REFERENCES

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019, May). Information security: A review of information security issues and Techniques. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). IEEE.

Alnatheer, M.A. (2014). A Conceptual Model to Understand Information Security Culture, *Int. J. Soc. Sci. Hum. 4*, pp. 104–107.

Alnatheer, M. & K. Nelson. (2009). Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. *Australian Information Security Management Conference*. pp. 6–17.

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of advances in information technology*, *3*(3), 176-183.

Antonio, P. & L. Labuschangne. (2012). "A Conceptual Model for Digital Forensic Readiness". *Proceedings of the 11th Information Security for South Africa (ISSA)*, pp. 1–8.

Anuar, N.B., S. Furnell, M. Papadaki & N. Clarke. (2011). "A Risk Index Model for Security Incident Prioritisation". *Proceedings of the 9th Australian Information Security Management Conference*, pp. 24–39.

Anuar, N.B., M. Papadaki, S. Furnell., & N. Clarke. (2010). "An Investigation and Survey of Response Options for Intrusion Response Systems (IRSs)". *Proceedings of the 9th Information Security for South Africa (ISSA)*, pp. 1–8.

Arcy, J. D., A. Hovav, D. Galletta. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, *Inf. Syst. Res. 20*, pp. 79–98.

Arora A., D. Hall, C.A Pinto, D. Ramsey, R. Telang. (2004). Measuring the Risk-Based Value of IT Security Solutions, *IT Prof. 6*, pp. 35–42.

Babbie, E. (2017). *Fundamentals of Social Research*. Scarborough, ON: Nelson Thomson Learning.

BAE Systems Detica 2012 (2014). botCloud - An Emerging Platform for Cyber-Attacks. Retrived from http://baesystemsdetica.blogspot.com.au. Accessed on 18th June 2014.

Balduzzi, M. Zaddach, J. Balzarotti & S. Loureiro. (2012). "A Security Analysis of Amazon's Elastic Compute Cloud service". *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, pp. 1427–1434.

Bandura, A. (1977). Self-Efficacy: Toward a Unifying Theory of Behavioral Change, *Psychological Review*, vol. 84, no. 2, pp. 191–215.

Bang, J., C. Lee, S. Lee, & K. Lee. (2013). Damaged Backup Data Recovery Method for Windows Mobile, *The Journal of Supercomputing, vol. 66, no. 2*, pp. 875–887.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9).

Barske, D., A. Stander, & J. Jordaan. (2010). "A Digital Forensic Readiness Framework for South African SME's*". Proceedings of the 9th Information Security for South Africa*, pp. 1–6.

Bartock, M. et al. 2016. "Guide for Cybersecurity Event Recovery". *NIST Special Publication 800-184*. December.

Bashir, M.N., J.P. Kesan, C.M. Hayes & R. Zielinski. (2011). "Privacy in the Cloud: Going Beyond the Contractarian Paradigm*". Proceedings of the 2011 Workshop on Governance of Technology, Information, and Policies*, pp. 21–27.

Baskerville, R. (1991). Risk Analysis as a Source of Professional Knowledge. *Computers & Security*, 10(8), pp.749–764.

Baskerville, R. (1991). Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security. *European Journal of Information Systems*, *1*(2), 121-130.

Baskerville, R., P. Spagnoletti, & J. Kim. (2014). Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response, *Information & Management*, vol. 51, no. 1, pp. 138–151.

Bagozzi, R.P. and Y. Yi, 1988. On the evaluation of structural equation models. Journal of the Academy of Marketing Science, 16(1): 74-94.

Beebe, N.L. & J.G. Clark. (2005). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process, *Digital Investigation*, vol. 2, no. 2, pp. 147–167.

Bentler, P. M. (1990). Comparative fit indices in structural models. Psychological Bulletin, 107, 238–246.

Bentler, P.M. & Bonett, D.G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. Psychological Bulletin. 88: 588-606.

Berita Harian (2015). Lebih 60 Laman Web Agensi Kerajaan Kena Godam. Retrived from https://www.bharian.com.my/bhplus-old/2015/05/53333/lebih-60-laman-web-agensi-kerajaan-kena-godam. Accessed on 7 May 2015.

Bhilare, D.S., A.K. Ramani, & S. Tanwani. (2010). An Architecture For a Distributed Collaborative Inter University Incident Handling Mechanism, *International Journal of Computer and Internet Security*, vol. 2, no. 1, pp. 29–39.

Bing, S., W. Hai-Feng, & C. Ling. (2012). "Study of Network Security Situation in Honeynet". *Proceedings of 2012 International Conference on Modelling, Identification and Control*, Shanghai, pp. 519–523.

Birk, D. & C. Wegener. (2011). "Technical Issues of Forensic Investigations in Cloud Computing Environments". *Proceedings of the 6th IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 1–10.

Blank, R. & P. Gallagher. (2012). *NIST SP 800-30: Guide for Conducting Risk Assessments*, Gaithersburg, Tech. Rep.

Böhme, R. (2010). Security Metrics and Security Investment Models, *Advances in Information and Computer Security*, Springer Berlin Heidelberg, pp. 10–24.

Böhme, R., & Moore, T. (2016). The "iterated weakest link" model of adaptive security investment. *Journal of Information Security*, *7*(02), 81.

Böhme, R., Laube, S., & Riek, M. (2019). A fundamental approach to cyber risk analysis. *Variance*, *12*(2), 161-185.

Bojanc, R. (2012). A Quantitative Model for Information-Security Risk Management, *Engineering Management Journal*, vol. 25, no. 2, pp. 25–37.

Bojanc, R., & B. Jerman-Blažič. (2012). A Quantitative Model for Information-Security Risk Management. *Engineering management journal*, *25*(2), 25-37.

Bojanc, R., B. Jerman-Blažič & M. Tekavčič. (2013). Managing the Investment in Information Security Technology by Use of a Quantitative Modeling, *Information Processing & Management*, vol. 48, no. 6, pp. 1031–1052.

Bollen, K. A., and Jackman, R. A. 1990. Regression diagnostics: an expository treatment of outliers and influential cases. In Modern methods of data analysis, eds. J. Fox and J. S. Long, pp. 257–291. Newbury Park, CA: Sage.

Bollen, K.A. (1989). A new incremental fit index for general structural equation models. Sociological Methods and Research 17: 303-316

Boltz, D., & B. Westbrook. (1999). *U.S. Patent No. 5,943,620*. Washington, DC: U.S. Patent and Trademark Office.

Boltz, J. (1999). *Informational Security Risk Assessment: Practices of Leading Organizations.* DIANE Publishing.

Bozkus, K. S. and Caliyurt, K. (2018). "Cyber security assurance process from the internal audit perspective", *Managerial Auditing Journal*, Vol. 33 No. 4, pp. 360-376.

Bourgeois, D. (2014). *Information Systems for Business and Beyond.* Montreal. Pressbooks.

Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

Braber F.D., I. Hogganvik, M.S Lund, K. Stølen., F. Vraalsen. (2007). Model-Based Security Analysis in Seven Steps - A Guided Tour to the CORAS Method. *BT Technology Journal*, 25(1), pp.101–117.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime prevention: Theory and applications*. Springer Nature.

Briney, A. (2000). Security focused. *Information Security*, 40-68.

British Standards Institution (2007). *BIP 0107:2008 Foundations of It Service Management Based On Itil V3*, UK.

Brown, T. A. (2006) *Confirmatory Factor Analysis for Applied Research*, The Guilford Press: New York and London.

Bugcrowd (2015). BUGCROWD. Retrived from https://bugcrowd.com. Accessed on 1st May 2015.

Butian (2015). 360. Retrived from http://loudong.360.cn. Accessed on 1st May 2015.

Buyya, R., C. Vecchiola, & S.T. Selvi. (2013). *Cloud computing architecture*, in *Mastering Cloud Computing: Technologies and Applications Programming*, Morgan Kaufmann, pp. 111–140.

Byrne, B. M. (2010). Structural Equation Modelling with AMOS: basic concepts, applications, and programming (2nd ed.). New York: Taylor and Francis Group, LLC.

Cavusoglu, H., Phan, T. Q., Cavusoglu, H., & Airoldi, E. M. (2016). Assessing the impact of granular privacy controls on content sharing and disclosure on Facebook. *Information Systems Research*, *27*(4), 848-879.

Chadwick, D.W. & Hibbert M. (2013). "Towards Automated Trust Establishment in Federated Identity Management". IFIPTM 2013, IFIP AICT, vol. 401 (2013), pp. 33-48.

Chang S.L, S.Y. Hung, D.C. Yeng & P.J. Lee. (2010). Critical Factors of ERP Adoption for Small- and Medium- Sized Enterprises: An Empirical Study. *Journal of Global Information Management* 18(3):82-106.

Chen Y., D.L Nazareth., K. W. Wen. (2010). "Research in Information Security: A Literature Review Using a Multidimensional Framework". *Proceedings of the Thirty-Ninth Annual Western Decision Sciences Institute Conference (WDSI 2010)*, Lake Tahoe, NV, 2010, pp. 3681–3687.

Child, J. (2018). Information technology and organization. In Innovation and Management (pp. 255-302). De Gruyter.

Chong, E. E., Nazim, A., & Ahmad, S. B. (2014). A comparison between individual confirmatory factor analysis and pooled confirmatory factor analysis: An analysis of library service quality, a case study at a public university in Terengganu. International Journal of Engineering Science and Innovative Technology, 3(1), 110-116

Chua, Y.P. (2006). *Asas Statistik Penyelidikan. Buku 2*. Kuala Lumpur: Mc Graw Hill.

Comrey, A.L. and Lee, H.B. (1992), A First Course in Factor Analysis, 2nd ed., Lawrence Erlbaum Associates, Hillsdale, NJ.

Conner, B., T. Noonan & R.W Holleyman. (2003). Information Security Governance: Toward a Framework for Action. *Business Software Alliance BSA*. pp. 1–11.

Conway, J. M., & A. I. Huffcutt. (2003). A Review and Evaluation of Exploratory Factor Analysis Practices in Organizational Research. *Organizational research methods*, *6*(2), 147-168.

Cooper, R.B., (1983). "Decision production-A step toward a theory of managerial Information Requirements". *Fourth International Conference on Information Systems*. pp. 215–268.

Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of applied psychology*, *78*(1), 98.

Craig, P., M. Caldeira, J. Ward. (2011). Organizational Information Systems Competences in Small and Medium-Sized Enterprises. *Information & Management*. Volume 48, Issue 8, Pages 353-363.

Creswell, J. W., & J. D. Creswell. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Cybersecurity Malaysia (2021). Cybersecurity Malaysia. Statistics. Retrived from https://www.mycert.org.my/statistics. Accessed on 7th January 2021.

Dacosta, I., Chakradeo, S., Ahamad, M., & Traynor, P. (2012). One-time cookies: Preventing session hijacking attacks with stateless authentication tokens. *ACM Transactions on Internet Technology (TOIT)*, *12*(1), 1-24.

Daigle, A. (2020). Social media and professional boundaries in undergraduate nursing students. *Journal of Professional Nursing*, *36*(2), 20-23.

Drost, E. A. (2011). Validity and Reliability in Social Science Research. *Education Research and Perspectives, 38(1),* pp 105-123.

Ebad, S. A. (2020). Healthcare software design and implementation—A project failure case. *Software: Practice and Experience*, *50*(7), 1258-1276.

Eckel, M., & Laffey, T. (2020). Ensuring the integrity and security of network equipment is critical in the fight against cyber attacks. *Network Security*, *2020*(9), 18-19.

Edwards, P. N., Jackson, S. J., Bowker, G. C., & Knobel, C. P. (2007). Understanding infrastructure: Dynamics, tensions, and design. Ann Arbor: Deep Blue.

Ernst, Young, (2012). Fighting to close the gap. Retrieved from http://www.ey.com/Publication/vwLUAssets/Fighting to close the gap: 2012 Global Information Security Survey/$FILE/2012 Global Information Security Survey Fighting to close the gap.pdf on Ernst & Young's 2012 Global Information Security Survey

Esther, C. (2009). *Developing a best Practice Framework for Implementing Public Private Partnership (PPP) in Hong Kong*. (Ph.D. Thesis). Queensland University of Technology.

Field, A. (2009). Discovering statistics using SPSS: (and sex and drugs and rock 'n' roll) (3rd ed.). Thousand Oaks, CA: Sage publications Inc.

Fonseca J., M. Vieira & H. Madeira. (2013). Evaluation of Web Security Mechanisms using Vulnerability and Attack Injection, *IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99*, pp. 1-1.

Forman, C., Ghose, A., & Wiesenfeld, B. (2008). Examining the relationship between reviews and sales: The role of reviewer identity disclosure in electronic markets. Information Systems Research, 19(3), 291-313. doi 10.1287/isre.1080.0193.

Fornell, C. and Larcker, D. 1981. Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18: 39–50.

Franceschini, F., M. Galetto, & P. Cecconi. (2006). A Worldwide Analysis of ISO 9000 Standard Diffusion Considerations and Future Development. *Benchmarking: An International Journal*, 13(4), pp.523–541.

Garson, G. D. (2012). Testing Statistical Assumption, Blue Book series. Statistical Associates Publishing. Retrieved September 15, 2020, from: www.statisticalassociates.com/assumptions.pdf

Gary, S., G. Alice and F. Alexis. (2002). *Risk Management Guide for Information Technology Systems*. NIST Special Publication 800-30, July, Falls Church, VA.

Greenbaum, J., & Kyng, M. (Eds.). (2020). *Design at work: Cooperative design of computer systems*. CRC Press.

Ghozali, I. (2013). *Applications Multivariate Analysis with SPSS Program*, Diponegoro Publishing's, Semarang

Gritzalis D., S. Furnell & M. Theoharidou. (2012). A Response Strategy Model for Intrusion Response Systems, *Information Security and Privacy Research*, Springer Berlin Heidelberg, pp. 573–578.

Guha, B., and B. Mukherjee. (1997). Network security via reverse engineering of TCP code: vulnerability analysis and proposed solutions. *Network, IEEE 11*, *4*, pp. 40–48.

Guo K.H., Y. Yuan. (2012). The effects of multilevel sanctions on information security violations: a mediating model, *Inf. Manage. 49*, pp. 320–326.

HackerOne (2015). HackerOne. Retrived from https://www.hackerone.com/. Accessed on 1st May 2015.

Hadlington, L., & Chivers, S. (2020). Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors. *Policing: A Journal of Policy and Practice*, *14*(2), 479-492.

Hair, Jr. J. F., A. H. Money, P. Samouel, & M. Page. (2007). *Research Methods for Business*. Chichester: John Wiley and Son Ltd.

Hair, J. F., Jr., Anderson, R. E., Tatham, R. L. and Black, W. C. (2014) Multivariate Data Analysis, 7th ed, Pearson Education Limited, Esses.

Hair, J.F., Hult, G.T.M., Ringle, C., Sarstedt, M., (2017). A Primeron Partial Least Squares Structural Equation Modeling (PLS-SEM), seconded. SAGE, London: Thousand Oaks

Haes, S. D., T. Huygh, A. Joshi. (2017). Exploring the Contemporary State of Information Technology Governance Transparency in Belgian Firms. *Information Systems Management* 34:1, pages 20-37.

Hall, T., Beecham, S., Bowes, D., Gray, D., & Counsell, S. (2011). A systematic literature review on fault prediction performance in software engineering. *IEEE Transactions on Software Engineering*, *38*(6), 1276-1304.

Hanseth, O., & Lundberg, N. (2001). Designing work oriented infrastructures. *Computer Supported Cooperative Work (CSCW)*, *10*(3), 347-372.

Henderson & Kyng, M (eds.) (1992). Design at Work: Cooperative Design of Computer Systems, Lawrence Erlbaum Publishers

Henn, M., M. Weinstein, & N. Foard. (2016). *A Short Introduction to Social Research*. London: Sage.

Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards changes in information security education. *Journal of Information Technology Education: Research*, *5*(1), 221-233.

Héroux S. & Fortin. (2018). The Moderating Role Of IT-Business Alignment in The Relationship Between IT Governance, IT Competence, and Innovation. *Information Systems Management* 35:2, pages 98-123

Hertzog, M.A. (2008) Consideration in Determining Sample Size for Pilot Study. *Research in Nursing and Health*, *31(2)*, pp. 180-191.

Hock, M. and Ringle, C.M. (2006), "Strategic networks in the software industry: an empirical analysis of the value continuum", IFSAM VIIIth World Congress, Vol. 28, Berlin, pp. 2010-2016.

Holmes-Smith, P. (2006). School socio-economic density and its effect on school performance. http://www.curriculum.edu.au/verve/_resources/SES_Report.pdf

Höne, K., & Eloff, J. H. P. (2002). What makes an effective information security policy? *Network security*, *2002*(6), 14-16.

Hovav A., 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. *Inf. Manage. 49*, pp. 99–110.

Howitt, D. (2010). *Introduction to qualitative methods in psychology*. Prentice Hall New Jersey: NJ.

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling, 6(1), 1-55.

Iacob, M. E., L. O. Meertens, H. Jonkers, D. A. Quartel, L. J. Nieuwenhuis & M. J. Van Sinderen. (2014). From enterprise architecture to business models and back. *Software & Systems Modeling*, *13*(3), 1059-1083.

Iacob, V.S. (2014). Risk Management and Evaluation and Qualitative Method within the Projects. *Ecoforum Journal*, 3(1), 10.

Imenda, S., (2014). Is There a Conceptual Difference between Theoretical and Conceptual Frameworks? *Journal of Social Sciences*, 38(2), pp.185–195.

INFOSEC Business Advisory Group (1993), The IBAG Framework for Commercial IT Security. Frankfurt. version 2.0.

International Standard ISO/IEC. (2014). Information Technology Security Techniques Information Security Management Systems Overview and Vocabulary, ISO/IEC 27000:2014(E).

ISO/IEC 27005 (2008). Information Technology – Security Techniques – Information Security Risk Management, International Organization for Standardization, Geneva.

Ivano B. (2019). The Least Secure Places in the Universe? A Systematic Literature Review on Information Security Management in Higher Education. *Computers & Security*. Volume 86, Pages 350-357,

Jaeger, J. (2013). Human error, not hackers, cause most data breaches. Compliance Week, 10(110), 56–57.

Jang-Jaccard, J. & Nepal, S. (2014). A Survey of Emerging Threats in Cybersecurity. *Journal of Computer and System Sciences*. Volume 80, Issue 5, 2014, Pages 973- 993.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework. *MIS quarterly*, *39*(1), 113-134.

Jourdan, Z. et al. (2010). An Investigation of Organizational Information Security Risk Analysis. *Journal of Service Science*, 3(2), pp.33–42.

Julious, S.A. (2008). Sample Size of 12 per Group Rule of Thumb for a Pilot Study. *Pharmaceutical Statistics, 4(4)*, pp. 287-291.

Jun S., A. Punit & S. Kai. (2011). The More Secure the Better? A Study of Information Security Readiness. *Journal of Industrial Management & Data Systems, vol. 111 no. 4*, 570-588.

Karasti, H., Baker, K. S., & Millerand, F. (2010). Infrastructure time: Long-term matters in collaborative development. *Computer Supported Cooperative Work (CSCW)*, *19*(3-4), 377-415.

Karim, M., Leemans, K., Akester, M., & Phillips, M. (2020). Performance of emergent aquaculture technologies in Myanmar; challenges and opportunities. *Aquaculture*, *519*, 734875.

Kheir, N., H. Debar, C.N. Boulahia, F. Cuppens & J. Viinikka. (2009). "Cost Evaluation for Intrusion Response Using Dependency Graphs". *Proceedings of the 1st IFIP International Conference on Network and Service Security*, pp. 1–6.

Khidzir, N. Z., Mat Daud, K. A., Ismail, A. R., Ghani, A., Affendi, M. S., Ibrahim, M., & Hery, A. (2018). Information security requirement: The relationship between cybersecurity risk confidentiality, integrity and availability in digital social media. In *Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016)* (pp. 229-237). Springer, Singapore.

Khorshed, T., Ali, ABMS & S.A. Wasimi. (2012). A Survey on Gaps, Threat Remediation Challenges and Some Thoughts for Proactive Attack Detection in Cloud Computing, *Future Generation Computer Systems, vol. 28, no. 6*, pp. 833–851.

Khurana, H., J. Basney, M. Bakht, M. Freemon, V. Welch, & R. Butler. (2009). "Palantir: A Framework for Collaborative Incident Response and Investigation". *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, pp. 38–51.

Khurana, H., M. Hadley, N. Lu & D.A. Frincke. (2010). Smart-Grid Security Issues, *IEEE Security & Privacy*, vol. 1, no. Jan/Feb 2010, pp. 81–85.

Killcrece, G. (2003). *State of The Practice of Computer Security Incident Response Teams (CSIRTS)*, CMU/SEI, Pittsburgh.

Killcrece, G., K.P. Kossakowski, R. Ruefle, & M. Zajicek. (2003). *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*, CMU/SEI, Pittsburgh.

Kim A.C., S.M. Lee, D.H. Lee. (2012). Compliance Risk Assessment Measures of Financial Information Security Using System Dynamics, *Int. J. Secur. Appl. 6*, pp. 191–200.

Kim, S.H, S.S. Choi, H.S. Park & J.W. Choi. (2011). Advanced Bot Response Mechanism Based on DNS Sinkhole, *Information International Interdisciplinary Journal*, vol. 14, no. 7, pp. 2499–2521.

Klein, G., H. Rogge, F. Schneider, J. Toelle, M. Jahnke, & S. Karsch. (2010). "Response Initiation in Distributed Intrusion Response Systems for Tactical MANETs". *Proceedings of the 2010 European Conference on Computer Network Defense*, pp. 55– 62.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. International Journal of e-Collaboration (ijec), 11(4), 1-10.

Kohn, M.D., M.M. Eloff & J.H.P. Eloff. (2013). Integrated Digital Forensic Process Model, *Computers & Security*, vol. 38, no. 2013, pp. 103–115.

Koivunen, E. (2012). Why Wasn ‖T I Notified? Information Security Incident Reporting Demystified. *Information Security Technology for Application*, Springer Berlin Heidelberg, pp. 55–70.

Kostina, A., N. Miloslavskaya & A. Tolstoy. (2009). "Information Security Incident Management Process". *Proceedings of the 2nd International Conference on Security of Information and Networks - SIN '09*, p. 93.

Kozlovszky, M., L. Kovacs, M. Torocsik, G. Windisch, S. Acs, D. Prem, G. Eigner, P. Sas, T. Schubert & V. Póserné. (2013). "Cloud Security Monitoring and Vulnerability Management". *Proceedings of the 17th IEEE International Conference on Intelligent Engineering Systems*, no. 70, pp. 265–269.

Krejcie, R. V. & D. W. Morgan. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*. *30*(3), 607-610.

Kulikova, O., R. Heil, J. van den Berg & W. Pieters. (2012). "Cyber Crisis Management: A Decision-Support Framework for Disclosing Security Incident Information". *Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, pp. 103–112.

Kumar, R., & Bhatia, M. P. S. (2020, October). A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability. In *2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON)* (pp. 334-337). IEEE.

Kundu, A. & S.K. Ghosh. (2014). Game Theoretic Attack Response Framework for Enterprise Networks, in *Distributed Computing and Internet Technology*, Springer International Publishing, pp. 263–274.

Kurowski, S. & S. Frings. (2011). "Computational Documentation of IT Incidents as Support for Forensic Operations". *Proceedings of the 6th International Conference on IT Security Incident Management and IT Forensics*, pp. 37–47.

Landwehr C.E. (1981). *Formal Models for Computer Security*, ACM Comput. Surv. 13, pp. 247–278.

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM*, *51*(3), 71-76.

Laudon K.C and J.P. Laudon. (2012). *Management Information System: Managing theDigital Firm*. New Jersey. Prentice Hall.

Lee, S.H., 2006. *Constructing Effective Questionnaires*, Hoboken, NJ: Pfeiffer Wiley.

Lee, Y.W. et al. (2002). AIMQ: A Methodology for Information Quality Assessment. *Information & Management*, 40(2), pp.133–146.

Leszczyna, R. (2019). Cost of cybersecurity management. In *Cybersecurity in the Electricity Sector* (pp. 127-147). Springer, Cham.

Lestari, C. P. (2010). Factor Analysis about Exclusive Breastfeeding Achievement Level among Mothers Who Provide Breastmilk to Their Children. *Jurnal Ners*, *5*(1), 55-61.

Line, M. B., & Albrechtsen, E. (2016). Examining the suitability of industrial safety management approaches for information security incident management. *Information & Computer Security*.

Livingstone, S., Stoilova, M., & Nandagiri, R. (2020). Data and privacy literacy: The role of the school in educating children in a datafied society. *The handbook of media education research*, 413-425.

Lyu, M. R., & Lau, L. K. (2000, October). Firewall security: Policies, testing and performance evaluation. In *Proceedings 24th Annual International Computer Software and Applications Conference. COMPSAC2000* (pp. 116-121). IEEE.

Maiyaki, A. A. & S. M. M. Sany. (2011). Determinants of Consumer Behavioural Responses: A Pilot Study. *International Business Research, (4)1*, pp. 193-197.

Malik, M. S. M. M. S. (2019). Cyber Security-Incident Response and Management. *International Journal for Electronic Crime Investigation*, *3*(3), 6-6.

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32-44.

Marsh, H.W., & Hocevar, D. (1985). Application of confirmatory factor analysis to the study of self-concept: First- and higher order factor models and their invariance across groups. Psychological Bulletin, 97, 362-582.

Marshall C, G.B. Rossman (2016). *Designing Qualitative Research*. Fifth edition. Sage Publications, Thousand Oaks CA.

May J. (2008). "Analyzing the Socio-Organizational Constructs for IS Security within Organizations". *Proceedings of the 11th IFIP TC Working Conference on Information Security Management*. pp. 103–117.

Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E., & Wieringa, R. (2019). An integrated conceptual model for information system security risk

management supported by enterprise architecture management. *Software & Systems Modeling*, *18*(3), 2285-2312.

Mayer, N., & Feltus, C. (2017). Evaluation of the risk and security overlay of archimate to model information system security risks. In *2017 IEEE 21st International Enterprise Distributed Object Computing Workshop (EDOCW)* (pp. 106-116). IEEE.

Melara C., J.M. Sarriegui, J.J. Gonzalez, A. Sawicka, D.L. Cooke (2003). *A System Dynamics Model of an Insider Attack on an Information System. From Modeling to Managing Security: A System Dynamics Approach.* Norwegian Academic Press, Kristiansand, Norway, 2003, pp. 9–36.

Menard, S. (1995). Applied logistic regression analysis. Sage university paper series on quantitative applications in the social sciences, 07-106. Thousand Oaks, CA: Sage.

Mirtsch, M., Kinne, J., & Blind, K. (2020). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE Transactions on Engineering Management*, 68(1), 87-100.

Mishra, S., D. J. Caputo, G. J. Leone, F. G. Kohun & P. J. Draus. (2014). The Role of Awareness and Communications in Information Security Management: A Health Care Information Systems Perspective. *International Journal of Management & Information Systems (IJMIS)*, *18*(2), 139-148.

Morrison, P., Moye, D., Pandita, R., & Williams, L. (2018). Mapping the field of software life cycle security metrics. *Information and Software Technology*, *102*, 146-159.

Mouw, E., G. van't Noordende, B. Louter & S. D. Olabarriaga. (2013). A Model-based Information Security Risk Assessment Method for Science Gateways. *IWSG*, *42*, 46.

Nazim, A., & Ahmad, S. (2013). Assessing the unidimensionality, reliability, validity and fitness of influential factors of 8th grade student's mathematics achievement in Malaysia'. International Journal of Advance Research, 1(2), 1-7.

Norton, R. 9 May 2016. 2016 Norton Cybersecurity Insight Report. *Norton*. https://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/2016-Norton-Cyber-Security-Insights Report.pdf

Nwankpa J. K. & Datta P. (2017). Balancing Exploration and Exploitation of IT Resources: The Influence of Digital Business Intensity on Perceived Organizational Performance. *European Journal of Information Systems*. 26:5, pages 469-488.

Nwankwo, M. I. (2020). *IT Security Managers' Strategies for Mitigating Data Breaches in Texas School Districts* (Doctoral dissertation, Walden University).

Onwubiko, C. (2009). A security audit framework for security management in the enterprise. In *International Conference on Global Security, Safety, and Sustainability* (pp. 9-17). Springer, Berlin, Heidelberg.

Pallant, J. (2010). *SPSS Survival Manual*. 4th ed. Australia: Allen & Unwin Book Publishers.

Park S.H., S.M. Lee, S.N. Yoon, S.J. Yeon. (2008). A Dynamic Manpower Forecasting Model for the Information Security Industry. *Ind. Manage. Data Syst. 108*, pp. 368–384.

Pfleeger, S. L., & Cunningham, R. K. (2010). Why Measuring Security Is Hard. IEEE Security & Privacy Magazine, 8(4), 46.

Phillips, J. N. (2013). How are Nonprofit Organizations Influenced to Create and Adopt Information Security Policies? *Issues in Information Systems*, *14*(2).

Podsakoff PM, MacKenzie SB, Lee J-Y, Podsakoff NP. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. J. Appl. Psychol. 88:879–903

Potlapally, N. (2011). Hardware security in practice: Challenges and opportunities. In *2011 IEEE International Symposium on Hardware-Oriented Security and Trust* (pp. 93-98). IEEE.

Pereira, T., & Santos, H. (2010). A security audit framework to manage Information system security. In *International Conference on Global Security, Safety, and Sustainability* (pp. 9-18). Springer, Berlin, Heidelberg.

Radianti J., J.J. Gonzalez. (2006). Toward a Dynamic Modeling of the Vulnerability Black Market. *The Workshop on the Economics of Securing the Information Infrastructure (WESII)*. Washington, DC, p. 19.

Rahman, S. (2014). *Introduction to E-Commerce Technology in Business*. Munich, GRIN Verlag.

Raghunathan, S. (1999). Impact of Information Quality and Decision-Maker Quality on decision quality: A Theoretical Model and Simulation Analysis. *Decision Support Systems,* 26(4), pp.275–286.

Ribes, D., & Finholt, T. A. (2009). The long now of technology infrastructure: articulating tensions in development. Journal of the Association for Information Systems (JAIS), Special Issue on e-Infrastructure, vol. 10, no. 5, pp. 375–398.

Richardson, H. A. (2015). Marker Variable Choice, Reporting, and Interpretation in the Detection of Common Method Variance: A Review and Demonstration. *Organizational Research Methods, 18*(3), 473-511.

Rostami, E., Karlsson, F., & Gao, S. (2020). Requirements for computerized tools to design information security policies. *computers & security*, *99*, 102063.

Rubenstein, S., & Francis, T. (2008). Are your medical records at risk? Wall Street Journal—Eastern Edition, 251(100), D1–D2.

Rubin, R. B., Palmgreen, P., & Sypher, H. E. (2020). Revised Self-Disclosure Scale. In *Communication Research Measures* (pp. 322-326). Routledge.

Salkind, N. J. (Ed.). (2010). *Encyclopedia of Research Design (Vol. 1)*. Sage.: New Jersey.

Salkind, N.J. (2013). *Exploring Research* (8th edn.) Salt River, NJ: Pearson Publications.

Sarriegi J.M., J. Santos, J.M. Torres, D. Imizcoz, E. Egozcue, D. Liberal. (2008). Modeling and Simulating Information Security Management. *Critical Information Infrastructures Security*, Springer-Verlag, Berlin, pp. 327–336.

Segars, A. H. & V. Grover. (1993). Re-Examining Perceived Ease of Use and Usefulness: A Confirmatory Factor Analysis. *MIS Quarterly*, 517-525.

Sehgal N.K. (2011). Information Security and Cloud Computing. *IETE Technical Review, Vol 28, Issue 4*, pp. 279-291.

Sehgal, N. K., P. C. P. Bhatt & J. M. Acken. (2011). Cloud Computing Pyramid. *Cloud Computing with Security* (pp. 49-59). Springer, Cham.

Sekaran U. (2010). *Research Methods for Business, a Skill Building Approach*, 4th Edition. Carbondale: John Wiley and sons.

Sekaran, U. & R. Bougie. (2016). *Research Methods for Business: A Skill Building Approach*. John Wiley & Sons.

Sekaran, U. (2003). Research methods for business: A skill building approach (4th ed.). New York, NY: John Wiley & Sons, Inc.

Sendi, A.S. et al. (2010). "FEMRA: Fuzzy Expert Model for Risk Assessment". *Internet Monitoring and Protection (ICIMP), 2010 Fifth International Conference on IEEE, 2010.* pp. 48–53.

Sensuse, D.I., S. Rohajawati, & P. Anggia. (2014). "Models and Frameworks of Knowledge Management: A Literature Review". *International Conference in Information Science, Electronics and Electrical Engineering (ISEEE) -IEEE*. pp. 1166–1170.

Shahibi M. S. and S.K.W. Fakeh. (2011). Security Factor and Trust in E-Commerce Transactions, *Australian Journal of Basic and Applied Sciences, vol. 5*, pp. 2028-2033.

Shedden, P., R. Scheepers, W. Smith & A. Ahmad. (2011). Incorporating a Knowledge Perspective into Security Risk Assessments. *Journal of Information and Knowledge Management Systems*, 41(2), pp.152–166.

Shedden, P., R. Scheepers, W. Smith & A. Ahmad. (2011). *Incorporating a Knowledge Perspective into Security Risk Assessments*. Vine.

Shedden, P., W. Smith & A. Ahmad. (2010). Information Security Risk Assessment: Towards a Business Practice Perspective. *Australian Information Security Management Conference*. pp. 119–130.

Simmonds A., P. Sandilands, L.V. Ekert. (2004). An Ontology for Network Security Attacks, *Applied Computing*, Springer, Berlin, 2004, pp. 317–323.

Singh, A. N., A. Picot, J. Kranz, M. P. Gupta & A. Ojha, (2013). Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. *Global Journal of Flexible Systems Management*, *14*(4), 225-239.

Singh, G. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications*, *67*(19).

Siponen M., R. Willison. (2009). Information Security Management Standards: Problems and Solutions, *Inf. Manage. 46*, pp. 267–270.

Siponen M.T. (2005). An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice. *Eur. J. Inf. Syst. 14*, pp. 303–315.

Siponen, M., M. A. Mahmood & S. Pahnila. (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study. *Information & management*, *51*(2), 217-224.

Skinner, V., K. Agho, T.L. White & J. Harris. (2007). The Development of a Tool to Stress Levels of Stress and Burnout. *Australian Journal of Advanced Nursing, 24(4)*, pp. 8-13.

Smith, C. L. & Brooks, D. J. (2013). Security Science, Butterworth-Heinemann, Oxford, UK.

Sobug (2015). Sobug. Retrived from https://sobug.com. Accessed on 1st May 2015.

Solms, R. (2005). Management of Risk in the Information Age. *Computers & Security*. *24*(1), 16-30.

Solms, S. P. (2005). A Responsibility Framework for Information Security. *Security Management, Integrity, and Internal Control in Information Systems.* 205-221.

Sophos (2016). Sophos Security Threat Report 2013. Sophos. Retrived from https://nakedsecurity.sophos.com/2012/12/04/sophos-security-threat-report. Accessed on 9th May 2016.

Spiezia, V. (2013). ICT Investments and Productivity. *OECD Journal: Economic Studies*, (1), 199-211.

Steiger, J. H. (2007). Understanding the limitations of global fit assessment in structural equation modeling. Personality and Individual differences, 42(5), 893-898.

Stoneburner G., A. Goguen and A. Feringa. (2002). *Computer Security. Risk Management Guide for Information Technology Systems - NIST*. Falls Church, VA – USA.

Straub D.W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, *1*(3). pp. 255–276.

Straub, D. W., W. D. Nance (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quart. 14(1)* pp. 45–60.

Straub, D. W., R. J. Welke (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quart. 22(4)* pp. *441–469*.

Sunyaev A., F. Tremmel, C. Mauro, J.M. Leimeister, H. Krcmar. (2009). "A Reclassification of IS Security Analysis Approaches". *Proceedings of the 15th Americas Conference on Information Systems (AMCIS 2009)*, San Francisco, CA, Paper 570.

Susanto, H., & Almunawar, M. N. (2018). *Information security management systems: A novel framework and software as a tool for compliance with information security standards*. Apple Academic Press.

Sveen F.O., J.M. Sarriegi, E. Rich, J.J. Gonzalez. (2007). Toward Viable Information Security Reporting Systems. *Inf. Manage. Comput. Secur. 15*, pp. 408–419.

Syalim A, Y. Hori, K. Sakurai. (2009). "Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide". *International Conference on Availability, Reliability and Security*. IEEE Computer Society, pp. 726–731.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior, 29*, 821–826.

Tan, T.C.C., A.B. Ruighaver & A. Ahmad. (2014). "Information Security Governance: When Compliance Becomes More Important than Security". *IFIP International Information Security Conference*. Springer Berlin Heidelberg, pp. 55–67.

Tavakol, M. & R. Dennick. (2011). Making Sense of Cronbach's Alpha. *International Journal of Medical Education, 2,* pp. 53-55.

Tehranipoor, M. & Wang C. (2012). *Introduction to Hardware Security and Trust.* Springer, Connecticut.

Trcek D. (2006). Security Models: Refocusing on the Human Factor. *Computer 39*, pp. 103–104.

Trcek D. (2008). U.K. Using System Dynamics for Managing Risks in Information Systems. *WSEAS Trans. Inf. Sci. Appl. 2*, pp. 175–180.

Thomson, M. E., & Von Solms, R. (1998). Information security awareness: educating your users effectively. *Information management & computer security*.

Tripathi A., Singh (2011). "Taxonomic Analysis of Classification Schemes in Vulnerability Databases". *Computer Sciences and Convergence Information Technology (ICCIT), 2011 6th International Conference on. IEEE*. p. 686–91.

Tu Z., Yuan Y. (2014). "Critical Success Factors Analysis on Effective Information Security Management: A Literature Review". *20th Americas Conference on Information Systems (2014), pp. 1874-1886*

Tudosa, I., Picariello, F., Balestrieri, E., De Vito, L., & Lamonaca, F. (2019). Hardware security in IoT era: The role of measurements and instrumentation. In *2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4. 0&IoT)* (pp. 285-290). IEEE.

Turel O., P. Liu & C. Bart. (2017). Board-Level Information Technology Governance Effects on Organizational Performance: The Roles of Strategic Alignment and Authoritarian Governance Style. *Information Systems Management*, 34:2, 117-136

UNCTAD. (2019). Digital Economy Report 2019. United Nations Conference on Trade and Development.

US-CERT (2015). Common Vulnerabilities and Exposures (CVE). Retrived from https://cve.mitre.org. Accessed on 1st May 2015.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems, 29*(4), 263-290.

Vance A., M. Siponen, S. Pahnila. (2012). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. *Inf. Manage. 49*, pp. 190–198.

Verizon. (2014). Data Breach Investigations Report 2014.

Verizon. (2015). Data Breach Investigations Report 2015.

Verizon. (2016). Data Breach Investigations Report 2016.

Vivo, M.D., G. Vivo. (1998). Isern, Internet Security Attacks at the Basic Levels. *ACM SIGOPS Oper. Syst. Rev. 32*, pp. 4–15.

VulReport (2015). Vulreport. Retrived from https://vulreport.net. Accessed on 1st May 2015.

Wallerstein, I. (1998). Time and duration: The unexcluded middle, or reflections on Braudel and Prigogine. *Thesis Eleven*, *54*(1), 79-87.

Walliman, N. (2016). *Research Methods: The Basics*. Abingdon: Routledge.

Wang, S. L., Wang, J., Feng, C., & Pan, Z. P. (2016). Wireless network penetration testing and security auditing. In *ITM Web of Conferences* (Vol. 7, p. 03001). EDP Sciences.

Whitman M.E., H.J. Mattord. (2017). *Principles of Information Security, sixth ed.*, Course Technology, Boston, MA.

Whitman, M. E. (2018, August). Industry priorities for cybersecurity competencies. In *Journal of the Colloquium for Information Systems Security Education* (Vol. 6, No. 1, pp. 21-21).

Weisband, S., & Kiesler, S. (1996, April). Self disclosure on computer forms: Meta-analysis and implications. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 3-10).

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security.

Wooyun (2015). Wooyun. Retrived from http://www.wooyun.org. Accessed on 1st May 2015.

Yang S.C., Y.L. Wang. (2011). Insider Threat Analysis of Case Based System Dynamics. *Adv. Comput. 2*, pp. 1–17.

Yar, M. (2018). A failure to regulate? The demands and dilemmas of tackling illegal content and behaviour on social media. *International Journal of Cybersecurity Intelligence & Cybercrime*, *1*(1), 5-20.

Yegneswaran, V., P. Barford, & V. Paxson. (2005). "Using Honeynets for Internet Situational Awareness". *Proceedings of the 4th Workshop on Hot Topics in Networks (HotNets IV)*. pp. 17–22.

Yeniman, Y., Ebru Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small-and medium-sized enterprises: a case study from turkey. International Journal of Information Management, 31(4), 360–365

Yeung, F.Y. (2007). *Developing a Partnr Performance Index (PPI) for Construction Project – a Fuzzy Set Theory Approach*. Hong Kong Polytechnic University: Ph.D. Thesis.

Young, W. D. (1991). *Verifiable computer security and hardware: Issues*. Computational Logic, Incorporated.

Yu, X., L. Jiang, H. Shu, Q. Yin & T. Liu. (2009). A Process Model for Forensic Analysis of Symbian. *Advances in Software Engineering*, Springer Berlin Heidelberg, pp. 86– 93.

Yuill, J., F. Wu, J. Settle, F. Gong, R. Forno, M. Huang & J. Asbery. (2000). Intrusion-Detection for Incident-Response, Using a Military Battlefiled-Intelligence Process. *Computer Networks*, vol. 34, no. 4, pp. 671–697.

Yunos, Z., R. Ahmad & N.A Mohd Sabri. (2015). A Qualitative Analysis for Evaluating a Cyberterrorism Framework in Malaysia. *Information Security Journal: A Global Perspective*, vol. 24, no. 1-3, pp. 15–23.

Zainudin, A. (2012). Research Methodology and Data Analysis 5th Edition. Shah Alam: University Technology MARA Publication Centre (UiTM Press).

Zambon, E., S. Etalle, R.J. Wieringa & P. Hartel. (2010). Model-Based Qualitative Risk Assessment for Availability of IT infrastructures. *Software & Systems Modeling*, vol. 10, no. 4, pp. 553–580.

Zan, X., F. Gao, J. Han, X. Liu & J. Zhou. (2010). "NAIR: A Novel Automated Intrusion Response System Based on Decision Making Approach". *Proceedings of the 5th IEEE International Conference on Information and Automation*, pp. 543–548.

Zeng, J., X. Feng, D. Wang & L. Fang. (2014). Implemention of Cyber Security Situation Awareness Based On Knowledge Discovery With Trusted Computer. *Web Technologies and Applications*. Springer.

Zhang, G., Y. Yang & X. Mao. (2011). "Disaster Recovery Evaluation PROC Model Framework Based on Information Flow". *Proceedings of the 1st International Conference on Computer Science and Network Technology (ICCSNT)*, pp. 1841–1845.

Zhang, L. & W. Wang. (2011). "Constructions on Disaster Tolerant Backup System of Management Information System". *Proceedings of the 6th International Conference on Computer Science & Education (ICCSE)*. pp. 425–427.

Zhang, X., K. Liang & X. Zhang. (2012). "Research on the Recovery Strategy of Incremental-Data-Based Continuous Data Protection". *Proceedings of the 14th International Conference on Computer Science and Electronics Engineering*, pp. 498– 502.

Zhang, X., N. Wuwong, H. Li, & X. Zhang. (2010). "Information Security Risk Management Framework for the Cloud Computing Environments". *Proceedings of the 10th IEEE International Conference on Computer and Information Technology*, pp. 1328–1334.

Zhang, Q., Cho, J. H., Moore, T. J., & Chen, R. (2020). Vulnerability-Aware Resilient Networks: Software Diversity-based Network Adaptation. *IEEE Transactions on Network and Service Management*, *18*(3), 3154-3169.

Zhao, W. & G. White. (2014). "Designing a Formal Model Facilitating Collaborative Information Sharing for Community Cyber Security". *Proceedings of the 47th Hawaii International Conference on System Sciences*. pp. 1987–1996.

Zhou, M. & G. Yao. (2012). "Improved Cost-Sensitive Model of Intrusion Response System Based On Clustering*". Proceedings of the 2011 International Conference in Electrics, Communication and Automatic Control*. pp. 931–937.

Zielińska, E., W. Mazurczyk, & K. Szczypiorski. (2014). Trends in Steganography. *Communications of the ACM*, vol. 57, no. 3, pp. 86–95.

Zimmerman, S. & D. Glavach. (2011). Cyber Forensics in the Cloud. *IAnewsletter*, vol. 14, no. 1, pp. 4–7.

Zissis, D. & D. Lekkas. (2012). Addressing Cloud Computing Security Issues. *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592.

Zonouz, S. & P. Haghani. (2013). Cyber-Physical Security Metric Inference in Smart Grid Critical Infrastructures Based on System Administrator's Responsive Behavior. *Computers & Security*, vol. 39, pp. 190–200.

Zonouz, S. A., H. Khurana, W.H. Sanders & T.M. Yardley. (2014). RRE: A Game-Theoretic Intrusion Response and Recovery Engine. *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 395–406.