# Appendix A. Instrumentation

**Table A1.** Questionnaire items and sources

# Perceived likelihood

Please indicate your perceptions of the likelihood of an information security incident affecting your organisation:

Scale: 1= Extremely Unlikely, 2 = Unlikely, 3 = Neither Likely nor Unlikely, 4 = Likely, 5 = Extremely Likely

|  |  |  |
| --- | --- | --- |
| No. | Question | Source |
| 1 | It is \_\_\_\_\_\_\_\_ that a security incident will occur at my organisation that will result in a business critical information system being unavailable for a prolonged period. | Adapted from Herath and Rao (2009a). |
| 2 | It is \_\_\_\_\_\_\_\_ that a security incident will occur at my organisation that will result in confidential information being disclosed to an unauthorised party. | Adapted from Herath and Rao (2009a). |
| 3 | It is \_\_\_\_\_\_\_\_ that a security incident will occur at my organisation that will result in the integrity of information stored in a system being compromised. | Adapted from Herath and Rao (2009a). |

# Perceived impact

Please indicate your perceptions of the impact an information security incident would have on your organisation:

Scale: 1 = Extremely Insignificant, 2 = Insignificant, 3 = Neither significant nor insignificant, 4 = Significant, 5 = Extremely Significant

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 4 | The impact my organisation would be \_\_\_\_\_\_\_\_ if a business critical information system was unavailable for a prolonged period. | Adapted from Herath and Rao (2009a). |
| 5 | The impact on my organisation would be \_\_\_\_\_\_\_\_ if confidential information was disclosed to an unauthorised party. | Adapted from Herath and Rao (2009a). |
| 6 | The impact on my organisation would be \_\_\_\_\_\_\_\_ if information was corrupted within business critical information system. | Adapted from Herath and Rao (2009a). |

##

## Response costs

Please indicate to what extent you agree with the following statements:

Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree nor Disagree, 4 = Agree, 5 = Strongly Agree

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 7 | The inconvenience of performing information security behaviours exceeds the benefits | Adapted from Workman et al. (2008). |
| 8 | The cost of performing information security behaviours exceeds the benefits | Adapted from Workman et al. (2008). |
| 9 | The impact to my work from performing information security behaviours exceeds the benefits | Adapted from Workman et al. (2008). |

## Response efficacy

Please indicate your perceptions of the effectiveness of the information security behaviours you are expected to perform:

Scale: 1 = Very Ineffective, 2 = Ineffective, 3 = Neither Effective nor Ineffective, 4 = Effective, 5 = Very Effective

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 10 | The information security behaviours I am expected to perform are \_\_\_\_\_\_\_\_ at protecting the confidentiality of my organisation’s information. | Adapted from Workman et al. (2008). |
| 11 | The information security behaviours I am expected to perform are \_\_\_\_\_\_\_\_ at protecting the integrity of my organisation’s information. | Adapted from Workman et al. (2008). |
| 12 | The information security behaviours I am expected to perform are \_\_\_\_\_\_\_\_ at protecting the availability of my organisation’s information. | Adapted from Workman et al. (2008). |

Please indicate to what extent you agree with the following statements:

Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree nor Disagree, 4 = Agree, 5 = Strongly Agree

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 13 | The information security behaviours I am expected to perform make a difference to the security posture of my organisation. | Adapted from Herath and Rao (2009a). |

## Response benefits

Please indicate to what extent you agree with the following statements:

Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree nor Disagree, 4 = Agree, 5 = Strongly Agree

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 14 | I feel content if I comply with my organisation’s information security behaviours. | Adapted from Bulgurcu et al. (2010). |
| 15 | I feel satisfied if I comply with my organisation’s information security behaviours. | Adapted from Bulgurcu et al. (2010). |
| 16 | I feel accomplished if I comply with my organisation’s information security behaviours. | Adapted from Bulgurcu et al. (2010). |
| 17 | I feel fulfilled if I comply with my organisation’s information security behaviours. | Adapted from Bulgurcu et al. (2010). |

Please indicate the likelihood of the following statements:

Scale: 1= Extremely Unlikely, 2 = Unlikely, 3 = Neither Likely nor Unlikely, 4 = Likely, 5 = Extremely Likely

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 18 | I will receive a pay rise if I comply with my organisation’s information security behaviours. | Adapted from Bulgurcu et al. (2010). |
| 19 | I will receive a promotion if I comply with my organisation’s information security behaviours. | Adapted from Bulgurcu et al. (2010). |

##

## Cues to action

Please indicate the frequency with which your organisation performs the following:

Scale: 1 = Never, 2 = Rarely; 3 = Occasionally, 4= Often, 5 = Always.

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 20 | My organisation \_\_\_\_\_\_\_\_ distributes security awareness material to all employees using email newsletters and intranet articles. | Adapted from Ng et al. (2009). |
| 21 | My organisation \_\_\_\_\_\_\_\_ organises security talks/presentations for IT employees. | Adapted from Ng et al. (2009). |

Please indicate to what extent you agree with the following statements:

Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree nor Disagree, 4 = Agree, 5 = Strongly Agree

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 22 | My organisation constantly reminds me of my responsibility to practice information security behaviours.  | Adapted from Ng et al. (2009). |
| 23 | My organisation ensures that information security policies are available to all employees. | Adapted from Herath and Rao (2009a). |
| 24 | My organisation’s information security policies are written in plain English and are easy to understand. | Adapted from Herath and Rao (2009a). |

# Social norms

Please indicate to what extent you agree with the following statements:

Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree nor Disagree, 4 = Agree, 5 = Strongly Agree

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 25 | Senior management thinks that I should comply with the organisation’s required information security behaviours | Adapted from Herath and Rao (2009a). |
| 26 | My manager thinks that I should comply with the organisation’s required information security behaviours | Adapted from Herath and Rao (2009a). |
| 27 | My colleagues think that I should comply with the organisation’s required information security behaviours | Adapted from Herath and Rao (2009a). |

## Detection

Please indicate the frequency with which your organisation performs the following actions:

Scale: 1 = Never, 2 = Rarely; 3 = Occasionally, 4= Often, 5 = Always

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 28 | My organisation \_\_\_\_\_\_\_\_ monitors IT employee’s actions to detect violations of information security behaviours. | Adapted from Herath and Rao (2009a). |

Please indicate to what extent you agree with the following statement:

Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree nor Disagree, 4 = Agree, 5 = Strongly Agree

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 29 | If I violate my organisation’s required information security behaviours I will be caught. | Adapted from Herath and Rao (2009a). |
| 30 | I would feel embarrassed if I was caught violating my organisation’s information security behaviours. | New |

## Sanctions

Please indicate to what extent you agree with the following statements:

Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree nor Disagree, 4 = Agree, 5 = Strongly Agree

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 31 | My organisation disciplines IT employees who violate information security behaviours. | Adapted from Herath and Rao (2009a). |
| 32 | My organisation terminates employees who repeatedly violate information security behaviours. | Adapted from Herath and Rao (2009a). |

Please indicate the likelihood of the following sanctions being imposed by your organisation:

Scale: 1= Extremely Unlikely, 2 = Unlikely, 3 = Neither Likely nor Unlikely, 4 = Likely, 5 = Extremely Likely

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 33 | I will be punished if I was caught violating my organisation’s information security behaviours. | Adapted from Herath and Rao (2009a). |
| 34 | I will receive written reprimand if I was caught violating my organisation’s information security behaviours  | Adapted from Bulgurcu et al. (2010). |
| 35 | I will receive verbal reprimand if I was caught violating my organisation’s information security behaviours  | Adapted from Bulgurcu et al. (2010). |
| 36 | I will be demoted if I was caught violating my organisation’s information security behaviours. | Adapted from Bulgurcu et al. (2010). |
| 37 | I will incur non-monetary penalties if I was caught violating my organisation’s information security behaviours. | Adapted from Bulgurcu et al. (2010). |
| 38 | I will incur monetary penalties if I was caught violating my organisation’s information security behaviours. | Adapted from Bulgurcu et al. (2010). |

##

## Self-efficacy

Considering the information security behaviours that your organisation expects you to perform as part of your job, please indicate to what extent you agree with the following statements:

Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree nor Disagree, 4 = Agree, 5 = Strongly Agree

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 39 | It is difficult for me to perform the information security behaviours required by my organisation. | Adapted from Workman et al. (2008). |
| 40 | I have the necessary skills to protect my organisation from information assets from security incidents. | Adapted from Workman et al. (2008). |
| 41 | It is easy for me to perform the information security behaviours required by my organisation. | Adapted from Herath and Rao (2009a). |
| 42 | My organisation provides adequate training for me to perform the information security behaviours expected of me. | New  |

# Intention

Please indicate to what extent you agree with the following statements:

Scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neither Agree nor Disagree, 4 = Agree, 5 = Strongly Agree

|  |  |  |
| --- | --- | --- |
| No. | Question |  |
| 43 | I intend to comply with the information security behaviours required by my organisation. | Adapted from Bulgurcu et al. (2010). |
| 44 | I intend to protect information and technology resources according to the information security behaviours required by my organisation. | Adapted from Bulgurcu et al. (2010). |
| 45 | I intend to carry out my information security responsibilities prescribed by my organisation when I use information and technology. | Adapted from Bulgurcu et al. (2010). |

**Appendix B. Model validation**

**Table B1.** Factor loadings to latent constructs, variance extracted, and composite reliabilities

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Construct | Item | Text | Factor loading | Variance extracted | Composite reliability |
| Perceived likelihood | 1 | It is \_\_\_\_\_\_\_\_ that a security incident will occur at my organisation that will result in a business critical information system being unavailable for a prolonged period. | 0.667 | 0.722 | 0.884 |
|  | 2 | It is \_\_\_\_\_\_\_\_ that a security incident will occur at my organisation that will result in confidential information being disclosed to an unauthorised party. | 0.924 |  |  |
|  | 3 | It is \_\_\_\_\_\_\_\_ that a security incident will occur at my organisation that will result in the integrity of information stored in a system being compromised. | 0.931 |  |  |
| Perceived impact | 4 | The impact my organisation would be \_\_\_\_\_\_\_\_ if a business critical information system was unavailable for a prolonged period. | 0.834 | 0.646 | 0.784 |
|  | 5 | The impact on my organisation would be \_\_\_\_\_\_\_\_ if confidential information was disclosed to an unauthorised party. | Dropped |  |  |
|  | 6 | The impact on my organisation would be \_\_\_\_\_\_\_\_ if information was corrupted within business critical information system. | 0.771 |  |  |
| Response costs | 7 | The inconvenience of performing information security behaviours exceeds the benefits. | 0.872 | 0.744 | 0.896 |
|  | 8 | The cost of performing information security behaviours exceeds the benefits. | 0.736 |  |  |
|  | 9 | The impact to my work from performing information security behaviours exceeds the benefits | 0.964 |  |  |
| Response efficacy | 10 | The information security behaviours I am expected to perform are \_\_\_\_\_\_\_\_ at protecting the confidentiality of my organisation’s information. | Dropped | 0.594 | 0.814 |
|  | 11 | The information security behaviours I am expected to perform are \_\_\_\_\_\_\_\_ at protecting the integrity of my organisation’s information. | 0.828 |  |  |
|  | 12 | The information security behaviours I am expected to perform are \_\_\_\_\_\_\_\_ at protecting the availability of my organisation’s information. | 0.718 |  |  |
|  | 13 | The information security behaviours I am expected to perform make a difference to the security posture of my organisation. | 0.762 |  |  |
| Response benefits | 14 | I feel content if I comply with my organisation’s information security behaviours. | 0.892 | 0.750 | 0.923 |
|  | 15 | I feel satisfied if I comply with my organisation’s information security behaviours. | 0.921 |  |  |
|  | 16 | I feel accomplished if I comply with my organisation’s information security behaviours. | 0.858 |  |  |
|  | 17 | I feel fulfilled if I comply with my organisation’s information security behaviours. | 0.789 |  |  |
|  | 18 | I will receive a pay rise if I comply with my organisation’s information security behaviours. | Dropped |  |  |
|  | 19 | I will receive a promotion if I comply with my organisation’s information security behaviours. | Dropped |  |  |
| Cues to action | 20 | My organisation \_\_\_\_\_\_\_\_ distributes security awareness material to all employees using email newsletters and intranet articles. | 0.712 | 0.621 | 0.867 |
|  | 21 | My organisation \_\_\_\_\_\_\_\_ organises security talks/presentations for IT employees. | Dropped |  |  |
|  | 22 | My organisation constantly reminds me of my responsibility to practice information security behaviours.  | 0.861 |  |  |
|  | 23 | My organisation ensures that information security policies are available to all employees. | 0.854 |  |  |
|  | 24 | My organisation’s information security policies are written in plain English and are easy to understand. | 0.712 |  |  |
| Social norms | 25 | Senior management thinks that I should comply with the organisation’s required information security behaviours. | Dropped | 0.788 | 0.881 |
|  | 26 | My manager thinks that I should comply with the organisation’s required information security behaviours. | 0.924 |  |  |
|  | 27 | My colleagues think that I should comply with the organisation’s required information security behaviours. | 0.849 |  |  |
| Detection | 28 | My organisation \_\_\_\_\_\_\_\_ monitors IT employee’s actions to detect violations of information security behaviours. | 0.675 | 0.634 | 0.772 |
|  | 29 | If I violate my organisation’s required information security behaviours I will be caught. | 0.901 |  |  |
|  | 30 | I would feel embarrassed if I was caught violating my organisation’s information security behaviours. | Dropped |  |  |
| Sanctions  | 31 | My organisation disciplines IT employees who violate information security behaviours. | 0.695 | 0.511 | 0.807 |
|  | 32 | My organisation terminates employees who repeatedly violate information security behaviours. | 0.700 |  |  |
|  | 33 | I will be punished if I was caught violating my organisation’s information security behaviours. | 0.627 |  |  |
|  | 34 | I will receive written reprimand if I was caught violating my organisation’s information security behaviours. | 0.711 |  |  |
|  | 35 | I will receive verbal reprimand if I was caught violating my organisation’s information security behaviours. | Dropped |  |  |
|  | 36 | I will be demoted if I was caught violating my organisation’s information security behaviours. | 0.720 |  |  |
|  | 37 | I will incur non-monetary penalties if I was caught violating my organisation’s information security behaviours. | Dropped |  |  |
|  | 38 | I will incur monetary or non-monetary penalties if I was caught violating my organisation’s information security behaviours. | Dropped |  |  |
| Self-efficacy | 39\* | It is difficult for me to perform the information security behaviours required by my organisation. | -0.757 | 0.610 | 0.823 |
|  | 40 | I have the necessary skills to protect my organisation from information assets from security incidents. | Dropped |  |  |
|  | 41 | It is easy for me to perform the information security behaviours required by my organisation. | 0.883 |  |  |
|  | 42 | My organisation provides adequate training for me to perform the information security behaviours expected of me. | 0.691 |  |  |
| Intention | 43 | I intend to comply with the information security behaviours required by my organisation. | 0.967 | 0.940 | 0.979 |
|  | 44 | I intend to protect information and technology resources according to the information security behaviours required by my organisation. | 0.973 |  |  |
|  | 45 | I intend to carry out my information security responsibilities prescribed by my organisation when I use information and technology. | 0.968 |  |  |

\* = Reverse coded

**References**

Ajzen, I. 1991. “The theory of planned behaviour.” *Organizational Behavior and Human Decision Processes* 50 (2): 179-211.

Ajzen, I., and M. Fishbein. 1980. *Understanding attitudes and predicting social behaviour*. Upper Saddle River, NJ: Prentice-Hall.

Anderson, C. L., and R. Argawal. 2010. “Practicing safe computing: a multimethod empirical examination of home computer user security behavioural intentions.” *MIS Quarterly* 34 (3): 613-643.

Bagozzi, R. P., F. D. Davis, and P. R. Warshaw. 1992. “Development and test of a theory of technological learning and usage.” *Human Relations* 45 (7): 659-686.

Bandura, A. 1977. “Self-efficacy: toward a unifying theory of behavioral change.” *Psychological Review* 84 (2): 191-215.

Boss, S. R., D. F. Galletta, P. B. Lowry, G. Moody, and P. 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* 39 (4): 837-864.

Brehm, J. W. 1966. *A theory of psychological reactance*. Academic Press.

Bulgurcu, B., H. Cavusoglu, and I. Benbasat. 2010. “Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness.” *MIS Quarterly* 34 (3): 523-548.

Burns, A. J., C. Posey, T. L. Roberts, and P. B. Lowry. 2017. “Examining the relationship of organizational insiders’ psychological capital with information security threat and coping appraisals.” *Computers in Human Behavior* 68: 190-209.

Certified Information Systems Professional. Accessed October 2018 from https://www.isc2.org

Chin, W. W. 1998. “Issues and opinion on structural equation modelling.” *MIS Quarterly* 22 (1): vii-xvii.

D’Arcy, J., A. Hovav, and D. Galletta. 2009. “User awareness of security countermeasures and its impact on information systems misuse.” *Information Systems Research* 20 (1): 79-98.

Deci, E. L. 1975. *Intrinsic motivation*. Berlin: Plenum Press.

Deci, E. L., and R. M. Ryan. 1985. *Intrinsic motivation and self-determination in human behaviour*. Berlin: Plenum Press.

Fishbein, M., and I. Ajzen. 1975. *Belief, attitude, intention, and behavior: an introduction to theory and research*. Boston: Addison-Wesley.

Fornell, C., and D. F. Larcker. 1981. “Evaluating structural equation models with unobservable variables and measurement error.” *Journal of Marketing Research* 48: 39-50.

Glanz, K., B. K. Rimer, and K. Viswanath. 2008. *Health behavior and health education: theory, research, and practice*. Hoboken, NJ: Jossey-Bass.

Gliner, J. A., G. A. Morgan, and N. L. Leech. 2000. *Research methods in applied settings: an integrated approach to design and analysis.* Hove: Psychology Press.

Hair, J. F., R. E. Anderson, R. L. Tatham, and W. C. Black. 1998. *Multivariate data analysis*. 5th ed. Upper Saddle River, NJ: Prentice Hall.

Hair, J. F., G. T. M. Hult, C. Ringle, and M. Sarstedt. 2013. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. London: Sage Publications.

Harrison, R. 2005. “The 10 most important things an IT person must understand about security across the enterprise.” *Information Systems Control Journal* 3.

Herath, T., and H. R. Rao. 2009a. “Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness.” *Decision Support Systems* 47: 154-165.

Herath, T., and H. R. Rao. 2009b. “Protection motivation and deterrence: a framework for security policy compliance in organisations.” *European Journal of Information Systems* 18: 106-125.

Hinkin, T. R. 1998. “A brief tutorial on the development of measures for use in survey questionnaires.” *Organizational Research Methods* 1 (1): 104-121.

Hovav, A., and J. D’Arcy. 2012. “Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea.” *Information & Management* 49: 99-110.

Hsu, J. S.-C., S.-P. Shih, Y. W. Hung, and P. B. Lowry. 2015. “The role of extra-role behaviors and social controls in information security policy effectiveness.” *Information Systems Research* 26 (2): 282-300.

Ifinedo, P. 2014. “Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition.” *Information & Management* 51: 69-79.

Ifinedo, P. 2012. “Understanding information systems security policy compliance: an integration of the theory of planned behaviour and the protection motivation theory.” *Computers & Security* 31: 83-95.

Igbaria, M., T. Guimaraes, and G. B. Davis. 1995. “Testing the determinants of microcomputer usage via a structural equation model.” *Journal of Management Information Systems* 11 (4): 87-113.

International Organization for Standardization ISO/IEC 27000:2018. Accessed October 2018 from https://www.iso.org/standard/73906.html

Janz, N. K., and M. H. Becker. 1984. “The health belief model: a decade later.” *Health Education Behavior* 11 (1): 1-47.

Johnston, A.C., M. Warkentin, M., and M. Siponen. (2015). “An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric.” *MIS Quarterly*  39 (1): 113-134.

Johnston, A. C., and M. Warkentin. 2010. “Fear appeals and information security behaviors: an empirical study.” *MIS Quarterly* 34 (3): 549-566.

Kankanhalli, A., H. H. Teo, B. C. Tan, and K. K. Wei. 2003. “An integrative study of information systems security effectiveness.” *International Journal of Information Management* 23 (2): 139-154.

Lee, Y., and K. R. Larsen. 2009. “Threat or coping appraisal: determinants of SMB executives’ decision to adopt anti-malware software.” *European Journal of Information Systems* 18: 177-187.

Lowry, P. B., and G. D. Moody. 2015. “Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies.” *Information Systems Journal* 25: 433-463.

Lowry, P. B., C. Posey, R. J. Bennett, and T. L. Roberts. 2015. “Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust.” *Information Systems Journal* 25: 193-230.

Maddux, J. E., and R. W. Rogers. 1983. “Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change.” *Journal of Experimental Social Psychology* 19 (5): 469-479.

McAdams, R. H. 1997. “The origin, development and regulation of norms.” *Michigan Law Review* 96 (2): 338-433.

Milne, S., P. Sheeran, and S. Orbell. 2000. “Prediction and intervention in health-related behaviour: a meta-analytic review of protection motivation theory.” *Journal of Applied Social Psychology* 30 (1): 106-143.

Moody, G. D., M. Siponen, and S. Pahnila. 2018. “Toward a unified model of information security compliance”. *MIS Quarterly* 42 (1): 285-311.

Neuwirth, K., S. Dunwoody, and R. J. Griffin. 2000. “Protection motivation and risk communication.” *Risk Analysis* 20 (5): 721-734.

Ng, B.-Y., A. Kankanhalli, and Y. Xu. 2009. “Studying users’ computer security behavior: a health belief perspective.” *Decision Support Systems* 46 (4): 815-825.

Nunnally, J. 1978. *Psychometric methods.* New York: McGraw.

Pahnila, S., M. Karjalainen, and M. Siponen. 2013. “Information security behaviour: towards a multi-stage model.” *PACIS 2013 Proceedings*, Paper 102.

Pahnila, S., M. Siponen, and A Mahmood. 2007. “Employees’ behaviour towards IS security compliance.” *Proceedings of the 40th Hawaii International Conference on Systems Sciences.*

Paternoster, R., and S. Simpson. 1996. “Sanction threats and appeals to morality: testing a rational choice model of corporate crime.” *Law and Society Review* 30 (3): 549-584.

Podsakoff, P. M., S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff. 2003. “Common method biases in behavioural research: a critical review of the literature and recommended remedies.” *Journal of Applied Psychology* 88 (5): 879-903.

Posey, C., T. L. Roberts, P. B. Lowry, and R. T. Hightower. 2014. “Bridging the divide: A qualitative comparison of information security through patterns between information security professionals and ordinary organizational insiders.” *Information & Management* 51: 551-567.

Prentice-Dunn, S., and R. W. Rogers. 1986. “Protection motivation theory and preventive health: beyond the health belief model.” *Health Education Research* 1 (3): 153-161.

Ringle, C., S. Wende, and A. Will. 2017. *SmartPLS 3 Professional*.

Rogers , R. W. 1983. “Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation.” In J. R. Cacioppo, and R. E. Petty (eds.), *Social psychology: a sourcebook.* New York, NY: Guilford Press, pp.153-176.

Rogers, R. W. 1975. “A protection motivation theory of fear appeals and attitude change.” *Journal of Psychology* 91 (1): 93-114.

Schultz, E. 2005. “The human factor in security.” *Computers & Security* 24 (6): 425-426.

Shostack, A., and A. Stewart. 2008. *The new school of information security*. Boston: Addison Wesley.

Siponen, M. T. 2000. “Conceptual foundation for organizational information security awareness.” *Information Management & Computer Security* 8 (1): 31-41.

Siponen, M., M. A. Mahmood, and S. Pahnila. 2014. “Employees’ adherence to information security policies: an exploratory field study.” *Information & Management* 51: 217-224.

Siponen, M., S. Pahnila, and M. A. Mahmood. 2007. “Employees’ adherence to information security policies: an empirical study.” *New approaches for security, privacy and trust in complex environments* 232: 133-144.

Siponen, M., S. Pahnila, and A. Mahmood. 2006. “Factors influencing protection motivation and IS security policy compliance.” *Innovations in Information Technology* November: 1-5.

Siponen, M., and A. Vance. 2010. “Neutralization: new insights into the problem of employee information systems security policy violations.” *MIS Quarterly* 34 (3): 487-502.

Siponen, M., A. Vance, and R. Willison. 2012. “New insights into the problem of software piracy: the effects of neutralization, shame, and moral beliefs.” *Information & Management* 49: 334-341.

Son, J.-Y. 2011. “Out of fear or desire? Toward a better understanding of employees’ motivation to follow IS security policies.” *Information & Management* 48: 296-302.

Straub, D. 1990. “Effective IS security: an empirical study.” *Information Systems Research* 1 (3): 255-276

Straub, D. W., and R. J. Welke. 1998. “Coping with systems risk: security planning models for management decision-making.” *MIS Quarterly* 22 (4): 441-469.

Ungerman, M. 2005. “Creating and enforcing an effective information security policy.” *Information Systems Control Journa*l 6: 1-2.

Urbach, N., and F. Ahlemann. 2010. “Structural equation modeling in information systems research using partial least squares.” *Journal of Information Technology Theory and Application* 11 (2): 2.

Vance, A., and M. Siponen. 2012. “IS security policy violations: a rational choice perspective.” *Journal of Organizational and End User Computing* 24 (1): 21-41.

Vance, A., M. Siponen, and S. Pahnila. 2012. “Motivating security compliance: insights from habit and protection motivation theory.” *Information & Management* 49: 190-198.

Verizon. Data Breach Investigations Report 2018. 11th ed. Accessed May 2018 from

https://www.verizonenterprise.com/resources/reports/rp\_DBIR\_2018\_Report\_en\_xg.pdf

Willison, R. 2002. *Opportunities for computer abuse: assessing a crime specific approach in the case of Barings bank*: *PhD thesis.* University of London.

Willison, R., and J. Backhouse. 2006. “Opportunities for computer crime: considering systems risk from a criminological perspective.” *European Journal of Information Systems* 15 (4): 403-414.

Willison, R. and Warkentin, M. 2013. “Beyond deterrence: An expanded view of employee computer abuse.” *MIS Quarterly* 37 (1): 1-20.

Wood, C. C. 1997. “Policies alone do not constitute a sufficient awareness effort.” *Computer Fraud & Security* 12: 14-19.

Wood, C. C., and W. W. Banks Jr. 1993. “Human error: an overlooked but significant information security problem.” *Computers and Security* 12 (1): 51-60.

Workman, M., W. H. Bommer, and D. Straub. 2008. “Security lapses and the omission of information security measures: a threat control model and empirical test.” *Computers in Human Behavior* 24 (6): 2799-2816.