UNIT 2 – COLLABORATIVE DISCUSSION 1 – PEER RESPONSE

The post demonstrates a clear and relevant understanding of Industry 4.0, selecting cloud-based analytics and IoT as pertinent examples. These examples are appropriate; however, their contribution could be strengthened by explicitly linking them to specific business model components (Osterwalder, Pigneur and Tucci, 2005).
For instance, cloud-based services and analytics directly relate to “key resources” and to “customer relationships“ (Osterwalder, Pigneur and Tucci, 2005). Similarly, IoT technologies are closely associated with “value propositions” and with “customer channels” (Osterwalder, Pigneur and Tucci, 2005). Establishing these links would directly align the examples with the structural and strategic shifts in business models highlighted in the source literature.

In the section outlining the risks identified by Kovaitė and Stankevičienė (2019), the categorisation of technical and financial risks is well-articulated, providing a clear basis for further analysis and application. To build on this strength, the discussion could be enriched through the integration of real-world examples that demonstrate how these risks have materialised in practice. For instance, the reference to technical risks leading to cyber-attacks could be illustrated by the 2017 WannaCry ransomware incident, which exploited unpatched systems and disrupted operations of the NHS (Ghafur et al., 2019) Indeed, as Tamvada and others point out (2022), SMEs face significant financial risks when adopting Industry 4.0, with high upfront investments, unclear economic benefits, and long, uncertain periods often forcing them to rely on debt. Such delays in ROI can strain cash flow and threaten business sustainability if anticipated gains are not realised.

The inclusion of Pfeifer (2021) offers a meaningful extension by introducing empirical evidence from a real-world SME case, which demonstrates that even with a structured Industry 4.0 integration plan, significant technical challenges can persist to the point of project abandonment. This evidence expands the discussion beyond the theoretical risk framework of Kovaitė and Stankevičienė (2019) by showing how these risks—particularly technical and financial—manifest in practice, and by highlighting additional external factors that may influence adoption outcomes.

References

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. and Aylin, P. (2019) ‘A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS’, *NPJ Digital Medicine*, 2(1). Available at: https://www.nature.com/articles/s41746-019-0161-6 (Accessed: 12 August 2025).

Kovaitė, K. and Stankevičienė, J. (2019) ‘Risks of digitalisation of business models’, *Proceedings of 6th International Scientific Conference Contemporary Issues in*

Business, Management and Economics Engineering 2019. Available at: https://doi.org/10.3846/cibmee.2019.039 (Accessed: 30 July 2025).

Osterwalder, A., Pigneur, Y., & Tucci, C. L. C. (2005) ‘Clarifying business models: origins, present, and future of the concept’, *Communications of the Association for Information Systems*, *16*(1), 1-25. Available at: https://doi.org/10.17705/1CAIS.01601 (Accessed: 30 July 2025).

Pfeifer, M. (2021) ‘SMEs in Failed Transition Towards Industry 4.0: A case study of a Czech SME’, *Journal of Innovation and Business Best Practice*, 2021 (2021), pp.1–16. Available at: https://doi.org/10.5171/2021.707843 (Accessed: 12 August 2025).

Tamvada, J.P., Narula, S., Audretsch, D., Puppala, H. and Kumar, A. (2022) ‘Adopting new technology is a distant dream? The risks of implementing Industry 4.0 in emerging economy SMEs’, *Technological Forecasting and Social Change*, 185, p.122088. Available at: https://doi.org/10.1016/j.techfore.2022.122088 (Accessed: 10 August 2025).

Tutor response
This is a well-informed peer-response — well-done!

The post effectively reflects Kovaitė and Stankevičienė's (2019) definition of Industry 4.0 as a digitally driven transformation, with IoT and Big Data well-chosen as examples. The ransomware and smart city protocol incompatibility examples align well with the "data privacy and security" and "technical" risk categories, adding practical relevance.

The analysis could be strengthened by linking these risks more explicitly to Osterwalder's business model components (2005). For instance, ransomware can disrupt customer channels through service outages, while protocol incompatibility in smart city infrastructure can compromise key resources or damage customer relationships. Making these links explicit would highlight not only the nature of the risks but also their specific operational and strategic impacts.

Additionally, the post would benefit from concrete, real-world cases to illustrate these impacts. For instance, ransomware can disrupt customer channels through service outages, as seen in the 2017 WannaCry attack on the UK's National Health Service, which led to lost operational capacity (NHS England, 2023). Similarly, protocol incompatibility in smart city infrastructure can damage customer relationships, as occurred in the 2018 Atlanta ransomware incident, where multiple city services were taken offline for days (Goldberg and Zlatev, 2022).

The use of Culot et al. (2019) provides credible support for the cybersecurity and technical dimensions, particularly regarding vulnerabilities in interconnected systems. However, this focus is narrower than the multi-dimensional approach in the cited study, which cautions against concentrating solely on technical risks. Kovaitė and Stankevičienė emphasise that competence, organisational acceptance, customer trust, and financial constraints are equally important in understanding Industry 4.0 risks (2019).

Overall, the post establishes a solid foundation. Mapping risks to business model components, integrating illustrative real-world cases, and broadening the scope to include additional risk categories would deepen the analysis and strengthen its strategic relevance.

References

Culot, G., Fattori, F., Podrecca, M. and Sartor, M. (2019) 'Addressing Industry 4.0 Cybersecurity Challenges', IEEE Engineering Management Review, 47(3), pp. 79–86. Available at: https://ieeexplore.ieee.org/document/8758411 (Accessed: 11 August 2025).

Goldberg, A. and Zlatev, J. (2022) *Atlanta Ransomware Attack.* Available at: https://www.hbs.edu/faculty/Pages/item.aspx?num=62893 (Accessed: 11 August 2025).

Kovaitė, K. and Stankevičienė, J. (2019) 'Risks of digitalisation of business models', Contemporary Economics, *Proceedings of 6th International Scientific Conference*

Contemporary Issues in Business, Management and Economics Engineering 2019, 13(4), pp. 471–484. Available at: https://doi.org/10.3846/cibmee.2019.039 (Accessed: 30 July 2025).

NHS England (2023) *NHS England business continuity management toolkit case study: WannaCry attack*. Available at: https://www.england.nhs.uk/long-read/case-study-wannacry-attack/ (Accessed: 11 August 2025).

Osterwalder, A., Pigneur, Y., & Tucci, C. L. C. (2005) 'Clarifying business models: origins, present, and future of the concept', *Communications of the Association for Information Systems*, *16*(1), 1-25. Available at: https://doi.org/10.17705/1CAIS.01601 (Accessed: 30 July 2025).

Tutor response

Very good engagement!