engineering proceedings

MDPI

Abstract

Safeguarding Food Industry: Understanding Cyberthreats and Ensuring Cybersecurity [†]

Adel Alqudhaibi *, Ashish Krishna, Sandeep Jagtap, Mohamed Afy-Shararah and Konstantinos Salonitis

Sustainable Manufacturing Systems Centre, School of Aerospace Transport and Manufacturing, Cranfield University, Cranfield MK43 0AL, UK; ashish.krishna.831@cranfield.ac.uk (A.K.); s.z.jagtap@cranfield.ac.uk (S.J.); m.a.shararah@cranfield.ac.uk (M.A.-S.); k.salonitis@cranfield.ac.uk (K.S.)

* Correspondence: adel.alqudhaibi@cranfield.ac.uk

[†] Presented at the International Conference on Industry 4.0 for Agri-food Supply Chains: Addressing Socio-economic and Environmental Challenges in Ukraine, Leicester, UK and Online, 24–25 July 2023.

Abstract: The food industry stands as one of the most vital manufacturing sectors globally, with an ever-increasing reliance on digitalization and technology-driven processes. However, this advancement comes with an inherent risk of cyberattacks, encompassing data breaches and system disruptions, which can severely impact production and disrupt the entire food supply chain. Consequently, such cyberthreats can lead to consumer fear and mistrust, potentially tarnishing a company's brand image. Additionally, the sector is becoming the focus of cyberthreat actors owing to the current crisis in Ukraine, revealing the severity of the rippling effects of these disruptions. This research aims to delve into the current perception of cyberthreats within the food industry, emphasizing the importance of cybersecurity and analyzing the measures taken by stakeholders to mitigate the risks associated with cyberattacks. The findings reveal that although the food industry acknowledges the potential threats posed by inadequate cybersecurity measures, these risks are perceived as insignificant due to the unique nature of the industry. Moreover, an extensive literature review highlights that the food industry places great emphasis on adopting innovative information technologies to enhance operational efficiency and cost-effectiveness. However, it remains vulnerable to cyberattacks, necessitating continuous employee education and training to strengthen the security landscape. This holistic approach fosters a seamless, reliable, and sustainable growth environment for the industry. By analyzing the existing challenges and requirements, this study underscores the need for proactive measures to safeguard the food industry against cyberthreats. It emphasizes the significance of implementing robust cybersecurity protocols and cultivating a culture of awareness and preparedness within organizations. Furthermore, the research emphasizes the importance of employee education and training, equipping them with the necessary knowledge and skills to identify and mitigate potential cyber risks. In conclusion, while cognizant of the risks posed by cyberattacks, the food industry must prioritize cybersecurity measures to protect its production and supply chain. Enhancing the security environment through ongoing employee education and training is crucial for fostering consumer trust and enabling seamless growth within the industry. By adopting a proactive approach to cybersecurity, the food industry can ensure the sustainability and reliability of its operations in the face of evolving cyberthreats.

Keywords: cybersecurity in the food industry; cyberthreats and food production; food industry and cyberattacks; preventing cyberattacks in food distribution; importance of employee education in food industry cybersecurity

Citation: Alqudhaibi, A.; Krishna, A.; Jagtap, S.; Afy-Shararah, M.; Salonitis, K. Safeguarding Food Industry: Understanding Cyberthreats and Ensuring Cybersecurity. *Eng. Proc.* **2023**, *40*, 11. https://doi.org/10.3390/engproc2023040011

Academic Editor: Hana Trollman

Published: 17 July 2023

Author Contributions: Data curation, A.A. and A.K.; Formal analysis, A.A., A.K., S.J., M.A.-S. and K.S.; validation, A.A. and S.J.; investigation, A.A., A.K., S.J. and M.A.-S.; methodology, A.A., A.K., S.J. and M.A.-S.; Writing—original draft, A.A., A.K., S.J., M.A.-S. and K.S.; writing—review and editing, A.A., A.K., S.J., M.A.-S. and K.S.; visualization, S.J. and K.S.; supervision, S.J.; software, A.A., S.J. and M.A.-S.; resources, M.A.-S.; project administration, K.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare that they have no known competing financial interest or personal relationships that could have appeared to influence the work reported in this paper.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.