Initial Post

Kovaitė & Stankevičienė, (2019) define industry 4.0 as “The 4th industrial revolution…”. It is characterised by the process of digitization of industries (Marr, 2018) and the leveraging of technologies such as the cloud computing, Big Data artificial intelligence (AI) and the Internet of things, among others, to increase both productivity and quality (IBM, N.D.). For example, in a warehouse, using sensors connected to shelves and connected software could be used to monitor and maintain inventory levels (AMFG, 2019). Since stock control and ordering are labour intensive tasks, and under / overstocking have a potential financial and reputational risk, the benefits of digitalisation have been well documented (Emily et al. 2020).

There are risks which come with digital transformation. Two examples are.

Financial Risks

Small & Medium Enterprises have less access to the capital investment required to implement the required hardware and software (Yigitbasioglu, 2015).

Data Security Risks

Since a fully digitised enterprise is likely to have a larger attack service (Dimitrov, 2020) there is an increased risk of to data through cyber attack (Tupa et al., 2017).

Chouaibi et al. (2021), agree with Kovaitė & Stankevičienė, (2019) in that digital transformation brings with it risks and discusses the importance of adaptive change management to minimise potential risks.

References

AMFG. (2019). Industry 4.0: 7 Real-World Examples of Digital Manufacturing in Action. Available from: https://amfg.ai/2019/03/28/industry-4-0-7-real-world-examples-of-digital-manufacturing-in-action/ [Accessed 11th March 2023].

Chouaibi, S., Festa, G., Quaglia, R. & Rossi, M. (2022). The risky impact of digital transformation on organizational performance – evidence from Tunisia, *Technological Forecasting and Social Change*, Volume 178, Article 121571.

Dimitrov, W. (2020). The Impact of the Advanced Technologies over the Cyber Attacks Surface. In: Silhavy, R. (eds) Artificial Intelligence and Bioinspired Computational Methods. CSOC 2020. *Advances in Intelligent Systems and Computing*, vol 1225. Springer, Cham. https://doi.org/10.1007/978-3-030-51971-1_42

Emily H., Mondher F., & Imed B. (2015). The shape of digital transformation: a systematic literature review, Ninth Mediterranean Conference on Information Systems (MCIS), Samos, Greece, 431-443.

IBM. (N.D.). What is industry 4.0? Available from: https://www.ibm.com/topics/industry-4-0 [Accessed 11th March 2023].

Marr, B. (2018). What is Industry 4.0? Here's A Super Easy Explanation For Anyone. Available from: https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/ [Accessed 11th march 2023].

Tupa, J., Simota, J., & Steiner, F. (2017). Aspects of risk management implementation for Industry 4.0. *Procedia Manufacturing*, 11, 1223-1230. https://doi.org/10.1016/j.promfg.2017.07.248

Yigitbasioglu, O. M. (2015). The role of institutional pressures and top management support in the intention to adopt cloud computing solutions*. Journal of Enterprise Information Management*, 28(4), 579-594.

Peer responses to my initial post

by Matjaz Galicic - Monday, 20 March 2023, 9:19 AM

Hi Steve,

You raised two good points: financial risks and data security risks. This is aligned with the research by Kazemargi and Spagnoletti (2020), who looked at the gap between Industry 4.0 and financial issues the Italian Small and Medium sized Enterprises (SMEs) are facing. While SMEs are dependent on the interconnectivity of devices and systems, they are facing cyber-security issues of data in their supply chains (Kazemargi and Spagnoletti, 2020). They often have to trade-off between investing into specialist technologies and training their employees, and struggle with mitigating against cyber-attacks, which can have a negative impact on their reputation (Kazemargi and Spagnoletti, 2020).

Sustainability also seems to be an issue of Industry 4.0. According to Bai et al. (2020), Industry 4.0 can reduce energy consumption through electronic component recycling, as well as reduction of resource consumption (Ejsmont et al., 2020). This can, however, increase the electronic waste and cause an impact on employment, depending on the type of technology used (Bai et al., 2020).

Interestingly, Jamai et al. (2020) list three main attack surfaces in Industry 4.0: systems, devices and networks, leading to attacks on industrial systems and their components, including sensors, actuators, valves, etc. Sensors, for example, can serve as protection measures to ensure workers' safety. If compromised, this could lead to serious workplace accidents.

References

Bai, C., Dallasega, P., Orzes, G. and Sarkis, J. (2020) Industry 4.0 technologies assessment: A sustainability perspective. *International journal of production economics* 229, p.107776.

Ejsmont, K., Gladysz, B. and Kluczek, A. (2020) Impact of industry 4.0 on sustainability—bibliometric literature review. *Sustainability* 12(14), p.5650.

Jamai, I., Azzouz, L.B. and Saïdane, L.A. (2020) Security issues in Industry 4.0. In 2020 International Wireless Communications and Mobile Computing (IWCMC) (pp. 481-488). IEEE.

Kazemargi, N. and Spagnoletti, P. (2020) IT investment decisions in industry 4.0: evidences from SMEs. In Digital Business Transformation: Organizing, Managing and Controlling in the Information Age (pp. 77-92). Cham: Springer International Publishing.

Summary Post

The potential benefits and challenges to small businesses of Industry 4.0 have been well documented by Masood & Sonntag, (2020). Matjaz raises some important points regarding financial and data security risks as both are closely linked. There have been many cases around the world where companies have been fined by various oversight bodies for their lack of attention to data security and although it only tends to be the cases involving the largest fines which make the headlines, data from the GDPR Enforcement Tracker, (N.D.) gives several examples of UK small businesses and charities being fined for GDPR breaches as shown in Table 1.

Date of Judgement	Organisation	Fine (£)	GDPR Breach
18/10/22	HIV Scotland	11,800	Insufficient technical and organisational measures to ensure information security
10/3/22	Tuckers Solicitors LLP	115,000	Non-compliance with general data processing principles
5/7/22	Mermaids	29,000	Insufficient technical and organisational measures to ensure information security

Table 1: UK small businesses fined under GDPR. After GDPR Enforcement Tracker (N.D.)

It is interesting to note that charities / non profit organisations are of particular risk as they are often poorly prepared for implementing GDPR (Henriksen-Bulmer, et al., 2019). This is further demonstrated by the Cyber Security Breaches Survey (2019) where the mean spend by charities on cybersecurity is less than half that of micro / small businesses (£1,500 compared to £3,480) and 59% of spend nothing at all! The Information Commissioner's Office has issued free guidelines to help charities comply with GDPR and can be found at https://ico.org.uk/for-organisations/fundraising-and-data-protection/

References

Henriksen-Bulmer, J., Faily, S. and Jeary, S., (2019). Implementing GDPR in the charity sector: A case study. *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers 13*, pp.173-188.

Masood, T. & Sonntag, P., (2020). Industry 4.0: Adoption challenges and benefits for SMEs. *Computers in Industry*, *121*, p.103261.

Vaidya, R., (2019). Cyber security breaches survey 2019. *Department for Digital, Culture, Media and Sport*, *66*.