**Based on your reading of the case study listed above (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.*

The authors refer to Industry 4.0 as the 4th digitalization revolution focused on the Internet as important asset for decentralization. They describe Industry 4.0 as a range of technological drivers that facilitate communication between people and machines. These drivers include big data, cloud computing, and artificial intelligence among others. By providing these essential pillars, authors discuss risks associated to the fast and unpredictable technological advancements caused by IoT (Kovaitė & Stankevičienė, 2019).

* *Give two real-world examples of risks that fit into the authors categories.*

**Data security risks**: In 2014 Yahoo data breach reached over 500 million people of whose data was stolen. These included names, birthdays, telephone numbers and other sensitive data. The attackers managed to forge Yahoo Email cookies that allowed access without requiring a password (Trautman & Ormerod, 2017).

**Technical risks:**Vulnerabilities in St. Jude Medical’s devices. The technical issue arose in pacemaker devices. The vulnerability was reported by Medical device cybersecurity solutions (MedSec) where the investigation discovered that an attacker could crash implantable cardiac devices and drain their batteries at a faster rate (Arghire, 2017).

* *Find another journal article that either supports or contradicts the points made in the cited study.*

Similar article that discusses risks related to the industry 4.0 refers to manufacturing where authors of the article “A Review of Industry 4.0 Manufacturing Process Security Risks” highlight the disruptive nature of technological advancements. They reveal industrial espionage and deliberate disruption of manufacturing processes by malicious hackers as an example of concerns revolving around IoT (Prinsloo et. al., 2019).

**References**

Arghire, I. (2017) St. Jude Medical Recalls 465,000 Pacemakers Over Security Vulnerabilities. SecurityWeek. Available from: [**https://www.securityweek.com/st-jude-medical-recalls-465000-pacemakers-over-security-vulnerabilities/**](https://www.securityweek.com/st-jude-medical-recalls-465000-pacemakers-over-security-vulnerabilities/) [Accessed 15 June 2024]

Kovaitė, K. and Stankevičienė, J. (2019) Risks of digitalisation of business models. Contemporary Issues in Business, Management and Economics Engineering. Available from: [**https://www.researchgate.net/publication/333063956\_Risks\_of\_digitalisation\_of\_business\_models**](https://www.researchgate.net/publication/333063956_Risks_of_digitalisation_of_business_models) [Accessed 15 June 2024]

Prinsloo, J. et. al. (2019) A Review of Industry 4.0 Manufacturing Process Security Risks. *Applied Sciences*. Available from: [**https://www.mdpi.com/2076-3417/9/23/5105**](https://www.mdpi.com/2076-3417/9/23/5105) [Accessed 15 June 2024]

Trautman, L. J. & Ormerod, C. P. (2017) Corporate directors’ and officers’ cybersecurity standard of care: the yahoo data breach. american university law review. Available from: [**https://aulawreview.org/au\_law\_review/wp-content/uploads/2017/09/03-TrautmanOrmerod.pdf**](https://aulawreview.org/au_law_review/wp-content/uploads/2017/09/03-TrautmanOrmerod.pdf) [Accessed 15 June 2024]