The fourth industrial revolution, or Industry 4.0, is human society's 4th generational industrial advancement. This evolution is transforming business models with technologies that can provide enormous growth and innovation (Bai, c. et al., 2020, p.2).

Industry 4.0 includes new technologies like Cloud computing, the Internet of Things (IoT), and Big data but is not limited to it (Kovaitė, K. et al. 2019, p.380). We can see the use of cloud computing in our daily lives, i.e., online shopping and social media. For example, cloud computing is a business approach to selling IT services to conveniently share the network without owning any infrastructure (e.g., servers, storage). This model has allowed many businesses to start with less pre-purchase due to the pay-for-use model (Atobishi T, et al., 2018, p.11). Similarly, Big data is also a new concept where massive amounts of data are used to perform effective analysis to generate business value, i.e., user-based targeted advertisements (Atobishi T et al., 2018, p.13).

These technologies have brought significant changes to our society. However, they require more attention and evaluation as there are many risks to business models utilizing the new technologies from industry 4.0 (Kovaitė, K. et al. 2019, p.381). For instance, the wide use of the cloud providers such as Amazon web services and Azure can tightly couple the financial and technological decisions, as any changes in their system affect the business directly, making them less flexible (Tamvada J, 2022, p.3), thus creating a business risk. Furthermore, it can also create risk on the technical side as the system's complexity rises significantly, making it more prone to failure (Tamvada J, 2022, p.3).

In 2019, Facebook, a heavy user of AWS cloud computing services, faced
a significant data breach exposing 530 million users' data. This event caused Facebook to pay a massive fine of $5 billion to the US federal government as a settlement which is a significant legal risk(Bowman, E. (2021)).

Another example is a DDoS attack executed by hacked IoT devices known as Mirai Botnet. This botnet attack carried out a DDoS attack from multiple hacked devices and took down several major websites like CNN, Netflix, and Twitter(Uberoi, A. (2022)).

Despite the various risks, industry 4.0 is now a reality, and its implementation is used in various processes in the industry to achieve high efficiency. It is also used in susceptible areas such as healthcare industries providing consumers with easy access to its services (Badri, A. et al., 2018, p.410). As significant changes are implemented, previously implemented preventive measures will be outdated and present different risks to the existing business. Therefore the use of industry 4 technologies will be more ever present in our society.

The authors Badri, A., Boudreau-Trudel, B. and Souissi, A.S., 2018 also agree with the view shared by Kovaitė, K. and Stankevičienė, J. (2019) and dive more into the incorporation of industry 4 technologies in a sensitive sector like healthcare.

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.

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.

Atobishi, T., Gábor, S.Z. and Podruzsik, S., 2018. Cloud computing and big data in the context of industry 4.0: opportunities and challenges.

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.

Bowman, E. (2021) After data breach exposes 530 million, Facebook says it will not notify users, NPR. NPR. Available at: https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users (Accessed: March 11, 2023).

Uberoi, A. (2022) IOT security: 5 cyber-attacks caused by IOT security vulnerabilities, 9ine. Available at: https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-c yber-attacks-caused-by-iot-security-vulnerabilities (Accessed: March 11, 2023).

Badri, A., Boudreau-Trudel, B. and Souissi, A.S., 2018. Occupational health and safety in the industry 4.0 era: A cause for major concern?. Safety science, 109, pp.403-411.