Unit 5: Future Trends in Security and Risk Management

1. Describe the main emerging trends in the field.

The World Economic Forum (2023) offers a crucial perspective on the future of cybersecurity, outlining pivotal issues, tensions, and trade-offs that will define the industry. Its emphasis on the necessity of investing in security technology and combating cybercrime, along with its cautionary note on the potential risks of AI and ML technology, provides a comprehensive understanding of the field's trajectory, thereby underscoring the importance of this topic.

The advent of emerging trends and technologies is revolutionising the future of risk management. These innovations, such as artificial intelligence, machine learning, cybersecurity, big data analytics, and effective risk governance, empower organisations to avoid potential threats by proactively identifying, assessing, and mitigating risks. This transformation is projected to significantly influence research (Khan, 2023), thereby underscoring the importance of staying abreast of these developments and their transformative impact on the field.

Edge computing is poised to revolutionise data processing and analysis. By integrating advanced technologies like artificial intelligence and machine learning, real-time analytics, data visualisation, privacy and security measures, and ethical considerations, organisations can effectively handle, analyse, and interpret vast amounts of data. These advancements will empower businesses to extract valuable insights from complex data sets, driving informed decision-making and making edge computing a pivotal element of any successful data strategy (Amber Innovations Limited, 2023), thereby highlighting the field's future direction.

Therefore, Khan (2023) states that the emerging security and risk management trends include big data analytics and AI/ML. Big data analytics allows organisations to extract insights from data sources and proactively identify potential risks. AI/ML provides advanced analytics capabilities that enable organisations to analyse vast amounts of data, assess real-time risks, detect anomalies, and automate risk assessment processes. AI techniques are increasingly used for managing operational, credit, market, liquidity, and compliance risks, specifically in financial risk management. Integrating AI in risk management transforms how businesses predict, analyse, and mitigate uncertainties, improving the efficiency and accuracy of risk assessment strategies.

2. **Delve into the potential impact of these emerging trends on research, providing a comprehensive understanding of their implications.**

The impact of new technologies in the next decade will be significant, shaping global economic, social, and military developments. Four technology arenas, including information technology, new manufacturing and automation technologies, breakthroughs in critical technologies, and the latest health technologies, will bring about drastic changes in the world. Governments and societies must find ways to capture the benefits of these new technologies while dealing with the latest threats they present. The growth and diffusion of these technologies will present significant challenges for governments and societies, and they must rise to the occasion (DNI, 2012).

Emerging security and risk management trends will significantly impact our lives by 2030 (ENISA, 2023). The increasing risk of supply chain compromise of software

dependencies, advanced disinformation and influence operations campaigns, and the rise of digital surveillance authoritarianism will lead to a loss of privacy.

Moreover, we should be aware of potential threats such as human error, exploited legacy systems within cyber-physical ecosystems, targeted attacks (such as ransomware) enhanced by smart device data, and a lack of analysis and control of space-based infrastructure and objects.

We need to tackle advanced hybrid threats, address the shortage of skilled personnel, and be wary of cross-border ICT service providers that could become a single point of failure. We cannot ignore AI's potential abuse, as it could be exploited for nefarious purposes.

Additionally, we must prepare for increased digital currency-enabled cybercrime, exploitation of e-health and genetic data, tampering with deep fake verification software supply chain, attacks using quantum computing, exploitation of unpatched and out-of-date systems within the overwhelmed cross-sector tech ecosystem, AI disrupting/enhancing cyber-attacks, malware insertion to disrupt the food production supply chain, technological incompatibility of blockchain technologies, disruptions in public blockchains, physical impacts of natural/environmental disruptions on critical digital infrastructure, and manipulation of systems necessary for emergency response.

It is crucial to take all these threats seriously and work together to mitigate their risks, as ENISA (2023) highlights.

3. **Recommend which you think will be most influential.**

Edge computing is a technology that processes client data at the network's edge, allowing for real-time processing and reducing latency and bandwidth limitations (Bigelow, 2021). Edge computing is expected to significantly impact the industry in the

next few years, as per Pratt's (2024) statement, with the market projected to grow exponentially due to increasing demand for sustainable products and the adoption of cutting-edge technologies (The Industry Outlook Report, 2024). While it offers benefits such as improving cybersecurity and increasing computer speed, it also presents security risks that require strict auditing protocols and access restrictions (Nolle, 2021).

References:

- World Economic Forum. (2023). *7 trends that could shape the future of cybersecurity in 2030*. [online] Available at: https://www.weforum.org/agenda/2023/03/trends-for-future-of-cybersecurity/.
- Khan, M. S. (2023). *The Future Emerging Trends in Risk Management – Key Highlights for 2024 & Beyond*. [online] Available at: https://www.linkedin.com/pulse/future-emerging-trends-risk-management-key-highlights-m-salman-khan--3vxif.
- Amber Innovations Limited (2023). *Edge Computing: The Future of Data Processing and Analysis*. [online] Available at: https://www.linkedin.com/pulse/edge-computing-future-data-processing-analysis-amber-innovations-vyi8c/.
- DNI (2012). *Global Trends 2030*. [online] Available at: https://www.dni.gov/files/documents/GlobalTrends_2030.pdf.
- ENISA (2023). *ENISA Foresight Cybersecurity Threats for 2030*. [online] Available at: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030.
- Bigelow, S.J. (2021). *What Is Edge Computing? Everything You Need to Know*. [online] Techtarget. Available at: https://www.techtarget.com/searchdatacenter/definition/edge-computing.
- Pratt, M. K. (2024). *5 edge computing trends to watch in 2022 and the future*. [online] Available at: https://www.techtarget.com/searchcio/tip/Top-edge-computing-trends-to-watch-in-2020.
- Industry Outlook Report (2024). Edge Computing Market Challenges (2023-2030). [online] Available at: https://www.linkedin.com/pulse/edge-computing-market-challenges-2023-2030/.
- Nolle, T. (2021). *Edge computing security risks and how to overcome them*. [online] IoT Agenda. Available at: https://www.techtarget.com/iotagenda/tip/Edge-computing-security-risks-and-how-to-overcome-them.