ICRMAT 2022 Proceedings of the International Conference on Research in Management & Technovation pp. 209–213
DOI: 10.15439/2022M4720
ISSN 2300-5963 ACSIS, Vol. 34

Technology Threat Avoidance Factors Affecting Cybersecurity Professionals' Willingness to Share Information

Willie Session, Ph.D., MBA
Assistant Professor of Cybersecurity
Capitol Technology University
Laurel, MD, USA
Email: willie.session@gmail.com

S. Raschid Muller, DBA, Ph.D.
Assistant Professor of Cybersecurity
Capitol Technology University
Laurel, MD, USA
Email: srmuller@captechu.edu
https://orcid.org/0000-0002-1742-7575

***Abstract*—Through the Cybersecurity Information Sharing Act of 2015, a DHS information-sharing program was mandated to protect U.S. businesses and critical infrastructure and mitigate cyberattacks. The present study examined cybersecurity professionals' willingness to collaborate and share information regarding cybersecurity threats via that program. The technology threat avoidance theory (TTAT) served as the study's theoretical framework. This research examined to what extent technology threat avoidance factors affect cybersecurity professionals' willingness to collaborate and share information regarding cybersecurity threats. Threat avoidance factors consisted of perceived susceptibility, perceived severity, perceived threat, prevention effectiveness, prevention cost, and self-efficacy. This cross- sectional study used partial least squares-structural equation modeling to analyze data collected from 137 cybersecurity professionals with a minimum of five years of cybersecurity experience. The data analysis indicated that perceived susceptibility and perceived severity significantly predicted participants' perceptions of cybersecurity threats, and perceived threat explained 44% of the variance in avoidance motivation. Prevention effectiveness, prevention cost, and self-efficacy were not significant predictors of avoidance motivations and the willingness to participate in the DHS's information- sharing program. These results indicate that more research is necessary to understand the factors influencing information sharing among cybersecurity professionals working in U.S. organizations.**

***Index Terms*—cybersecurity, TTAT, PLS-SEM, Dept. of Homeland Security, information sharing.**

I. Introduction

Cybersecurity has become a topic of national interest for countries worldwide [26], [29], [31]. In the United States, the Cybersecurity Information Sharing Act of 2015 (CIS) sought to facilitate cyber threat information sharing between the U.S. federal government and the private sector through the Department of Homeland Security (DHS). The DHS implemented an information-sharing program to bolster collaborative security efforts between the public and private sectors and mitigate threats to critical infrastructure from persistent cyberattacks. Unfortunately, companies in the private sector have been slow to participate in the DHS program ([13], [17], [25]. Federal cybersecurity initiatives help clarify government regulations on cybersecurity, and scholars have noted the benefits of federal government support, information sharing, and collaboration in the fight against cybercrime [32], [35]. The proposed study will examine how technology avoidance threat factors influence cybersecurity professionals' willingness to share information through the DHS program.

A. Information Sharing

Information sharing. In the context of the proposed study, information sharing refers to the exchange of cybersecurity threat and mitigation data through the DHS program established by the Cybersecurity Information Sharing Act of 2015. Information sharing is defined in the literature as the set of organizational activities aimed at exchanging information with others proactively and on request to address a business or regulatory requirement, aid the needs of another, or resolve mutual problems [13]. The sharing involves technical and manual platforms accessed through formal and informal relationships and systems [13].

II. Literature Review

The present study will examine the factors affecting cybersecurity professionals' willingness to collaborate and share information regarding cybersecurity threats. Liang and Xue's [19] technology threat avoidance theory (TTAT) will be used as a conceptual framework to support the proposed study. The premise of the TTAT is that individuals, such as cybersecurity professionals, are influenced by motivations to safeguard against technology threats. The TTAT model's leading independent variables are perceived threat, protect effectiveness, safeguard cost, and self-efficacy. The TTAT model also includes perceived susceptibility and severity as independent variables influencing perceived threat. Together, the independent variables influence a user's avoidance motivation, which, in turn, affects avoidance behavior.

Many scholars have used the TTAT to examine cybersecurity-related behaviors [3], [4], [5], [8], [15]. The TTAT model effectively determines whether specific threat avoidance factors influence cybersecurity professionals' willingness to collaborate and share information regarding cybersecurity threats through inter-organizational collaboration. Figure 1 presents the study's conceptual model based on the TTAT.

The United States is transiting from a society of nearly 4 billion Internet-connected users to a new age of automation, big data, and the Internet of things [14]. Threats posed by cyberattacks cannot be ignored, and virtual walls cannot be built to keep bad actors out [18]. In the 21st century, cybersecurity plans must address iPhone or Android devices that have become virtual repositories of sensitive personal and business information [7]. Personal smart devices contain client and personal contact lists and correspondence, graphic

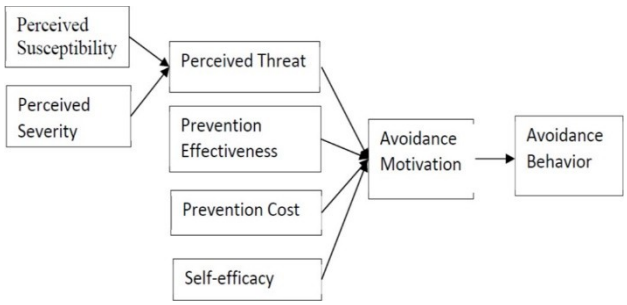

Figure 1 – The Study's Conception Framework. Note. From "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," by H. Liang & Y. Xue, 2010, *Journal of the Association for Information Systems, 11*(7), p. 402 (https://doi.org/10.17705/1jais.00232). Copyright Association for Information Systems.

images, photographs, health data, financial data, and intellectual property [7]. Personally identifiable information, proprietary data, and intellectual property must be protected from data breaches through defined cybersecurity programs [7].

Cybersecurity risks have been identified as one of the most serious national security and economic challenges facing the United States, and it appears to be misunderstood by policy actors [30]. The Internet represents an environment where large volumes of data are collected, stored, and readily transmitted, resulting in more significant social privacy implications and an increasing need for protective measures [9]. Cybersecurity involves protecting digital devices and the ability to communicate securely on the Internet and preventing unauthorized access or operating disruptions [23].

Security practitioners face various asymmetrical cyber threats [24]. These advanced persistent threats (APT) and financially motivated cyberattacks fall into ten categories identified as distributed denial of service (DDoS), session hijacking/man-in-the-middle, phishing/spear-phishing, drive-by, structured query language (SQL) injection, cross-site scripting (XSS), password, eavesdropping, birthday, and malware which are used in furtherance of financial gain [24]. Cybercrime uses computers as an instrument, target, or warehouse to further criminal activity such as identity theft, child exploitation, fraud, extortion, gambling, and hacking [24], [25].

A. Cybersecurity Threat Prevention

Many security professionals apply a perimeter defense strategy for cybersecurity by building a wall around the network for protection, relying on firewalls, conducting virus scanning, and deploying intrusion protection [5]. Organizations assume that everything inside the perimeter is secure and trusted when sophisticated threat actors defeat vulnerable perimeter defenses and security processes [5]. Applying the zero-trust security model ensures that all network resources are accessed securely and strictly on a need-to-know basis. All network traffic is subject to inspection and logging [5].

Prevention of cyberattacks, vulnerabilities, and technology failures that can lead to disruptions of operations and services is built around an organization's security structure and strategy[21]. Often protective methods rely on solid leadership, collaborative relationships between the private sector and federal government, and shared responsibilities for defensive and responsive actions [27]. Costs play a significant role in security and resiliency development and implementation in many cases. In 2018, the price per lost or stolen record through a cyberattack was approximately $148 [12]. Viewing that cost at scale, the magnitude of a cybersystem breach cost Yahoo roughly $440 billion, making preventive strategies essential [12].

III. Research Design and Methodology

The research design for the present study was a quantitative, non-experimental, cross-sectional design using partial lease squares-structural equation modeling (PLS-SEM). The research model contained the six constructs of the TTAT (i.e., perceived susceptibility, perceived severity, perceived threat, prevention effectiveness, prevention cost, and self-efficacy). Avoidance behavior serves as a dependent variable. The research design analyzed each TTAT construct to determine the predictive significance of these factors when considering information security leaders' behavioral intentions to share cyber threat information to implement safeguard measures. The overarching research question asked: To what extent do technology threat avoidance factors affect cybersecurity professionals' willingness to collaborate and share information regarding cybersecurity threats? Potential participants included full-time cybersecurity professionals working in the United States.

The present study uses a modified version of the TTAT (Liang & Xue, 2010). Liang and Xue (2010) designed the TTAT to measure security behaviors related to personal computer usage. The modified version of the TTAT used in the present study will examine perceptions and behaviors associated with information sharing to reduce cybersecurity threats. Permission to use and modify the instrument was obtained from Liang and Xue before the data collection began.

The modified survey used consists of 49 questions. Five questions collect demographic data on age, gender, and work experiences. The remaining 44 items measure the independent variables of perceived susceptibility (5 questions), perceived severity (10 questions), perceived threats (5 questions), prevention effectiveness (6 questions), prevention cost (3 questions), and self-efficacy (10 questions) and the dependent variable of avoidance behavior (5 questions). All items on the TTAT survey instrument will be measured using a 7-point Likert-type scale. All but one of the variables are calculated using a scale that ranges from 1 (Strongly disagree) to 7 (Strongly agree). The one exception is perceived severity, measured on a 7-point Likert type scale ranging from 1 (Extremely innocuous) to 7 (Extremely devastating).

IV. Results

This study used the technology threat avoidance theory (TTAT) to identify the most significant factors influencing cybersecurity professionals' willingness to collaborate and share information regarding cybersecurity threats. After evaluating the model constructs to ensure an acceptable fit,

A PLS-SEM path analysis was conducted. Figure 2 presents the path analysis for the PLS-SEM model. The strength and significance of each path coefficient are presented with the significance values shown in parentheses. Green arrows represent significant relationships between model constructs ($p < 0.05$), whereas red arrows indicate non-significant relationships ($p > 0.05$). Perceived susceptibility and perceived severity were significantly and positively associated with perceived threat, explaining 67% of the variance in perceived threat ($R2 = 0.669$). Additionally, perceived threat was a significant predictor, explaining 44% of the variance in avoidance motivation ($R2 = 0.441$). None of the other variable relationships within the model were significant.

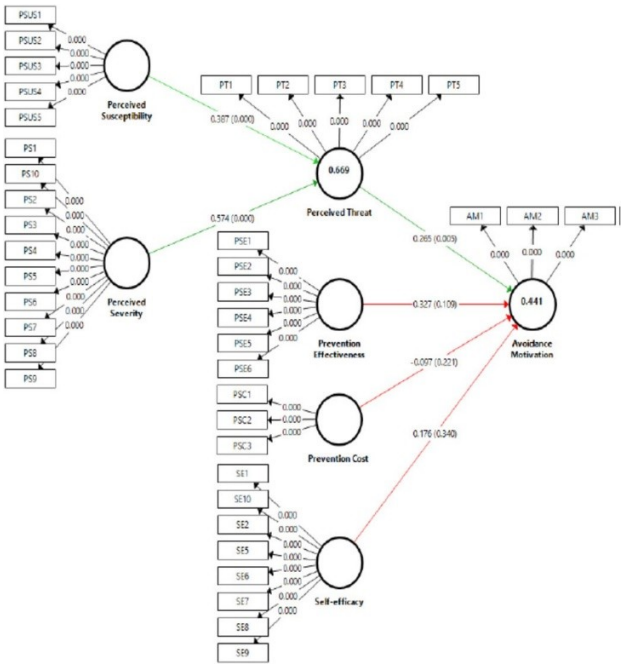

Figure 2 - Path Analysis Model.

Table 1 reports the hypothesis testing results of the path analysis in table format. The path coefficients represent the strength and direction of the variable relationships used to test the study's hypotheses, and the p-values indicate the significance of the statistical relationships. Significance values below 0.05 indicate that the relationship is significant and the null hypothesis should be rejected, while p-values above 0.05 indicate that the null hypothesis cannot be rejected.

In summary, a PLS-SEM path analysis was used to analyze data collected from N = 137 cybersecurity professionals in the United States. The study's purpose was to use the TTAT to identify the most significant factors influencing cybersecurity professionals' willingness to collaborate and share information regarding cybersecurity threats. The presented results demonstrate how technology threat avoidance factors affected cybersecurity professionals' willingness to avoid cybersecurity threats through information sharing. The findings indicated that cybersecurity professionals' perceptions of attack susceptibility and severity were significantly related to their perceived threat levels. Additionally, perceived threat was a significant predictor of avoidance motivation. Prevention effectiveness, prevention cost, and self-efficacy were not significant predictors of avoidance motivations.

Table 1 - Note. PS = perceived severity, PSUS = perceived susceptibility, PT = perceived threat, PSE = prevention effectiveness, PSC = prevention cost, SE = self-efficacy, and AM = avoidance motivation.

Results of the Hypothesis Testing

Paths	Path Coefficients	T Statistics	P values	Null Hypothesis Results
PS -> PT	0.574	7.053	0.000	Rejected
PSUS -> PT	0.387	4.714	0.000	Rejected
PT -> AM	0.265	2.802	0.005	Rejected
PSC -> AM	-0.097	1.226	0.221	Not Rejected
PSE -> AM	0.327	1.605	0.109	Not Rejected
SE -> AM	0.176	0.956	0.340	Not Rejected

V. Conclusion

A. Discussion of the Findings

The study addressed the specific problem of the lack of information regarding how perceived susceptibility, perceived severity, perceived threat, prevention effectiveness, prevention cost, and self-efficacy influence information sharing and collaborative protection behaviors among cybersecurity professionals responsible for securing organizational data. When evaluating the full TTAT model, the results of the PLS- SEM path analysis revealed that prevention cost, prevention effectiveness, and self-efficacy were not significantly related to cybersecurity professionals' willingness to collaborate and share information regarding cybersecurity threats. Instead, participants were motivated to act based on their perceived threat level, which was influenced by threat severity (magnitude) and susceptibility (vulnerability). Liang and Xue [20] and Carpenter et al. [6] reported significant relationships between perceived threat and avoidance motivation. However, the remainder of the model was not explanatory in the context of cybersecurity professionals' willingness to share information via the DHS.

B. Limitations of the Study

The scope of this research was limited to the study of U.S. cybersecurity professionals' technology threat avoidance and information-sharing perceptions and behaviors. The study's main design limitation was that it only collected quantitative data. This decision meant that the data only addressed the TTAT variables, and descriptive narrative data was not included in the study. Using quantitative data to examine the relationships between variables is standard practice. Still, the results will not reflect the details of specific cybersecurity incidents or the participants' reflections [28], [33]. The research design did not assess the different types and sizes of organizations, which also limited the findings. Cybersecurity professionals at differently sized U.S. organizations might approach cybersecurity and participation in the DHS information-sharing program differently [13], [16], [2], [11]. However, the study's goal was not to compare different company types or sizes when evaluating the variable relationships.

C. Implications for Practice

From a theoretical perspective, this study supported the TTAT as a research model that explains some avoidance motivations related to information sharing and I.T. threats [20]. From a practical perspective, cybersecurity professionals, information security leaders, organizations, and policymakers can use the study's findings to enhance the governance and risk management of cyber and information security programs. The findings partially explain how users respond to I.T. threats [19]. The study contributed to information and cybersecurity and provided a deeper understanding of the human factors influencing an individual's threat avoidance motivation [6]. The study also highlighted aspects of the TTAT that may not relate to information sharing and cybersecurity.

Information sharing has become a very important aspect of threat mitigation for U.S. organizations. The emphasis on information has evolved from the occasional voluntary participation in industry-based information-sharing alliances toward more policy-driven participation in collaborative information-sharing between organizations. U.S. government organizations are implementing policies mandating cyber threat reporting and information sharing for critical infrastructure and publicly traded organizations. The results and conclusions of the study provide insight to Congress and the DHS Cybersecurity & Infrastructure Security Agency on cybersecurity professionals' information sharing and threat prevention motivations.

D. Recommendations for Further Research

It is important to understand technology users' and cybersecurity professionals' technology threat avoidance motivations and behaviors from scholarly and practical perspectives. The current study addressed the lack of knowledge regarding how perceived threat susceptibility, perceived threat severity, prevention effectiveness, prevention cost, and self-efficacy influence information sharing and collaborative protection behaviors. These factors have been shown to affect threat avoidance motivations and behaviors [3], [4], [15], [19]. However, the present study's findings were mixed, and additional research is needed to further explore the TTAT's applicability in cybersecurity and information-sharing contexts.

Cybersecurity is a global issue, and research should be conducted to determine technology threat avoidance information sharing from an international perspective [1], [22], [31]. The data were collected through a web-based survey, increasing the potential for self-selection, desirability, and acquiescence bias. Future studies should include design factors that help reduce those potential biases. Additionally, researchers should use qualitative methods to obtain descriptive narrative data from participants using the TTAT framework to identify potential latent variables that were not examined in this study. Combining quantitative and qualitative data collection methods could provide a more comprehensive picture of cybersecurity professionals' technology threat avoidance behaviors [10], [28], [33], [22].

The study addressed a knowledge gap regarding perceived threat susceptibility, perceived threat severity, prevention effectiveness, cost, and self-efficacy in U.S. cybersecurity professionals' information-sharing and collaborative protection behaviors. These factors have been shown to affect threat avoidance motivations and behaviors in some settings [3], [4], [15], [19]. This population's information- sharing was a critical issue because of low participation in the DHS's information-sharing program.

In summary, this study addressed the general problem of the lack of inter-organizational collaboration on cybersecurity threats between private firms and the U.S. federal government by exploring cybersecurity professionals' perceptions of cybersecurity threats and attitudes toward information sharing. By studying these factors, the present study revealed that cybersecurity professionals' willingness to share cyber threat information was significantly influenced by perceived threat (e.g., susceptibility and severity). These findings can be used to improve threat avoidance through information sharing. The study contributes to the threat avoidance literature and the U.S. government's efforts to strengthen national cybersecurity through information sharing.

References

[1] N. Akhtar, "Latest trends in cybersecurity after the Solar Wind hacking attack." Foundation University Journal of Engineering and Applied Science, 1(2), 14-

[2] 24, 2020. https://doi.org/10.33897/fujeas.v1i2.347 [Accessed Sept. 10, 2022]

[3] M. Amanowicz, Towards building national cybersecurity awareness. International Journal of Electronics and Telecommunications, 66(2), 321-326, 2020. https://doi.org/ 10.24425/ijet.2020.131881 [Accessed Oct. 11, 2022]

[4] F. Aribake and Z. Aji, Assessment on phishing avoidance behavior among Internet banking users in Nigeria: A conceptual model. Journal of Information System and Technology Management, 5(16), 1-14, 2020. https://doi.org/ 10.35631/JISTM.516001 [Accessed Oct. 11, 2022]

[5] K. Asante-Offei, and W. Yaokumah. Cyber- identity theft and fintech services: Technology threat avoidance perspective. Journal of Information Technology Research, 14(3), Article 1, 2021. https://doi.org/10.4018/JITR.2021070101 [Accessed Oct. 11, 2022]

[6] J. Baker and K. Waldron. "5G and zero trust networks." 2020. https://www.jstor.org/stable/resrep27016 [Accessed Aug. 11, 2022].

[7] D. Carpenter, D. Young, P. Barrett, and A. McLeod, Refining technology threat avoidance theory. Communications of the Association for Information Systems, 44, Article 22., 2019. https://doi.org/10.17705/1CAIS.04422

[8] M. Cavelty, C. Mauer, and F. Krishna-Hensel, F., Power and security in the information age: Investigating the role of the state in cyberspace, 2016. New York, NY: Routledge

[9] H. Chen and W. Li, Mobile device users' privacy security assurance behavior: A technology threat avoidance perspective. Information and Computer Security, 25(3), 330-344, 2017. https://doi.org/10.1108/ICS-04-2016-0027

[10] M. Chertoff, Exploding data: Reclaiming our cyber security in the digital age, 2018. New York, NY: Atlantic Monthly Press [Accessed Aug. 4, 2022].

[11] J.W. Creswel and J.D. Creswell, Research design: Qualitative, quantitative, and mixed methods approaches, 2017. Sage Publications.

[12] P. Datta, Hannibal at the gates: Cyberwarfare & the Solarwinds sunburst hack. Journal of Information Technology Teaching Cases, 2021. https://doi.org/10.1177%2F204388692 1993126

[13] H. Hammouchi, O. Cherqi, G. Mezzour, M. Ghogho, and M. Koutbi, "Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time." Procedia Computer Science. 151. 1004-1009, 2019. 10.1016/j.procs. 2019.04.141, [Accessed Sept. 4, 2022].

[14] J. Jaffer, Carrots and sticks in cyberspace: addressing critical issues in the Cybersecurity Information Sharing Act of 2015, 2016. SCL Rev., 67, 585. [Accessed Aug. 4, 2022].

[15] C. James. "Cybersecurity: Threats challenges opportunities", 2016, https://www.bing.com/search?q=cybersecurity+threats%2c+challenges+opportunities&qs=NW&pq=cybersecurity+threats

%2c+challenges+oppor&sk=NWU1
&sc=339&cvid=0529FF8B243C428F8074A83D428EC0E8&FORM=
QBRE&sp=2&ghc=1 [Accessed July 20, 2021]
[16] A. Jibril, M. Kwarteng, R. Botchway, J. Bode, and M. Chovancova, "The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. Cogent Business & Management," 7(1), Article 1832825, 2020. https://doi.org/10.1080/23311975.2020.1832825
[17] D. Johnson, "The federal government has big plans for the Automated Indicator Sharing program, but agency officials and members of Congress continue to express frustration at the sluggish pace of enrollment", 2017, https://fcw.com/security/2017/11/enrollment-for-threat-sharing-program-continues-to-lag/227957/ [Accessed Feb. 5, 2020].
[18] D. Johnson, "How info sharing can get unstuck", 2018. https://fcw.com/security/2018/11/how-info-sharing-can-get-unstuck/199096/ [Accessed Feb. 5, 2020].
[19] S. Landau, Listening in: Cybersecurity in an insecure age, 2017. New Haven, CT: Yale University Press
[20] H. Liang and Y. Xue, Avoidance of information technology threats: A theoretical perspective. Management Information Systems Quarterly, 33(1), 71-90, 2009. http://dx.doi.org/10.2307/20650279 [Accessed Oct. 4, 2022].
[21] H. Liang and Y. Xue, Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394-413, 2010. http://dx.doi.org/ 10.17705/1jais.00232 [Accessed Aug. 12, 2022].
[22] I. Mandritsa, I. Tebueva, V. Peleshenko, V. Petrenko, O. Mandritsa, I. Solovyova, A. Fensel, and M. Mecella, "Defining a cybersecurity strategy of an organization: criteria, objectives and functions", 2018, http://ceur-ws.org [Accessed July 20, 2021].
[23] M. Mark, "An Analysis of Factors Influencing Phishing Threat Avoidance Behavior: A Quantitative Study", Capella University ProQuest Dissertations Publishing, 2021. 28320611.https://www.proquest.com/dissertations-theses/analysis-factors-influencing-phishing-threat/docview/2506645080/se-2?accountid= 44888
[24] R. Meeuwisse, Cybersecurity for beginners, 2017. London, United Kingdom: Cyber Simplicity Ltd
[25] J. Melnick, "Top 10 most common types of cyber-attacks" 2018. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ [Accessed Aug. 4, 2022].
[26] S. R. Muller, "An Intersection of Information Security Policies and I.A. Awareness, While Factoring in End-User Behavior: A NIST Cybersecurity Framework Perspective on "Identify", 2020. Proceedings of International Conference on Research in Management and Technovation, ICRMAT 2020 Vol (24). Annals of Computer Science and Information Systems ISSN 2300-5963
[27] S.R. Muller, and D.N. Burrell, "Social Cybersecurity and Human Behavior", 2022. International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), 6(1). Hershey, PA: IGI Global
[28] S.R. Muller, and M. Lind, "Factors in information assurance professionals' intentions to adhere to information security policies", 2020. International Journal of Systems and Software Security and Protection, 11(1). Hershey, PA: IGI Global
[29] S. Rahi, Research design and methods: A systematic review of research paradigms, sampling issues, and instruments development. International Journal of Economics & Management Sciences, 6(2), Article 10000403, 2017. http://dx.doi.org/10.4172/2162-6359.1000403
[30] G. Sharkov, Assessing the maturity of national cybersecurity and resilience. Connections: The Quarterly Journal, 19(4), 5-24, 2020. [Accessed Aug. 4, 2022]. https://doi.org/10.11610/Connections.19.4.01
[31] P. Singer and A. Friedman, Cybersecurity and cyberwar: What everyone needs to know? New York, NY: Oxford University, 2014.
[32] M. Tvaronavičienė, T. Plėta, S. Casa and J. Latvys, Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia, and Lithuania. Insights into Regional Development, 2(4), 802-813, 2020. http://doi.org/10.9770/IRD.2020.2.4(6)
[33] N. Yang, T. Singh, A. Johnston, A replication study of user motivation in protecting information security using protection motivation theory and self-determination theory. AIS Transactions on Replication Research, 6(10), 2020. https://doi.org/10.17705/1atrr.00053
[34] N. Zeng, Y. Liu, P. Gong, M. Hertogh, and M. König, Do right PLS and do PLS right: A critical review of PLS-SEM application in construction management research. Frontiers of Engineering Management, 2021. https://doi.org/10.1007/s42524-021- 0153-5
[35] A. Zibak and A. Simpson, "Cyber threat information sharing: Perceived benefits and barriers, August 2019. Proceedings of the 14th international conference on availability, reliability, and security (pp. 1-9).

Dr. Willie Session is a strategic information and technology security consultant, collaborator, and leader who consistently works across the enterprise to achieve positive mission outcomes. He leads teams in cyber and physical security operations, monitoring, engineering, insider threat, technology risk, executive protection, and business contingency. His national and domestic security and intelligence career spans successful roles in the Federal Bureau of Investigation and the U.S. Air Force. He earned a Ph.D. in Cybersecurity Leadership from Capitol Technology University and an MBA from National University.

Dr. S. Raschid Muller is a Cybersecurity Executive with the Department of Defense (DoD) at Fort Meade, Maryland. He teaches cybersecurity at the undergraduate and graduate levels at Arizona State University, the University of Maryland Global Campus, and Capitol Technology University. Dr. Muller is a 2020 Brookings Institute Fellow (LEGIS) who served on the House Committee for Homeland Security and was *assigned to the Cybersecurity, Infrastructure Protection, and Innovation subcommittee in the United States Congress. He also is a 2021 U.C. Berkeley Executive Leadership Academy Fellow from the Goldman School of Public Policy. He earned a Ph.D. in Information Technology (IA/Cybersecurity) from Capella University, a Ph.D. in Cybersecurity Leadership and D.B.A. in Supply Chain Management from Capitol Technology University. He is a member of IEEE, ISACA, NDIA, and AFCEA.