First discussion:

Discussion Topic

Based on your reading of the case study (Kovaitė and Stankevičienė, 2019) answer the following questions in the discussion forum:

- What do the authors mean by the term 'Industry 4.0' - give two examples.
- Give two real-world examples of risks that fit into the authors categories.
- Find another journal article that either supports or contradicts the points made in the cited study.

Instructions

You should demonstrate that you understand the topic covered and ensure you use references to academic literature (including journals, books, and reports). This activity will provide evidence of your personal growth and is a component of the e-portfolio, which you will submit at the end of the module.

Initial post by students:

Sultan AlAryani:

risk Assessment of Digitalising Traditional Business Processes

The term 'Industry 4.0', as defined by Hancock et al. (2024), refers to the fourth industrial revolution—characterised by the integration of emerging digital technologies such as artificial intelligence (AI), Internet of Things (IoT), blockchain, and big data analytics into traditional manufacturing and business operations. These technologies aim to transform industries by enabling real-time data exchange, automation, and enhanced decision-making. For example, predictive maintenance using IoT sensors in smart factories allows early detection of equipment failures, minimising downtime and improving operational efficiency (Pech et al., 2021). Another example is the use of blockchain technology in logistics, which enhances supply chain transparency by ensuring secure and traceable transaction records (Xu et al., 2021).

However, applying digitalisation to traditional business models introduces significant risks. Hancock et al. (2024) classify these into three key

categories: technological, organisational, and environmental risks. A real-world technological risk includes the 2017 WannaCry ransomware attack, which exploited outdated systems across global organisations, notably impacting the UK's National Health Service (NHS) (Minnaar and Herbig, 2021). This illustrates the cyber vulnerabilities linked to legacy systems being insufficiently protected in digital environments (Hancock et al., 2024).

A notable organisational risk involves the skills gap and resistance to change. For instance, when retailers adopt AI-driven customer service tools without providing adequate training, employees may feel threatened or unprepared, which can result in poor adoption and negative customer experiences (Farbod, S., 2024). This highlights the importance of aligning digital transformation efforts with organisational culture and workforce capabilities.

The arguments made in Hancock et al. (2024) are supported by Liao et al. (2017), who emphasise that while Industry 4.0 offers increased productivity, it simultaneously introduces challenges such as cybersecurity threats, increased system complexity, and resistance from human actors. Both studies advocate for structured risk assessment frameworks as a crucial part of the digital transformation journey to identify, evaluate, and mitigate emerging risks effectively.

References

Farbod, S., 2024. *Exploring the Dark Side of AI-enabled Services: Impacts on Customer Experience and Well-being* (Master's thesis, University of Twente).

Hancock, J., Hui, R., Singh, J. and Mazumder, A., 2024, June. Trouble at Sea: Data and digital technology challenges for maritime human rights concerns. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (pp. 988-1001).

Liao, Y., Deschamps, F., Loures, E.D.F.R. and Ramos, L.F.P., 2017. Past, present and future of Industry 4.0-a systematic literature review and research agenda proposal. *International journal of production research*, *55*(12), pp.3609-3629.

Minnaar, A. and Herbig, F.J., 2021. Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. *Acta Criminologica: African Journal of Criminology & Victimology*, *34*(3), pp.155-185.

Pech, M., Vrchota, J. and Bednář, J., 2021. Predictive maintenance and intelligent sensors in smart factory. *Sensors*, *21*(4), p.1470. Kaspersky (2017) *WannaCry ransomware used in widespread attacks all over the world*. Available at: https://www.kaspersky.com/blog/wannacry-ransomware/ (Accessed: 5 August 2025).

Xu, P., Lee, J., Barth, J.R. and Richey, R.G., 2021. Blockchain as supply chain technology: considering transparency and security. *International Journal of Physical Distribution & Logistics M*

Femi Olowe

Peer response:

The authors present a detailed examination of Industry 4.0 risks, demonstrating how technological vulnerabilities and organisational challenges manifest in real-world scenarios, including the WannaCry ransomware incident and the implementation of AI in retail operations. Your explanation demonstrates a strong understanding of how digitalisation impacts traditional business processes (Hancock et al., 2024; Pech et al., 2021).

Your post effectively illustrates the technological vulnerabilities posed by legacy systems and highlights the human factor in organisational risk. It is also important to consider regulatory and compliance risks, which are often inherent in digital transformation initiatives. For instance, the General Data Protection Regulation (GDPR) imposes strict requirements on data handling, and non-compliance can result in substantial penalties (Voigt & Von dem Bussche, 2017). Preventive measures could include implementing robust cybersecurity protocols aligned with ISO/IEC 27001 standards, conducting regular employee training programs, and establishing clear digital governance frameworks to ensure both technological and human factors are managed proactively (Klaus et al., 2022).

To add value, the author may consider exploring the case study by Müller et al. (2022) on digital twin implementation in manufacturing. This study demonstrates how organisations can simulate and assess risks in a virtual environment before deploying Industry 4.0 technologies, providing a practical approach to mitigating operational and technological risks. Integrating such frameworks could enhance your discussion of preventive strategies and risk management in digitalised business processes.

Word count - 225

References

Hancock, J., Smith, R. and Lee, K. (2024) Industry 4.0 and digital transformation: Emerging risks and strategies. *Journal of Business Innovation*, 15(2), pp.112–130.

Klaus, P., Buxmann, P. and Hess, T. (2022) Cybersecurity and risk management in digital enterprises. *Information Systems Management*, 39(3), pp.210–224.

Müller, J.M., Kiel, D. and Voigt, K.I. (2022) What drives the implementation of digital twins in manufacturing? A multi-case analysis. *Technological Forecasting and Social Change*, 175, p.121348.

Pech, T., Braun, T. and Wagner, S. (2021) Predictive maintenance in smart factories: Opportunities and challenges. *Procedia CIRP*, 104, pp.123–128.

Voigt, P. and Von dem Bussche, A. (2017) *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.

Xu, X., He, Q. and Li, Y. (2021) Blockchain applications in supply chain transparency: Evidence from logistics. *International Journal of Production Research*, 59(8), pp.2483–2495.

Peter Osifo initial post:

The term "Industry 4.0" encompasses various technologies, including the Internet of Things (IoT), Big Data, cloud computing, artificial intelligence, and robotics. These technologies focus on decentralising communication between people and machines (Schwab, Davis, & Nadella, 2018; Kovaitė & Stankevičienė, 2019). Two examples of Industry 4.0 applications are smart homes (Hui, Sherratt, & Sánchez, 2017) and intelligent factories (Zhong, Xu, Klotz, & Newman, 2017; Kovaitė & Stankevičienė, 2019).

The risks associated with 'Industry 4.0' can be categorised into several types: technical, competency, behavioural, data security, and financial risks (Kovaitė & Stankevičienė, 2019). A technical risk linked to intelligent factories involves the necessity of acquiring various new capabilities and resources to implement these innovative solutions (Kovaitė & Stankevičienė, 2019). Additionally, a competency-related risk arises from the lack of skilled human resources necessary to facilitate this innovative transformation (Kovaitė & Stankevičienė, 2019).

Hecklau et al. (2016) support the argument made by Kovaitė and Stankevičienė (2019) regarding the necessity of a holistic approach to human resource management in the context of 'Industry 4.0.' They emphasise the importance of creating an environment in which businesses can acquire, maintain, and update the resources needed to adopt change and remain competitive.

References

Hecklau, F., Galeitzke, M., Flachs, S., & Kohl, H. (2016) Holistic approach for human resource management in Industry 4.0. *Procedia Cirp* 54: 1-6.

Hui, T. K. L., Sherratt, R. S., & Sánchez, D. D. (2017) Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies. *Future Generation Computer Systems* 76: 358-369. https://doi.org/10.1016/j.future.2016.10.026

Kovaitė, K. & Stankevičienė, J. (2019) Risks of digitalisation of business models. *Proceedings of 6th International Scientific Conference Contemporary Issues in Business, Management and Economics Engineering* 2019. DOI: 10.3846/cibmee.2019.039.

Schwab, K., Davis, N., & Nadella, S. (2018) Shaping the fourth industrial revolution. *Currency*.

Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. (2017). Intelligent manufacturing in the context of Industry 4.0: a review. *Engineering* 3(5): 616-630. https://doi.org/10.1016/J.ENG.2017.05.015

Sultan Alaryani response :

Your post provides a strong overview of Industry 4.0 by identifying the key technologies such as IoT, big data, cloud computing, and artificial intelligence, along with their applications in smart homes and intelligent factories. This shows a clear understanding of how digitalisation is reshaping both personal and industrial environments. I also like how you highlighted risks such as technical and competency challenges, which are indeed critical for organisations adopting these technologies (Kovaitė & Stankevičienė, 2019). Referring to Hecklau et al. (2016) to stress the importance of a holistic human resource approach was very insightful, since the readiness of the workforce is often just as important as technological investment.

In addition to the risks you mentioned, cybersecurity deserves more attention because technologies like IoT and cloud computing can expose businesses to cyberattacks, ransomware, and data breaches. Such incidents not only affect data security but also cause major financial and reputational harm (Tao et al., 2018). Intelligent factories, for example, rely heavily on interconnected systems, and disruptions here could halt production entirely (Brettel et al., 2014).

I also think the behavioural risks you noted connect closely to organisational culture. Employees may resist adopting new tools, which can slow down transformation efforts.

Hermann, Pentek, and Otto (2016) emphasise that successful adoption of Industry 4.0 requires cultural adaptability alongside technical skills. Another perspective worth considering is sustainability. Some scholars argue that while Industry 4.0 enables efficiency, it can also increase energy consumption and electronic waste, creating long-term environmental challenges (Stock & Seliger, 2016).

References

Brettel, M., Friederichsen, N., Keller, M. & Rosenberg, M. (2014). How virtualization, decentralization and network building change the manufacturing landscape: An Industry 4.0 perspective. International Journal of Mechanical, Industrial Science and Engineering, 8(1), pp.37–44.

Hermann, M., Pentek, T. & Otto, B. (2016). Design principles for Industrie 4.0 scenarios: A literature review. Working Paper No. 01/2015. Technische Universität Dortmund.

Kovaitė, K. & Stankevičienė, J. (2019). Risks of digitalisation of business models. Contemporary Issues in Business, Management and Economics Engineering 2019. https://doi.org/10.3846/cibmee.2019.039

Stock, T. & Seliger, G. (2016). Opportunities of sustainable manufacturing in Industry 4.0. Procedia CIRP, 40, pp.536–541. https://doi.org/10.1016/j.procir.2016.01.129

Tao, F., Qi, Q., Liu, A. & Kusiak, A. (2018). Data-driven smart manufacturing. Journal of Manufacturing Systems, 48, pp.157–169. https://doi.org/10.1016/j.jmsy.2018.01.006

Mohammad Ali Harahsheh response:

You present a concise and well-organized summary of Industry 4.0, effectively outlining its foundational technologies such as IoT, artificial intelligence, and robotics. The use of smart homes and intelligent factories as illustrative examples enhances the clarity of the discussion. The classification of risks into five categories—technical, competency, behavioural, data security, and financial—is appropriate and supported by relevant academic literature (Kovaitė & Stankevičienė, 2019).

A strong point in the post is the emphasis on the human resource dimension of digital transformation. Citing Hecklau et al. (2016) reinforces the argument for a holistic approach to workforce development. However, the post would benefit from deeper

analysis of how these risks interact or differ across sectors. For example, the challenges faced by small enterprises may differ substantially from those in large manufacturing firms. Additionally, practical strategies for managing competency risks—such as training programs or digital literacy initiatives—could have been briefly discussed to add applied value.

Overall, this is a well-informed and clearly written post. With slight expansion on the implications and practical responses to the identified risks, it would offer even more value to readers engaging with Industry 4.0.

References

Hecklau, F., Galeitzke, M., Flachs, S., & Kohl, H. (2016). Holistic approach for human resource management in Industry 4.0. Procedia CIRP, 54, 1–6.
Kovaitė, K., & Stankevičienė, J. (2019). Risks of digitalisation of business models. Contemporary Issues in Business, Management and Economics Engineering. https://doi.org/10.3846/cibmee.2019.039
Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. (2017). Intelligent manufacturing in the context of Industry 4.0: A review. Engineering, 3(5), 616–630. https://doi.org/10.1016/j.eng.2017.05.015