Summary Post

Introduction

According to Ortwin et al. (2021), digitalisation can drive the sustainable transformation of society and industry. Many of the opportunities of Industry 4.0 (Internet of Things (IoT), big data, cloud computing, robotics, and artificial intelligence) are linked with several cyber risks. The dynamics and uncertainties of digitalisation are complex; it is hence, imperative to develop a process, policy and structure that will help identify all information assets and dependencies within an organisation either stored, in transport or processed.

Technical and Behavioural Risks

Two real-world risks that fit into the authors' categories could be Technical Risks and Behavioural Risks.

Technical Risks could be System Compatibility and or Failure.

For example, to optimise its production processes, a manufacturing company that already uses SCADA (supervisory control and data acquisition) decides to implement IoT sensors and data analytics. However, while implementing it, it becomes evident that the new IoT sensors are not fully compatible with the existing hardware and software systems. This technical incompatibility could involve challenges related to technology integration and compatibility. According to NASA (N.D.), technical risk is associated with the evolution of the design and the production of the system of interest affecting the level of performance necessary to meet the stakeholder expectations and technical requirements. This concept is in line with Reim et al., (2016) findings stating that ‘Business must acquire numerous new capabilities and resources to be able to offer product-service solutions (PSS)’ as mentioned in Kovaitė & Stankevičienė, (2019).

Behavioural Risk on the other hand could be about Employee Resistance to Change.

For example, a retail company decided to implement a digital customer relationship management (CRM) system as part of its Industry 4.0 transformation. However, some employees are resistant to adopting the new system, fearing that it might replace their roles or require them to learn new skills. This behavioural risk could result in slower adoption rates, a lack of enthusiasm for using the new system, and reduced employee productivity.

To further identify security risks, industry 4.0 organisations can choose two or more threat modeling systems (e.g. STRIDE and OWASP) to decompose attacks into fundamental elements and plan responses to perceived threats.

I find the OWASP-recommended indicative actions for threat modeling to be both absorbing and encompassing. It employs a Cyber Kill chain, attack tree and weakness library (similar to MITRE ATT&CK).

While the above is suitable for new products or assets within an organisation, we must consider existing assets. 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. Companies must, therefore, create models that consider the ability to patch an IoT or automation asset and ensure there are compensating controls created around assets that might be difficult to patch or update in the future.

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.

Conclusion

Conclusively, experts must decide on which risk management system to adopt when outsourcing cloud computing services. 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 personal data confidentiality and the availability of a company’s private network system by an unauthorized person (Sarangam, A. 2022).

Finally, Deloitte's paper on Managing Risk in Digital Transformation (2018) supports the cited study while speaking directly to an established Digital transformation.

References

Deloittes (2018). Deloitte’s Digital Risk Framework. Available from: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_managing_risk_in_digital_transformation_112018.pdf. [Accessed 12 August].

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 10 August 2023]

Ortwinorcid, R., Grischaorcid, B., & Pia-Johanna S. (2017) The opportunities and risks of digitalisation for sustainable development: a systemic perspective. Available from: https://www-ingentaconnect-com.uniessexlib.idm.oclc.org/content/oekom/gaia/2021/00000030/00000001/art00007;jsessionid=1b6u9tefoolxy.x-ic-live-01 [Accessed 30 August 2023].

University of Essex Online Lecturecast 2 (2023) Threat Management and Modelling. Available from: https://www.my-course.co.uk/Computing/Cyber Security/SRM/SRM Lecturecast 2/content/index.html. [Accessed 27 August 2023].

Sarangam, A. (2021). Unext. Top 14 Challenges of Cloud Computing. Available from:https://u-next.com/blogs/cloud-computing/challenges-of-cloud-computing/ [Accessed 30 August 2023].