Initial Post

In their paper Risk of Digitalisation of Business Models, Kovaitė & Stankevičienė (2019) created a risk assessment matrix to assess potential risks, resulting from digitalisation of business models in the context of Industry 4.0, which they refer to as follows.

“The 4th industrial revolution moves from there and encompasses a range of technological drivers as the Internet of things (IoT), big data, cloud computing, robotics, artificial intelligence and explores the decentralisation of communication between people and machine.”

For their matrix, they identified the following 6 types of risk:

- Technical
- Competence
- Acceptance by staff
- Acceptance by customers
- Data security
- Financial risks

In May 2023, Ireland's Data Protection Commission (DPC) fined Meta Platform Ireland Limited €1.2 billion for violating GDPR by transferring personal data from the EU/EEA to the US without adequate safeguards (Sharman & Hill, 2024).

General Electric's (GE) digital transformation project, Predix, failed despite significant investments due to overambitious goals, technical complexities, and organisational misalignment. The project aimed to build an industrial IoT platform but faced challenges integrating diverse data and lacked internal capabilities to sustain development. As a result, GE incurred $7 billion in costs, missed revenue targets, and fell behind competitors in the IoT market (Pereira, N.D.)

The second example emphathises that the complexity which digitalisation projects can contain, must not be underestimated. Kharlamova and Kharlamov (2019) elaborate about the importance of the development of human capital in digitalisation and conclude the following:

- **Impact on Human Capital**: Effective organisation of work for personnel managing digital risks enhances employees' innovative and creative potential, leading to positive changes in their motivation and overall development of the company’s human capital, especially during the transition to digital business platforms.
- **Managerial Action Framework**: A seven-stage sequence of managerial actions for handling information related to digital risks has been proposed. This structured approach provides new benchmarks for the organisational behavior of risk management personnel and is shown to improve the company’s human capital when effectively implemented.

Word count: 330

References:

Kovaitė, K., & Stankevičienė, J. (2019) 'Risks of digitalisation of business models', *Contemporary Issues in Business, Mangement and Economic Engineering*. Vilnius Gediminas Technical University, Lithuania, 9 - 10 May 2019. DOI: https://doi.org/10.3846/cibmee.2019.039

Sharma, S. & Hill, M. (2022) The 12 biggest data breach fines, penalties, and settlements so far. Available from: https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html [Accessed 4 August 2024]

Pereira, S. (N.D.) How GE burned $7B on their platform (and how to avoid doing the same) Available from: https://platformengineering.org/blog/how-general-electric-burned-7-billion-on-their-platform [Accessed 4 August 2024]

Kharlamova, T. & Kharlamov, A. (2019) Human capital development in the digitalization risk management process. *Proceedings of the International Conference on Digital Technologies in Logistics and Infrastructure*: 199-203. DOI: https://doi.org/10.2991/icdtli-19.2019.37

Answer 1

Thank you David, for your post about Industry 4.0 with regards to risk management.

The example of IoT in Manufacturing with sensor-generated data to optimise production is something that I only recently became aware of. A friend of mine bought himself an EV and was frustrated about the number of charging station which are malfunctioning due to heat problems while fast charging. Sensors can not only reduce risks in charging but moreover they can detect early when a charging station is about to fail (Li et al., 2021).

I agree, that the Snowden leak, where he stole some 1.7 million classified documents from NSA’s computers, while he was under contract as a data specialist through a subcontractor, was indeed a behavioural risk. The core of the debate revolved around whether Snowden was a patriot for exposing a controversial intelligence program to the public or a traitor for unauthorisedly leaking classified information (Johnson et al., 2014).

Furthermore, you have shown an alternative risk management framework which divides risks into 5 different sections. Unfortunatelly, the alternative framework neither inclundes the human as a risk factor nor does it mention the affects to them with regards to Industry 4.0.

Word count: 196

References:

Li, L., Liu, W., Li, D., Li, X. & Liu, X. (2021) Research on charging safety and early warning of intelligent networked electric vehicles. *E3S Web of Conferences*, 237(02013): 1-4. DOI: https://doi.org/10.1051/e3sconf/202123702013

Johnson, L.K., Aldrich, R.J., Moran, C., Barrett, D.M., Hastedt, G., Jervis, R., Krieger, W., McDermott, R., Omand, D., Phythian, M. & Wark, W.K. (2014) An INS Special Forum: Implications of the Snowden Leaks. *Intelligence and National Security*, 29(6): 793–810. DOI: https://doi.org/10.1080/02684527.2014.946242

Answer 2

Thank you, Nelson, for your post which discusses a critical event in the recent history of civil aviation.

I would argue that the Boeing 737 Max case was indeed a cascading effect of different issues. To be able to compete with Airbus' A320neo, Boeing had to come up with something new, since the A320neo was much more efficient compared to Boeings 737. Boeing made a conscious decision to use the same aircraft type and optimise the engines. The strategy was to keep the same airplane type, to avoid costly training for pilots. The strategy was to keep the same type to avoid costly training for the pilots as it was the same type of aircraft. To make the 737 more efficient, the engines were enlarged, but also had to be moved further forward so that they were still far enough away from the ground. As the aircraft behaved completely differently as a result, an attempt was made to compensate for this with software (MACS) that corrected the aircraft's attitude by overriding the pilot. Consequently, the pilots were taken by surprise, when the software suddenly intervened and changed the aircraft's behaviour (Gonela et al., 2020).

Therefore, I would even go so far and declare this catastrophe as a major failure in Boeing's leadership, since the management team prioritised financial aspects over safety. This fundamental error could not be corrected by software and skipping flight simulator training did not help either.

Friendly reminder Nelson, please be aware that the University of Essex Online asks us to use British English, i.e. s instead of z. I realise that my spell check sometimes lets me down too and switches to American English.

Word count: 278

References:

Gonela, S., Laeequddin, M., Dikkatwar, R. & NS, S. (2020) Cascading Effect of Boeing’s 737 Max Technology Development.*International Journal of Recent Technology and Engineering (IJRTE)* 8(5): 5208-5215.
DOI: https://doi.org/10.35940/ijrte.e4863.018520

Summary Post

Hi Doug, Gesine, Mark and Mustafa,

Thank you for your posts which added some valid points. It appears that above of technical-, financial-, security- and other risks, there is something more crucial, which is man made decisions and are called cognitive risks.

Bone and Lee (2023) argues that traditional risk management approaches are outdated and inadequate for the new challenges presented by the digital era. Therefore he introduces a "Cognitive Risk Framework" that integrates the human element into risk management strategies, emphasising the importance of understanding and addressing human behavior and cognitive biases as critical factors in mitigating risks. The five pillars of the cognitive risk framework are:

1. Cognitive governance - A formal process to explore risks and uncertainties through a multidisciplinary lens.
2. Intentional controls design - Designing controls to reduce risks by streamlining processes and enhancing situational awareness.
3. Cybersecurity and enterprise risk - Recognising the human element as the greatest vulnerability and rearchitecting people-technology interactions.
4. Human factors and socio-technical risk - Analysing how job, individual and organisational factors influence human behavior and performance.
5. Cognitive risk mitigation - Mitigating bias and noise in decision-making through formal processes.

The paper calls for a paradigm shift in risk management, moving away from purely technical solutions to a more holistic approach that places human cognition at the center of risk assessment and mitigation strategies.

Word count: 226

References:

Bone, J. & Lee, J.H. (2023) *Cognitive Risk*. 1st ed. Boca Raton: CRC Press. DOI: https://doi.org/10.1201/9781003189657