Collaborative Discussion 1: Digitalisation – What are the security implications of the digital economy?

Initial Post

by Gokul Kurunthasalam - Thursday, 23 June 2022, 11:04 AM
Number of replies: 3

What is a 'fully digital enterprise' (Banerji, 2019)?

The new digital business model orchestrates participants in the value chain with surprisingly low management and contracting overhead by making clever use of information and technology. It gives businesses the freedom to focus only on providing value to customers while delegating tasks to others who are better at them. Infinitely more capable of adapting to changing client needs will be the digital utility. (Banergi, 2019)

Cyber Security challenges/concerns with a fully digital enterprise:

The following cyber security issues/challenges could affect a fully digital enterprise: web-based attacks, malware, phishing, insider threats, ransomware, identity theft, data breaches and loss of mobile devices. (Spreić & Šimunic, 2018)

Cyber security challenges for a bricks and mortar SME wanting to become a digital enterprise:

Due to the online migration of everything, including people, processes, data, and infrastructure, 2020 witnessed the first-ever mass migration of SMEs toward digitization on a worldwide scale. Businesses of all sizes are susceptible to cyberattacks due to evolving work dynamics and the acceleration of digital transformation. They may cause loss of intellectual property, corporate data, customer trust, and other types of business harm. According to the HIPPA Journal (September 2020) the following are the cyber security challenges for a bricks and mortar SME wanting to become a digital enterprise (Kamaljeet Sandhu, 2021)

- Use of outdated technology Hardware and software
- Attacks using Third-Party Exposure
- Mobile Security threats
- Internet and Cloud Vulnerabilities
- Attacks through Social Engineering
- Highly Developed and Rising Ransomware Attacks
- Threats Related to Cutting-edge Technology
- Lack of In-house Trained Security Staff as well as Security Experts

Do you agree with the views expressed in the blog, especially in light of the 'energy crisis' experienced worldwide in 2022?

Yes, I agree with their views. Infinitely more capable of adapting to changing client needs will be the digital utility. Utility distribution companies are aware of this. According to our Digitally Enabled Grid research, most see growth opportunities as providers of energy-related data services to consumers, led by “distributed tariff information” (77 percent), “demand response program information and notifications” (71 percent) and “energy usage information provision” (69 percent). (Banergi, 2019)

References:

Kamaljeet Sandhu (University of New England, Australia) "Advancing Cybersecurity for Digital Transformation: Opportunities and Challenges" Source Title: Handbook of Research on Advancing Cybersecurity for Digital Transformation; Release Date: June, 2021; Copyright: © 2021; Pages: 16; DOI: 10.4018/978-1-7998-6975-7

Irvine Clarke III (James Madison University, USA) and Theresa B. Flaherty (James Madison University, USA). "Challenges of Transforming a Traditional Brick-and-Mortar Store into a Bricks-and-Clicks Model: A Small Business Case Study" Source Title: Journal of Electronic Commerce in Organizations (JECO) 2(4) copyright: © 2004 |Pages: 15; DOI: 10.4018/jeco.2004100106

G. Culot, F. Fattori, M. Podrecca and M. Sartor, "Addressing Industry 4.0 Cybersecurity Challenges," in IEEE Engineering Management Review, vol. 47, no. 3, pp. 79-86, 1 thirdquarter,Sept. 2019, doi: 10.1109/EMR.2019.2927559.

Spremić, M. & Šimunic, A. (2018). Cyber Security Challenges in Digital Economy. Proceedings of the World Congress on Engineering 2018 (1).

Banerji, R. (2019) Will the T&D utility of the future have a digital DNA? https://www.accenture.com/us-en/blogs/accenture-utilities-blog/will-the-td-utility-of-the-future-have-a-digital-dna [Accessed on 23rd Jun 2022