HO CHI MINH CITY NATIONAL UNIVERSITY
INTERNATIONAL UNIVERSITY

TRAN VAN DIEN

PPMIU22002

Topic name:

Unlocking the potential of government communications and organizational cybersecurity policy: The role of key factors influencing employee cybersecurity behavior

NEW POINTS OF DOCTORAL THESIS

Major: Public Administration

Code: 9340403

SCIENTIFIC INSTRUCTOR:

Associate Professor, Dr. Nguyen Van Phuong

HO CHI MINH CITY, 2024

I. RESEARCH GAP

1. Research context

With the development of the 4.0 era, most companies are implementing digital transformation to stay competitive (Demirbas et at., 2018; Salunke et at., 2019). Digital transformation and IT service outsourcing play an important role, making cybersecurity a major concern as the risk of cyber attacks and data breaches increases (Gozman & Willcocks., 2019 ; Makridis & Dean., 2018).

Vietnam is developing rapidly in information technology. According to the International Telecommunication Union (ITU), Vietnam ranks 9th in the world in terms of the number of people proficient in digital technology with 7.5 million people. The WIPO report ranked Vietnam 48/132 countries in the Global Innovation Index 2022, especially in digital technology based on supercomputers, artificial intelligence (AI) and automation. Currently, the Vietnamese Government is promoting the construction of a digital government to reform administration, but there are still many potential risks and challenges regarding cybersecurity.

In Vietnam, cyber attacks on critical information infrastructures of the Government and large organizations have become increasingly complex and dangerous. According to the Ministry of Public Security, every year thousands of Vietnamese websites are attacked by hackers to steal information and install malware. In the first 6 months of 2019, more than 2,500 Vietnamese news sites and electronic information portals were attacked, and hundreds of thousands of computers were infected with malware. Vietnam ranks 4th out of 10 countries controlled by botnets.

Cyberspace and cybersecurity are new fields that are evolving faster than scientific research (Dawson & Thomson., 2018). The field is not only faced with technological challenges but is also dominated by human behavior. Although technology experts play an important role, they cannot guarantee that ANM is completely effective. Humans also play a key role, with more than 70% of successful breaches of systems or data being caused by human error (IBM Global Technology Services., 2014; Carlton & Levy., 2015).

In February 2023, the H05 BCA Information Technology Department discovered a new spyware variant appearing in the BCA's internal computer network, collecting documents (.doc, docx, xlsx, ppt, pdf) automatically encrypting files or copying them to external storage devices, searching for internet connections to transmit collected data to servers located abroad. Hacker groups have further improved the text editing module to deceive users. This is a spyware variant that bypasses the recognition mechanism of many anti-virus and anti-malware software.

According to the recent reports on the situation of functional foods in 2020, 2021, 2022, and 2023 by the Ministry of Public Security, the group of functional foods is increasing rapidly in both quantity and number of cases; security and information security attacks by hackers are increasingly diverse in all different fields and aspects; according to (Maglaras et al., 2019), the main target of cyber attacks is a country's Critical National Infrastructure (CNI) such as ports, hospitals, water, gas or electricity producers, which use and rely on Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) to manage their production operations. Protecting CNI has become an essential issue that needs to be considered.

Summarizing the work of protecting state secrets in 2023, the Government discovered that state secrets were leaked through cyberspace (such as Zalo network, email, electronic information pages, etc.) by government agencies and departments, from the central to local levels, unintentionally leaking 3,184 documents, including 2,000 top secret documents; In the first 6 months of 2023, the Ministry of Public Security discovered the leak of 236 documents containing state secrets belonging to the Ministry of Public Security and the Ministry of National Defense transmitted via unencrypted telecommunications lines (226 documents related to national security and defense).

To maintain business operations and protect information in cyberspace, employee cybersecurity behavior is key (Li et al., 2019). Despite the attention, research on cybersecurity has not been effectively exploited in countries with developing economies. In Vietnam, there has been research on cybersecurity but mainly using interdisciplinary social marketing methods to examine how employees experience and comply with security initiatives (Pham et al., 2019).

This study will explore the innovation and creativity of IT and cybersecurity service providers in Vietnam in the context of globalization and cyberspace. Data will be collected from IT providers, experts, and public sector employees through structured questionnaires and interviews. The thesis will use PLS-SEM model to explore the factors affecting employees’ cybersecurity awareness and behavior, and understand how they deal with IT security threats and risks.

Ensuring cyber security and national security cannot be done individually within regions, organizations, agencies, or individuals. Compliance with cyber security prevention measures must be implemented synchronously nationwide, from the central to local levels. Therefore, studying cyber security issues in Vietnam in the current context is necessary to identify systemic and comprehensive causes. From there, it is possible to propose solutions to ensure cyber security that are urgent, strategic, and appropriate to national realities. In which, the human factor also plays a very important role in this process.

2. Research Gap

First, from the overall review of previous studies, it is found that there is a need for more in-depth research on employees' CSA and their behaviors in protecting organizational information systems. However, scholars often focus on assessing intentions, attitudes, or behavioral likelihood, which may not provide comprehensive guidance for organizations that want to understand the impact of security awareness on employee behavior (Anderson & Agarwal, 2010 ; Herath & Rao., 2009 ; Johnston & Warkentin., 2010 ; Ng et at., 2009 ; Siponen et at., 2014 ; Wu, 2020 ; Li et at., 2019 , 2022). Therefore, in this thesis, we will apply PMT theory, TPB theory, and CT theory to evaluate the impact of CSA on IPM, ISPC, ATT, and employee information security behavior. CSA will be evaluated through five main variables of PMT: PS of threat, PV of threat, RE, SE, and PB. This will make the measurement more comprehensive.

Second, the development of legal policy documents based on international standards can contribute to the development of a comprehensive information security culture for each organization (Chen et at., 2015). However, the effectiveness of ANM policies has not yet reached a consensus in current studies. Some scholars argue that ANM policies do not have a significant effect on computer abuse intentions and behaviors, including modifying, stealing, or destroying software and data (D'Arcy et at., 2009; Lee & Larsen., 2009) . Despite the provision of written policies and guidelines, some employees still ignore or underestimate the risks (Han et at., 2017; Ifinedo., 2012, 2014; Li et at., 2019). Given these conflicting results, this paper examines the impact of organizational ANM policies on employees' ANM perceptions and EPB.

Third, government agencies are increasingly leveraging social media accounts for crisis management (Guo et al., 2021). However, existing studies mainly focus on exploring the reasons why people engage with government social media (GSM) during crises and classifying GSM emergency messaging strategies (Tang et al., 2021). This highlights the lack of examination of the impact of GSM on citizens, especially employees. In Vietnam, the Ministry of Information and Communications has been actively strengthening monitoring, proactively reviewing and evaluating statistics, promoting propaganda and warnings on mass media to inform users and avoid the risk of cyberattacks. Therefore, with the implementation of CT theory as a theoretical framework, the influence of the GMS approach on employees' CSA in organizations should also be more carefully examined.

Public organizations and enterprises in Vietnam are gradually digitizing and actively pursuing digitalization policies to optimize the circulation and storage of information. However, the lack of comprehensive government policies, decrees and circulars to coordinate technical infrastructure among agencies and organizations from the central to local levels has forced these agencies to install computer systems and networks independently, based on their available knowledge and budget. This approach lacks in-depth assessment of infrastructure procurement and provision packages, leading to shortcomings in the management and use of computer systems, posing significant risks to information security. More importantly, some civil servants, despite having basic knowledge of cybersecurity, do not comply with agency regulations due to the lack of guiding regulations, circulars and decrees. This leads to non-compliance such as copying unverified data using USB drives or using computers against regulations, which endangers information security in public sector computer systems. Therefore, this thesis is necessary to provide a solid basis for senior leaders of organizations and the Government in making strategic decisions on cybersecurity. The study will help overcome shortcomings in the administration, use and operation of computer network systems, ensure information security and improve the operational efficiency of public agencies.

This thesis limits the scope of research related to cybersecurity of organizations in Vietnam.

3. Reasons for choosing the topic and the urgency of the topic

Maglaras et al. (2019) noted that the main target of cybercriminals *(hackers)* today is to attack critical national infrastructures such as ports, hospitals, water, gas and electricity plants, using SCADA and ICS systems to manage production activities. Therefore, protecting CNI becomes an essential issue that needs to be considered. In general, existing cyber security measures are classified according to legal, technical, organizational, construction, capacity and cooperation aspects.

According to the Global Services Location Index (GSLI) 2019, Vietnam ranked fifth among the top 50 countries for IT outsourcing services, based on four key factors: financial incentives, workforce and skills pool, business environment, and digital resonance. Therefore, the use of Vietnam's IT outsourcing services is increasingly attractive to both international and domestic customers thanks to its cost efficiency and professional workforce with high IT adaptability. Moreover, the business environment for the IT industry in Vietnam has been significantly improved thanks to foreign investments from giants such as Intel, IBM, Samsung, LG, and Microsoft and innovative startups.

However, along with the strong development of IT services, cybersecurity has become a real challenge for organizations. Since 2018, Vietnam has witnessed a series of data breaches and cyber attacks that have disrupted business operations and negatively affected business results. Incidents such as hackers blocking VOV radio broadcasts in 2021 and the attack on the national population database in 2023 are typical examples. Most businesses suffer the consequences of these cyber attacks, partly due to employees' reckless cybersecurity behavior; for example, computers are infected with viruses, employees forget to log out of the system, or click on phishing emails (Ponsard & Grandclaudon, 2020). These situations stem from employees' lack of awareness and knowledge of cybersecurity (Gratian et al., 2018).

According to the 2023 State Secret Protection Summary Report of the Ministry of Public Security, government agencies from central to local levels, including the Ministry of Public Security and the Ministry of National Defense, have leaked thousands of documents containing state secrets on cyberspace due to failure to comply with regulations on IT and ANM security protection. IT crime groups are increasing in number and diversifying in their methods of operation on cyberspace, mainly taking advantage of users' lack of vigilance and lack of understanding of cybersecurity, including civil servants and public employees (typically, fraud cases through cybercriminals stealing personal social network users' accounts or bank account information to commit crimes).

In the recent 2024 digital economic forum report to strengthen financial and banking development in Vietnam, in 2023 there were about 14,000 cyber attacks and 16,000 online fraud reports, causing economic losses of about more than 390 trillion VND, accounting for 3.6% of GDP.

Although the legal system and circulars and decrees on cybersecurity in Vietnam have been issued by the Government, they are still incomplete and overlap in management and implementation. Legal regulations have not yet ensured a safe environment in cyberspace for all citizens.

In addition, Vietnam is an emerging economy with high adaptability to rapid technological change, the government is still struggling to promote the digital economy while facing threats and controlling cyber attacks. Most businesses from developed countries invest heavily in cybersecurity due to concerns about unexpected disasters such as hackers, viruses or software intrusions, but this activity is very expensive (Dreibelbis et at., 2018).

Although the topic of ANM has received much love and care in many recent studies, it has not been effectively exploited in countries with developing economies, especially from the perspective of cognition and behavior in Vietnam. These reasons have motivated the author to choose this topic as a research thesis.

II. CONTRIBUTIONS OF THE RESEARCH

1.1. Background and importance of the study:

Research adds to our understanding of the impact of GSM on information security. Although information security behaviors have been extensively investigated, the impact of GSM is still in its infancy. Previous studies have examined how individuals are protected from cyber threats with the support of GSM in both organizational and individual contexts. However, GSM is a powerful platform for governments and international organizations to raise awareness and protect the public from cyber threats.

1.2. Focus on actual protective behavior:

The surveys emphasize the importance of employees implementing actual information security EPBs rather than focusing solely on intentions. Existing surveys focus primarily on security-related intentions, whereas these surveys comprehensively measure ISPC, IPM, and EPBs. This provides a better understanding of the mechanisms through which protective behaviors are developed and implemented in organizations.

1.3. Impact of GSM:

The findings show that GSM has a positive impact on CSA and IPM. GSM has both direct and indirect effects on compliance attitudes and EPB. In particular, IPM plays a mediating role in this relationship, indicating that the use of GSM can improve employees' CSA and IPM knowledge in protecting information security.

1.4. Combining the Protection Motivation Theory and the Propaganda Theory:

The research integrates PMT theory and CT theory to provide a comprehensive theoretical framework for ANM. PMT theory has been extended to include tangible activities, and CT theory provides a better understanding of how these factors influence EPB in individual and organizational contexts.

1.5. Application of the Theory of Planned Behavior (TPB):

The studies incorporate TPB theory to explore the relationships between perceptions, attitudes, intentions, and EPB. TPB theory helps clarify how CSA and IPM perceptions shape ISPC and EPB.

1.6. Application in practical context:

The findings of the study suggest that PP compliance increases CSA, although the impact on EPB is indirect. This highlights the importance of integrating security policies and resources into workplace culture to promote employee safety behaviors. In addition, the study explores the impact of knowledge acquisition through GSM on the antecedents of CSA.

1.7. Comparison with previous investigations:

These studies add to the body of knowledge by providing theoretical explanations for the consequences of using PMT and CT theories in ANM situations. Although information security behaviors have been widely investigated in relation to technological advances, the investigation of these behaviors in relation to the impact of GMS is still in its infancy. Few studies have examined how best to protect individuals from security threats with the aid of GMS, although many have been conducted in both organizational and individual contexts. This is important because social media is a powerful platform for governments and international organizations to use to raise public awareness and make recommendations on how to prevent cybercrime.

1.8. Conclusion and theoretical contribution of the study:

The study provides insights into the effectiveness of government cybersecurity initiatives, assessing actual actions rather than just intentions, and suggesting improvements in employee prevention practices. It strengthens the literature on the behavioral aspects of cybersecurity and highlights the importance of enhancing awareness and EPB in government organizations. By integrating PMT theory, CT theory, and TPB theory, this study provides a comprehensive theoretical framework and practical implications for improving the effectiveness of cybersecurity policies and programs.

This thesis not only expands the understanding of PMT theory, CT theory and TPB theory but also provides practical evidence on their application in the context of cybersecurity, especially in government organizations in developing countries like Vietnam.

2. Contributions on managerial implications

In addition to the theoretical contributions, the thesis also makes an important contribution in providing managerial implications related to information security and cyber security. The managerial implications are drawn from three articles related to the investigation of ANM and provide specific recommendations for managers and professionals in this field. The findings highlight the importance of protecting ANM in the context of digital transformation and how organizations can apply it to strengthen information security effectiveness.

2.1. The Importance of Cybersecurity in Digital Transformation

Our findings highlight the importance of ANM in the context of digital transformation. Executives need to address cybersecurity concerns related to remote working while also enhancing team productivity. Professionals need to understand the role of social media in mitigating cybersecurity risks, as well as the importance of personal protection. Safeguards such as complex login processes and secure web browsing should be in place.

2.2. Impact of Threat Assessment and Response Strategy

Empirical research evidence shows that users' attitudes and motivations toward security measures are influenced by their assessment of threats and coping strategies. Governments and organizations should provide information security training to enhance their ability to assess risks and apply remedial measures. Education and information campaigns should be conducted on an ongoing basis to increase CSA awareness and effectiveness in dealing with security issues.

2.3. Impact of GSM on Information Security Behavior

Our findings suggest that GSM has a significant impact on information security behaviour. Governments should expand their involvement in disseminating accurate information about GSM, ensuring that messages are carefully crafted. This will help raise awareness of information security and encourage protective measures.

2.4. Improving Security Attitudes and Motivation

Positive attitudes and motivation can improve security behaviors. Employees need to perceive cybersecurity as a shared responsibility across the organization. Organizations should emphasize the importance of cybersecurity precautions and encourage employees to engage in security activities through rewards and career advancement.

2.5. Recommendations For Managers

Establish a Governance Framework: Managers should design and disseminate ANM guidelines and conduct educational campaigns to increase the organization's understanding of information security.

Training and CSA: Security training programs should include specific examples of security breaches and preventative measures. Encourage the exchange of knowledge and experience in dealing with cyber risks.

Threat Awareness: Employees need to understand cyber threats and the benefits of protective measures. Senior management involvement in strategic planning is necessary to convince employees of the importance of information security.

2.6. Strengthening Policy Compliance

Cybersecurity policy compliance is a key factor influencing EPB. Organizations need to invest in training and awareness campaigns to effectively disseminate policies and enhance CSA. Governments should maintain an active role in disseminating cybersecurity information through GSM channels, ensuring that information is communicated promptly and accurately.

In summary, this thesis provides a basis for organizations to develop strategic solutions, enhance governance, and protect network systems. Increased training, awareness, and policy compliance are key factors to improve cybersecurity in today's digital landscape.

References

Albashrawi, M., Asiri, Y., Binsawad, M. and Alqahtani, L. (2022), “The effect of social media use on empathy and well-being: a personality perspective in Saudi Arabia”, *Journal of Asia Business Studies* , Vol. 16 No. 2, pp. 406–423, doi: 10.1108/JABS-11-2020-0461.

AlKalbani, A., Deng, H., Kam, B. and Zhang, X. (2017), “Information Security Compliance in Organizations: An Institutional Perspective”, *Data and Information Management,* Vol. 1 No. 2, pp. 104-114, doi: 10.1515/dim-2017-0006.

Alshaikh, M., Maynard, S.B. and Ahmad, A. (2021), “Applying social marketing to evaluate current security education training and awareness programs in organizations”, *Computers and Security,* Vol. 100, pp. 1-19, doi: 10.1016/j.cose.2020.102090.

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior, 136,* 107376. https://doi.org/10.1016Zj.chb.2022.107376

Alghamdi, MI (2021). Withdrawn: Determining the impact of cyber security awareness on employee behavior: A case of Saudi Arabia. *Materials Today: Proceedings*. https:ZZdoi.org/10.1016Zj.matpr.2021.04.093

Allam, S., Flowerday, S.V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security, 42,* 56-65. doi:10.1016/j.cose.2014.01.005

Ameen, N., Tarhini, A., Shah, M.H., Madichie, N., Paul, J. and Choudrie, J. (2021), "Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen -Mobile workforce", *Computers in Human Behavior* , Vol. 114, p. 106531, doi: 10.1016/j.chb.2020.106531.

Anderson, CL and Agarwal, R. (2010), "Practicing safe computing: A multimethod empirical examination of home computer user behavioral security intentions", *MIS Quarterly: Management Information Systems* , Vol. 34 No. 3, pp. 613–643, doi: 10.2307/25750694.

Ani, UPD, He, H. (Mary), & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology, 1* (1), 32-74. https://doi.org/10.1080/23742917.2016.1252211

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action Control* (pp. 11-39). Berlin: Springer. https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision > Processes, 50* (2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human behavior and emerging technologies* , *2* (4), 314-324. https://doi.org/10.1002/hbe2.195

Armitage, C.J., & Conner, M. (2001). Efficacy of the theory of planned behavior: A meta-analytic review. *British Journal of Social Psychology* , *40* (4), 471-499. https://doi.org/10.1348/014466601164939

Bandura, A., & Adams, N.E. (1977). Analysis of self-efficacy theory of behavioral change. *Cognitive Therapy and Research* . https://doi.org/10.1007/BF01663995

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American psychology* , *37* (2), 122.

Bauer, S., Bernroider, EWN and Chudzikowski, K. (2017), "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks", *Computers & Security*, Vol. 68, pp. 145-159, doi: 10.1016/j.cose.2017.04.009.

Barlow, J.B., Warkentin, M., Ormond, D., & Dennis, A.R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violations. *Computers & Security, 39,* 145159. https://doi.org/10.1016/j.cose.2013.05.006

Bauer, S., & Bernroider, E.W.N. (2017). From information security awareness to reasoned compliant action. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 48* (3), 44-68. https://doi.org/10.1145/3130515.3130519

Beaunoyer, E., Dupéré, S. and Guitton, MJ (2020), "COVID-19 and digital inequalities: Reciprocal impacts and mitigation strategies", *Computers in Human Behavior* , Vol. 111, p. 106424, doi: 10.1016/J.CHB.2020.106424.

Bellovin, S.M., & Cheswick, W.R. (1994). Network firewalls. *IEEE communications magazine* , *32* (9), 50-57.

Bin-Abbas, H., & Bakry, S.H. (2014). Assessment of IT governance in organizations: A simple integrated approach. *Computers in Human Behavior, 32,* 261-267. https://doi.org/10.1016/j.chb.2013.12.019

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivates protective security behaviors. *MIS Quarterly, 39(4),* 837-864. https://doi.org/10.25300/MISQ/2015/39.4.5

Broeders, D. (2016). *The public core of the internet: An international agenda for internet governance* (p. 116). Amsterdam University Press.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly: Management Information Systems* , Vol. 34 No. 3, pp. 523–548, doi: 10.2307/25750690.

Campbell, M. (2019). Sample size: methods of calculation and reporting. *African Journal of Midwifery and Women's Health* , *13* (2), 1-9.

Carlton, M., & Levy, Y. (2015, April). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. In *SoutheastCon 2015* (pp. 1-6). IEEE.

Carr, M. M., & Erskine, T. (2016). Beyond "quasi-norms": The challenges and potential of engaging with norms in cyberspace. NATO Cooperative Cyber Defense Center of Excellence.

Conner, M., & Armitage, C.J. (1998). Extending the theory of planned behavior: A review and avenues for further research. *Journal of applied social psychology* , *28* (15), 1429-1464. https://doi.org/10.1111/j.1559-1816.1998.tb01685.x

Collier, J. (2019). *Cyber security assemblages: the theory and practice of diffuse security provision* (Doctoral thesis, University of Oxford).

Collier, J.E., & Sherrell, D.L. (2009). Examining the influence of control and convenience in a self-service setting. *Journal of the Academy of Marketing Science, 38(4),* 490-509. DOI 10.1007/s11747-009-0179-4.

Corallo, A., Lazoi, M., Lezzi, M. and Luperto, A. (2022), "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review", Computers in Industry, Vol. 137, pp. 1-16, doi: 10.1016/j.compind.2022.103614. https://cdn.techscience.cn/ueditor/files/TSP_CSSE-37-3/TSP_CSSE_15206/TSP_CSSE_15206.pdf

Cohen, J. (1988). "In Statistical power analysis for the behavioral sciences" (2nd ed). Lawrence Erlbaum Associates, Hillsdale, NJ. https://doi.org/10.4324/9780203771587

Cohen, J. (1992). A Power Primer Psychological Bulletin, 112. *T55–159 https://doi. org/70* , *1037* , 0033-2909.

Chatterjee, S., Chaudhuri, R., Vrontis, D., Thrassou, A. and Ghosh, SK (2021), "ICT-enabled CRM system adoption: a dual Indian qualitative case study and conceptual framework development", *Journal of Asia Business Studies* , Vol. 15 No. 2, pp. 257–277, doi: 10.1108/JABS-05-2020-0198.

Chakravorti, Bhaskar, and Ravi Shankar Chaturvedi. "Digital planet." (2017).

Chen, Q., Min, C., Zhang, W., Wang, G., Ma, X. and Evans, R. (2020), "Unpacking the black box: How to promote citizen engagement through government social media during the COVID-19 crisis", *Computers in Human Behavior* , Vol. 110, p. 106380, doi: 10.1016/j.chb.2020.106380.

Chen, X., Chen, L. and Wu, D. (2018), "Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective", *Journal of Computer Information Systems,* Vol. 58 No. 4, pp. 312-324, doi: 10.1080/08874417.2016.1258679.

Chen, Y., Ramamurthy, K. (Ram), & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems, 55(3),* 11-19. https://doi.org/10.1080/08874417.2015.11645767 .

Cheng, JW, Mitomo, H., Otsuka, T. and Jeon, SY (2016), "Cultivation effects of mass and social media on perceptions and behavioral intentions in post-disaster recovery: The case of the 2011 Great East Japan Earthquake" , *Telematics and Informatics* , Vol. 33 No. 3, pp. 753–772, doi: 10.1016/J.TELE.2015.12.001.

Chowdhury, NH, Adam, MTP and Skinner, G. (2019), "The impact of time pressure on cybersecurity behavior: a systematic literature review", *Behavior and Information Technology,* Vol. 38 No. 12, pp. 1290-1308, doi: 10.1080/0144929X.2019.1583769.

Chin, W. (1998a), "Issues and opinions on structural equation modeling", *MIS Q* , Vol. 22 No. 1, pp. 7–16. http://cits.tamiu.edu/kock/NedWebArticles/Chin1998.pdf

Chin, WW (1998b), "The partial least squares approach to structural equation modeling", *Modern Methods for Business Research* , Mahwah, NJ, Vol. 295 No. 2, pp. 295–336.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security, 1* (3), 18-41. https://doi.org/10.1080/15536548.2005.10855772

Chang, LYC, & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers & Security, 97,* 101959. https://doi.org/10.1016/j.cose.2020.101959

Criado, JI, Sandoval-Almazan, R. and Gil-Garcia, JR (2013), "Government innovation through social media", *Government Information Quarterly,* Vol. 30 No. 4, pp. 319–326, doi: 10.1016/J.GIQ.2013.10.003.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security* , Vol. 32, pp. 90–101, doi: 10.1016/J.COSE.2012.09.010.

Dang, VA, Vu Khanh, Q., Nguyen, VH, Nguyen, T., & Nguyen, DC (2023). Intelligent healthcare: Integration of emerging technologies and Internet of Things for humanity. *Sensors* , *23* (9), 4200.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20(1),* 79-98. https://doi.org/10.1287/isre.1070.0160

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in psychology* , *9* , 744.

Demirbas, D., Wilkinson, L., & Bennett, D. (2018). Supplier impact relations within the UK automotive industry. *Benchmarking: An International Journal* , *25* (8), 3143-3161.

Del Vecchio, P., Mele, G., Passiante, G., Vrontis, D. and Fanuli, C. (2020), "Detecting customers knowledge from social media big data: toward an integrated methodological framework based on netnography and business analytics ”, *Journal of Knowledge Management* , Vol. 24 No. 4, pp. 799-821, doi: 10.1108/JKM-11-2019-0637.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8(1),* 386-408. https://doi.org/10.17705/1jais.00133 .

Dreibelbis, Rachel C.; Martin, Jaclyn; Coovert, Michael D.; Dorsey, David W. . (2018). *The Looming Cybersecurity Crisis and What It Means for the Practice of Industrial and Organizational Psychology. Industrial and Organizational Psychology, 11(2), 346–365.* doi:10.1017/iop.2018.3

Donalds, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management, 51,* 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056

Eminagaoglu, M., Uear, E., & Eren, §. (2009). The positive outcomes of information security awareness training in companies: A case study. *Information Security Technical Report, 14(4),* 223-229. https://doi.org/10.1016/jjstr.2010.05.002 . https://csbweb01.uncw.edu/people/cummingsj/classes/MIS534/Articles/Ch5UserTraining.pdf

Farooq, A., Laato, S. and Najmul Islam, AKM (2020), “Impact of online information on self-isolation intention during the COVID-19 pandemic: Cross-sectional study”, *Journal of Medical Internet Research* , Vol. 22 No. 5, p. e19128, doi: 10.2196/19128. https://www.utupub.fi/bitstream/handle/10024/164912/pdf.pdf?sequence=1

Floyd, D.L., Prentice-Dunn, S., & Rogers, R.W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology* , *30* (2), 407-429.

Floyd, D.L., Prentice-Dunn, S. and Rogers, R.W. (2006), “A meta-analysis of research on protection motivation theory”, *Journal of Applied Social Psychology* , Vol. 30 No. 2, pp. 407–429, doi: 10.1111/J.1559-1816.2000.TB02323.X.

Fornell, C., & Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39. https://doi.org/10.2307/3151312.

Fosch-Villaronga, E. and Mahler, T. (2021), “Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots”, *Computer Law & Security Review* , Vol. 41, pp. 1-13, doi: 10.1016/j.clsr.2021.105528.

Gasser, M. (1988). *Building a secure computer system* (p. 85). New York: Van Nostrand Reinhold Company.

Gefen, D., Straub, D. and Boudreau, M.-C. (2000), “Structural equation modeling and regression: Guidelines for research practice”, *Communications of the Association for Information Systems* , Vol. 4 No. 1, p. 7. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=3787715114e286042aac4fd9b612114c226c6fe9

Gerbner, G. and Gross, L. (1976), “Living with television: The violence profile”, *Journal of Communication* , Vol. 26 No. 2, pp. 172–199, doi: 10.1111/J.1460-2466.1976.TB01397.X.

Gerbner, G., Gross, L., Signorielli, N., & Morgan, M. (1980). Television violence, victimization, and power. *American behavioral scientist* , *23* (5), 705-716.

Gerbner, G., Gross, L., Morgan, M., Signorielli, N., & Shanahan, J. (2002). Growing up with television: Cultivation processes. In *Media effects* (pp. 53-78). Routledge.

Gerbner, G., Gross, L., Morgan, M., Shanahan, J. and Signorielli, N. (2009), "Growing up with television: Cultivation processes", (2nd Ed) *Media Effects: Advances in Theory and Research* , Routledge, NY, pp. 34–49, doi: 10.4324/9781410602428-7.

Gozman, D., & Willcocks, L. (2019). The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations. *Journal of Business Research* , *97* , 235-256.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *computers & security* , *73* , 345-358.

Guo, J., Liu, N., Wu, Y. and Zhang, C. (2021), "Why do citizens participate on government social media accounts during crises? A civic voluntarism perspective", *Information and Management* , Vol. 58 No. 1, doi: 10.1016/j.im.2020.103286.

Guo, K.H., Yuan, Y., Archer, N.P., & Connelly, C.E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28* (2), 203-236. https://doi.org/10.2753/MIS0742-1222280208

Guchev, F., Damjanovska Krstikj, L., Bozhinovski, G., Perchinkova-Mishevska, S., & Jordanovska-Gucheva, N. (2022). Secondary Sjogren's syndrome in patients with rheumatoid arthritis.

Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior.

Hair, J.F., Black, William. C., Babin, Barry. J., & Anderson, Rolph. E. (2010). *Multivariate Data Analysis* (7th ed.). New York, Pearson. https://www.researchgate.net/profile/Jouini-Abdelhafid/post/Can_any_one_explain_me_the_Akaike_Information_Criterion_sensing-based_in_cognitive_radio2/attachment/59d623ec79197b80779823b4/AS%3A309790092267520%401450871121 033/download/194866033.pdf

Hair, J.F. (2011), "Multivariate data analysis: An overview", in Lovric, M. (Ed.), *International Encyclopedia of Statistical Science* , Springer, Berlin, pp. 904–907, doi: 10.1007/978-3-642-04898-2_395.

Hair, JF, Jr., Hult, GTM, Ringle, CM and Sarstedt, M. (2014), "A primer on partial least squares structural equations modeling (PLS-SEM)", *European Journal of Tourism Research* , Vol. 6 No. 2, pp. 211–213.

Hair, J., Risher, J., Sarstedt, M., & Ringle, C. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31(1),* 2-24. https://doi.org/10.1108/EBR-11- 2018-0203^r

Hair Jr., JF, Howard, MC and Nitzl, C. (2020), "Assessing measurement model quality in PLS- SEM using confirmatory composite analysis", *Journal of Business Research* , Vol. 109, pp. 101-110, doi: https://doi.org/10.1016/j.jbusres.2019.11.069 .

Han, JY, Kim, YJ and Kim, H. (2017), "An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective", *Computers and Security* , Vol. 66, pp. 52–65, doi: 10.1016/j.cose.2016.12.016.

Hanus, B. and Wu, Y. "Andy". (2016), "Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective", *Information Systems Management* , Vol. 33 No. 1, pp. 2–16, doi: 10.1080/10580530.2015.1117842.

Hanus, B., Windsor, J. C., & Wu, Y. (2018). Definition and multidimensionality of security awareness: Close encounters of the second order. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* , *49* (SI), 103-133.

Handford, C.E., Dean, M., Spence, M., Henchion, M., Elliott, C.T., & Campbell, K. (2015). Awareness and attitude towards the emerging use of nanotechnology in the agri-food sector. *Food Control, 57,* 24-34. https://doi.org/10.1016/j.foodcont.2015.03.033

Harris, MA and Patten, KP (2014), "Mobile device security considerations for small- and medium-sized enterprise business mobility", *Information Management and Computer Security* , Vol. 22 No. 1, pp. 97–114, doi: 10.1108/IMCS-03-2013-0019/FULL/XML.

Hassan, L.M., Shiu, E., & Parry, S. (2016). Addressing the cross-country applicability of the theory of planned behavior (TPB): A structured review of multi-country TPB studies. *Journal of Consumer Behavior* , *15* (1), 72-86.

Hasan, S., Ali, M., Kurnia, S. and Thurasamy, R. (2021), "Evaluating the cyber security readiness of organizations and its influence on performance", *Journal of Information Security and Applications,* Vol. 58, pp. 1-16, doi: 10.1016/j.jisa.2020.102726.

He, W. (2012), "A review of social media security risks and mitigation techniques", *Journal of Systems and Information Technology* , Vol. 14 No. 2, pp. 171–180, doi: 10.1108/13287261211232180.

He, W. (2013), "A survey of security risks of mobile social media through blog mining and an extensive literature search", *Information Management & Computer Security* , Vol. 21 No. 5, pp. 381–400, doi: 10.1108/IMCS-12-2012-0068.

Henseler, J., Ringle, C.M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43* (1), 115-135. https://doi.org/10.1007/s11747-014-0403-8

Henseler, J., Ringle, C.M., & Sarstedt, M. (2016). Testing measurement invariance of composites using partial least squares. *International marketing review* , *33* (3), 405-431.

Herath, T., & Rao, H.R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of Information Systems, 18* (2), 106125. https://doi.org/10.1057/ejis.2009.6 1.

Hermann, E., Eisend, M. and Bayón, T. (2020), "Facebook and the cultivation of ethnic diversity perceptions and attitudes", *Internet Research* , Vol. 30 No. 4, pp. 1123–1141, doi: 10.1108/INTR-10-2019-0423/FULL/XML.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security: a neo-institutional perspective. *The Journal of Strategic Information Systems, 16(2),* 153-172. https://doi.org/10.1016/jjsis.2007.05.004 .

Hina, S., Panneer Selvam, DDD and Lowry, PB (2019), "Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world", *Computers & Security* , Vol. 87, p. 101594, doi: 10.1016/j.cose.2019.101594.

Hina, S. and Dominic, PDD (2020), "Information security policies' compliance: a perspective for higher education institutions", *Journal of Computer Information Systems,* Online First, doi: 10.1080/08874417.2018.1432996.

Hooper, V. and Blunt, C. (2020), "Factors influencing the information security behavior of IT employees", *Behavior and Information Technology* , Vol. 39 No. 8, pp. 862–874, doi: 10.1080/0144929X.2019.1623322.

Hooper, V., & Blunt, C. (2019). *Factors affecting the information security behavior of IT employees. Behavior & Information Technology, 1–13.* doi:10.1080/0144929x.2019.1623322

Ifinedo, P. (2012), "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory", *Computers & Security* , Vol. 31 No. 1, pp. 83–95, doi: 10.1016/j.cose.2011.10.007.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51* (1), 69-79. https://doi.org/10.1016/j.im.2013.10.001

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems, 61* (4), 345-356. https://doi.org/10.1080/08874417.2019.1650676

Intravia, J., Wolff, KT, Paez, R. and Gibbs, BR (2017), "Investigating the relationship between social media consumption and fear of crime: A partial analysis of mostly young adults", *Computers in Human Behavior* , Vol. 77, pp. 158–168, doi: 10.1016/J.CHB.2017.08.047.

Islm, T., Meng, H., Pitafi, A.H., Ullah Zafar, A., Sheikh, Z., Shujaat Mubarik, M. and Liang, X. (2021), "Why DO citizens engage in government social media accounts during COVID-19 pandemic? A comparative study", *Telematics and Informatics,* Vol. 62, p. 101619, doi: 10.1016/j.tele.2021.101619.

Jain, N. and Raman, TV (2023), "The interaction of perceived risk, perceived benefit and generation adoption cohort in digital finance", *EuroMed Journal of Business,* Vol. 18 No. 3, pp. 359-379, doi: 10.1108/EMJB-09-2021-0132.

Janmaimool, P. (2017). Application of protection motivation theory to investigate sustainable waste management behaviors. *Sustainability, 9(7),* 1079. https://doi.org/10.3390/issue9071079 .

Johnson, RD and Marakas, GM (2000), "The role of behavioral modeling in computer skills acquisition: Toward refinement of the model", *Information Systems Research* , INFORMS, Vol. 11 No. 4, pp. 402–417, doi: 10.1287/ISRE.11.4.402.11869.

Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: An empirical study", *MIS Quarterly: Management Information Systems* , Vol. 34 No. 3, pp. 549–566, doi: 10.2307/25750691.

Johnston, A.C., Warkentin, M., Dennis, A.R. and Siponen, M. (2019), "Speak their language: Designing effective messages to improve employees' information security decision making", *Decision Sciences* , Vol. 50 No. 2, pp. 245–284, doi: 10.1111/DECI.12328.

Kannan, VR and Tan, KC (2005), “Just in time, total quality management, and supply chain management: understanding their linkages and impact on business performance”, *Omega* , Vol. 33 No. 2, pp. 153–162, doi: https://doi.org/10.1016/j.omega.2004.03.012 .

Kim, J., Yang, K., Min, J., & White, B. (2022). Hope, fear, and consumer behavior change amid COVID-19: Application of protection motivation theory. *International Journal of Consumer Studies, 46* (2), 558-574. https://doi.org/10.1111/ijcs.12700^^^^

Kim, SC and Hawkins, KH (2020), “The psychology of social media communication in investigation prevention intentions during the 2019 US measles outbreak”, *Computers in Human Behavior* , Vol. 111, p. 106428, doi: 10.1016/J.CHB.2020.106428.

Kock, N. (2015), “Common method bias in PLS-SEM: A full collinearity assessment approach”, *International Journal of E-Collaboration,* Vol. 11 No. 4, pp. 1-10, doi: 10.4018/ijec.2015100101.

Klein, G. and Zwilling, M. (2023), “The Weakest Link: Employee Cyber-Defense Behaviors While Working from Home”, *Journal of Computer Information Systems* , pp. 1-15, doi: 10.1080/08874417.2023.2221200. https://www.tandfonline.com/doi/pdf/10.1080/08874417.2023.2221200

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and H. Breitner, M. (2014), “Information security awareness and behavior: a theory-based literature review”, *Management Research Review* , Vol . 37 No. 12, pp. 1049–1092, doi: 10.1108/MRR-04-2013-0085.

Lee, MJ and Cho, H. (2018), “Uses of social media in government agencies: Content analyzes of public relations strategies and message tactics comparison between South Korea and the United States of America in 2011 and 2014”, *Journal of Public Affairs* , Vol. 18 No. 2, p. e1687, doi: 10.1002/PA.1687.

Lee, C.S., & Kim, D. (2023). Pathways to cybersecurity awareness and protection behaviors in South Korea. *Journal of Computer Information Systems, 63* (1), 94-106. https://doi.org/10.1080/08874417.2022.2031347

Lee, J., & Lee, Y. (2002). A comprehensive model of computer abuse within organizations. *Information Management & Computer Security, 10(2),* 57-63. https://doi.org/10.1108/09685220210424104

Lee, K.G., Chong, C.W., & Ramayah, T. (2017). Website characteristics and web users' satisfaction in a higher learning institution. *International Journal of Management in Education, 11(3),* 266. https://doi.org/10.1504/IJMIE.2017.084926

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems, 50* (2), 361-369. https://doi.org/10.1016/j.dss.2010.07.009

Lee, SM, Lee, SG and Yoo, S. (2004), “An integrative model of computer abuse based on social control and general deterrence theories”, *Information and Management* , Vol. 41 No. 6, pp. 707-718, dot: 10.1016/j.im.2003.08.008.

Lee, Y. and Larsen, K.R. (2009), “Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software”, *European Journal of Information Systems,* Vol. 18 No. 2, pp. 177-187, doi: 10.1057/ejis.2009.11. *S')*

Li, L., Xu, L., He, W., Chen, Y., & Chen, H. (2016). *Cyber Security Awareness and Its Impact on Employee's Behavior.* https://doi.org/10.1007/978-3-319-49944-4_8

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019), “Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior”, *International*

Journal of Information Management , Vol. 45, pp. 13–24, doi: 10.1016/j.ijinfomgt.2018.10.017.

Li, Y., Chandra, Y. and Fan, Y. (2022), "Unpacking government social media messaging strategies during the COVID-19 pandemic in China", *Policy & Internet* , Vol. 14 No. 3, pp. 651–672, https://doi.org/10.1002/poi3.282 .

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports* , *5* , 100165. https://doi.org/10.1016/j.chbr.2021.100165 . https://www.sciencedirect.com/science/article/pii/S2451958821001135/pdfft?md5=2341e9955bc7a16f6adefe1d004fb402&pid=1-s2.0-S2451958821001135-main.pdf

Liao, C., Chen, J.-L., & Yen, D.C. (2007). Theory of planning behavior (TPB) and customer satisfaction in the continued use of e-service: An integrated model. *Computers in Human Behavior, 23* (6), 2804-2822. https://doi.org/10.1016/j.chb.2006.05.006

Liang, H. and Xue, Y. (2010), "Understanding security behaviors in personal computer usage: A threat avoidance perspective", *Journal of the Association for Information Systems* , Vol. 11 No. 7, p. 1, doi: 10.17705/1jais.00232.

Lu, Y. and Xu, L. Da. (2019), "Internet of things (IoT) cybersecurity research: A review of current research topics", *IEEE Internet of Things Journal,* Vol. 6 No. 2, pp. 2103-2115, doi: 10.1109/JIOT.2018.2869847.

Ma, X. (2022), "IS professionals' information security behaviors in Chinese IT organizations for information security protection", *Information Processing and Management* , Vol. 59 No. 1, p. 102744, doi: 10.1016/j.ipm.2021.102744. https://e-tarjome.com/storage/panel/fileuploads/2021-10-03/1633241034_E15626.pdf

Makridis, C., & Dean, B. (2018). Measuring the economic effects of data compiled on firm outcomes: Challenges and opportunities. *Journal of Economic & Social Measurement* , *43* .

Maglaras, L., Ferrag, M.A., Derhab, A., Mukherjee, M., & Janicke, H. (2019). Cyber security: From regulations and policies to practice. In *Strategic Innovative Marketing and Tourism: 7th ICSIMAT, Athenian Riviera, Greece, 2018* (pp. 763-770). Springer International Publishing. https://doi.org/10.1007/978-3-030-12453-3_88 .

Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity, 3* (1), 10. https://doi.org/10.1186/s42400-020-00050-w

Maddux, JE and Rogers, RW (1983), "Protection motivation and self-efficacy: A revised theory of fear attractions and attitude change", *Journal of Experimental Social Psychology* , Vol. 19 No. 5, pp. 469–479, doi: 10.1016/0022-1031(83)90023-9.

Martens, M., De Wolf, R. and De Marez, L. (2019), "Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general", *Computers in Human Behavior* , Vol. 92, pp. 139–150, doi: 10.1016/J.CHB.2018.11.002.

Mahon, D., Cowan, C., & McCarthy, M. (2006). The role of attitudes, subjective norm, perceived control and habit in the consumption of ready meals and takeaways in Great Britain. *Food Quality and Preference, 17(6),* 474-481. https://doi.org/10.1016/j.foodqual.2005.06.001

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce, 9* (1), 23-41. https://doi.org/10.1080/15332861.2010.487415 X

Menard, P., Bott, G.J., & Crossler, R.E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems, 34(4),* 1203-1230. https://doi.org/10.1080/07421222.2017.1394083

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security, 9* (1), 47-67. https://doi.org/10.1080/15536548.2013.10845672

Michael, K., Kobran, S., Abbas, R., & Hamdoun, S. (2019). Privacy, data rights and cybersecurity: Technology for good in the achievement of sustainable development goals. *2019 IEEE International Symposium on Technology and Society (ISTAS),* 1-13. https://doi.org/10.1109/ISTAS48451.2019.8937956

Moletsane, T., & Tsibolane, P. (2020). Mobile information security awareness among students in higher education: An exploratory study. *2020 Conference on Information Communications Technology and Society (ICTAS),* 1-6. https://doi.org/10.1109/ICTAS47918.2020.233978

Medaglia, R. and Zhu, D. (2017), "Public disturbance on government-managed social media: A study on Weibo users in China", *Government Information Quarterly* , Vol. 34 No. 3, pp. 533–544, doi: 10.1016/j.giq.2017.05.003.

Moody, G.D., Siponen, M. and Pahnila, S. (2018), "Toward a unified model of information security policy compliance", *MIS Quarterly* , Vol. 42 No. 1, pp. 285–311, doi: https://doi.org/10.25300/MISQ/2018/13853 . https://jyx.jyu.fi/bitstream/handle/123456789/60225/1/moodyetaltowardaunified.pdf

Nair, J., Chellasamy, A. and Singh, BNB (2019), "Readiness factors for information technology adoption in SMEs: testing an exploratory model in an Indian context", *Journal of Asia Business Studies* , Vol. 13 No. 4, pp. 694–718, doi: 10.1108/JABS-09-2018-0254.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46* (4), 815-825. https://doi.org/10.1016/j.dss.2008.11.010

Ng, B.-Y., & Xu, Y. (2007). Studying users' computer security behavior using the health belief model. *PACIS 2007Proceedings,* 423-437.

Nguyen, TTU, Nguyen, P. Van, Huynh, HTN, Vrontis, D. and Ahmed, ZU (2023), "Identification of the determinants of public trust in e-government services and participation in social media based on good governance theory and the technological acceptance model", *Journal of Asia Business Studies* , Vol. ahead-of-print No. ahead-of-print, doi: 10.1108/JABS-04-2023-0160.

C.X. , Zhang , . 65, pp. 1-17, doi: 10.1016/j.ijinfomgt.2022.102498. https://durham-repository.worktribe.com/preview/1213246/35497.pdf

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42,* 165-176. https://doi.org/10.1016/j.cose.2013.12.003 .

Pérez-Morón, J. (2022), “Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, a review and future research agenda”, *Journal of Asia Business Studies* , Vol. 16 No. 2, pp. 371–395, doi: 10.1108/JABS-11-2020-0444.

Peréz-Morón, J., & Cantillo-Orozco, A.S. (2022). The applications of Industry 4.0 (I4. 0) technologies in the palm oil industry in Colombia (Latin America). *The Digital Agricultural Revolution: Innovations and Challenges in Agriculture through Technology Disruptions* , 109-142.

Posey, C., Roberts, TL and Lowry, PB (2015), “The impact of organizational commitment on insiders motivation to protect organizational information assets”, *Journal of Management Information Systems* , Vol. 32 No. 4, pp. 179–214, doi: 10.1080/07421222.2015.1138374.

Pham, H.C., Brennan, L., Parker, L., Phan-Le, NT, Ulhaq, I., Nkhoma, M.Z., & Nhat Nguyen, M. (2019). *Enhancing cyber security behavior: an internal social marketing approach. Information & Computer Security, 28(2), 133–159.* doi:10.1108/ics-01-2019-0023.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly* , 757-778.

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security* , *80* , 211-223.

Rippetoe, PA, & Rogers, RW (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology, 52* (3), 596-604. https://doi.org/10.1037/0022-3514.52.3.596

Romero Moreno, F., Harbinja, E., Leiser, M., Barker, K., & Couzigou, I. (2020). BILETA Response to EC Consultation on the Digital Services Act Package.

Ronald J. Deibert; Rafal Rohozinski. (2010). *Risking Security: Policies and Paradoxes of Cyberspace Security. , 4(1), 15–32.* doi:10.1111/j.1749-5687.2009.00088.x

Rogers, R.W. (1975). A protective motivational theory of fear appeals and attitude change. *Journal of Psychology, 91* (1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioral and organizational measures. *Information Security Technical Report, 15(3),* 112-133. https://doi.org/10.1016/j.istr.2010.11.002

Saadatdoost, R., Sim, ATH, Jafarkarimi, H., & Mei Hee, J. (2015). Exploring MOOC from education and Information Systems perspectives: a short literature review. *Educational Review, 67* (4), 505-518. https://doi.org/10.1080/00131911.2015.1058748

Sarkar, K.R. (2010). Assessing insider threats to information security using technical, behavioral and organizational measures. *information security technical report* , *15* (3), 112-133.

Salunke, S., Weerawardena, J., & McColl-Kennedy, J.R. (2019). The central role of knowledge integration capability in service innovation-based competitive strategy. *Industrial Marketing Management* , *76* , 144-156.

Safa, S. N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56,* 70-82. https://doi.org/10.1016/j.cose.2015.10.006

Safa, NS, Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015), "Information security conscious care behavior formation in organizations", *Computers and Security* , Vol. 53, pp. 65–78, doi: 10.1016/j.cose.2015.05.012.

Sexton, M. (2016). UK cybersecurity strategy and active cyber defense–issues and risks. *Journal of Cyber Policy* , *1* (2), 222-242.

Siponen, M., Mahmood, M.A., & Pahnila, S. (2009). Technical opinion: Are employees putting your company at risk by not following information security policies? *Communications of the ACM, 52* (12), 145-147. https://doi.org/10.1145/1610252.1610289

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables affecting information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security* , *22* (1), 42-75.

Sommestad, T., Karlzen, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security, 23(2),* 200-217. https://doi.org/10.1108/ICS-04-2014-0025

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information management & computer security* , *8* (1), 31-41.

Siponen, M., Adam Mahmood, M. and Pahnila, S. (2014), "Employees' adherence to information security policies: An exploratory field study", *Information and Management* , Vol. 51 No. 2, pp. 217–224, doi: 10.1016/j.im.2013.08.006.

Siponen, M. and Vance, A. (2010), "Neutralization: New insights into the problem of employee information systems security policy violations", *MIS Quarterly: Management Information Systems* , Vol. 34 No. 3, pp. 487–502, doi: 10.2307/25750688.

Shaw, RS, Chen, CC, Harris, AL, & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education* , *52* (1), 92-100. https://doi.org/10.1016/j.compedu.2008.06.011

Shah, Z., Chu, J., Ghani, U., Qaisar, S. and Hassan, Z. (2020), "Media and altruistic behaviors: The mediating role of fear of victimization in cultivating theory perspective", *International Journal of Disaster Risk Reduction* , Vol. 42, p. 101336, doi: 10.1016/J.IJDRR.2019.101336.

Sharma, S., Singh, G., Sharma, R., Jones, P., Kraus, S. and Dwivedi, YK (2020), "Digital health innovation: Exploring adoption of COVID-19 digital contact tracing apps", *IEEE Transactions on Engineering Management* , Online first, doi: 10.1109/TEM.2020.3019033.

Shmueli, G., Ray, S., Estrada, J.M.V., & Chatla, S.B. (2016). The elephant in the room: Predictive performance of PLS models. *Journal of business research* , *69* (10), 4552-4564.

Shmueli, G., Sarstedt, M., Hair, J.F., Cheah, J.H., Ting, H., Vaithilingam, S., & Ringle, C.M. (2019). Predictive model assessment in PLS-SEM: guidelines for using PLSpredict. *European journal of marketing* , *53* (11), 2322-2347.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1(3),* 255-276. https://doi.org/10.1287/isre.1.3.255 .

Swaim, JA, Maloni, MJ, Napshin, SA, & Henley, AB (2014). Influences on student intention and behavior toward environmental sustainability. *Journal of Business Ethics, 124(3),* 465-484. https://doi.org/10.1007/s10551-013-1883-z

Tanczer, L., Brass, I., Elsden, M., Carr, M., & Blackstock, J.J. (2019). The United Kingdom's emerging internet of things (IoT) policy landscape. *Rewired: Cybersecurity Governance* , 37-56.

Tang, Z., Miller, A.S., Zhou, Z. and Warkentin, M. (2021), "Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations", *Government Information Quarterly* , Vol. 38 No. 2, p. 101572, doi: 10.1016/j.giq.2021.101572.

Teo, T., & Beng Lee, C. (2010). Explaining the intention to use technology among student teachers. *Campus-Wide Information Systems, 27* (2), 60-67. https://doi.org/10.1108/10650741011033035

Tu, Z., Turel, O., Yuan, Y. and Archer, N. (2015), "Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination", *Information & Management* , Vol. 52 No. 4, pp. 506–517, doi: 10.1016/J.IM.2015.03.002.

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *computers & security , 70 ,* 376-391.

Tran, D. Van, Nguyen, P. Van, Nguyen, ATC, Vrontis, D., & Dinh, PU (2024). Exploring the influence of government social media on cybersecurity compliance: employee attitudes, motivation and behaviors. *Journal of Asia Business Studies, 18* (1), 204-223. https://doi.org/10.1108/JABS-09-2023-0343

Tsai, H.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., & Cotten, S.R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59,* 138-150. https://doi.org/10.1016/j.cose.2016.02.009

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New media & society , 20* (1), 141-161.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security , 52* , 128-141. https://doi.org/10.1016/j.cose.2015.04.006

Van Bavel, R., Rodriguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies, 123,* 29-39. *https://doi.org/10.1016/j.ijhcs.2018.11.003*

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management , 49* (3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002

Venkatesh, Morris, Davis, & Davis. (2003). User acceptance of information technology: Toward ^a unified view. *MIS Quarterly, 27(3),* 425-478. https://doi.org/10.2307/30036540

Verkijika, S.F., & De Wet, L. (2018). E-government adoption in sub-Saharan Africa. *Electronic Commerce Research and Applications , 30* , 83-93.

Vrhovec, S. and Mihelic, A. (2021), “Redefining threat evaluations of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation”, *Computers and Security,* Vol. 106, pp. 1-22, doi: 10.1016/j.cose.2021.102309.

Vrontis, D., Makrides, A., Christofi, M. and Thrassou, A. (2021), “Social media influencer marketing: A systematic review, integrative framework and future research agenda”, *International Journal of Consumer Studies* , Vol. 45 No. 4, pp. 617-644, doi: 10.1111/ijcs.12647.

Wall, J.D. and Warkentin, M. (2019), “Perceived argument quality's effect on threat and coping evaluations in fear appeals: An experiment and exploration of realism check heuristics”, *Information & Management* , Vol. 56 No. 8, p. 103157, doi: 10.1016/J.IM.2019.03.002.

Warkentin, M., Johnston, A.C. and Shropshire, J. (2011), “The influence of the informal social learning environment on information privacy policy compliance effectiveness and intention”, *European Journal of Information Systems* , Vol. 20 No. 3, pp. 267–284, doi: 10.1057/EJIS.2010.72.

Warkentin, M., Johnston, A.C., Shropshire, J. and Barnett, W.D. (2016), “Continuance of protective security behavior: A longitudinal study”, *Decision Support Systems* , Vol. 92, pp. 25–35, doi: 10.1016/J.DSS.2016.09.013.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs* , *59* (4), 329-349.

Witte, K. (1996). Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. In *Handbook of communication and emotion* (pp. 423-450). Academic Press.

Witte, K., Cameron, K.A., McKeon, J.K. and Berkowitz, J.M. (2010), “Predicting risk behaviors: Development and validation of a diagnostic scale”, *Journal of Health Communication* , Vol. 1 No. 4, pp. 317–341, doi: 10.1080/108107396127988.

Wong, LW, Lee, VH, Tan, GWH, Ooi, KB and Sohal, A. (2022), “The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities”, *International Journal of Information Management* , Vol. 66, p. 102520, doi: 10.1016/j.ijinfomgt.2022.102520.

Wu, D. (2020), “Empirical study of knowledge withholding in cyberspace: Integrating protective motivation theory and theory of reasoned behavior”, *Computers in Human Behavior* , Vol. 105, p. 106229, doi: 10.1016/J.CHB.2019.106229.

Wu, X., & Kuang, W. (2021). Exploring influence factors of WeChat users' health information sharing behavior: Based on an integrated model of TPB, UGT and SCT. *International Journal of Human-Computer Interaction, 37* (13), 1243-1255.> ^ https://doi.org/10.1080/10447318.2021.1876358

Whitman, M.E. (2003). Enemy at the gate. *Communications of the ACM, 46* (8), 91-95. https://doi.org/10.1145/859670.859675

Wiafe, I., Koranteng, F.N., Wiafe, A., Obeng, E.N., & Yaokumah, W. (2020). The role of norms in information security policy compliance. *Information & Computer Security, 28* (5), 743-761. https://doi.org/10.1108/ICS-08-2019-0095

Williams, PAH (2008). In a 'trusting' environment, everyone is responsible for information security. *Information Security Technical Report, 13* (4), 207-215. https://doi.org/10.1016/j.istr.2008.10.009

Workman, M. (2009). A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions. *Information and Organization, 19* (4), 218-232. https://doi.org/10.1016/j.infoandorg.2009.06.001 1

Yousuf, H., Al-Emran, M., & Shaalan, K. (2023). Evaluating individuals' cybersecurity behavior in mobile payment contactless technologies: Extending TPB with cybersecurity awareness. *International Conference on Human-Computer Interaction,* 542-554. https://doi.org/10.1007/978-3-031-35822-7_35

Yin, F., Xia, X., Pan, Y., She, Y., Feng, X. and Wu, J. (2022), "Sentiment mutation and negative emotion contagion dynamics in social media: A case study on the Chinese Sina Microblog", *Information Sciences,* Vol. 594, pp. 118–135, doi: 10.1016/J.INS.2022.02.029.

Zhang, J., Reithel, B.J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17* (4), 330-340. https://doi.org/10.1108/09685220910993980

Zhang, XJ, Li, Z. and Deng, H. (2017), "Information security behaviors of smartphone users in China: An empirical analysis", *Electronic Library* , Vol. 35 No. 6, pp. 1177–1190, doi: 10.1108/EL-09-2016-0183/FULL/XML.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H.N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62(1),* 82-97. https://doi.org/10.1080/08874417.2020.1712269