[8] P. Prince, “More Than Half of Enterprise Employees Receive No Security Training: Survey Finds,” security week, 2014. [Online]. Available:http://www.securityweek.com/more-half-enterprise-employees-receive-no-security-training-survey-finds. [Access Date: 01 May, 2015].

[9] The European Network and Information Security Agency (ENISA), “The new users ’ guide :How to raise information security awareness,” 2010.

[10] H. a Qudaih, M. a Bawazir, S. H. Usman, and J. Ibrahim, “Security Awareness in an Organization,” Persuas. Technol. Contrib. Towar. Enhanc. Inf. Secur. Aware. an Organ., vol. 10, no. 4, pp. 180–186, 2014.

[11] S. Furnell and K.-L. Thomson, “From culture to disobedience: Recognising the varying user acceptance of IT security,” Comput. Fraud Secur., vol. 2009, no. 2, pp. 5–10, Feb. 2009.

[12] S. Alfawaz, K. Nelson, and K. Mohannak, “Information security culture: A behaviour compliance conceptual framework,” in Conferences in Research and Practice in Information Technology Series, 2010, vol. 105, pp. 47–55.

[13] F. L. Greitzer, J. Strozer, S. Cohen, J. Bergey, J. Cowley, A. Moore, and D. Mundie, “Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies,” in 2014 47th Hawaii International Conference on System Sciences, 2014, pp. 2025–2034.

[14] B. Khan, K. S. Alghathbar, S. I. Nabi, and M. K. Khan, “Effectiveness of information security awareness methods based on psychological theories,” in African Journal of Business Management, 2011, vol. 5, no. 26, pp. 10862–10868.

[15] S. Furnell, “Malicious or misinformed? Exploring a contributor to the insider threat,” in Computer Fraud and Security, 2006, vol. 2006, pp. 8–12.

[16] C. Colwill, “Human factors in information security: The insider threat - Who can you trust these days?,” Inf. Secur. Tech. Rep., vol. 14, no. 4, pp. 186–196, 2009.

[17] G. Silowash, D. Cappelli, and A. Moore, “Common Sense Guide to Mitigating Insider Threats 4th Edition,” 2012.

[18] Global consulting firm Protiviti, “Bridging the Data Security Chasm,” 2014.

[19] I. Kirlappos, S. Parkin, and M. A. Sasse, “‘ Shadow Security ’ as a tool for the learning organization,” 2015, vol. 45, no. 1, pp. 29–37.

[20] I. Kirlappos, S. Parkin, and M. A. Sasse, “Learning from ‘Shadow Security’ : Why understanding non-compliant behaviors provides the basis for effective security,” 2014, no. February.

[21] A Da Veiga and J. Eloff, “A framework and assessment instrument for information security culture,” in Computers & Security, 2009.

[22] N. Badie and A. H. Lashkari, “A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP,” 2012, vol. 2, pp. 9331–9347.

[23] M. Alotaibi, S. Furnell, and N. Clarke, “Information Security Policies : A review of Challenges and Influencing Factors,” 2016.

[24] S. Pahnila, M. Siponen, A. Mahmood, P. O. Box, F.-Oulun, and E. M. Siponen, “Employees ’ Behavior towar ds IS Secur ity Policy Compliance University of Oulu , Department of Information Processing,” October, pp. 1–10, 2007.

[25] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information Security Policy Compliance: An Empiracal Study of Rationality-Based Beliefs and Information Security Awareness,” MIS Q., vol. 34, no. 3, pp. 523–548, 2010.

[26] K. Parsons, A. Mccormac, M. Butavicius, and L. Ferguson, “Human Factors and Information Security : Individual , Culture and Security Environment,” in Science And Technology, 2010, p. 45.

[27] M. Harris and S. Furnell, “Routes to security compliance: Be good or be shamed?,” Comput. Fraud Secur., vol. 2012, no. 12, pp. 12–20, 2012.

[28] L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai, “Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory,” Comput. Secur., vol. 39, no. PART B, pp. 447–459, 2013.

[29] P. Puhakainen and M. Siponen, “Research Article Improving Employees’ Compliance Through Information Systems Security Training :,” 2010, vol. 34, no. 4, pp. 757–778.

[30] G. Greene and J. D Arcy, “Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance,” in 5th Annual Symposium on Information Assurance, 2010, pp. 1–8.

[31] J. D’Arcy, A. Hovav, and D. Galletta, “User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach,” Inf. Syst. Res., vol. 20, no. 1, pp. 79–98, 2009.

[32] A. Yeo, M. Rahim, and Y. Ren, “Use of Persuasive technology to change end user’s IT security aware behavior: a pilot study,” in World Academy of Science, Engineering and Technology, 2008, vol. 2, no. 10, pp. 193–199.

[33] B. Fogg, “Persuasive computers: perspectives and research directions,” in … the SIGCHI conference on Human factors in computing …, 1998, vol. 98, no. April, pp. 225–232.

[34] M. Alotaibi, S. Furnell, and N. Clarke, “Towards dynamic adaption of user’s organisational information security behaviour,” in Australian Information Security Management Conference, 2015, vol. 2015, pp. 28–36