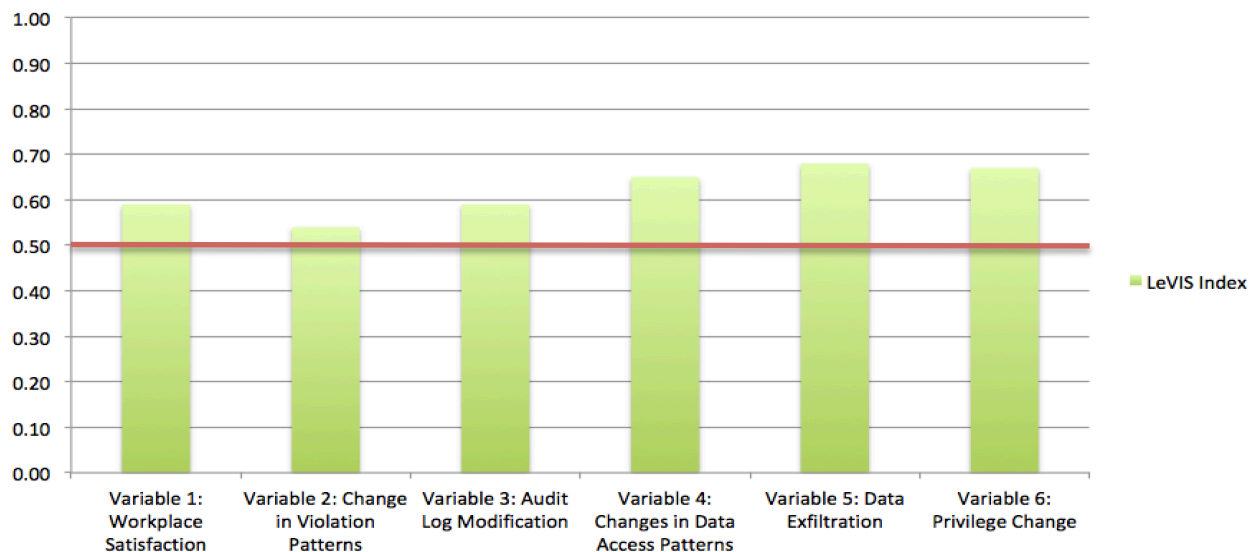


Figure 2. LeVIS Index Summary

Conclusion

An unanticipated outcome of the study indicated that workplace satisfaction was at the top of identified critical cyber visualization variables. The results from phase one suggest that cybersecurity analysts should initially focus on anomalies within the identified critical cyber visualization variables when using applications to detect potentially malicious insider cyber threats. The results from phase two suggest that cybersecurity analysts should be presented simplified visualizations using these visualization techniques when presenting the critical cyber visualization variables.

In giving the SMEs, all 45 variables to parse and select only five, they subjectively chose what seemed most pertinent without over analysis. When asked to identify valid visualization techniques though SMEs were drawn to the more unique visualization options, they opted to select the simple visualization techniques. Like medical professional's cybersecurity professionals may prefer simplified visualizations. Though requiring further research, it may be plausible to assume that simplified visualizations may reduce cognitive load during times of crisis.

A limitation of this study was that the developed visualization prototype intended to visualize complex correlations based on cybersecurity related data. The cybersecurity data needed to be

fed to the developed visualization prototype from viable data sources. The parsed data feeds were then utilized for generating the visualizations on the validated front-end. The prototype being developed would represent variables relevant to current applications and data sources. Therefore, future research may be required to apply the prototype that was developed using SMEs to future data sources.

The implications of the study relate to the existing body of knowledge in Information Systems and Information Security. This study developed a novel and effective detection method for the identification of anomalous activities when mitigating malicious insider cyber threats. Many cybersecurity tools presenting visualizations are rarely evaluated for effectiveness nor do they account for the needs of the user (Sethi, Paci, & Wills, 2016). This study provides companies with cybersecurity vital signs that are perceived as effective when identifying potentially malicious cyber insiders. Organizations can use the identified cybersecurity vital signs and the validated visualization techniques to aid in the identification of malicious insiders. QUICK.v™ addressed the challenge of detecting cyber insider threats in a novel way by enhancing the presentation of complex malicious insider cyber threat correlations. In addition, QUICK.v™ can be used with minor adjustments to enhance its effectiveness as a guide for alleviating the issues faced when using visualizations to identify potentially malicious insiders cyber threats.

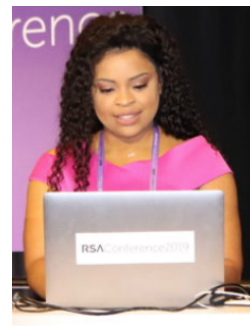
References

- Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An empirical evaluation of the system usability scale. *International Journal of Human-Computer Interaction*, 24(6), 574-594.
- Casey, T. (2007). *Threat agent library helps identify common security risks*. Retrieved from <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Intel%20-%20Threat%20Agent%20Library%20Helps%20Identify%20Information%20Security%20Risks.pdf>
- Clarke, K., & Levy, Y. (2017). Cybersecurity vital signs: The role of anomaly detection on insider threat triage. *Proceeding of the Knowledge Management (KM) 2017 Conference*, Novo Mesto, Slovenia, (pp. 79-89).
- Cole, E. (2015). Insider threats and the need for fast and directed response. *SANS*. Retrieved from <http://lp.spectorsoft.com/corp/sans-survey-report>
- Gorg, C., Kang, Y., Liu, Z., & Stasko, J. (2013). Visual analytics support for intelligence analysis. *IEEE Computer Society*, 46(7), 30-38. <http://doi.org/10.1109/MC.2013.76>
- Hueca, A. L., Clarke, K., & Levy, Y. (2016). Exploring the motivation behind cybersecurity insider threat and proposed research agenda. *Proceeding of the Knowledge Management (KM) 2016 Conference*, University of Lisbon, Portugal, (pp. 2-15).
- Inibhunu, C., Langevin, S., Ralph, S., Kronefeld, N., Soh, H., Jamieson, G. A., et al. (2016). Adapting level of detail in user interfaces for cybersecurity operations. *In Resilience Week*, 13-16.

-
- Jyothsna, V., Prasad, V. R., & Prasad, K. M. (2011). A review of anomaly based intrusion detection systems. *International Journal of Computer Applications*, 28(7), 26-35.
- Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershy, PA: IGI Global.
- Levy, Y. (2008). An empirical development of critical value factors (CVF) of online learning activities: An application of activity theory and cognitive value theory. *Computers & Education*, 51(4), 1664-1675.
- Levy, Y., & Ellis, T. J. (2011). A guide for novice researchers on experimental and quasi-experimental studies in information systems research. *Interdisciplinary Journal of Information, Knowledge, and Management*, 6, 151-161.
- Pfleeger, S., & Stolfo, S. (2009). Addressing the insider threat. *IEEE Security & Privacy Magazine*, 7(6), 10-13.
- 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.
- Qayyum, A., Islam, M., & Jamil, M. (2005). Taxonomy of statistical based anomaly detection techniques for intrusion detection. *Proceedings of the IEEE Symposium on Emerging Technologies* (pp. 270-276). <http://doi.org/10.1109/icet.2005.1558893>
- Santos, E., Nguyen, H., Yu, F., Kim, K., Li, D., Wilkinson, J., et al. (2012). Intelligence analyses and the insider threat. *IEEE Transactions on Systems Management and Cybernetics*, 42(2), 331-347.
- Sethi, A., Paci, F., & Wills, G. (2016). EEVi-framework for evaluating the effectiveness of visualization in cyber-security. *Proceedings of the 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 340-345). IEEE.
- Shneiderman, B. (1996). The eyes have it: A task by data type taxonomy for information visualizations. *Proceedings of the IEEE Symposium on Visual Languages* (pp. 336-343). IEEE.
- Shneiderman, B., & Plaisant, C. (2015). Sharpening analytic focus to cope with big data volume and variety. *IEEE Computer Graphics and Applications*, 35(3), 10-14. <http://doi.org/10.1109/mcg.2015.64>
- Shneiderman, B., Plaisant, C., Cohen, M., & Jacobs, S. (2010). *Designing the user interface: Strategies for effective human-computer interaction*. Boston, MA: Addison-Wesley.

Authors' Biographies

Karla Clarke, Ph.D. is a Manager in KPMG LLP's Cyber practice and part-time professor at the School of Information Technology for Middle Georgia State 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, and a Ph.D. in Information Systems from Nova Southeastern 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.



Yair Levy, Ph.D. is a Professor of IS and Cybersecurity at Nova Southeastern University (NSU), the Director of the Center for Information Protection, Education, and Research (CIPhER), and chair of the Cybersecurity Faculty Group at the college. He earned BS.c. in Aerospace Engineering (Technion), MBA and Ph.D. in MIS from Florida International University. During the mid to late 1990s, Dr. Levy assisted NASA to develop e-learning platforms as well as manage Internet and Web infrastructures. He heads the Levy CyLab (<http://CyLab.nova.edu>), which conducts innovative research from the human-centric lens of cybersecurity. He authored numerous peer-review publications. Dr. Levy was trained by the Federal Bureau of Investigation (FBI) on various topics as part of the Citizen's Academy, and actively serves as a Board Member and the Education Section Chief of the FBI/InfraGard South-Florida chapter, as well as consults local, state, and federal agencies on cybersecurity topics. He is frequently invited as a Subject Matter Expert (SME) on cybersecurity topics to provide keynote talks at national and international meetings, as well as regular media interviews in print, radio, and TV. Find out more about Dr. Levy and his research lab via: <http://www.nova.edu/~levyy/>



Laurie Dringus, Ph.D. is a Professor in the College of Engineering and Computing at Nova Southeastern University. Her research interests include human-computer interaction, user experience (UX) and information design, and usability. She has published widely in journals and conferences on many aspects of the user experience in various technology contexts, including the complex nature of human interaction and discourse in online settings. In addition to HCI, Laurie has been dedicated to the advancement of the field of online learning since 1983, having joined the pioneer group that developed online programs at NSU. From 1998-2014, she served as Editor-in-Chief of The Internet and Higher Education, a top ranked, internationally recognized research journal published by Elsevier. She served as Conference Co-Chair for the Online Learning Consortium (OLC) Accelerate 2017 Conference and Program Co-Chair for Accelerate 2016. She has received several distinctions and awards including being



named as an OLC Fellow in 2017, CEC Distinguished Professor of the Year, 2015-2016, and the co-recipient of a research grant awarded by the NSU 2017-2018 President's Faculty Research and Development Grants Award competition. One of her former Ph.D. students, Dr. Harold Henke, established a student scholarship fund in her name.

Shonda Brown, Ph.D. is a manager at a Fortune 500 company and part-time professor at the School of Information Technology for Middle Georgia State University. She has served as a referee research reviewer and editor for several international scientific journals and conference proceedings. A number of her papers won the 'best paper' award in national and international peer-review conference proceedings. Dr. Brown's research interests include information security and privacy. Moreover, she received a Bachelor's degree in Information Systems from Howard University, Master's degree in Information Systems from Drexel University, and Ph.D. in Information Systems with a concentration in Information Security from Nova Southeastern University. She is also a member of AIS, IEEE, ACM, and Upsilon Pi Epsilon Honor Society (UPE).

