Annotated Bibliography

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.

The authors are affiliated with the International Information Systems Security Certification Consortium, the Graduate School of Computer and Information Sciences at Nova Southeastern University, and the Korea University Business School. This research focuses on the effect of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills in relation to user misuse behavior using survey questionnaire data from a government agency. According to the study, intentional and unintentional computer misuse poses significant cybersecurity risks, and awareness of countermeasures likely decreases misuse. The authors found that user awareness and cybersecurity skill reduced computer misuse, and user awareness of policies contributed to increased cybersecurity skills. The authors also note that the majority of participants in the sample were at least 40 years old. The younger participants were observed to make fewer errors and took less time to learn cybersecurity skills. It is recommended that further studies investigate the relationship between age and computer misuse. Similarly to Onarlioglu, Yilmaz, Kirda, and Balzarotti (2012), Othmane et al. (2013), and Pfleeger and Caputo (2012), this study addresses the effects of human behavioral factors on cybersecurity skill and awareness.

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.

The authors conduct research on cybersecurity at Mississippi State University and Virginia Tech. In this study, the authors examined the effectiveness of Protection

Motivation Theory in explaining individual security behaviors using survey data. Protection Motivation Theory is defined as the understanding of processes undertaken when making decisions on security behaviors. The authors expanded on the research gap and discussed the focus of several studies to examine specific security behaviors rather than several collective security behaviors. It is suggested that because human error is a significant source of security threats and technical solutions alone cannot adequately address the problem, personal security measures must be taken to ensure cyber safety. The authors described an individual who updates anti-virus software but has no firewall and very poor passwords as an example of an individual who might be incorrectly ranked as having safe security practices when studies only examine one security measure. This study differed in that it incorporated holistic interpretations of security behaviors. It was found that as perceived vulnerability increased, participant security safety decreased, and as perceived vulnerability decreased, participant security safety increased. This study differed from the study by Salleh et al. (2012) that found all constructs of Protection Motivation Theory to be significant mediators for privacy behaviors.

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.

The authors are affiliated with the Institute for the Protection and Security of the Citizen, Joint Research Center, and the Royal Institute of Technology. The authors examine Cloud usage on mobile smart devices and security and privacy issues from a user perspective. The authors argued that smart phones are particularly vulnerable as they are exposed to adverse environments, cybersecurity code development is not a priority for mobile application development, and users can be strongly linked to smart

phones, greatly impacting the security and privacy of a user's smart phone contents. A use case scenario is used to examine smart phone security risks, and the authors provide an overview of the types of security risks and vulnerabilities present in smart phone applications. The authors further recommended prioritizing cybersecurity in mobile application development and instilling safe user practices. This study was similar to Wang's (2013) study through its focus on Cloud security risks.

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

This study was funded by the EU Seventh Framework Programme, the National Science Foundation, the Austrian Research Promotion Agency, and Secure Business Austria, with authors contributing from Northeastern University, Bilkent University, and Institute Eurecom. In this study, the authors conducted experiments with 164 participants to test user behavior when confronted with cyber security attack scenarios. The authors found that several non-technical users were able to thwart cyber security attacks solely by following intuition. However, sophisticated attacks were not thwarted as successfully. Users often relied on misleading information such as the size and length of URLs (short URLs were thought to be safe), and users did not adequately protect themselves against trick banners on file sharing websites. The authors concluded that non-technical users do not benefit from URL expansion websites aimed at protecting users from security threats because they were not aware of the websites or the concept behind malicious URL shortening. This study is supported by Choi, Levy, and Hovav (2013), Othmane et al. (2013), and Pfleeger and Caputo (2012).

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.

This study received partial funding from the Dutch national HTAS innovation program. The authors are affiliated with the Department of Mathematics and Computer Science at Eindhoven University of Technology, CERIAS and Computer Sciences at Purdue University, and the Faculty of Computing at Universiti Teknologi Malaysia. This research demonstrates an overview of security solutions, collective knowledge, common practices, and intuitive common behavior approaches for security improvement. The authors discuss the use of personal incentives, games, certification, and education to improve security awareness. Personal incentives include moral, accountability, and reward incentives for following policies to prevent security attacks. Games are used to simulate attacks and require users to discover threats and protect themselves in order to promote security awareness. Certification involves requiring periodic certification renewal for employees that handle sensitive information. Finally, education involves adopting mandatory classes and exposure for cybersecurity awareness and safety. The authors also proposed mandating two-step authentication mechanisms for sensitive information and communication through security awareness programs. This study supports Choi, Levy, and Hovav (2013), Onarlioglu et al. (2012), and Pfleeger and Caputo (2012).

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

The authors are affiliated with the University of Southern California and the T-Labs in Germany. This research examines compulsory monopolistic insurance scenarios

to incentivize users to invest in cybersecurity defense. The authors proposed a mechanism to proportionally adjust fines and rebates for cyber-insurance premiums in order to generate better estimates of risk values and increase user safety. In the article, benefits of cyber-insurance are discussed and argued to increase self-defense mechanisms and security awareness. The authors suggested optimal fine (rebates) per user could be allocated based on the model mechanism's estimates. According to the authors, cyber-insurance will allow for third party risk mitigations that are aligned with the interests of users, insurers, and security software vendors. This study mirrors the arguments made by Pal, Golubchik, Psounis, and Hui (2014) and Yang and Lui (2014), but differs from Toregas and Zahn (2014) by focusing on cyber-insurance as a solution.

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

The authors are affiliated with the University of Southern California and the HKUST and T-Labs in Germany. The authors argued in favor of cyber-insurance as a risk management technique to help improve cybersecurity measures. It is suggested that the inability to implement successful cyber-insurance markets is due to information asymmetry, defined as the inability to distinguish between users with different levels of risk, and the nature of cyber risks. The authors proposed a supply-demand model of regulated cyber-insurance markets and examined the success of theoretical cyber-insurance markets. It is suggested that security vendors form symbiotic relationships with insurers, as it would be difficult for cyber-insurance markets to survive with the inability to generate profit and maximize social welfare in a network. This study

supports Pal and Hui (2012) and Yang and Lui (2014), but does not offer a comprehensive view of cyber-insurance as seen in the study by Toregas and Zahn (2014).

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

This research was supported by grants from the Institute for Information Infrastructure Protection at Dartmouth College. The authors conduct research at the Institute for Information Infrastructure Protection and MITRE Corporation. In this study, the authors examine human behavior patterns regarding cybersecurity in order to develop improved cybersecurity models and technological designs that incorporate human factors. Qualitative interviews with government and industry employees were conducted. The authors found users may become overwhelmed, untrusting, and unresponsive to cyber security measures despite having technical competence. The authors also expanded on themes that emerged from the research. It was found that security is affected by human behavior during task or goal completion, analysis capabilities, inability to notice unexpected events, security bias, and risk perceptions. Similarly to Choi, Levy, and Hovav (2013), Onarlioglu et al. (2012), and Othmane et al. (2013), this study focused on human behavior and cybersecurity skill and awareness.

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.

The authors conduct social science research at the University of Queensland and University of Exeter. The study used the theory of planned behavior to investigate online privacy and security in survey data from Facebook users. The authors measured and compared behavior two weeks after the study. Attitude, subjective injunctive norms

(what people approve or disprove of), subjective descriptive norms (what people actually do), perceived behavioral control, implicit perceived risk, trust of other Facebook users, and online privacy intentions were assessed. The theory of planned behavior predicts behavior from intentions based on attitudes, subjective norms, and perceived behavioral control. The results showed that privacy intention behaviors were predicted by subjective descriptive and subjective injunctive norms. This study, like Crossler and Bélanger (2014) and Salleh et al. (2012), examined behavior using a theoretical framework, however, the other studies were framed by Protection Motivation Theory models.

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

The authors are affiliated with the Computer Science Department at Columbia University. In this study, a methodology is formulated for conducting user studies to examine masquerade attack detection techniques. The authors also discussed the prevalent research gap in consistent user data on cybersecurity. A threat model was used to collect data to show how other studies can use a similar model to gather data on masquerade attacks. The limitations, design considerations, and methodology of user experiments are outlined in the study. The model particularly involved examining how modeling user search behavior can be used to detect masqueraders. The authors recommended that further studies attempt to reduce user bias, increase experimental sensitivity, and improve the quality of data. This study was similar to Onarlioglu et al. (2012) in that it used experimental data to access security behaviors.

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.

The authors are associated with the International Islamic University and Universiti Teknologi in Malaysia. This study reports on survey data of social network website user privacy behaviors using Protection Motivation Theory as a framework. The authors found that trust on social network websites and perceived benefits influenced information disclosure behavior. The study contradicted Crossler and Bélanger (2014) and showed that all Protection Motivation Theory constructs correlated with privacy behaviors, but privacy concern and risk were not related to disclosure behavior. The authors suggested that this might have occurred because sharing information was often not perceived as risky behavior; therefore, privacy was not a concern with disclosure behavior. The authors suggested expanding research to include older individuals as well as the effects of security features, user locus of control, and social influence.

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.

The authors are associated with Columbia University, Accenture Technology Labs, and Allure Security Technologies. The article focuses on fog computing approaches to cybersecurity risks, involving the release of decoy information to the attacker in order to protect user data. Experiments were conducted using decoy data for protection and as sensors to detect unauthorized access. The authors suggested that advantages of using this technique include the detection of masquerade activity, confusing attackers and protecting real information, and prevention and deterrence of masquerade activity. The results showed that this was an effective method, and masquerade activity was detectable. The authors recommend monitoring user patterns to detect malicious access to profiles and documents.

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

The authors conduct research on cybersecurity at George Washington University. This research draws from existing studies and interview data on the cyber-insurance market. The authors discussed barriers and potential for developing cyber-insurance to mitigate security risk. The authors argued that benefits of cyber-insurance include the ability to transfer risk management to third parties, incentivized investments in cybersecurity, and systemic resilience. Arguments against cyber-insurance posit that risks are not quantifiable and therefore premiums cannot be determined and that cyber-insurance allows companies to avoid working on security improvements by simply using insurance. The authors also indicated uncertainty in the capabilities of cyber-insurance companies to determine and provide incentives for increased cybersecurity protection. This study provides a more holistic view of various views on cyber-insurance than Pal and Hui (2012) and Pal et al. (2014), that specifically address the need for cyber-insurance.

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

The author conducts research on cybersecurity at the Department of Cybersecurity and Information Assurance at the University of Maryland University College. The study focuses on creating a model of assessment of user cybersecurity knowledge by examining technical knowledge and competency in identifying cybersecurity risks. Survey methods were used to examine knowledge and competence on anti-phishing techniques and the intention to use anti-phishing solutions. Statistical analyses showed a positive correlation

between technical knowledge and intent to use anti-phishing solutions. Direct and indirect self-assessments of cybersecurity knowledge were also positively correlated. The author suggested that many studies have attempted to examine human behavior in relation to cyber security, but few studies have focused on the assessment of cybersecurity knowledge and the intent to adopt safer practices and solutions. It is recommended that future studies examine malware risks, anti-malware solutions, botnets, and Cloud security risks and solutions. Like Geneiatakis, Kounelis, Loeschner, Fovino, and Stirparo (2013), this study emphasized the need to examine Cloud security issues.

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

The authors conduct research on cybersecurity at the Department of Computer Science and Engineering at The Chinese University of Hong Kong. This study focuses on how security adoption may be affected by "network externality" with "node heterogeneity." The authors also examine cyber-insurance risk management. The network externality effect is described as the adoption of security measures as a result of an epidemic of security risks. Nodes make decisions through risk evaluation depending on the extent of available information. The authors constructed mathematical models to determine how nodes make decisions on security investment and whether cyber-insurance can be adopted in various scenarios. The authors established that cyber-insurance has the ability to be a positive incentive for security measures when moral hazard effects are not present, and partial insurance can be a beneficial incentive when moral hazard effects are present. This study supports arguments made by Pal and Hui (2012) and Pal et al. (2014).