In the case study by Kovaitė and Stankevičienė (2019), the term "Industry 4.0" refers to the fourth industrial revolution, characterized by the integration of digital technologies and automation into manufacturing processes. Two examples of Industry 4.0 technologies are:

1. Internet of Things (IoT): This technology enables machines and devices to connect and communicate with each other, facilitating real-time data exchange and automation in manufacturing.
2. Artificial Intelligence (AI): AI systems can analyze vast amounts of data, make decisions, and perform tasks that traditionally required human intervention. In Industry 4.0, AI is used for predictive maintenance, quality control, and optimizing production processes.

Real-world examples of risks that fit into the categories mentioned by the authors are:

1. Cybersecurity breaches: With the increasing connectivity of devices and systems in Industry 4.0, there is a higher risk of cyberattacks. These attacks can disrupt operations, lead to data breaches, or compromise the safety of the industrial processes.
2. Job displacement: As automation and AI technologies advance, there is a concern that certain job roles may become obsolete or significantly reduced. This can lead to unemployment and social implications if not properly managed.

The introduction of case study Kovaitė and Stankevičienė, 2019 discusses the impact of Industry 4.0 and digitalization on businesses and individuals. It highlights the technological drivers of Industry 4.0, such as the Internet of things, big data, cloud computing, robotics, and artificial intelligence. The lack of a systematic approach to assessing risks and testing changes in business models due to digitalization is also mentioned. The article is divided into four sections: exploring recent scientific publications on the risks of digitalization, explaining the empirical methodology of the research, presenting the research findings, and providing conclusions and suggestions for further research. The researchers use an analysis of scientific literature and the

The literature review on risk assessment in business models driven by Industry 4.0 focused on articles related to risk, Industry 4.0, digitalization, and business models. Only 15 articles were found that discussed all dimensions between 2014 and 2018, indicating a research gap in this area. Risk was defined as the probability of loss and its impact on the enterprise. Business models were described as a set of mechanisms that create and capture value for customers. The use of Osterwalder's Business Model Canvas was prevalent in the reviewed research. While the advantages of

Industry 4.0 are widely discussed, the risks and uncertainties associated with this transformation are not thoroughly investigated, particularly in decision-making related to alternative business models driven by Industry 4.0. These risks include data value, cybersecurity, function criticality, scalability of failure, misuse of ownership, and cost of mistakes.

Data Breach: One example of a risk related to data value and cybersecurity is a data breach in a financial institution. In 2017, Equifax, one of the largest credit reporting agencies, suffered a massive data breach that exposed sensitive personal information of approximately 147 million individuals.

The breach not only resulted in financial losses for Equifax but also exposed individuals to identity theft and financial fraud, highlighting the importance of robust cybersecurity measures and the value of protecting customer data. The scientific focus on Industry 4.0 has primarily been on individual pillars such as the Internet of Things, big data, and cloud computing. Digitalization and Industry 4.0 have been studied in various areas such as smart homes, healthcare, and intelligent factories. Different patterns of business models, such as supply chain and value creation, have also been explored. While the advantages and benefits of Industry 4.0 are widely discussed, there is limited research on the risks and uncertainties associated with this transformation, particularly in decision-making for alternative business models. Risks include data value, cybersecurity, function criticality, scalability of failure, misuse of ownership, and cost of mistakes.

The article concludes by highlighting the contributions it makes to the scientific literature, practical level, and national level. It introduces a matrix of risk assessment called RADi, which evaluates the relation between two factors against an object. RADi can be used as a decision-making support tool for enterprises planning and implementing changes in their business models driven by Industry 4.0. It also has implications for policymakers, who can use RADi to identify risky areas of business model digitalization. The article acknowledges the limitations of the research and suggests future studies that could integrate macro-level risks and explore the concept of Industry 5.0.

The scientific focus on Industry 4.0 has primarily been on individual pillars such as the Internet of Things, big data, and cloud computing. Digitalization and Industry 4.0 have been studied in various areas such as smart homes, healthcare, and intelligent factories. Different patterns of business models, such as supply chain and value creation, have also been explored. While the advantages and benefits of Industry 4.0 are widely discussed, there is limited research on the risks and uncertainties associated with this transformation, particularly in decision-making for alternative business models. Risks include

data value, cybersecurity, function criticality, scalability of failure, misuse of ownership, and cost of mistakes.

The article concludes by highlighting the contributions it makes to the scientific literature, practical level, and national level. It introduces a matrix of risk assessment called RADi, which evaluates the relation between two factors against an object. RADi can be used as a decision-making support tool for enterprises planning and implementing changes in their business models driven by Industry 4.0. It also has implications for policymakers, who can use RADi to identify risky areas of business model digitalization. The article acknowledges the limitations of the research and suggests future studies that could integrate macro-level risks and explore the concept of Industry 5.0.

The introduction of case study Kovaitė and Stankevičienė, 2019 discusses the impact of Industry 4.0 and digitalization on businesses and individuals. It highlights the technological drivers of Industry 4.0, such as the Internet of things, big data, cloud computing, robotics, and artificial intelligence. The lack of a systematic approach to assessing risks and testing changes in business models due to digitalization is also mentioned. The article is divided into four sections: exploring recent scientific publications on the risks of digitalization, explaining the empirical methodology of the research, presenting the research findings, and providing conclusions and suggestions for further research. The researchers use an analysis of scientific literature and the FARE method for multicriteria decision support. (Schwab, Davis, & Nadella, 2018; Li, 2018; L. D. Xu, E. L. Xu, & Li, 2018; Roblek, Meško, & Krapež, 2016).

The literature review on risk assessment in business models driven by Industry 4.0 focused on articles related to risk, Industry 4.0, digitalization, and business models. Only 15 articles were found that discussed all dimensions between 2014 and 2018, indicating a research gap in this area. Risk was defined as the probability of loss and its impact on the enterprise. Business models were described as a set of mechanisms that create and capture value for customers. The use of Osterwalder's Business Model Canvas was prevalent in the reviewed research. While the advantages of Industry 4.0 are widely discussed, the risks and uncertainties associated with this transformation are not thoroughly investigated, particularly in decision-making related to alternative business models driven by Industry 4.0. These risks include data value, cybersecurity, function criticality, scalability of failure, misuse of ownership, and cost of mistakes.

Data Breach: One example of a risk related to data value and cybersecurity is a data breach in a financial institution. In 2017, Equifax, one of the largest credit reporting agencies, suffered a massive data breach that exposed sensitive personal information of approximately 147 million individuals. The breach not only resulted in financial losses for Equifax but also exposed individuals to identity theft and financial fraud, highlighting the importance of robust cybersecurity measures and the value of protecting customer data.

The scientific focus on Industry 4.0 has primarily been on individual pillars such as the Internet of Things, big data, and cloud computing. Digitalization and Industry 4.0 have been studied in various areas such as smart homes, healthcare, and intelligent factories. Different patterns of business models, such as supply chain and value creation, have also been explored. While the advantages and benefits of Industry 4.0 are widely discussed, there is limited research on the risks and uncertainties associated with this transformation, particularly in decision-making for alternative business models. Risks include data value, cybersecurity, function criticality, scalability of failure, misuse of ownership, and cost of mistakes.

The article concludes by highlighting the contributions it makes to the scientific literature, practical level, and national level. It introduces a matrix of risk assessment called RADi, which evaluates the relation between two factors against an object. RADi can be used as a decision-making support tool for enterprises planning and implementing changes in their business models driven by Industry 4.0. It also has implications for policymakers, who can use RADi to identify risky areas of business model digitalization. The article acknowledges the limitations of the research and suggests future studies that could integrate macro-level risks and explore the concept of Industry 5.0.

Reference:

Krebs, B. (2017, September 14). Equifax Hackers Stole 200k Credit Card Accounts in One Fell swoop Equifax Hackers Stole 200k Credit Card Accounts in One Fell Swoop – Krebs on Security

System Failure in Critical Infrastructure: Another example of a risk related to function criticality and scalability of failure is a system failure in critical infrastructure. In 2018, the Atlanta city government experienced a ransomware attack that crippled several key systems, including the court system, public safety operations, and even the payment processing for water bills. The incident disrupted critical services, leading to delays, financial losses, and public inconvenience, highlighting the vulnerability of essential infrastructure systems to cyber threats.

Reference:

Kelli, Young. (2021, Sept 20) Cyber Case Study: City of Atlanta Ransomware Incident - CoverLink Insurance - Ohio Insurance Agency