Collaborative Discussion 1

Peer Review 1

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

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].

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 Review 2

Hello Iyad,

It was enlightening reading your Initial Post, and I like that you particularly mentioned the ‘increase in attack surface’ resulting from the rapid adoption of the new technologies as cited by the authors Kovaitė, K. & Stankevičienė, J. (2019).

The adoption of new technologies like IoT, AI, machine learning, robotics etc. has resulted in a dynamic and fast-paced cyber ecosystem. One of the major setbacks is that organizations see the need to move fast and increase production but tend to think about security in the later stage of business. As you rightly mentioned, ‘companies rarely evaluate or re-evaluate the change in the business model by implementing new technologies to avoid financial loss by adopting new business models.’ Another challenge affecting IoTs and other industry 4.0 technologies is the lack of updatable/patchable Operation Systems (OS). Most IoT devices currently in the market are difficult to patch.

According to an article by Zou .X. (N.D.) the biggest and most apparent security challenge with Internet of Things (IoT) devices such as connected medical devices is the inability to easily upgrade or patch them. Zou further explained that medical device manufacturers lack the expertise to support dynamic patches to their medical devices.

Little wonder why there are several vulnerable IoT devices on Shodan with known Cybersecurity and Infrastructure Security Agency's (CISA) top exploitable vulnerability and remain unpatched over the years.

As we know, anything connected to the internet has the potential of being hacked (increased attack surface). Therefore, some medical IoT devices are not connected to the internet, making it impossible to get the required update/patch to keep the devices vulnerability-free.

The above makes it extremely necessary to consider several risk assessment processes, especially Risk assessment for the Digitalization matrix RADi as mentioned by the authors. Ensuring that all key channels, key resources, and key activities are put into consideration to uncover the macro level in the risk assessment matrix.

References

1. 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].

2. Xu Zou (N.D.). IoT devices are hard to patch: Here's why—and how to deal with security. Available from: https://techbeacon.com/security/iot-devices-are-hard-patch-heres-why-how-deal-security. [Accessed 29 August 2023].