Literature Review Outline

1. **Introduction**
    a. A systematic review was conducted to identify studies on cybersecurity, cyber risk management behavior, cyberinsurance, and theoretical studies on Protection Motivation Theory and the theory of planned behavior.
        i. The database was used to search the terms including: *cybersecurity, cybersecurity risk, online privacy, cyberinsurance, Protection Motivation Theory, theory of planned behavior, cybersecurity and age, cybersecurity and gender, cybersecurity and ethnicity, digital divide, online risk, social media, information sharing, cybersecurity practices, cybersecurity perceptions*, and *mobile security.*
        ii. Publications were restricted to peer-reviewed journals and only recent publications (since year 2011) were used except for a minority of earlier seminal publications.
        iii. Reference lists in publications were also used to screen for acceptable studies.
        iv. There is a potential for selection bias as the search was limited to published, peer-reviewed studies written in English. However, due to the nature of the study, sources applicable to Internet-use in the United States were of interest.
    b. Inadequate cyber safety measures significantly impact the security of privacy and economic stability individuals (Choi, Levy, & Hovav, 2013; Onarlioglu, Yilmaz, Kirda, & Balzarotti, 2012; Othmane et al., 2013; Pfleeger & Caputo, 2012).
        i. Human error accounts for 50% to 75% of data breaches.
        ii. $20 billion in economic losses are a result of cybersecurity breaches (Choi, Levy, & Hovay, 2013; Lagrule, 2015).
        iii. Factors such as age, gender, and ethnicity have not adequately been examined in contexts of technology use, accessibility, and safety practices (Chakraborty, Vishik, & Rao, 2013; Maaß, 2011; Sánchez, Kaplan, & Bradley, 2015; Kisekka, Bagchi-Sen, & Rao, 2013; Sofo & Sofo, 2014; Thelwall, 2011; Whitty, Doodson, Creese, & Hodges, 2015).
        iv. The proposed study will examine cybersecurity practices and perceptions using Protection Motivation Theory and the theory of planned behavior (Crossler & Bélanger, 2014; Saeri et al., 2014; Salleh et al., 2012).
    c. Transition to next section.
        i. Research has shown that cybersecurity risks are not always adequately addressed or realized (Claar & Johnson, 2012; Hettema et al., 2014).
2. **Cybersecurity Risks**
    a. Cybersecurity risks threaten micro-level stability such as individual financial stability and unethical use of personal information as well as

macro-level stability including organizational and governmental stability and functionality (Choi, Levy, & Hovav, 2013; Levy, Ramim, & Hackney, 2013; Onarlioglu, Yilmaz, Kirda, & Balzarotti, 2012; Othmane et al., 2013; Pfleeger & Caputo, 2012).

b. Human error and misuse is a substantial factor in cybersecurity breaches (Choi, Levy, & Hovay, 2013; Lagrule, 2015).
    i. There is a gap in consistent data on the impact of human behaviors and perceptions on safe security practices (Choi, Levy, & Hovay, 2013; Crossler & Bélanger, 2014; Onarlioglu et al., 2012; Othmane et al., 2013; Pfleeger & Caputo, 2012; Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014; Salleh et al., 2012).
    ii. There is also a need to examine perceptions that keep individuals from adopting safe security practices (Claar & Johnson, 2012; Crossler & Bélanger, 2014).

c. Transition to next section.
    i. Protection Motivation Theory is a framework often used to analyze behavioral factors that affect security adoption behaviors.

3. Protection Motivation Theory

a. Protection Motivation Theory is used to understand fear and risk motivation (Crossler & Bélanger, 2014; Salleh et al., 2012).
    i. Crossler and Bélanger (2014) found that the literature is not consistent on the effect of perceived severity and vulnerability with safe security practices.
    ii. Salleh et al. (2012), found that cybersecurity behaviors were mediated by all of the tenets of PMT.

b. Perceived vulnerabilities, perceived severity, previous incidents, and response efficacy affect the adoption of safe security practices (Anwar et al., 2015; Choo et al., 2015; Crossler & Bélanger, 2014; Salleh et al., 2012).
    i. Skill is not as much of a factor as perceptions and beliefs in the adoption of safe security practices (Anwar et al., 2015; Choo et al., 2015; Crossler & Bélanger, 2014; Salleh et al., 2012).
    ii. More research is needed to separate insider deviant behavior and misbehavior, understand hackers, and improve security compliance (Crossler et al., 2013).

c. Some research suggests perception of responsibility and personal and work boundaries also affect the adoption of safe security practices (Ifinedo, 2012; McBride, Carter, & Warkentin, 2012; Safa et al., 2015; Warkentin, Malimage, & Malimage, 2012).
    i. Individuals that do not feel continuity in organizational cybersecurity policies and their role in the organization are less likely to consistently adopt and use safe security practices (Ifinedo, 2012; McBride, Carter, & Warkentin, 2012; Safa et al., 2015; Warkentin, Malimage, & Malimage, 2012).

d. Cultural differences in risk perceptions affect security habits (Bada, Sasse, & Nurse, 2014; Crossler et al., 2013; Whitty et al., 2015).

e. Threat appraisals may be more successful in promoting safe security practices than coping appeals (Boss et al., 2015; Lee, 2011).
f. Transition to next section.
    i. The theory of planned behavior is also used to examine cybersecurity behavior by linking beliefs to behaviors.

4. Theory of Planned Behavior

a. The theory of planned behavior posits that subjective norms mediate behavior intentions (Ajzen, 1991; Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014).
b. Tenets of the theory of planned behavior, including security experience and involvement, attitude, subjective norms, threat appraisal, and self-efficacy, positively affect user behavior (Claar & Johnson, 2012; Ifinedo, 2012; Safa et al., 2015; Sommestad & Hallberg, 2013).
    i. Online behaviors, attitudes, and normative beliefs are mediated through intentions (Burns & Roberts, 2013).
    ii. Perceived behavioral control affects security behaviors (Burns & Roberts).
    iii. Technical knowledge, organizational impact, and attacker assessment are correlated with cybersecurity awareness (Mejias, 2012).
c. Cultural differences affect sharing behavior (Hassandoust, Kazerouni, & Perumal, 2012).
d. Security incidents affect safe security practice adoption (Lee & Lee, 2012).
e. Transition to next section.
    i. Online habits, social media practices, and information disclosure results in a privacy paradox between social interaction and cybersecurity practices (Lewis, 2011; Taddicken & Jers, 2011; Trepte & Reineke, 2011; Ziegele & Quiring, 2011).

5. Information Disclosure and Privacy

a. Cybersecurity misconceptions, smart device use, lack of awareness, and information disclosure behavior affect security risks (Geneiatakis, Kounelis, Loeschner, Fovino, & Stirparo, 2013; Henshel, Cains, Hoffman, & Kelley, 2015; Manson & Pike, 2014; McClain et al., 2015; Onarlioglu et al., 2012, Othmane et al., 2013; Pfleeger & Caputo, 2012; Salem & Stolfo, 2011; Wang, 2013).
b. Social capital theory has been used to explain information sharing behavior.
    i. Lack of sharing leads to reduced user experience and may be seen as anti-normative in some contexts (Ellison, Vitak, Steinfield, Gray, & Lampe, 2011; Joinson, Houghton, Vasalou, & Marder, 2011; Papacharissi & Gibson, 2011).
    ii. Privacy can be seen as a way to control personal information or to control outside perceptions (Debatin, 2011; Yao, 2011).
    iii. Privacy is dynamic and defined by users (Hartmann, 2011).

c. Social networking provides avenues for self-presentation and new avenues for presenting the self (Krämer & Haferkamp, 2011; Papacharissi & Gibson, 2011).
    i. Social networking and the ability to present the self may conflict with privacy maintenance (Krämer & Haferkamp, 2011).
d. Transition to next section.
    i. Cybersecurity practices are affected by access, technological exposure, and perceptions mediated by age, ethnicity, and sex.

6. Cybersecurity Practices and the Digital Divide

a. Research has shown older individuals and women are greatly impacted by cybersecurity threats (Sánchez, Kaplan, & Bradley, 2015).
b. Social media use in older individuals has doubled from 2009 to 2010 (Maaß, 2011).
    i. Email and internet searches are the most commonly used Internet functions in older individuals (Maaß, 2011).
c. Individuals over the age of 55 are more vulnerable to cybersecurity threats (Sánchez, Kaplan, & Bradley, 2015).
d. Older individuals are more likely to disclose private information online (Chakraborty, Vishik, & Rao, 2013; Kisekka, Bagchi-Sen, & Rao, 2013).
    i. Older adults are influenced by friends on social media and may feel more comfortable with sharing information when they observe their friends sharing information (Chakraborty, Vishik, & Rao, 2013).
e. Older individuals also face barriers, such as medical issues, to acquiring technological skill (Sofo & Sofo, 2014).
f. Specific cybersecurity concerns, such as cyberbullying and stalking, affect women more frequently (Thelwall, 2011).
    i. Some women are more likely to use Internet websites due to the perceived safety of communicating online verses in person (where the threat of physical violence is a possibility) (Thelwall, 2011).
g. Transition to next section.
    i. Cybersecurity measures can be taken to aid in providing technological security.

7. Cyberinsurance

a. Cyberinsurance and safety measures, including decoy information fogging, can provide individuals and network providers with solutions to dealing with cybersecurity threats (Bowen, Devarajan, & Stolfo, 2011; Pal & Hui, 2012; Pal, Golubchik, Psounis, & Hui, 2014; Silva et al., 2014; Stolfo, Salem, & Keromytis, 2012; Toregas, C., & Zahn, 2014; Zang and Lui, 2014).
b. Risk estimation can be calculated using connection network information, user behavior, health insurance models, and prediction markets (Bandyopadhyay, 2012; Barracchini & Addessi, 2014; Bonner, 2012; Garrie & Mann, 2014; Herath & Herath, 2011; Lazka, 2014; Pal & Hui, 2012; Pal et al., 2014; Pandey & Snekkenes, 2014; Stolfo, Salem, & Keromytis, 2012; Toregas, C., & Zahn, 2014; Zang and Lui, 2014).

i. Some research, however, suggests that cyberinsurance is impractical because security is interdependent on an individual's own security and network security (Schwartz, Shetty, & Walrand, 2013).
ii. Biener, Eling, & Wirfs (2015) argue that because cyber systems are designed in similar ways, they are vulnerable to the same risks; therefore, cyberinsurance can be designed based on risk estimation.

c. Transition to next section.
i. Several methodological issues in the literature on cybersecurity must be addressed.

8. Summary

a. Self-reporting may be a limiting factor in the quantitative studies that assessed cybersecurity behaviors.
b. There is a lack in consistency in qualitative studies on cybersecurity behaviors (Boss et al., 2015; Choi, Levy, & Hovay, 2013; Crossler & Bélanger, 2014; Onarlioglu et al., 2012; Othmane et al., 2013; Pfleeger & Caputo, 2012; Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014; Salleh et al., 2012).
c. Cyberinsurance has been theoretically examined, but user perceptions on cyberinsurance have not been addressed (Bandyopadhyay, 2012; Barracchini & Addessi, 2014; Lazka, 2014; Pal & Hui, 2012; Pal et al., 2014; Pandey & Snekkenes, 2014; Stolfo, Salem, & Keromytis, 2012; Toregas, C., & Zahn, 2014; Zang and Lui, 2014).

9. Conclusion

a. In order to improve cybersecurity awareness and safe security practice adoption, research needs to analyze decision-making processes, attitudes and beliefs, subjective norms, and perceived behavioral control factors that mediate cybersecurity behaviors.
b. Future research should focus on analyzing the effect size, the homogeneity of samples, digital divide effects, cyberinsurance perceptions, sensitivity analyses, robustness of results, the accuracy of self-reported and questionnaire data, and the ability of Protection Motivation Theory and the theory of planned behavior to accurately describe cybersecurity practices.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Anwar, M., Ash, I., He, W., Li, L., Xu, L., & Yuan, X. (2015). A security behavior model of employees in cyberspace. *Information Systems Security, Assurance, and Privacy.*

Bada, M., Sasse, A., & Nurse, J. R. (2014). Cyber security awareness campaigns: Why do they fail to change behaviour? *Global Cyber Security Capacity Centre*, 1-38.

Bandyopadhyay, T. (2012). Organizational adoption of cyber insurance instruments in IT security risk management–A modeling approach. *Organizational Adoption of Cyber Insurance Instruments in IT Security Risk Management*, 23-29.

Barracchini, C., & Addessi, M. E. (2014). Cyber risk and insurance coverage: An actuarial multistate approach. *Review of Economics & Finance*, *4*(1), 57-69.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*(1), 131-158.

Bonner, L. (2012). Cyber risk: How the 2011 Sony data breach and the need for cyber risk insurance policies should direct the federal response to rising data breaches. *Washington University Journal of Law and Policy*, *40*, 257-277.

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 motivate protective security behaviors. *MIS Quarterly*, 1-70.

Bowen, B. M., Devarajan, R., & Stolfo, S. (2011). International Conference on Technologies for Homeland Security (HST): *Measuring the human factor of cyber security*.

Burns, S., & Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, *15*(1), 48-64.

Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems*, *55*(4), 948-956.

Choi, M., Levy, Y., & Hovav, A. (2013). Proceedings of the pre-ICIS workshop on information security and privacy (WISP 2013): *The Role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse.* Milan, Italy.

Choo, K. K. R., Heravi, A., Mani, D., & Mubarak, S. (2015). Employees' intended information security behaviour in real estate organisations: A protection motivation perspective. *Information Security Behaviour in Real Estate Organizations*, 1-11.

Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal of Computer Information Systems*, *52*(4), 20-29.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, *32*, 90-101.

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection Motivation Theory and a unified security practices (USP) instrument. *ACM SIGMIS Database*, *45*(4), 51-71.

Cuhls, K. (2015). Delphi method [PDF]. Retrieved from http://www.unido.org/fileadmin/import/16959_DelphiMethod.pdf

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. *Privacy Online*, 47-60.

Ellison, N.B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. *Privacy Online*, 19-32.

Garrie, D., & Mann, M. (2014). Cyber-security insurance: Navigating the landscape of a growing field. *John Marshall Journal of Information Technology and Privacy Law*, *31*(3), 379-392.

Geneiatakis, D., Kounelis, I., Loeschner, J., Fovino, I. N., & Stirparo, P. (2013). Security and privacy in mobile cloud under a citizen's perspective. *Cyber Security and Privacy*, 16-27.

Glaser, B.G. & Strauss, A.L. (1977). *The discovery of grounded theory: Strategies for qualitative research.* Chicago: Aldine.

Hartmann, M. (2011). Mobile privacy: Contexts. *Privacy Online*, 191-204.

Hassandoust, F., Kazerouni, M. F., & Perumal, V. (2012). Socio-behavioral factors in virtual knowledge sharing: Theory of reasoned action and theory of planned behavior perspective. *International Journal of Knowledge-Based Organizations (IJKBO)*, *2*(2), 40-53.

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a human factor in holistic cyber security risk assessment. *Procedia Manufacturing*, *3*, 1117-1124.

Herath, H., & Herath, T. (2011). Copula-based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations*, *2*(1), 7-20.

Hettema, H., Watters, P., Sarrafzadeh, H., Fourie, L., Kingston, T., & Pang, S. (2014). Global Business and Technology Association Conference. *The global cyber security workforce: An ongoing human capital crisis.*

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*(1), 83-95.

Johansson, R. (2003). Proceedings from the International Conference '03: *Case Study Methodology*. Methodologies in Housing Research: Stockholm.

Joinson, A.N., Houghton, D.J., Vasalou, A., & Marder, B.L. (2011). Digital crowding: Privacy, self-disclosure, and technology. *Privacy Online*, 33-46.

Kisekka, V., Bagchi-Sen, S., & Rao, H. R. (2013). Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users. *Computers in Human Behavior*, *29*(6), 2722-2729.

Krämer, N.C. & Haferkamp, N. (2011). Online self-presentation: Balancing privacy concerns and impression construction on social networking sites. *Privacy Online*, 127-143.

Lagrule, C. M. (2015). *The association and probability of a predictive relationship between cyber security incidents and type of Internet connectivity: A quantitative study* (Doctoral dissertation).

Laszka, A., Johnson, B., Grossklags, J., & Felegyhazi, M. (2014). Estimating systematic risk in real-world networks. *Financial Cryptography and Data Security*, 417-435.

Laszka, A., & Grossklags, J. (2015). Should cyber-insurance providers invest in software security? *Computer Security,* 483-502.

LeCompte, M.D. & Schensul, J.J. (2010). *Designing and conducting ethnographic research: An introduction*. Boulder, Colorado: Altamira Press.

LeCompte, M.D. & Schensul, J.J. (2013). *Essential ethnographic methods: A mixed methods approach.* Boulder, Colorado: Altamira Press.

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, *50*(2), 361-369.

Lee, M., & Lee, J. (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the Internet. *Information Systems Frontiers*, *14*(2), 375-393.

Lewis, K. (2011). The co-evolution of social network ties and online privacy behavior. *Privacy Online*, 91-110.

Levy, Y., Ramim, M. M., & Hackney, R. A. (2013). Assessing ethical severity of e-learning systems security attacks. *The Journal of Computer Information Systems*, *53*(3), 75-84.

Maaß, W. (2011). The elderly and the Internet: How senior citizens deal with online privacy. *Privacy Online*, 235-249.

Manson, D., & Pike, R. (2014). The case for depth in cybersecurity education. *ACM Inroads*, *5*(1), 47-52.

McBride, M., Carter, L., & Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *Institute for Homeland Security Solutions*, 1-36.

McClain, J., Silva, A., Emmanuel, G., Anderson, B., Nauer, K., Abbott, R., & Forsythe, C. (2015). Human performance factors in cyber security forensic analysis. *Procedia Manufacturing*, *3*, 5301-5307.

Mejias, R. J. (2012). 45th Hawaii International Conference on System Science (HICSS): *An integrative model of information security awareness for assessing information systems security risk*, 3258-3267.

Moustakas, C. (1994). *Phenomenological research methods.* London: Sage.

Onarlioglu, K., Yilmaz, U. O., Kirda, E., & Balzarotti, D. (2012). Insights into user behavior in dealing with Internet attacks. *NDSS*. Retrieved from http://mail.seclab.tuwien.ac.at/papers/onarlioglu_ndss12.pdf

Othmane, L. B., Weffers, H., Ranchal, R., Angin, P., Bhargava, B., & Mohamad, M. M. (2013). A case for societal digital security culture. *Security and Privacy Protection in Information Processing Systems*, 391-404.

Pal, R., & Hui, P. (2012). CyberInsurance for cybersecurity: A topological take on modulating insurance premiums. *ACM SIGMETRICS Performance Evaluation Review*, *40*(3), 86-88.

Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2014). Will cyber-insurance improve network security? A market analysis. *INFOCOM, 2014 Proceedings IEEE*, 235-243.

Pandey, P., & Snekkenes, E. A. (2014). Using prediction markets to hedge information security risks. *Security and Trust Management*, 129-145.

Papacharissi, Z. & Gibson, P.L. (2011). Fifteen minutes of privacy: Privacy, sociality, and publicity. *Privacy Online*, 75-90.

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

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior. *The Journal of Social Psychology*, *154*(4), 352-369.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65-78.

Salem, M. B., & Stolfo, S. J. (2011). On the design and execution of cyber-security user studies: Methodology, challenges, and lessons learned. *CSET*. Retrieved from https://www.usenix.org/legacy/event/cset11/tech/final_files/Salem.pdf

Salleh, N., Hussein, R., Mohamed, N., Karim, N. S. A., Ahlan, A. R., & Aditiawarman, U. (2012). Examining information disclosure behavior on social network sites using protection motivation theory, trust and risk. *Journal of Internet Social Networking & Virtual Communities*, *2012*, 1-11.

Sánchez, M., Kaplan, M. S., & Bradley, L. (2015). Using technology to connect generations: Some considerations of form and function. *Comunicar, 45*, 1-11.

Schwartz, G., Shetty, N., & Walrand, J. (2013). Why cyber-insurance contracts fail to reflect cyber-risks. *Communication, Control, and Computing*, 781-787.

Silva, A., McClain, J., Reed, T., Anderson, B., Nauer, K., Abbott, R., & Forsythe, C. (2014). Proceedings of the Interservice/Interagency Training, Simulation and Education Conference: *Factors impacting performance in competitive cyber exercises*. Orlando, FL.

Sofo, M., & Sofo, F. (2014). Participatory barriers to the informal learning of older Australians using the Internet and Web 2.0 technologies. *Adult and Continuing Education: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*, 88-110.

Sommestad, T., & Hallberg, J. (2013). A review of the theory of planned behaviour in the context of information security policy compliance. *Security and Privacy Protection in Information Processing Systems*, 257-271.

Stolfo, S. J., Salem, M. B., & Keromytis, A. D. (2012). Fog computing: Mitigating insider data theft attacks in the cloud. *Security and Privacy Workshops (SPW), 2012*, 125-128.

Taddicken, M. & Jers, C. (2011). The uses of privacy online: Trading a loss of privacy for social web gratifications? *Privacy Online*, 143-157.

Thelwall, M. (2011). Privacy and gender in the social web. *Privacy Online*, 251-266.

Trepte, S. & Reinecke, L. (2011). The social web as a shelter for privacy and authentic living. *Privacy Online*, 61-74.

Toregas, C., & Zahn, N. (2014). Insurance for cyber attacks: The issue of setting premiums in context. *George Washington University*. Retrieved from http://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/54203258e4b000f16802b810/1411396184449/cyberinsurance_paper_pdf.pdf

Wang, P. A. (2013). International Conference on Internet Monitoring and Protection (ICIMP). *Assessment of cyber security knowledge and behavior: An anti-phishing scenario.*

Warkentin, M., Malimage, N., & Malimage, K. (2012). Proceedings of the Pre-ICIS Workshop on Information Security and Privacy: *Impact of protection motivation and deterrence on IS security policy compliance: A multi-cultural view*. Orlando, FL.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3-7.

Wolf, Z. R. (2012). Ethnography: The method. *Nursing research: A qualitative perspective*, 285-335.

Yang, Z., & Lui, J. C. (2014). Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation*, *74*, 1-17.

Yao, M.Z. (2011). Self-protection of online privacy: A behavioral approach. *Privacy Online*, 111-126.

Ziegele, M. & Quiring, O. (2011). Privacy in social network sites. *Privacy Online*, 175-190.