Feedback (Response from Peers and Tutor)

Peer Response - Njideka
By Blessing Monsi - Tuesday, 22 August 2023, 7:24 AM

Hello Njideka,

Your initial post is spot on, and your point of view regarding the real-life example strikes a code. Rounding up your first paragraph by pointing out that the article also 'explores decentralisation of communication between people and machines' speaks a lot about the 4th industrial revolution.

Providing further real-life examples of some of the 4th industrial revolution concepts is also very helpful to a layman. You mention IoT assets being tracking devices used in tracking the location, condition, and status of assets in a manufacturing operation process. And inventory scanning drones to autonomous mobile robots that pick and place operations. I could not have agreed more on how you have been able to dissect your understanding of new technology and some uses that are very relatable.

Furthermore, the real-world scenarios you mentioned are very relatable in our industry today. We can not discuss cyber security without emphasising Data Security Risk as well as the role of DoS in today's technology. As you spotlighted in the Cybalt White paper, the probability of smart factories being subject to vulnerability exploitation is very high.

Outsourcing of cloud computing management services is one risk I believe is being taken for granted. As you mentioned, most companies expose enormous volumes of sensitive information to third-party companies, and the compromise of any critical password might lead to a breach of organisational and personal data confidentiality, integrity and make a company's data accessible to unauthorised persons (Sarangam, A. 2022).

It was fun and educational reading your initial post, and my response highlights my understanding and lessons.

Thank you,
Regards **Blessing**

References:

1. Cybalt Whitepaper. Industry 4.0 Cyber Security Challenges – How real it is? Available from :https://www.cybalt.com/docs/default-source/white_papers/cybalt-white-paper---industry-4.0-cyber-security-challenges---how-real-it-is.pdf[Accessed 22 August 2023].
2. Kovaitė, K. & Stankevičienė, J. (2019). Risks of Digitalisation of Business Models. Available from: https://www.researchgate.net/publication/333063956_Risks_of_digitalisation_of_business_models DOI:10.3846/cibmee.2019.039 [Accessed 20 August 2023].

Peer Response - Njideka
by Iyad Atieh - Friday, 25 August 2023, 5:39 PM

Dear Njideka,

Thanks for the informative post,

This is a very useful detail, where you have provided a reasonable explanation for the Internet of Things (IoT) and autonomous robots. However, I would like to add in addition to what you have explained, that the amount of data that IoT devices collect and transfer in the open internet made it out of control in terms of privacy since customers don't have the choice to agree or disagree on collecting these data. as an example, many of the big malls worldwide implement a vast number of IoT devices that monitor and collect the visitors behaviour while they are inside the mall that can help them to make business decisions and plan mall business.

I agree with your analysis of the technical risks of using cloud computing, and the stakes become higher if the company selects a cloud service provider that doesn't have a good level of security and data protection; because of that, companies have to make sure as part of the cloud provider selection process to perform vendor security risk assessment to assess their security maturity level.

Finally, the balance between new technology adoption and information security implementation is essential to minimise the risks that come with these technologies.

Thanks

Re: Summary Post
by Zeeshan Siddiqui - Friday, 8 September 2023, 11:49 AM

Hi Njideka,

A good discussion overall and a good use of the resources. I would recommend visiting the seminar recording to have more insight on this topic.

Thanks.
Dr Siddiqui.