Kalpa Publications in Computing

Volume 12, 2019, Pages 85–94

Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019

Industry 4.0 Business Perspective: Fostering a Cyber Security Culture in a Culturally Diverse Workplace

Tapiwa Gundu[1], Mark Idi Maronga[2], and Duane Boucher[2]

[1] Sol Plaatje University, Kimberley, South Africa

[2] University of Fort Hare, East London, South Africa

tapiwa.gundu@spu.ac.za

Abstract

The rapid pace of technological developments of the fourth industrial revolution (Industry 4.0) increasingly leads to the need for cyber skills amongst the organizational workforce. However, some countries are lagging in the necessary skills required, so organizations need to access a diverse pool of employees for recruitment purposes. The establishment of culturally diverse workforces requires a more mindful approach to how they are managed in order to foster a cyber security culture in the workplace. Typically, culturally diverse workforces cause more cyber security breaches, threats, and incidents, because of inherent trust issues amongst culturally diverse employees. A literature review was conducted to identity relevant critical success factors to foster a cyber security culture for a culturally diverse workforce. The researchers identified n=668 articles from Google Scholar using three key phrases. These articles were then filtered for a ten-year range (2009-2019), which returned n=117. A review of the key phrases in these articles identified n=20 relevant articles. From these eight critical success factors were identified, which are discussed in brief and related to the Theory of Planned Behavior and Hofstede's Cultural Dimensions Theory. Suggestions of action items for each critical success factor are provided.

Keywords: Information Security Culture; Information Security Awareness; Cultural Diversity; 4IR; Cultural Dimensions; Fourth Industrial Revolution.

1 Introduction

The fourth industrial revolution (Industry 4.0 / 4IR) tsunami is upon us, with sweeping and overwhelming technological disruption occurring in areas such as additive manufacturing (3D printing),

artificial intelligence, biotechnology, cyber systems, nanotechnology, and robotics (Rojko, 2017). The development of these areas increasingly realizes smart systems to manage cities, factories, homes, farms, and energy grids, which assist in tackling problems by making information more readily accessible for real-time analytics and use. However, while 4IR promises personalized consumption patterns, efficient production and the creation of new employment opportunities, it also poses major challenges (socio-economic, demographic and geopolitical) that require proactive adaptation by business, employees and governments (Schwab, 2016). Least of which is the need for a better understanding of how cyber security is impacted in these entities as applied to the engagement of work.

As industries and stakeholders adjust to 4IR, occupations will evolve, cease to exist, or be created anew, with the development of different skillsets that are reliant on the adaptability of a global employment pool to engage with cyber–physical systems (Schwab, 2016). Where possible, skilled employees will migrate (physically or virtually) to complete a given job function for a specified period in a dynamic work environment (McKenzie, 2017).

When recruiting employees (physically and virtually) for 4IR associated innovations and opportunities, organizations will access a globally diverse employment pool that translates into an increasingly culturally diverse workforce. These employees will be expected and trusted to engage with the organization's cyber assets and data storage repositories, which increasingly are transacted over cloud-based network resources (Gundu, 2019; Gundu, 2013). However, not all prospective employees will present with a natural affinity to cybersecurity intent. These naïve employees have the potential to perpetuate behavior that subjects the organization to cybersecurity breaches and threats (AlHogail, 2015; Furnell, Alotaibi, & Esmael, 2019). Employee ignorance usually exposes an organization to a risk such as unauthorized access to cyber assets, which can ultimately lead to data theft and/or exploitation of information (confidentiality and privacy breaches) (Astakhova, 2014). Therefore, organizations need to understand the factors associated with a diverse culture when formalizing cyber security awareness and education amongst employees in order to facilitate a cyber security culture (CSC) (Nasir, Arshah, & Ab Hamid, 2017; Tang, Li, & Zhang, 2016). The intended CSC should shape employees' attitudes, and behaviors, such that they are motivated to behave securely to comply with the organization's information security policies (ISPs) (Gundu, Flowerday, & Renaud, 2019; Van Niekerk & Von Solms, 2005; Da Veiga & Martins, 2015).

The paper presents a concise discussion of the literature relevant to organizational culture. Thereafter, the Theory of Planned Behavior (TPB) and Hofstede's Cultural Dimensions Theory are introduced, as the theoretical precept for why individuals might behave as they do, given a cultural bias. The research design followed and proposed critical success factors. The discussion expands on the critical success factors in the context of CSC and cultural diversity.

2 Literature Review

In this section, we review the relevant literature which discusses the concept of Industry 4.0, its effects on employment trends, the effects of cultural diversity on the organization, ethnic perspectives linked to cultures and cyber security culture (CSC).

2.1 Industry 4.0

The term Industry 4.0 originated in Germany (Rojko, 2017), but is also recognized by other leading industrial nations, although referred to using different terminology. In the United States (US), it is known as "Connected Enterprise" and in the United Kingdom (UK) as the "Fourth Industrial Revolution". Industry 4.0 builds on three prior technological revolutions, namely: steam power (1st Industrial Revolution, circa 19th Century), electricity (2nd Industrial Revolution, circa beginning of 20th century), and computer era (3rd Industrial Revolution, circa end of the 20th century) (Morrar,

Arman, & Mousa, 2017; World Economic Forum, 2016). The pace and impact of Industry 4.0 is fueled by the high growth in the demand of information and communication technologies (ICTs) by business and their application to cyber-physical systems and information management, which is expected to residually impact on employment in converging societal sectors (Morrar, Arman, & Mousa, 2017).

2.2 Employment Trends

The debate on employment transformations caused by Industry 4.0 are from two schools of thought, those predicting numerous employment opportunities to surface and those predicting substantial loss of jobs (McKenzie, 2017). However, we view this as indicative to the skill set, region, type of industry, as well as various stakeholders' abilities to manage change in the short term. There is an obvious long term need for specialist cyber-related skills in certain job categories which means businesses are likely to encounter major recruitment challenges, as the current and future labor pool is nurtured to meet the skills needed (Schwab, 2016).

The question that needs debate in society is how businesses, governments and individuals will react to these challenges. Currently the responses vary, with businesses opting for reskilling and upskilling of their current workforce, while governments focus on reforming current basic education, and those individuals nearing the "shelf life" of their job skills, resorting to migrating to regions where their skill sets are still needed and of value (World Economic Forum, 2016). However, the major challenge faced is that although technology is changing exponentially, it is not possible to leapfrog the cyber-related skills shortage gap without waiting for the 4IR ready next generation workforce that is currently being prepared in schools and universities (Schwab, 2016). Part of the 4IR readiness needs to focus on inculcating the precepts of a cyber security culture in current and future employees.

2.3 Cultures

This section discusses ethnic and organizational culture and goes on to suggest that the ethnic culture of a workforce influences the organizational culture, which ultimately influencing the CSC, which is in itself a subset of organizational culture.

Ethnic culture refers to the ideas, customs, and social behavior of particular people (Mazur, 2010). Ethnic cultural diversity is categorized into primary, secondary, and tertiary dimensions. The primary dimension refers to the natural differences among employees that remain the same such as gender and geographic origin. The secondary dimension are those characteristics that change over time, such as the work experience, education and religion. The tertiary dimension focuses on the learnt organizational ethos and shared history such as beliefs, assumptions, attitudes, feelings, perceptions and values that manifest behavioral intentions as a core identity within employees (Dike, 2013; Mazur, 2010).

Employees' personal attitudes and behaviors are the result of their evolving development arising from their ethnic origins (Tang, Li, & Zhang, 2016). Employees feel included and respected in the workplace when there is acknowledgement of ethnic backgrounds within the organizational culture (Saxena, 2014).

Organizational culture is indicative of the sharing of a set of assumptions, beliefs and values, which govern how employees of an organization behave (Safa, et al., 2015). Subsequently, the formation of an organizational culture over time is a strong influencer and controlling factor of how employees act and perform daily organizational tasks (Hofstede, Hofstede, & Minkov, 2005). Organizational cultural diversity is addressed by infusing multiple cultures into a shared culture as opposed to superseding one culture over another. When ethnic minority employees encounter a majority ethnic group in the workplace, they cannot generally forget their minority identity (Shaban, 2016). The feeling of displacement or ethnic identity isolation can facilitate internal and external conflicts if employee diversity is not properly managed (Saxena, 2014; Shaban, 2016). Establishing the nature and impact of

cultural diversity within an organization's workforce provides significant insights into how employees will interact with cyber assets (Heinzl & Leidner, 2012).

Given the importance of cyber assets, organizational culture is expected to incorporate CSC as a core subculture (Van Niekerk & Von Solms, 2005; Schlienger & Teufel, 2003). CSC is defined as the collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with cyber assets in an organization with the aim to influence an employee's security and privacy behavior related to information breaches (AlHogail & Mirza, 2014); AlHogail, 2015; Karyda, 2017). These information breaches cost organizations large sums of money due to various forms of consumer litigation, the recovery of lost data, manpower lost hours, needed improvements in security measures and the clean-up of data breaches (AlHogail, 2015; AlHogail & Mirza, 2014).

3 Theoretical Background

The Theory of Planned Behavior (TPB) was utilized as the underlying theory for this paper, as it relates to an individual's actions in a given context. TPB stipulates that employee's intention to perform a behavior is driven by the attitude towards a behavior, perceived behavioral control and subjective norms (Ajzen, 2011; Aurigemma & Panko, 2012; Gundu, Flowerday, & Renaud, 2019). Furthermore, it explains how current behavior is enhanced to realize more efficient behavior (Safa, et al., 2015). For example, an employee's cyber security behavior can be changed by improving the employee's knowledge through awareness and training, which enhances their skills and experience to exercise a positive attitude and behavior for preserving cyber assets (Safa & Von Solms, 2016; Schlienger & Teufel, 2003). The views expressed by peers and their actions towards cyber security will affect how the individual responds to the need to act with positive cyber security intent within the given cultural context.

Linked to the behavior of employees is the national culture dimension as categorized by Hofstede's Cultural Dimensions Theory. Hofstede has identified six different dimensions: power distance; individualism vs. collectivism; uncertainty avoidance; masculinity vs. feminism; long-term orientation vs. short-term orientation; and, indulgence vs. restraint (Hofstede, 2011). How individuals from a different culture behave in a given setting is influenced by these dimensions, which in turn will influence their behavior and participation in the organizational CSC.

4 Methodology

A review of literature was conducted to better understand what critical success factors need to be present to foster a cyber security culture. Google Scholar was used as the search engine to cultivate these articles because it searches across a wide range of indexed databases. Three key phrases were chosen for the search: "cyber security culture", "cultural diversity" and "industry 4.0 cybersecurity". The combination of key phrases resulted in n=668 articles. A filtering parameter of 2009 to 2019 was applied for currency and returned n=117 articles. For each of the filtered articles, the researchers searched for the three key phrases and reviewed the text to identify the relevance to our research study. The final relevant article count was n=20.

The Zotero reference management software was used to manage the relevant articles while the remainder were considered irrelevant and excluded from the study due to weak or no relevance. The n=20 articles were analyzed to identify a relevant critical success factor(s) associated with cyber security culture in a culturally diverse workplace, which resulted in the summary in Table 1. The critical success factors identified are intended to inform the organization's management and business practices to refine how cyber assets are engaged by employees, such that they positively demonstrate a CSC.

Critical Success Factors	Authors
CSF1: Embrace cultural change and diversity	(Heckelman, Unger, & Garofano, 2013)
CSF2: Commitment by top management	(Cummings & Worley, 2014) (Da Veiga & Martins, 2015) (Nasir, Arshah, & Ab Hamid, 2017)
CSF3: Improve cyber attitudes of employees	(AlHogail, 2015) (Aurigemma & Panko, 2012) (Da Veiga & Martins, 2015) (Musarurwa, Flowerday, & Cilliers, 2017) (Van Niekerk & Von Solms, 2010)
CSF4: Administer diversity management initiatives	(Ayub, Aslam, & Razzaq, 2013) (Da Veiga & Martins, 2015) (Shaban, 2016)
CSF5: Promote awareness and training	(AlHogail & Mirza, 2014) (Astakhova, 2014) (Da Veiga & Martins, 2015) (Dike, 2013) (Hassan & Zuraini, 2016) (Tang, Li, & Zhang, 2016) (Tu & Yuan, 2014)
CSF6: Enforce information security policies (ISPs)	(AlHogail, 2015) (Bauer, Bernroider, & Chudzikowski, 2017) (Hassan & Zuraini, 2016) (Karyda, 2017) (Nasir, Arshah, & Ab Hamid, 2017) (Tang, Li, & Zhang, 2016)
CSF7: Introduce accountability	(Bauer, Bernroider, & Chudzikowski, 2017) (Da Veiga & Martins, 2015) (Nasir, Arshah, & Ab Hamid, 2017) (Tang, Li, & Zhang, 2016)
CSF8: Monitor and evaluate cyber security culture	(Da Veiga & Martins, 2015) (Gundu, 2017) (Gundu, Acknowledging and reducing the knowing and doing gap in employee cybersecurity complaince, 2019)

Table 1: Proposed critical success factors for a cyber security culture in a culturally diverse workplace

5 Discussion

As we progress through the 4IR, organizations will need to recruit individuals with the necessary cyber related skills from an increasingly diverse and globalized workforce. This evolving workforce will need to be guided towards inclusion in a CSC in the organization. To this end, it is necessary to explore the identified critical success factors for fostering a CSC when dealing with a culturally diverse workforce.

CSF1: Embrace cultural change and diversity

By embracing cultural change and diversity, an organization commits to designing and implementing interventions to develop an inclusive organizational culture that accommodates a diversified workforce. However, it is necessary to consider the cultural dimensions of employees (Hofstede, 2011), and how these influence the attitudes of employees with respect to their positive and negative feelings towards cyber security. The attitudes of the employees will determine how they behave (Ajzen, 2011), when faced with cyber security concerns.

Organizations can administer cyber security awareness questionnaires as part of the recruitment process to assist in identifying any cultural bias associated with cyber security by prospective employees. They can be administered in the organization, if they have never been done so before, to create a baseline profile of employee cultural influences of existing employees.

CSF2: Commitment by top management

Commitment by top management to cyber security initiatives targeted at all cultural groups promotes the subjective norm concept of the TPB, such that the employee perceives the behavior of management as positive in the given sphere of influence (Ajzen, 2011). Therefore, there is a

subconscious belief by an employee that the behavior of their peers determines their behavior, whether the influence is from top management or a peer (Safa & Von Solms, 2016). These are the beliefs in other people's normative expectations, which influence the perceived social pressure of individuals to comply (Aurigemma & Panko, 2012). Consideration needs to be made of the power distance cultural dimension (Hofstede, 2011), and the cultural compliance of employees of different cultures to the level of control, commitment and influence of managers of one culture over another.

Organizations should ensure that there is clear positive management reinforcement of cyber security initiatives, which indicates to the employee that cyber security is important to the organization, and instils suitable behavior for a CSC that encourages employees to behave securely (Aurigemma & Panko, 2012). Furthermore, a visible commitment by top management through regular communication on the matter and a corporate ethos towards cyber security awareness and education initiatives develops trust and strong beliefs that nurture the evolution of a CSC (Safa, et al., 2015).

CSF3: Improve cyber attitudes of employees

Employees' cyber attitudes need to be assessed, because if employees have the needed cyber security knowledge, but not the preferred cyber attitude, then it would result in insecure behavior. Similarly, if employees have the intended cyber attitude without the needed cyber security knowledge then they will inadvertently behave insecurely as proposed in the TPB (Safa & Von Solms, 2016). From the cultural dimension perspective, the sense of individualism and collectivism (Hofstede, 2011), amongst employees of different cultures, will be a determinant of whether there is a greater likelihood of generalized cyber security initiatives to be successful when targeted at a culturally diverse workforce.

Organizations need to invest in awareness and training programs that provide a culturally diverse workforce with culturally relevant cyber security knowledge, which helps to influence positive attitudes and behaviors that allow the secure handling of cyber assets (Safa, et al., 2015; Safa & Von Solms, 2016).

CSF4: Administer diversity management initiatives

The negative impacts of a disharmonious culturally diverse workforce include miscommunication, interpersonal conflict, high labor turnover due to feelings of victimization, increased cyber security incidents and breaches, and the exploitation of information assets (Tu & Yuan, 2014). The proper management of cultural diversity is anticipated to promote inclusion, creativity, flexibility, enhanced employee participation, positive employee attitudes and behavior, and create a shared vision of how cyber assets are handled (Bauer, Bernroider, & Chudzikowski, 2017).

To provide a foundation to support the success of cyber security initiatives and the establishment of a CSC, the organization needs to implement initiatives such as mandatory training workshops on cultural sensitivity, that consider the various cultural dimensions identified by Hofstede (2011).

CSF5: Promote awareness and training

When organizations communicate their cyber security policies to employees effectively, and in a manner that explains how they are to operationalize them in their daily work life, then risks are mitigated (Furnell, Alotaibi, & Esmael, 2019). Awareness and training programs help an organization to disseminate knowledge, values, and norms that empower and change employee's perceptions of their inadequacy in behaving securely (AlHogail & Mirza, 2014).

Organizations need to ensure that awareness and training initiatives for employees focus on initial face-to-face methods for cyber security communication and thereafter web-based training (Da Veiga & Martins, 2015). When preparing the training initiatives, the organization needs to focus on the delivery medium such that they are culturally neutral, and does not impose the cultural norms of one group in the company over another.

CSF6: Enforce information security policies (ISPs)

An organization must use its ISPs to communicate areas of prohibition (e.g. sharing passwords, sharing unwanted and unsolicited malware e-mails, and not securing removable media) (AlHogail, 2015). Employees' acceptance of established ISPs allows an organization to mitigate threats, breaches and incidents that threaten cyber security (Bauer, Bernroider, & Chudzikowski, 2017). Enforcing ISPs allows an organization to preserve confidential cyber assets (Karyda, 2017) by directing the behavior of employees towards protecting and securing the actual physical information assets and stored cyber assets.

Organizations can enforce ISPs by including instances of cyber asset management in employees' projects and their annual individual performance reviews, so that employees understand that the ISPs are part of their work commitments. To an extent, this aligns in part with Hofstede's uncertainty reduction cultural dimension, where the organization would impose a level of control over employees to ensure a better display of cyber security behavior.

CSF7: Introduce accountability

When employees are aware that ISPs hold them accountable for their actions when managing the cyber assets of the organization, then they are more likely to behave with cyber security in mind (Da Veiga & Martins, 2015).

If an organization increases the need for accountability by employees, then it assists the organization in mitigating insider cyber security threats and incidents, which still account for the greatest origin of cyber breaches (Karyda, 2017).

CSF8: Monitor and evaluate cyber security culture

Constant monitoring and evaluation of the organization's CSC ensures that it remains appropriate and relevant for the organization and the employees (Da Veiga & Martins, 2015). An organization can evaluate the level of its CSC using available CSC assessment tools, and benchmark them against previous findings to identify areas that need to be addressed (Gundu, Flowerday, & Renaud, 2019).

By managing a culturally diverse workforce, improvements can be made in an employee's level of engagement and cooperation in order to create mutual respect, which allows employees to increasingly harmonize their behavior and share the same values and beliefs.

Although the critical success factors are presented in a numerical order, they need not be sequential in their application in the organization.

6 Conclusion

The paper reviewed literature on cyber security in Industry 4.0 and culturally diverse environments. Eight critical success factors where identified for fostering a cyber security culture in a culturally diversified workforce. The critical success factors were briefly presented and related to the Theory of Planned Behavior and Hofstede's Cultural Dimensions Theory. Both theories were included to demonstrate that cultural factors need to be included when planning behavioral interventions in organizations to secure cyber assets in the context of the behavior of a diverse workforce.

Directions for future study include studying culturally appropriate training and awareness initiatives that factor in Hofstede's cultural dimensions, and exploring the interaction between the technological aspects and their link to human behaviors in the context of Industry 4.0. This study acknowledges that cyber security issues are best addressed through a combination of human and technological aspects, although this study focused only on the human cultural aspects.

References

Ajzen, I. (2011). The theory of planned behavior: reactions and reflections. *Psychology & Health, 26*(9), 1113-1127. doi:https://doi.org/10.1080/08870446.2011.613995

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in human behavior, 49*, 567-575. doi:http://dx.doi.org/10.1016/j.chb.2015.03.054

AlHogail, A., & Mirza, A. (2014). Information security culture: a definition and a literature review. *2014 World Congress on Computer Applications and Information Systems (WCCAIS)* (pp. 1-7). Hammamet: IEEE. doi:https://doi.org/10.1109/WCCAIS.2014.6916579

Astakhova, L. V. (2014). The concept of the information-security culture. *Scientific and Technical Information Processing, 41*(1), 22-28. doi:https://doi.org/10.3103/S0147688214010067

Aurigemma, S., & Panko, R. (2012). A composite framework for behavioral compliance with information security policies. *2012 45th Hawaii International Conference on System Sciences* (pp. 3248-3257). Maui: IEEE. doi:https://doi.org/10.1109/HICSS.2012.49

Ayub, A., Aslam, M. S., & Razzaq, A. (2013). Examining factors affecting diversity in the workplace. *CLEAR International Journal of Research in Commerce and Management, 4*(5), 136-138.

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security, 68*, 145-159. doi:https://doi.org/10.1016/j.cose.2017.04.009

Cummings, T. G., & Worley, C. G. (2014). *Organization development and change.* Stamford, CT, USA: Cengage Learning.

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49*, 162-176. doi:https://doi.org/10.1016/j.cose.2014.12.006

Dike, P. (2013). The impact of workplace diversity on organisations. *Thesis - Degree Programme in International Business*. Helsinki, Finland: Arcada University of Applied Science. Retrieved from http://urn.fi/URN:NBN:fi:amk-2013070314557

Furnell, S., Alotaibi, F., & Esmael, R. (2019). Aligning security practice with policy: Guiding and nudging towards better behavior. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, (pp. 5618-5627). Maui. Retrieved from http://hdl.handle.net/10125/59998

Gundu, T. (2013). Towards an information security awareness process for engineering SMEs in emerging economies. *Masters dissertation*. University of Fort Hare. Retrieved from http://hdl.handle.net/10353/d1007179

Gundu, T. (2017). An information security compliance reinforcement and assessment framework. *Doctrol thesis*. University of Fort Hare.

Gundu, T. (2019). Acknowledging and reducing the knowing and doing gap in employee cybersecurity complaince. *ICCWS 2019 14th International Conference on Cyber Warfare and Security* (pp. 94-102). Academic Conferences and publishing limited.

Gundu, T., Flowerday, S., & Renaud, K. (2019). Deliver security awareness training, then repeat: {Deliver; Measure Efficacy}. *2019 Conference on Information Communications Technology and Society (ICTAS)* (pp. 1-6). Durban, South Africa: IEEE. doi:https://doi.org/10.1109/ICTAS.2019.8703523

Hassan, N. H., & Zuraini, I. (2016). Information security culture in healthcare informatics: A preliminary investigation. *Journal of Theoretical & Applied Information Technology, 88*(2), 202-209. Retrieved from http://www.jatit.org/volumes/Vol88No2/2Vol88No2.pdf

Heckelman, W. L., Unger, S., & Garofano, C. (2013). Driving culture transformation during large-scale change. *OD Practitioner, 45*(3), 25-30.

Heinzl, A., & Leidner, D. E. (2012). Information systems and culture - The world might be flat, but it is culturally rich. *Business & Information Systems Engineering, 4*(3), 109-110. doi:https://doi.org/10.1007/s11576-012-0319-1

Hofstede, G. (2011). Dimensionalizing cultures: Hofstede Model in Context. *Online Readings in Psychology and Culture, 2*(1), 1-26. doi:https://doi.org/10.9707/2307-0919.1014

Hofstede, G., Hofstede, G. J., & Minkov, M. (2005). *Cultures and organizations: Software of the mind* (Vol. 2). New York: McGraw-Hill.

Karyda, M. (2017). Fostering information security culture in organizations: A Research Agenda. *Mediterranean Conference on Information Systems* (pp. 1-11). AIS Electronic Library. Retrieved from http://aisel.aisnet.org/mcis2017/28

Mazur, B. (2010). Cultural diversity in organisational theory and practice. *Journal of Intercultural Management, 2*(2), 5-15.

McKenzie, F. (2017). *The fourth industrial revolution and international migration.* Retrieved from http://hdi.handle.net/11540/7644

Morrar, R., Arman, M., & Mousa, S. (2017). The fourth industrial revolution (Industry 4.0): A social innovation perspective. *Technology Innovtion Management Review, 7*(11), 12-20. Retrieved from https://timreview.ca/sites/default/files/Issue_PDF/TIMReview_November2017.pdf#page=12

Musarurwa, A., Flowerday, S., & Cilliers, L. (2017). Individual traits that determine the Bring your Own Device information security culture: A case study of the banking sector in Zimbabwe. *Information Institute Conferences*, (pp. 1-18). Las Vegas.

Nasir, A., Arshah, R. A., & Ab Hamid, M. R. (2017). Information security policy compliance behavior based on comprehensive dimensions of information security culture: A conceptual framework. *Proceedings of the 2017 International Conference on Information Systems and Data Mining* (pp. 56-60). Charleston: ACM Digital Library. doi:https://doi.org/10.1145/3077584.3077593

Rojko, A. (2017). Industry 4.0 concept, background and overview. *International Journal of Interactive Mobile Technologies, 11*(5), 77-90. Retrieved from https://online-journals.org/index.php/i-jim/article/view/7072

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 54*, 442-451. doi:https://doi.org/10.1016/j.chb.2015.12.037

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78. doi:https://doi.org/10.1016/j.cose.2015.05.012

Saxena, A. (2014). Workforce diversity: A key to improve productivity. *Procedia Economics and Finance, 11*, 76-85. doi:https://doi.org/10.1016/S2212-5671(14)00178-6

Schlienger, T., & Teufel, S. (2003). Information security culture-from analysis to change. *South African Computer Journal, 31*, 46-52. Retrieved from https://hdl.handle.net/10520/EJC27949

Schwab, K. (2016). *The fourth industrial revolution.* Geneva: World Economic Forum.

Shaban, A. (2016). Managing and leading a diverse workforce: One of the main challenges of Management. *Procedia-Social and Behavioral Sciences, 230*, 76-84. doi:https://doi.org/10.1016/j.sbspro.2016.09.010

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management, 17*(2), 176-186. doi:https://doi.org/10.1007/s10799-015-0252-2

Tu, Z., & Yuan, Y. (2014). Critical success factors analysis on effective information security management: A literature review. *Twentieth Americas Conference on Information Systems*, (pp. 1-13). Savannah. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.819.6637

Van Niekerk, J. F., & Von Solms, R. (2005). A holistic framework for the fostering of an information security sub-culture in organizations. *International Information Security South Africa (ISSA) Conference*, (pp. 1-13). Sandton. Retrieved from https://dblp.org/rec/conf/issa/NiekerkS05

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476-486. doi:https://doi.org/10.1016/j.cose.2009.10.005

World Economic Forum. (2016). The future of jobs: Employment, skills and workforce strategy for the fourth industrial revolution. *Global Challenge Insight Report*. Geneva: World Economic Forum. Retrieved from https://www.voced.edu.au/content/ngv:71706