International Journal of Sustainable Transportation

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ujst20

A shift to green cybersecurity sustainability development: Using triple bottom-line sustainability assessment in Qatar transportation sector

Khalifa AL-Dosari, Noora Fetais & Murat Kucukvar

To cite this article: Khalifa AL-Dosari, Noora Fetais & Murat Kucukvar (2023): A shift to green cybersecurity sustainability development: Using triple bottom-line sustainability assessment in Qatar transportation sector, International Journal of Sustainable Transportation, DOI: 10.1080/15568318.2023.2171321

To link to this article: https://doi.org/10.1080/15568318.2023.2171321

Published online: 01 Feb 2023.

INTERNATIONAL JOURNAL OF SUSTAINABLE TRANSPORTATION
https://doi.org/10.1080/15568318.2023.2171321

A shift to green cybersecurity sustainability development: Using triple bottom-line sustainability assessment in Qatar transportation sector

Khalifa AL-Dosari, Noora Fetais, and Murat Kucukvar

College of Engineering, Qatar University, Doha, Qatar

ABSTRACT

Green cybersecurity is the emerging trend in the new era and this green cybersecurity technology minimizes the negative effects of IT operations and implements a green sustainable environment. Therefore, the study conceptually draws the concept of green cybersecurity by applying the theory of reasoned action (TRA) assumptions that logically support green information technology acceptance. Using a convenient sampling, the data were collected from Qatar transport industries, particularly the IT experts and managers, to get responses on the implementation of green cybersecurity and sustainability of 5 transport companies in Doha, Qatar. Using Smart PLS-SEM, the study employed the SEM technique to test the proposed hypotheses. The results reported that green cybersecurity's control/position, integrity, and authenticity significantly and positively influenced TBL sustainability, but confidentiality, availability, and utility do not. The implementation of industry 4.0 makes them accessible and more effective to ensure TBL sustainable development in the transport industries in Qatar. Applying green cybersecurity in this setting will improve services in transportation sector. A green cybersecurity platform will make it a point to systematically search for and promote innovations made possible by smart green technologies to avoid carbon-emission vehicles. Through the efficient and cutting-edge green, cybersecurity will be Qatar's transportation sector's primary responsibility to contribute to Qatar's sustainable development. In order to accomplish this goal, the regulator must create and implement it. In addition, it emphasizes the importance of adopting green cybersecurity to confront the difficulties facing city transportation all over Qatar as a foundational component of achieving long-term sustainable development.

ARTICLE HISTORY
Received 26 May 2022
Revised 29 September 2022
Accepted 18 January 2023

KEYWORDS
Green cybersecurity; quantitative research; sustainability development; transport sector; triple bottom-line

1. Introduction

Cybersecurity is one of the most critical global economic, social, and environmentally sustainable development issue. Qatar is facing the same in the transportation sector because Qatar has already paid a huge price to current cybersecurity frameworks (Al-Mhiqani et al., 2018). If the transportation system expands without proper planning, the government may become susceptible to long-term harm resulting in unpredictably high cyber-attacks (Badran, 2021; Brown, 2018). Quick degradation can occur due to cybersecurity practices such as expanding on low elevation land and failing to consider the need for resilience while planning and the critical challenges in the transport and communication sector because cybercrime crosses borders and affects information systems (Tabassum et al., 2018). Abeyratne (2019) reported that cybersecurity threats and attacks had disconnected Qatar air transport and it was happened due to cyber-attacks and illegal approaches to transport agencies. For long-term viability, transportation agencies are compelled to undergo a transformation that the industry has never seen before (Jabbar et al., 2022). And industry 4.0 makes cybersecurity practices more comment to handle cyber-attacks in any industry (Adjetey-Bahun et al., 2016; Akgül et al., 2018) because the Fourth Industrial Revolution, often known as Industry 4.0, is the ongoing automation of conventional manufacturing and production procedures through contemporary intelligent technologies (Awan, Sroufe & Shahbaz, 2021). The incorporation of machine-to-machine interaction and the internet of things (IoT) contributes to a rise in automation, an improvement in communications and self-monitoring, and the advancement of intelligent machines capable of analyzing and detecting potential problems.

The current cybersecurity system is inappropriate for eradicating cybersecurity threats and attacks, and advanced green technologies have always been neglected (Serdar et al., 2022; Sulich et al., 2021; Tvaronavičienė et al., 2020; Zhu et al., 2008). There is no literature about green cybersecurity; however, this study adapted the concept of green cybersecurity from Arpaci and Sevinc (2021) for economic, environmental, and social sustainability (i.e., triple bottom line sustainability), who developed and introduced the components of cybersecurity (i.e., confidentiality, control/-position, integrity, authenticity, availability, and utility). The concept of green cybersecurity has been drawn from

CONTACT Khalifa AL-Dosari 200704317@qu.edu.qa College of Engineering, Qatar University, Doha, Qatar.

green literature such as Hahanov et al. (2017) claimed that green cyber-physical culture is the ultimate enable of green social, technological, cyber, and environmentally sustainable development. Green cybersecurity covers not only the processes linked to energy generation but also those associated with manufacturing products and services (Pansare et al., 2023). The method's objective is to compare the degree of current cybersecurity and cybersecurity with green technological growth on the international stage, referred to as the Green Cybersecurity, and those working toward creating more economic sustainability (Eurostat, 2015). Sulich et al. (2021) made it possible to estimate the anticipated economic, social and environmental processes through green cybersecurity. The decision-making procedures addressed green cybersecurity and the element of sustainable development. Shackelford et al. (2016) prospects the green future of cybersecurity and IT technologies in sustainability development. They further stated that The time for change is now. To construct a path toward long-term cybersecurity, the route forward involves adopting what has succeeded and what hasn't in other situations, such as the green movement (i.e., green cybersecurity). Liu and Mishra (2022) and Addanki and Venkataraman (2017) stated that green technologies contribute to a greener future for humans, whereby users are more aware of the consequences of technology on economic, social, and environmental sustainability. Despite these benefits, there are still significant barriers to proposing, developing, and adopting green technologies.

In the case of Qatar's transportation blockages, several cyberattacks on a transport media outlet's information and communication platform formed the justification for transportation barricades that impacted Qatar's financial systems and public interest (Serdar et al., 2022). The cyberattack resulted in a spiraling disruption of transportation, as well as assisting economic repercussions for the Qatari government, community, and industry (Badran, 2021; Brown, 2018). These consequences were induced by public and private responses to the attacks, including the initial transport panic caused by the expansion of false news. In addition, the cyberattack had a negative impact on Qatari society (Badran, 2021; Serdar et al., 2022). The expansion of transportation is inextricably linked to the expansion of the economy. This is because green cybersecurity technologies offer green technologies that can cut the time and carbon emission wasted on the roads (Du et al., 2018; Pradhan & Bagchi, 2013; Wang et al., 2020). Furthermore, the integration of previous cybersecurity technologies and green cybersecurity create comprehensive modes of transportation, and the growing number of people driving electric vehicles both have the potential to significantly cut greenhouse gas emissions (Bertaud et al., 2011). Various dangers could have been posed to various cybersecurity technologies in the past, but now green cybersecurity is the emerging energy-transition strategy to remove negative effects (Serdar et al., 2022; Yang et al., 2020). Because of green cybersecurity, transportation accessibility to the general public affect the vital economic, social, and environmental roles that they play, the vast variety of potential victims that an assault could cause, and transportation networks are susceptible to being attacked by terrorists (Adjetey-Bahun et al., 2016; Tonn et al., 2021).

Lim and Taeihagh (2018) also explored that cybersecurity is the ultimate enable for sustainable development in the transportation sector. According to Arpaci and Sevinc (2021), cybersecurity is concerned with the accessibility of information with confidentiality, control/position, integrity, authenticity, availability, and utility. Organizations and agencies should put appropriate security measures to achieve efficient objectives. Such activities are referred to as green cybersecurity because they protect procedures and energy-saving, industry 4.0 to get a sustainable environment (Cheng et al., 2021; Sulich et al., 2021). Moreover, according to Sataloff et al. (2019), "the convergence of Industry 4.0-driven activities and the rapid advances of information technology means that It can minimize cybercrimes and security threats. The efficient deployment of Industry 4.0 ensures sustainability development (Díaz-Chao et al., 2020). Despite this, there has been little discussion in the literature on the major determinants of Industry 4.0 that operate as capacities and increase sustainability (Akhtar et al., 2020; Bai et al., 2020). Besides, even though it is clear that determinants are important, there has been little empirical research on their significance in Industry 4.0 and sustainability practices implementation (Díaz-Chao et al., 2020; Miśkiewicz & Wolniak, 2020) because the digitalization of industry is a critical component of Industry 4.0 and a prerequisite for meeting the Green goals and sustainability development (Miśkiewicz & Wolniak, 2020). Disclosing the uncovered area of green cybersecurity and sustainability development, this study conceptual explores the effects of green cybersecurity and its dimensions on Triple Bottom Line (TBL) sustainability through the mediating role of Industry 4.0 implementation (Jayashree et al., 2021) in the transportation sector of Qatar. Therefore, the study develops the research objectives:

1. To examines the influence of green cybersecurity factors on industry 4.0 implementation; (2) to assess the impact of industry 4.0 implementation on Qatar transportation TBL sustainability; and (3) to explore the mediating role of industry 4.0 implementation between the factors of green cybersecurity and Qatar transportation TBL sustainability.

This study identified research gaps and problem statements and then developed research objectives. In the literature review section, the study defines the underpinning theories that support the novel idea of green cybersecurity. Furthermore, the literature review section provides the literature that supports the development of research hypotheses. In the next methodology section, the study defined the research design, methods, and techniques to conduct a survey questionnaire. In the next results section, the study describes the results in detail, and the last section elaborates on the results, practical implications, and future directions.

2. Conceptual framework and hypotheses development

2.1. Green cybersecurity and underpinning theories

The present study defines green cybersecurity as refers to the procedures utilized to improve or optimize IT technologies. It encompasses processes that reduce energy wastage and consumption and includes the processes that conserve bandwidth and any other strategy to minimize energy usage and, indirectly, cost. Because green cybersecurity is an emerging issue that directly and indirectly deals with social, economic, and environmental concerns (Sulich et al., 2021), it enhances sustainable development. However, the concept of "security" in cybersecurity is frequently concerned with the provision of information's integrity, confidentiality, and accessibility (Pype et al., 2017). On the other side, the study reported that green IC technologies provide crucial measures to handle economic, social, and environmental issues and promote sustainable development (Bai et al., 2020; Rutkowska & Sulich, 2020). Technological advances with green IT should be designed and implemented regularly to ensure compliance with regulations and handle security threats (Rutkowska & Sulich, 2020).

The principle of Industry 4.0, along with its antecedents (Kazancoglu et al., 2021; Yadav et al., 2020), has emerged as a critical concept for transport agencies to achieve TBL sustainability in this modern world, prompting numerous types of research to be conducted throughout subject areas. The majority of the studies on Industry 4.0 embedded the Technology-Organization-Environment (TOE) theory and the Diffusion of Innovation (DOI) model as per recommended by Arnold et al. (2018) and Lin et al. (2018), and only one study paves the footprints of green cybersecurity toward Industry 4.0 determinants and TBL sustainability (Rutkowska & Sulich, 2020; Sulich et al., 2021) from the agency theory perspective (Díaz-Chao et al., 2020). Because Industry 4.0 represents a dynamic circular economy in which green resources must be designed to gain sustainability development, while examining the predictors to transportation sector. Thus, using the DCV, the present study demonstrates that the dimensions of green cybersecurity serve as the underpinnings for Industry 4.0 implementation and have a significant impact on TBL sustainability assessment, allowing Qatar transportation sector to achieve a competitive edge while remaining sustainable in terms of economic, social and environmental antecedents.

2.2. Green cybersecurity and TBL sustainability

The present study defines green cybersecurity as the procedures utilized to improve or optimize IT technologies. It encompasses processes that reduce energy wastage and consumption and includes the processes that conserve bandwidth and any other strategy to minimize energy usage and, indirectly, cost. The concept of "security" in cybersecurity, on the other hand, is typically focused on ensuring the integrity, confidentiality, and accessibility of data (Pype et al., 2017). Lim and Taeihagh (2018) also looked into how cybersecurity is the ultimate enabler for sustainable transportation development. Cybersecurity is related to the access of information with secrecy, control/position, integrity, validity, availability, and utility, according to Arpaci and Sevinc (2021). The idea of targeting green cybersecurity is that the next generations may implement cybersecurity, data protection, and sustainability that would be critical to the digital transformation process (Sulich et al., 2021).

The industries should work together to develop effective methods for sustainable development. Several studies in the literature enact the relationships between green IT, cybersecurity, and sustainability development, such as Sulich et al. (2021) prospect that green cybersecurity would have a significant role in adopting and setting sustainability development as well as for security and privacy purposes. Hahanov et al. (2017) also claimed the positive effects of green cyber-physical culture in implementing sustainable development. Mondejar et al. (2021) also stated that the modern digitalization of IT technologies might have a crucial role in developing social, economic, and environmentally sustainable development. Shackelford et al. (2016) and Liu and Mishra (2022) also claimed in favor of providing evidence that sustainable cybersecurity with future trends of the green movement is significantly related to reducing cyberattacks. The green trend of cybersecurity may have a bright future in managing and handling cyberattacks that would offer sustainable development. Based on the above pieces of literature facts, the study conceptually proposes the research hypotheses:

H_1. There is a direct positive and significant relationship between TBL sustainability and confidentiality (a), control/possession (b), integrity (c), authenticity (d), availability (e), and utility (f).

2.3. Triple bottom line and sustainability

Following the Brundtland Report (UN, 1987), the community has become more cognizant of the manufacturing company's environmental effects (Kiel et al., 2020; Rutkowska & Sulich, 2020). Aside from earnings, consumers and their concerns were given significant consideration (McWilliams et al., 2016), culminating in many corporate responsibilities in the manufacturing industries (Pansare et al., 2021; Paz et al., 2021). Sustainability has captivated the world's attention by designing the triple bottom line assessment due to its relevant ideas and suggestions about the environment and climate change (Khan et al., 2021; Sataloff et al., 2019). Industrial sustainability seeks profit (Schulz & Flanigan, 2016), while social and environmental sustainability promotes humans and the community (Bai et al., 2020). Furthermore, the TBL expects a progressive relationship between all three to avoid conflict. Sustainability requires considering all 3 components (Schulz & Flanigan, 2016). So, the study may have predicted that green cybersecurity and industry 4.0 implementation may enhance the sustainable development of the Qatar transportation sector through three dimensions of a sustainable assessment framework.

2.4. Green cybersecurity, industry 4.0 implementation, and TBL sustainability

Green cybersecurity and industry 4.0 technological advancements direct TBL sustainability because green practices over the internet highly recommend industry 4.0 advancements to increase TBL sustainable development in circular economy (Sulich et al., 2021; Yadav et al., 2020). The researchers also reported that green internet securities with industry 4.0 technology enact social, economic, and environmental sustainability (Sataloff et al., 2019). Surprisingly, Rutkowska and Sulich (2020) examined that green IC technologies play a significant role in implementing the industry 4.0 revolution and promoting TBL sustainability. That concept may happen in the transportation sector of Qatar because several IC technologies with green environmental backgrounds promote service sustainability (Añón Higón et al., 2017). As part of a massive 4th Industrial Revolution, AI machines and technologies that can analyze and evaluate identified problems are being developed to help increase mechanization and enhance communication and transportation industries (Awan, Sroufe, & Shahbaz, 2021). With the implementation of cybersecurity systems, Industry 4.0 introduces a unique industrial approach that allows for the development of economic, social, and environmental sustainability (Rutkowska & Sulich, 2020; Sulich et al., 2021).

Most of the green technologies and cybersecurity systems are tied to the internet, so to reduce cyber-attacks and security threats, carbon footprints, algorithms, and cybersecurity systems should be modernized according to green internet technologies (Vrchota et al., 2020); however, industry 4.0 made it possible to think in the future (Kazancoglu et al., 2021; Miśkiewicz & Wolniak, 2020; Rutkowska & Sulich, 2020; Vrchota et al., 2020). It can implement the solutions provided by green cybersecurity in virtually any sector (Sulich et al., 2021). The study places a strong emphasis on functioning with green cybersecurity systems (Sulich et al., 2021), intending to increase sustainability, so this also lessens the necessity and recurrence of repair or replacement (Fraser, 2020; Sataloff et al., 2019), as well as the ability to implement stepwise strategies for improvement instead of pressuring large-scale replacement parts of the equipment (Jayashree et al., 2021). They also introduced internet services with accurate green digital monitoring and reliable metrics in the transportation, manufacturing (Pansare et al., 2021), education, and scientific fields. Mondejar et al. (2021) also supported by offering solutions and supporting the sustainable development of a smart Green cyber, digitalization, and internet of things. The benefits of combining IoT, big data governance, and cybersecurity have already been proved.

These are essential organizational trends for boosting sustainable output (Bai et al., 2020). Industry 4.0 technologies help overcome obstacles such as fierce competition, changing market needs, modifications, and product life cycles (Kazancoglu et al., 2021; Telukdarie & Shisane 2018) while contributing to current societal sustainable growth (Reza et al., 2020; Sataloff et al., 2019). Besides, Industry revolution 4.0 contributes significantly to organizational and societal sustainability (Stock & Seliger, 2016). Jayashree et al. (2021) reported that industry 4.0 implementation significantly influences and promotes TBL sustainability in small and medium enterprises (SMEs). Reduced set-up times, labor costs, and lead times increase organizational profit (Bai et al., 2020). Such solutions reduce waste, boost energy efficiency (Zhu et al., 2008), and promote reuse and recycling (Kumar et al., 2020). Employees' safety measures are protected by digital and intelligent technology, which reduces monotony and repetitive duties, hence motivating employees and greater job satisfaction (Müller et al., 2018). Companies should develop eco-friendly Industry 4.0 technology for sustainable production methods to efficiently use resources (Ghobakhloo, 2020). Thus, adopting and implementing Industry 4.0 will help Indian manufacturing industries stay competitive and contribute to the country's sustainable development. Based on the literature evidence, the study proposes the research hypotheses (Figure 1).

H_2. Industry 4.0 implementation mediates the relationship between confidentiality and TBL sustainability

H_3. Industry 4.0 implementation mediates the relationship between control/possession and TBL sustainability

H_4. Industry 4.0 implementation mediates the relationship between integrity and TBL sustainability

H_5. Industry 4.0 implementation mediates the relationship between authenticity and TBL sustainability

H_6. Industry 4.0 implementation mediates the relationship between availability and TBL sustainability

H_7. Industry 4.0 implementation mediates the relationship between utility and TBL sustainability

3. Research methodology

The reason for using the Quantitative research method is that it is the more appropriate and advanced trend of investigating the significant relationships between cybersecurity implementation and industrial sustainability (Fraser, 2020). The study presents a flowchart that describes the flow of the research. First, the study defined the research objectives from the literature gaps. The study conducted a literature review and supported the research hypotheses with the help of underpinning theories and literature pieces of evidence. Third, the study used a quantitative research design to answer the research questions in the Qatar transportation sector. The study used a quantitative research design by following a deductive approach to do a cross-sectional approach. Later, the study conducted a survey questionnaire using a convenient sampling approach. In the end, the study used Smart PLS 3.3.3 software to extract the results to accept and reject the research hypotheses (Figure 2):

3.1. Data collection and sample size

The large number of software programs used by transport and transportation companies aim to increase operating

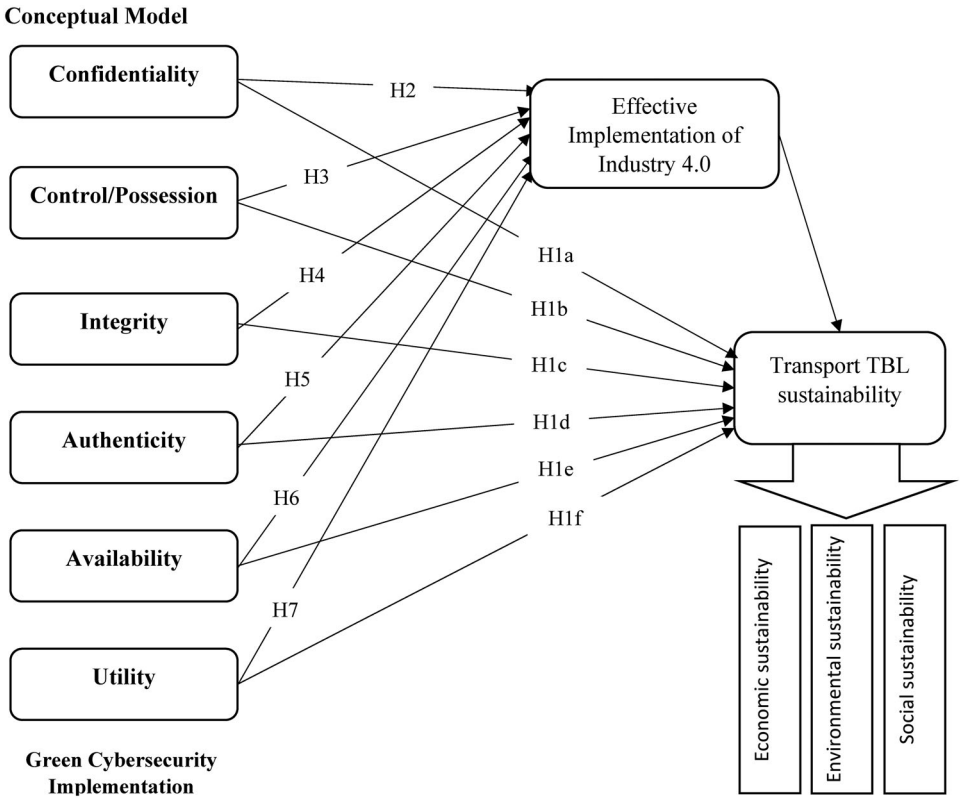

Figure 1. Conceptual model.

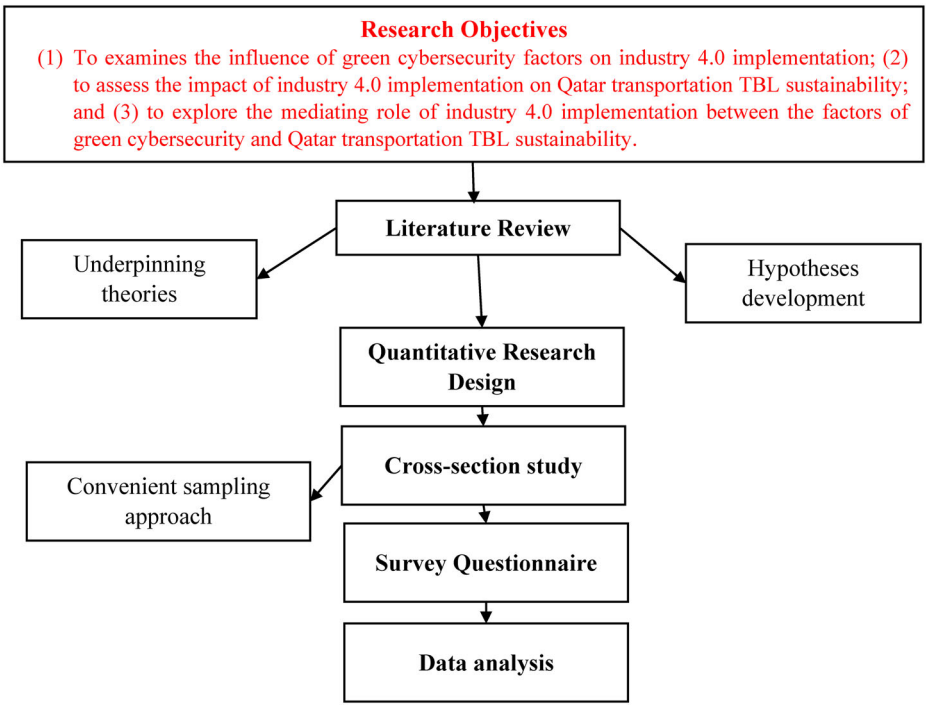

Figure 2. Research methodology flowchart.

efficiency. Still, this sector faces unwanted threats and security attacks, so this sector is at significant risk of being targeted by cybercriminals. Using software programs, they could access sensitive information such as the contents of shipments, the private details of their employees, company associates, customers, and other information. Finally, the study aims at implementing a green cybersecurity system with the help of industry 4.0 to obtain a maximum competitive advantage in sustainable development. The study particularly targets the IT experts in the Qatar transportation sector. Qatar's transportation sector faces the highest cyberattacks and threats to regular flights, ticket reservations, online booking, payment methods, fake entries, password stealing (Lange, 2019). The study will target different IT

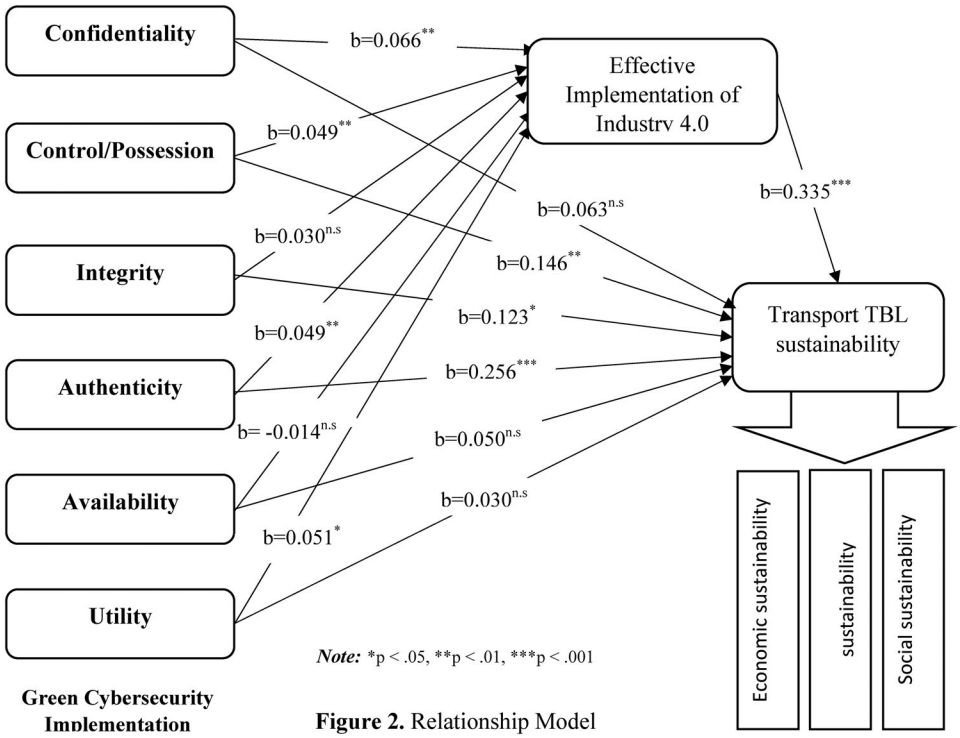

Figure 2. Relationship Model

Figure 3. Relationship Model.

experts to get responses on the implementation of green cybersecurity toward TBL sustainability development. The study targets transport companies in Doha, Qatar, i.e., Abdali general contracting WII, Arab Sat transportations and Cargo, Delwan Qatar WII, Kittco group, Mathews group, etc.

The study distributes 530 designed survey questionnaires among the IT experts/managers in the transportation sector of Qatar. The questionnaire comprises two portions, as the first portion demonstrates the individual characteristics. The second portion presents the research questions related to green cybersecurity, implementation of industry 4.0 and TBL sustainability, Qatar. The survey questionnaire approach requires less time with a higher yield rate and higher response rate because it allows clarification, is less expensive and time-saving, reaches people quickly, flexibility for respondents how and when they complete it, data accuracy, and easy interpretation (Jones et al., 2013). While collection the survey data, the study confirms the ethical guidelines and ensures the participants that the researcher does not disclose the information with anyone and it will keep the privacy with them. Finally, the study received 395 valid responses from the IT managers so the response rate was 74.53%. The study meets the sampling criteria of Comrey and Lee (1992), who suggested that a 300+ sample size is a good sample size, and the study uses a convenient sampling approach by following a cross-sectional study approach. It is easy for the researcher to approach the respondents who are very close to hand; particularly when we aim to target the respondents for cybersecurity and industry 4.0 research ideas (Akgül et al., 2018; Nsoh, 2021). Nsoh (20212021) further claimed that convenience sampling is a more suitable technique for testing cybersecurity challenges and using behaviors.

3.2. Survey instruments

The study uses valid survey questionnaires from the previously done research. According to Qatar's present study and the transportation sector, the study adopted the survey questions. The study takes a valid 25-items scale of cybersecurity developed and proposed by Arpaci and Sevinc (2021) comprising of confidentiality 4-items, control/possession 5-items, integrity 4-items, authenticity 5-items, availability 4-items and utility 3-items. In the previous study, all dimensions had good validity and reliability (Arpaci & Sevinc, 2021). 8-items including vertical integration and horizontal integration of industry 4.0 implementation, have been adapted from the study of Ramirez-Peña et al. (2020) and 10-items including economic sustainability, environmental sustainability and social sustainability of triple bottom line (TBL), have been adapted from the study of Jayashree et al. (2021). All measurement scales are measured on 5-Point Likert scales ranging from 1 = Strongly disagree (SD) to 5 = Strongly agree (SA). The demographic information of the respondents is enclosed in Table 1.

3.3. Normality test

For assessing an (SEM) structural equation modeling, the normality test assumes that the constructs and their items are normally distributed (Swiatkowski et al., 2020). Implementing the most appropriate normalcy tests is a significant responsibility for research. The study employed skewness and kurtosis normality tests to fix this issue, which are useful for large and small data. The normalcy test examined the data's accuracy before conducting the structural equation modeling test (Kline, 2005). The normality tests are used to determine if the data gathered is normal.

Table 1. Demographic information.

		N	%age	Valid %age	Cumulative %age
Age	Up to 30	102	25.8	25.8	25.8
	31-35 years	256	64.8	64.8	90.6
	36 and above years	37	9.4	9.4	100.0
Gender	Male	346	87.6	87.6	87.6
	Female	48	12.2	12.2	99.7
	Not specify	1	.3	.3	100.0
Marital Status	Single	240	60.8	60.8	60.8
	Married	155	39.2	39.2	100.0
Job title	IT Manager	43	10.9	10.9	10.9
	IT Expert	143	36.2	36.2	47.1
	Cybersecurity Advisor	114	28.9	28.9	75.9
	IT and Security Controller	95	24.1	24.1	100.0
Transport Company	Abdali general contracting WII	13	3.3	3.3	3.3
	Arab Sat transportations	57	14.4	14.4	17.7
	Cargo, Delwan Qatar WII	75	19.0	19.0	36.7
	Kittco group	118	29.9	29.9	66.6
	Mathews group	70	17.7	17.7	84.3
	Others	62	15.7	15.7	100.0
Educational level	Intermediate	6	1.5	1.5	1.5
	Graduation	78	19.7	19.7	21.3
	Master/CA/ACMA	259	65.6	65.6	86.8
	MS/MPhil/PhD	52	13.2	13.2	100.0

Depending on the composition of the values on either side, the skewness values are positive (-) or negative (+). Additionally, left-side skewness is indicated by a negative sign (-), while a positive (+) sign indicates right-side skewness. According to Kline (2005), the skewness threshold should be between −2 and +2, and the Kurtosis value should be between −7 and +7. Because the dimensions are unprecedented in the Qatar transportation context, it was necessary to evaluate whether the data are normally distributed.

3.4. Data analysis

The study employs variance-based SEM using Smart PLS 3.3.4 to test the proposed research hypotheses (Hair et al., 2020). Smart PLS 3 is a landmark in latent variable modeling. It combines cutting-edge technologies (such as PLS-POS and IPMA, as well as complicated bootstrapping processes) with a user interface that is simple to understand and easy to operate. When latent constructs are incorporated into the structural model, PLS-SEM is the method of choice to analyze the data (Wong, 2016). The following criteria are used to assess the validity and reliability of the measurement scales (Sarstedt & Cheah, 2019). PLS-SEM is a multivariate analytical tool that handles complex models using regression analysis (Castillo-Apraiz et al., 2019). It is used for the exploratory and explanatory research designs (Sarstedt & Cheah, 2019). The following are the reasons for employing PLS-SEM: (1) It is not required that the data be normal (Farrell, 2010; Voorhees et al., 2016); (2) the study evaluates the measurement model in one composite model (Wong, 2016); and (3) when the assessment indices are based on little data (Hair et al., 2019; Sarstedt & Cheah, 2019), i.e., sample size). PLS-SEM is used to do three evaluations: the first is a measurement model evaluation, the second is a path model or structural model evaluation, and the third is a model adequacy and accuracy evaluation (Sarstedt & Cheah, 2019). For this purpose, the study applies the PLS algorithm technique to assess the construct validity (i.e., convergent validity and discriminant validity) and reliability (i.e., Cronbach alpha and composite reliability) in the transportation sector of Qatar. Second, the study applies bootstrapping technique with 10000 sub-samples to test the proposed research hypotheses. Third, the study applies the blindfolding technique to assess the model fitness in terms of R^2 and adjusted R^2, Q^2, and F^2 (Hair et al., 2020).

3.5. Prepiloting and confirmatory factor analysis (CFA)

The researcher has consulted with two academic professionals and 3 IT experts/managers in the Qatar transportation sector. The scales have been adapted from the previously done research. It is very necessary to pre-launch a designed survey questionnaire to check its validity and reliability (Knight & Kvaran, 2014) in the transportation sector of Qatar. Through pre-piloting, the modified scales may have good responses and statistical interferences. The study distributed 100 survey questionnaires to test the conceptual model that is mandatory to check its validity and reliability, so the study with 67 responses, employed confirmatory composite analysis (CCA) in smart PLS because it deals with the confirmatory factor analysis using assessment measurement quality (Hair et al., 2020). For this purpose, an algorithm technique with 5000 sub-sample and factorization measures was used to find results. Hair et al. (2019) suggested the threshold values for convergent and discriminant validity (p. 15) in the case of reflective measures. Finally, the study found all values (factor loading, AVE, cross-loadings, and HTMT) within the threshold values (Hair et al., 2019; 2020), so it proved the validity and reliability (CCA) of the measurement constructs.

3.6. Common method bias

Later with 395 responses, Harman's single-factor methodology (Podsakoff et al., 2003) with unrotated principal axis

factoring was used to calculate common method variance (CMV) for all observable indicators in the model assess common method bias. The findings show that with eight latent factors and eigenvalues of more than 1, no single dominating factor accounted for 33.859 percent of the total variance, which is less than the threshold percentage of 50%. (Podsakoff et al., 2003). As a result, CMV is not an issue in this investigation, and the measurement construct is released for further testing.

4. Results

4.1. Construct Validity and reliability

The study examined validity and reliability statistics using the least-squares method since the researcher stated that before conducting a regression analysis, you should assess the path model (Sarstedt & Cheah, 2019). According to Ramayah et al. (2018), validity significance includes convergent validity (i.e., factor loadings and average variance extracted) and discriminant validity i.e., cross-loadings and Fornell-Larcker criteria (Farrell, 2010; Voorhees et al., 2016). In contrast, reliability includes Cronbach alpha (i.e., item-based internal consistency) and composite reliability (overall reliability). The factor loading is defined as the correlation between latent construct elements with a value greater than 0.7 (Wong, 2016). The study used 5000 sub-samples to run a series of PLS algorithms and found that 1 item of confidentiality (CON1 = 0.618), 1 item of vertical integration (VI4 = 0.044) and 2 items of horizontal integration (HI3 = 0.029, HI4 = 0.047) had lower factor loading than 0.70 (Ramayah et al., 2018; Sarstedt & Cheah, 2019). Deleted items with d, and final factor loadings are shown in Table 2. The average extracted variance (AVE) is a component of convergent validity. Its value is more than 0.50 (Sarstedt & Cheah, 2019), implying that the study explains more than half of the variance from observed variables to their hidden factor. Because AVE is an extracted variance in an endogenous construct that an external construct explains (Wong, 2016). Meanwhile, Cronbach alpha and composite reliability scores for each construct were greater than 0.7 (Farrell, 2010; Ramayah et al., 2018), indicating that the constructs were reliable.

Discriminant validity is the second phase of confirming the validity. The criteria for evaluating discriminant validity are based on two sorts of parameters: cross-loadings concerning the constructs' elements and the Fornell-Larcker criteria (Voorhees et al., 2016). According to Farrell (2010) and Cheung and Wang (2017) criteria for assessing cross-loadings, the loadings of a given construct's items should be higher than the loadings of another construct's items in the same column. The threshold conditions for assessing cross-loadings of the measurement constructs were confirmed. Second, the discriminant validity is assessed using the Fornell-Larcker criteria (Farrell, 2010; Voorhees et al., 2016). This criterion also confirms that a construct's value should be higher when compared to itself and the other constructs in the diagonal style (Cheung & Wang, 2017, Table 3). It's the square root of the extracted average variance, and a high number indicates good construct validity. Table 3 verifies the findings that a construct's worth is higher when compared to itself and another construct. As a result, it was demonstrated that discriminant validity was likewise high. Finally, the measuring constructs have a high level of validity and consistency.

4.2. Multicollinearity statistics (VIF)

During the residual analysis of various statistics, the study does not go beyond the assumptions of the multivariate regression analysis. Value of variance inflation factor (VIF) occasionally indicates a problem when its value goes higher than 5 (Ramayah et al., 2018; Wong, 2016). Still, in this case, VIF values were lower in the case of observed (outer VIF) and latent constructs (inner VIF) (Ramayah et al., 2018; Sarstedt & Cheah, 2019). Finally, multi-collinearity was not a problematic concern in the present study.

4.3. Assessment of path model

The path model was applied to test the research hypotheses (Ramayah et al., 2018; Sarstedt & Cheah, 2019). The study confirms the direct and indirect influence of green cyber security on triple bottom line sustainability via the effective implementation of industry 4.0. The study meets three recommended assumptions of testing the mediating relationships by Baron and Kenny (1987). However, control variables were not significantly tested in the research model. After analyzing the direct effects, the bootstrapping technique with 5000 subsamples was applied (Voorhees et al., 2016; Wong, 2016). Testing the proposed hypotheses, beta value, t-value, and p-value should be evaluated such as Wong (2016) and Ramayah et al. (2018) suggested that the beta value may be negative or positive in the case of proposed hypotheses, t-value is $\geq +1.96$ in case of 5% significance level, and the p-value is $p < 0.05$ (see Figure 2, Ramayah et al., 2018; Sarstedt & Cheah, 2019). The study uses a 5% significance level. Table 4 exerts that confidentiality of green cybersecurity did not significantly affect sustainability ($\beta = 0.063$, t-value = 1.245, p-value = 0.213) so, hypothesis (H1a+) was rejected. Control/position of green cybersecurity significantly and positively influenced sustainability ($\beta = 0.146$, t-value = 2.719, p-value = 0.007) so hypothesis (H1b+) was accepted. Additionally, the integrity of green cybersecurity significantly and positively influenced sustainability ($\beta = 0.123$, t-value = 2.126, p-value = 0.034), so the hypothesis (H1c+) was also accepted. The authenticity of green cybersecurity significantly and positively influenced green cybersecurity sustainability ($\beta = 0.256$, t-value = 5.300, p-value = 0.000), so hypothesis (H1d+) was also accepted. Unfortunately, utility of green cybersecurity did not significantly influence sustainability ($\beta = 0.050$, t-value = 0.873, p-value = 0.383) so hypothesis (H1e+) was rejected. At last, availability of green cybersecurity did not significantly influence sustainability ($\beta = 0.030$, t-value = 0.843, p-value = 0.399) so hypothesis (H1f+) was also rejected. Meanwhile, effective implementation of industry

Table 2. Construct validity and reliability.

Scales	F.L	α	C.R	AVE
Confidentiality (CON) (Arpaci & Sevinc, 2021)		0.702	0.831	0.621
CON1	0.618[d]			
CON2	0.801			
CON3	0.746			
CON4	0.816			
Control/Position (POS) (Arpaci & Sevinc, 2021)		0.779	0.857	0.601
POS1	0.791			
POS2	0.788			
POS3	0.709			
POS4	0.809			
Integrity (INT) (Arpaci & Sevinc, 2021)		0.784	0.861	0.609
IN1	0.805			
IN2	0.814			
IN3	0.793			
IN4	0.705			
Authenticity (AU) (Arpaci & Sevinc, 2021)		0.898	0.925	0.713
AU1	0.752			
AU2	0.883			
AU3	0.870			
AU4	0.873			
AU5	0.838			
Availability (AVA) (Arpaci & Sevinc, 2021)		0.878	0.907	0.710
AVA1	0.713			
AVA2	0.951			
AVA3	0.894			
AVA4	0.794			
Utility (UT) (Arpaci & Sevinc, 2021)		0.842	0.905	0.760
UT1	0.860			
UT2	0.878			
UT3	0.877			
Vertical integration (VI) Industry 4.0 implementation (Ramirez-Peña et al., 2020)		0.782	0.873	0.697
VI1	0.773			
VI2	0.856			
VI3	0.873			
VI4	0.044[d]			
Horizontal integration (HI) Industry 4.0 implementation (Ramirez-Peña et al., 2020)		0.785	0.903	0.823
HI1	0.905			
HI2	0.909			
HI3	0.029[d]			
HI4	0.047[d]			
Economic sustainability (ES) Triple bottom line sustainability (TBS) (Jayashree et al., 2021)		0.882	0.914	0.679
ES1	0.770			
ES2	0.835			
ES3	0.808			
ES4	0.864			
ES5	0.840			
Environmental sustainability (ENS) Triple bottom line sustainability (TBS) (Jayashree et al., 2021)		0.723	0.844	0.645
ENS1	0.786			
ENS2	0.871			
ENS3	0.747			
Social sustainability (SS) Triple bottom line sustainability (TBS) (Jayashree et al., 2021		0.778	0.900	0.818
SS1	0.910			
SS2	0.899			

Notes: F.L = Factor loadings, α= Cronbach alpha, C.R = Composite reliability, AVE = Average variance extracted.

Table 3. Fornell and Larcker criteria.

	1	2	3	4	5	6	7	8	9	10	11
Authenticity	0.844										
Availability	0.137	0.843									
Confidentiality	0.517	0.079	0.788								
Control/Position	0.518	0.108	0.656	0.775							
Economic Sustainability	0.628	0.099	0.543	0.572	0.824						
Environmental Sustainability	0.515	0.097	0.494	0.487	0.652	0.803					
Horizontal Integration	0.409	0.023	0.505	0.461	0.539	0.584	0.907				
Integrity	0.559	0.124	0.635	0.559	0.569	0.531	0.473	0.780			
Social Sustainability	0.547	0.147	0.525	0.514	0.657	0.730	0.484	0.504	0.904		
Utility	0.534	0.098	0.588	0.574	0.572	0.438	0.449	0.737	0.508	0.872	
Vertical Integration	0.561	0.062	0.511	0.500	0.593	0.536	0.608	0.500	0.501	0.524	0.835

4.0 significantly and positively influenced green cybersecurity sustainability ($\beta = 0.335$, t-value = 6.774, p-value = 0.000). The results claimed that the authenticity of green cybersecurity could have the strongest impact in implementing economic, environmental and social sustainability development in the transport industry of Qatar. It means

Table 4. Multi-collinearity statistics.

	Economic Sustainability	Environmental Sustainability	Horizontal Integration	Industry 4.0 Implementation	Social Sustainability	Triple bottom Line Sustainability	Utility	Vertical Integration
Authenticity				1.665		1.779		
Availability				1.025		1.028		
Confidentiality				2.214		2.286		
Control/Position				2.024		2.063		
Economic Sustainability								
Environmental Sustainability								
Horizontal Integration								
Industry 4.0 Implementation			1.000			1.843		1.000
Integrity				2.659		2.674		
Social Sustainability								
Triple bottom Line Sustainability	1.000	1.000			1.000			
Utility				2.463		2.505		
Vertical Integration								

Table 5. Path coefficients.

Green cybersecurity factors	Beta value	*t*-value	*p*-value
H1a-Confidentiality -> Triple bottom Line Sustainability	0.063	1.245	0.213
Confidentiality -> Industry 4.0 Implementation	0.198	3.461	0.001
H2b-Control/Position -> Triple bottom Line Sustainability	0.146	2.719	0.007
Control/Position -> Industry 4.0 Implementation	0.145	2.972	0.003
H3c-Integrity -> Triple bottom Line Sustainability	0.123	2.126	0.034
Integrity -> Industry 4.0 Implementation	0.090	1.349	0.177
H1d-Authenticity -> Triple bottom Line Sustainability	0.256	5.300	0.000
Authenticity -> Industry 4.0 Implementation	0.249	4.442	0.000
H1e-Availability -> Triple bottom Line Sustainability	0.030	0.843	0.399
Availability -> Industry 4.0 Implementation	−0.041	0.736	0.462
H1f-Utility -> Triple bottom Line Sustainability	0.050	0.873	0.383
Utility -> Industry 4.0 Implementation	0.152	2.531	0.011
Industry 4.0 Implementation -> Triple bottom Line Sustainability	0.335	6.774	0.000

Note: $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$.

authenticity, not targeting those materials and contents on the internet that have spam and cyberattacks (Table 5).

4.4. Mediating role of effective implementation of industry 4.0

By adding multiple mediators, bootstrapping with 5000 subsamples was again run, and common method variance was not a concern in predicting the outcome variable: green cybersecurity sustainability. Table 6 exerts that industry 4.0 implementation significantly and positively mediates the relationship between confidentiality of green cybersecurity and sustainability ($\beta = 0.066$, t-value = 3.309, p-value = 0.001), so hypothesis (H2+) was accepted, and there was full mediation because confidentiality did not directly influence sustainability but it positively and significantly influenced industry 4.0 implementation ($\beta = 0.198$, t-value = 3.461, p-value = 0.001). Industry 4.0 implementation significantly and positively mediates the relationship between control/position of green cybersecurity and sustainability (t-value = 0.049, t-value = 2.719, p-value = 007), and hypothesis H3 was also accepted. And there was partial mediation. Industry 4.0 implementation did not significantly and positively mediate the relationship between the integrity of green cybersecurity and sustainability ($\beta = 0.030$, t-value = 1.270, p-value = 0.204), so hypothesis (H4+) was rejected, and there was no mediation. Additionally, industry 4.0 implementation significantly and positively mediates the relationship between authenticity of green cybersecurity and sustainability ($\beta = 0.083$, t-value = 3.451, p-value = 0.001), so hypothesis (H5+) was accepted there was partial mediation. Industry 4.0 implementation did not significantly mediate the relationship between the availability of green cybersecurity and sustainability ($\beta = -0.014$, t-value = 0.701, p-value = 0.483), so hypothesis (H6+) was rejected, and there was no mediation. Finally, industry 4.0 implementation significantly and positively mediates the relationship between the utility of green cybersecurity and sustainability ($\beta = 0.051$, t-value = 2.262, p-value = 0.024), so hypothesis (H7+) was accepted, and there was full mediation. There was proved that confidentiality and utility of green cybersecurity depend on applying the industry 4.0 revolution in the transportation industry of Qatar.

4.5. Model adequacy and fitness

In the last part, the study examined model adequacy (effect size) and fitness and reported the significant and good model fit indices in terms of R^2 and Q^2. R^2 is used to test effect strength, and its value falls within the ranges ≥ 0.25; ≥ 0.50; and ≥ 0.75, indicating weak, moderate, and strong effect size (Sarstedt & Cheah, 2019; Wong, 2016). Meanwhile, the value of Q^2 for each endogenous construct is higher than zero (0) in both cross-validated redundancy and communality, as suggested by Ramayah et al. (2018). The study claimed 62.9% of the total variance in triple bottom line sustainability by all dimensions of green cybersecurity, and it means there was a moderate effect. On the

Table 6. Indirect path coefficients.

Green cybersecurity factors	Beta value	*t*-value	*p*-values
H2-Confidentiality -> Industry 4.0 Implementation -> Triple bottom Line Sustainability	0.066	3.309	0.001
H3-Control/Position -> Industry 4.0 Implementation -> Triple bottom Line Sustainability	0.049	2.719	0.007
H4-Integrity -> Industry 4.0 Implementation -> Triple bottom Line Sustainability	0.030	1.270	0.204
H5-Authenticity -> Industry 4.0 Implementation -> Triple bottom Line Sustainability	0.083	3.451	0.001
H6-Availability -> Industry 4.0 Implementation -> Triple bottom Line Sustainability	−0.014	0.701	0.483
H7-Utility -> Industry 4.0 Implementation -> Triple bottom Line Sustainability	0.051	2.262	0.024

Note: $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$.

other side, all dimensions explain 45.7% of the total variance in 'industry 4.0 implementation'. Besides, the Q^2 values for each sub-set were higher than zero, so there were good model adequacy and accuracy.

5. Discussion

The study conceptually explores the effect of each dimension of green cybersecurity on TBL sustainability in the Qatar transport industry through the mediating role of industry 4.0 implementation. Green cybersecurity on a multi-dimensional scale plays a significant role in determining the sustainability development in the Qatar transport industry, whereby industry 4.0 implementation made it possible to enhance transport industry sustainability in terms of the economic, social, and environment. The results reported that control/position, integrity, and authenticity of green cybersecurity significantly and positively impact sustainability development. Surprisingly authenticity of green cybersecurity has the strongest impact on implementing transport industry sustainability. The results align with the fact that control is the consistency that ensures all activities related to information access, regulatory measures, and system ownership that allow them to protect the information from cyberattacks (Vrchota et al., 2020). Integrity refers to the deletion and alteration of the protected information before disclosing it to someone (Miśkiewicz & Wolniak, 2020). And authenticity provides authentic ways of accessing the information and ensures the protection of all materials received through the internet (Arpaci & Sevinc, 2021). These are three dimensions of green cybersecurity that directly impact sustainability development. The fact is that green cybersecurity and green IT advancements are emerging trends and not fully implemented in determining sustainable development (Sulich et al., 2021), so there is a need for successfully implementing green cybersecurity in online transport and traveling facilities in Qatar. Additionally, confidentiality, utility, and availability of green cybersecurity did not significantly and directly influence sustainability development. It means there is still a need for implementing sustainable green cybersecurity to ensure confidentiality, usage of green cybersecurity, and availability of green practices in green cybersecurity.

The mediation results reported that industry 4.0 implementation significantly and positively mediates the relationship between confidentiality, authenticity, control/position, and utility of green cybersecurity and sustainability development. Industry 4.0 implementation fully mediated the relationship between confidentiality and utility of green cybersecurity and sustainability development. It means both authenticity and utility do not directly target the success of cybersecurity sustainability; however, it needs 4.0 industrial revolution strategies and measures to ensure a sustainable cybersecurity system in the Qatar transport industry. Additionally, control/position partially mediated the relationship, and both integrity and availability of green cybersecurity did not mediate the relationship, so there were no mediations. All previous systems based on cybersecurity are facing too many challenges despite good technological infrastructure and equipment (Sataloff et al., 2019; Shackelford et al., 2016; Sulich et al., 2021; Tabassum et al., 2018). Green cybersecurity is an emerging trend (Arpaci & Sevinc, 2021) in the transportation sector because it secures direct and indirect online processes and facilities. In the future, the multidimensionality of green cybersecurity could help Qatar to overcome cyber threats and attacks from unwanted provisions. For this reason, cybersecurity and computer technologies play a significant role in the implementation of sustainable development (Mondejar et al., 2021; Shackelford et al., 2016; Sulich et al., 2021). Developing sustainable social, economic, and environmental technologies with green cybersecurity is one of the emerging needs for domestic and international online travel facilities in determining sustainable development (Sulich et al., 2021). Moreover, these green cybersecurity and ICT technologies will ultimately solve Qatar's social, economic, and environmental issues (Rutkowska & Sulich, 2020).

Technological advancements in transportation efforts are becoming more widespread in Qatar, and the establishment and upkeep of safe and secure transportation facilities for all parties involved have become a vital prerequisite for assuring all concerned stakeholders, particularly end-users (Badran, 2021). It is necessary for all stakeholders, including public and private transport agencies, to collaborate in order to build a green environment that is sufficiently protective. This includes locating and mitigating any security concerns that could jeopardize users' confidential info. The importance of security rises to new heights in "Qatar transportation," characterized by the concurrent construction and deployment of "green cybersecurity" systems and devices. The devices and software utilized in transportation infrastructure may create weak areas that can be exploited by attackers looking to carry out attacks on key targets like the electric grid, traffic control centers, transports, and airports. This was done to ensure that cybercriminals are held accountable for their actions and to enhance Qatar's social, economic, and environmental sustainability (Brown, 2018). So, the overarching objective is to "establish and sustain

secure cyberspace to safeguard strategic interests and the core values and rights of the Qatar transportation sector.

5.1. Theoretical contributions

The study conceptually draws a model that will ultimately provide the solutions to social, economic, and environmental sustainability issues (i.e., TBL sustainability). The study is unique that provides significant solutions to TBL's sustainable development of the country Qatar. Unfortunately, there is no study in the literature that might focus on green cybersecurity development. Still, only Sulich et al. (2021) provide the significant interferences between green cybersecurity and sustainable development in the EU countries and expect to re-organize the security measures in green cybersecurity and sustainable development. Additionally, this study aims to place industry 4.0 technologies for the proper implementation of green cybersecurity toward TBL sustainability of the transportation sector in Qatar. This sort of activity referred to as Green Cybersecurity, will also provide protection and the mechanisms associated with products and services, the manufacture of goods, and the provision of services (Pansare et al., 2021; Sulich et al., 2021) in Qatar. Moreover, Sataloff et al. (2019) claim that "the convergence of Industry 4.0-driven operational processes, as well as the rapid pace of digitalization, means that cyber attackers can seem to have vaster consequences than it has ever been." Therefore, green cybersecurity, green management, and pro-ecological strategies will create higher economic, social, and environmentally sustainable development.

5.2. Policy Implications

The study provided the policy implications and looked at some of the parallels and differences between sustainable development measures and cyber challenges and opportunities, the growth of sustainability and the application of green cybersecurity, and a sustainable traveling environment to support long-term cybersecurity. The study looks into the tools established by travel businesses and policymakers to assist with sustainability and analyze their importance in terms of green cybersecurity (Sulich et al., 2021). Although calculating a cost comparison for green cybersecurity initiatives (i.e., confidentiality, availability, and utility) is more difficult than assessing the efforts designed for authenticity, integrity, and control/position, the Qatar transport industry would like to invest in implementing industry 4.0 to enhance the applicability of green cybersecurity in determining sustainable cybersecurity sustainable development that will save all travel facilities (i.e., ticket booking, reservation of tickets, travel products, and services, hotels, flights, cars, tours, cruises, activities) from cyber-attacks. The Qatar transport industry was harmed by many cyber-security vulnerabilities that took advantage of industrial machinery flaws in the cybersecurity systems. This results in data confidentiality, integrity, and accessibility loss, adversely affecting Qatar's sustainability development (Miśkiewicz & Wolniak, 2020). The green digital transformation of cybersecurity and new Industry 4.0 technologies employed in this study allow managers and owners of travel agencies in Qatar further to expand their new online cyber skills and knowledge, facilitating the adaption of significant sustainability development. Increasing interconnection, coordination, and asset sharing are forecast to increase cybersecurity sustainability development.

Automation and transformation of methods based on the participation of internet-connected devices over the Network result in increased susceptibility to cyber risks, which can hinder sustainable cybersecurity development in terms of economic, social, and environmental (Mathivathanan et al., 2022). As a result, green cybersecurity should have been regarded as a necessary component, and it should be at the heart of the unfolding Green 4th Industrial revolution. In this period when green IT approaches, and technologies are being developed, it is important to remember that green cybersecurity is paramount for investors, managers, and owners of the travel agencies that provide online services as well. Furthermore, the growth of ICT technologies has revolutionized virtually every area of our lives nowadays. But still, there are need to implement green cybersecurity to reduce energy wastage and consumption, IT implementation hazardous, and cyber-attacks.

During this transportation crisis, the operational measures implemented for public transportation have significantly varied from one country to the next. These procedures attempt to reduce both the spread of the virus and the expense of operations (Adjetey-Bahun et al., 2016). Nevertheless, these precautions are always subject to modification depending on the current state of the pandemic and the choices that policymakers make.

5.3. Practical implications

Thorough literature reviews on the subject of the assessment of the cybersecurity of transport systems have been carried out but no study was found in the literature that provides the solutions to the existing system of cybersecurity. So, Qatar should dictate a required threshold of green cybersecurity capability and an implication for assessing the green cybersecurity readiness for the public and private transportation sectors. The ultimate priority ought to be given to infrastructure systems, including transportation, financial, communication, and energy agencies. The study suggests that the proposed model be adopted as a method for assessing and ensuring compliance. Qatar can implement green cybersecurity without the need for additional new regulations, as sustainability comes within the scope of current industry revolution 4.0, regulations, and legislation. Alternatively, Qatar could implement green cybersecurity as an update to existing legislation. The current cybersecurity does not aspire to be a complete concept with comprehensive activities that have been worked out in great detail. Rather, green cybersecurity provides a transportation network that Qatari cybersecurity decision-makers can use to collaborate in order to pinpoint thoroughly researched and bargained operations that fall underneath industry 4.0

implementation. This comparison was the most crucial factor in the development of green cybersecurity. A legal framework that will increase the growth, sustainability, and flexibility of the Qatari green cybersecurity system is proposed in order to enhance triple bottom line sustainability.

5.4. Limitations and future directions

The researcher worked hard to ensure that the data were of excellent quality, yet, the sample size from the Qatar transport industry (i.e., online travel agencies) was rather small. The researchers decided to integrate the principles of green cybersecurity, Industry 4.0 implementation, and sustainability development when selecting the research objectives and boundaries of the study. The applicability of facts could pose the issue of whether green cybersecurity enables Industry 4.0 in determining the sustainability outcomes (i.e., economic, social, and environmental) have a truly positive effect, but some factors of green cybersecurity do not meet the expectation of the study so the future study may use the same conceptual framework to test in another country. While implementing green cybersecurity via Industry 4.0 in travel businesses has economic advantages, it is important to note that it can also have negative consequences for sustainability, particularly regarding the non-availability of green cybersecurity measures toward industry 4.0. The good sustainability results have been explored in connection to Industry 4.0 implementation that enables confidentiality and utility in determining and gaining sustainability development. Negative consequences are typically the polar opposite of positive benefits (cost reduction vs. cost increase, etc.) and are a major impediment to adopting green cybersecurity methods and technology. The ability to detect substantial negative effects in this study analysis may be harmed if greater emphasis is placed on good results. Additionally, future research may be done on the effectiveness of cybersecurity systems, and management commitment may play a significant role in implementing green cybersecurity and industry 4.0 revolutions to determine sustainable development. The present study is limited to only the transport industry, so other industries and agencies providing online services to their customers face cyber-attacks, threats, and unauthorized access, so these industries should be focused on. A practical framework should be designed to make them secure and save an environmental place where everyone would like to deal happily.

By providing solutions and facilitating sustainable development, green technology paves the way for intelligent and environmentally friendly cybersecurity. The combination of artificial intelligence, big data, and the Internet of Things has already provided many advantages. The consequences of unequal data access, which can lead to digital world and raise disparities rather than reduce the gap, deserve special attention (Mathivathanan et al., 2022). This focus should be devoted to the ramifications of unequal data access. Improvements should be made to the green cybersecurity of heavily networked systems hosted in the cloud. However, the advantages of incorporating big data into green cybersecurity can improve the circular economy and significantly assist in addressing sustainable issues.

Disclosure statement

The authors did not receive any funding and they have no confliction of interest.

References

Abeyratne, R. (2019). *Legal priorities in air transport*. Springer International Publishing.

Addanki, S. C., & Venkataraman, H. (2017). Greening the economy: A review of urban sustainability measures for developing new cities. *Sustainable Cities and Society*, *32*, 1–8. https://doi.org/10.1016/j.scs.2017.03.009

Adjetey-Bahun, K., Birregah, B., Châtelet, E., & Planchet, J. L. (2016). A model to quantify the resilience of mass railway transportation systems. *Reliability Engineering & System Safety*, *153*, 1–14. https://doi.org/10.1016/j.ress.2016.03.015

Akgül, A., Akbaş, H. E., & Gümüş, A. T. (2018). *A survey of students' perceptions on Industry 4.0 in a large public university in Turkey* (pp. 237–247). Londra: IJOPEC Publication Limited.

Akhtar, P., Ullah, S., Amin, S. H., Kabra, G., & Shaw, S. (2020). Dynamic capabilities and environmental sustainability for emerging economies' multinational enterprises. *International Studies of Management & Organization*, *50*(1), 27–42. https://doi.org/10.1080/00208825.2019.1703376

Al-Mhiqani, M. N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z. Z., Ali, N. S., & Abdulkareem, K. H. (2018). Cyber-security incidents: A review cases in cyber-physical systems. *International Journal of Advanced Computer*, (1), 499–508.

Añón Higón, D., Gholami, R., & Shirazi, F. (2017). ICT and environmental sustainability: A global perspective. *Telematics and Informatics*, *34*(4), 85–95. https://doi.org/10.1016/j.tele.2017.01.001

Arnold, C., Veile, J., & Voigt, K.-I. (2018). What drives industry 4.0 adoption? An examination of technological, organizational, and environmental determinants. In Paper presented at the 27th International Conference on Management of Technology (IAMOT), Birmingham, UK.

Arpaci, I., & Sevinc, K. (2021). Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. *Information Development*, *38*(2), 0266666921997512.

Awan, U., Sroufe, R., & Shahbaz, M. (2021). Industry 4.0 and the circular economy: A literature review and recommendations for future research. *Business Strategy and the Environment*, *30*(4), 2038–2060. https://doi.org/10.1002/bse.2731

Awan, U., Sroufe, R., & Shahbaz, M. (2021). Industry 4.0 and the circular economy: A literature review and recommendations for future research. *Business Strategy and the Environment*, 1–23.

Badran, A. (2021). Developing smart cities: Regulatory and policy implications for the State of Qatar. *International Journal of Public Administration*, 1–14. https://doi.org/10.1080/01900692.2021.2003811

Bai, C., Dallasega, P., Orzes, G., & Sarkis, J. (2020). Industry 4.0 technologies assessment: a sustainability perspective. *International Journal of Production Economics*, *229*, 107776. https://doi.org/10.1016/j.ijpe.2020.107776

Baron, R. M., & Kenny, D. A. (1987). The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical con-siderations. *Journal of Personality and Social Psychology*, *1*(986), 5.

Bertaud, A., Lefèvre, B., & Yuen, B. (2011). GHG emissions, urban mobility, and morphology: A hypothesis. In *Cities and climate change*, 87. eLibrary: World Bank Group.

Brown, R. D. (2018). *Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework*. International Review of Law.

Castillo-Apraiz, J., Richter, N. F., de Antonio, J. M., Ringle, C. M., & Gudergan, S. P. (2019). Customizing exploitation and exploration quality management practices to strategy: Implications for firm performance. In *Innovation, entrepreneurship and knowledge academy INEKA*.

Cheng, Y., Awan, U., Ahmad, S., & Tan, Z. (2021). How do technological innovation and fiscal decentralization affect the environment? A story of the fourth industrial revolution and sustainable growth. *Technological Forecasting and Social Change*, *162*, 120398. https://doi.org/10.1016/j.techfore.2020.120398

Cheung, G. W., & Wang, C. (2017). Current approaches for assessing convergent and discriminant validity with SEM: Issues and solutions [Paper presentation]. In *Academy of Management Proceedings*, 1, 12706. Briarcliff Manor, NY: Academy of Management. https://doi.org/10.5465/AMBPP.2017.12706abstract

Comrey, A. L., & Lee, H. B. (1992). Interpretation and application of factor analytic results. In A. L. Comrey & H. B. Lee (Eds.) *A first course in factor analysis* (p. 2). Hillsdale, NJ: Lawrence Eribaum Associates.

Díaz-Chao, A., Ficapal-Cusí, P., & Torrent-Sellens, J. (2020). Environmental assets, industry 4.0 technologies and firm performance in Spain: A dynamic capabilities path to reward sustainability. *Journal of Cleaner Production*, *281*, 125264.

Du, M., Cheng, L., Huang, L., & Tu, Q. (2018). Network optimization of conventional public transit based on urban rail transit. In 18th COTA International Conference of Transportation (Ed.) *CICTP 2018: Intelligence, connectivity, and mobility* (pp. 766–774). American Society of Civil Engineers.

Eurostat. (2015). ICT security in enterprises – Statistics explained. Retrieved February 12, 2021, form https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises

Farrell, A. M. (2010). Insufficient discriminant validity: A comment on Bove, Pervan, Beatty, and Shiu (2009). *Journal of Business Research*, *63*(3), 324–327. https://doi.org/10.1016/j.jbusres.2009.05.003

Fraser, D. (2020). Analysis of quantitative data: Cybersecurity knowledge and skills.

Ghobakhloo, M. (2020). Industry 4.0, digitization, and opportunities for sustainability. *Journal of Cleaner Production*, *252*, 119869. https://doi.org/10.1016/j.jclepro.2019.119869

Hahanov, V., Litvinova, E., & Chumachenko, S. (2017). Green cyber-physical computing as sustainable development model. In *Green IT engineering: Components, networks and systems implementation* (pp. 65–85). Springer.

Hair, J. F., Jr, Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in PLS-SEM using confirmatory composite analysis. *Journal of Business Research*, *109*, 101–110. https://doi.org/10.1016/j.jbusres.2019.11.069

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Jabbar, R., Dhib, E., Ben Said, A., Krichen, M., Fetais, N., Zaidan, E., & Barkaoui, K. (2022). Blockchain technology for intelligent transportation systems: A systematic literature review. *IEEE Access*. *10*, 20995–21031. https://doi.org/10.1109/ACCESS.2022.3149958

Jayashree, S., Reza, M. N. H., Malarvizhi, C. A. N., & Mohiuddin, M. (2021). Industry 4.0 implementation and Triple Bottom Line sustainability: An empirical study on small and medium manufacturing firms. *Heliyon*, *7*(8), e07753. https://doi.org/10.1016/j.heliyon.2021.e07753

Jones, T. L., Baxter, M. A., & Khanduja, V. (2013). A quick guide to survey research. *Annals of the Royal College of Surgeons of England*, *95*(1), 5–7. https://doi.org/10.1308/003588413X13511609956372

Kazancoglu, Y., Sezer, M. D., Ozkan-Ozen, Y. D., Mangla, S. K., & Kumar, A. (2021). Industry 4.0 impacts on responsible environmental and societal management in the family business. *Technological Forecasting and Social Change*, *173*, 121108. https://doi.org/10.1016/j.techfore.2021.121108

Khan, A., Hosseinzadehtaher, M., Shadmand, M. B., & Mazumder, S. K. (2021, June). Cybersecurity analytics for virtual power plants. In 2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG) (pp. 1–5). IEEE. https://doi.org/10.1109/PEDG51384.2021.9494255

Kiel, D., Müller, J. M., Arnold, C., & Voigt, K.-I. (2020). Sustainable industrial value creation: Benefits and challenges of industry 4.0. In *Digital disruptive innovation* (pp. 231–270). World Scientific.

Kline, T. (2005). *Psychological testing: A practical approach to design and evaluation*. Sage.

Knight, E. J., & Kvaran, G. (2014). Landsat-8 operational land imager design, characterization and performance. *Remote Sensing*, *6*(11), 10286–10305. https://doi.org/10.3390/rs61110286

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2020). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*. https://doi.org/10.1108/JEIM-06-2020-0240

Lange, A. (2019). https://www.tuvit.de/en/news/press-releases/press-release-detail/article/motc-and-tuevit-sign-mou-to-set-up-gulf-cooperation-councils-gcc-first-security-technology-lab-in-qatar/

Lim, H. S. M., & Taeihagh, A. (2018). Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications. *Energies*, *11*(5), 1062. https://doi.org/10.3390/en11051062

Lin, D., Lee, C. K. M., Lau, H., & Yang, Y. (2018). Strategic response to Industry 4.0: An empirical investigation on the Chinese automotive industry. *Industrial Management & Data Systems*, *118*(3), 589–605. https://doi.org/10.1108/IMDS-09-2017-0403

Liu, L., & Mishra, A. R. (2022). Enabling technologies challenges of green Internet of Things (IoT) towards sustainable development in the era of Industry 4.0. *Technological and Economic Development of Economy*, *0*(0), 1–32. https://doi.org/10.3846/tede.2022.16520

Mathivathanan, D., Agarwal, V., Mathiyazhagan, K., Saikouk, T., & Appolloni, A. (2022). Modeling the pressures for sustainability adoption in the Indian automotive context. *Journal of Cleaner Production*, *342*, 130972. https://doi.org/10.1016/j.jclepro.2022.130972

McWilliams, A., Parhankangas, A., Coupet, J., Welch, E., & Barnum, D. T. (2016). Strategic decision making for the triple bottom line. *BSE*, *25*(3), 193–204.

Miśkiewicz, R., & Wolniak, R. (2020). Practical application of the Industry 4.0 concept in a steel company. *Sustainability*, *12*(14), 5776. https://doi.org/10.3390/su12145776

Mondejar, M. E., Avtar, R., Diaz, H. L. B., Dubey, R. K., Esteban, J., Gómez-Morales, A., Hallam, B., Mbungu, N. T., Okolo, C. C., Prasad, K. A., She, Q., & Garcia-Segura, S. (2021). Digitalization to achieve sustainable development goals: Steps towards a Smart Green Planet. *Science of the Total Environment*, *794*, 148539. https://doi.org/10.1016/j.scitotenv.2021.148539

Müller, J. M., Kiel, D., & Voigt, K. I. (2018). What drives the implementation of Industry 4.0? The role of opportunities and challenges in the context of sustainability. *Sustainability*, *10*(1), 247. https://doi.org/10.3390/su10010247

Nsoh, J. (2021). *Exploring the strategies cybersecurity managers need to Bolster industry 4.0 from cyberattacks* [Doctoral dissertation]. Colorado Technical University.

Pansare, R., Yadav, G., & Nagare, M. R. (2021). Reconfigurable manufacturing system: A systematic review, meta-analysis and future research directions. *Journal of Engineering, Design and Technology*, *21*(1), 228–265. https://doi.org/10.1108/JEDT-05-2021-0231

Paz, T., Caiado, R. G. G., Quelhas, O. L. G., Gavi∼ao, L. O., & Lima, G. B. A. (2021). Assessment of sustainable development through a multi-criteria approach: Application in Brazilian municipalities. *Journal of Environmental Management*, *282*, 111954.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879. https://doi.org/10.1037/0021-9010.88.5.879

Pradhan, R. P., & Bagchi, T. P. (2013). Effect of transportation infrastructure on economic growth in India: The VECM approach. *Research in Transportation Economics*, *38*(1), 139–148. https://doi.org/10.1016/j.retrec.2012.05.008

Pype, P., Daalderop, G., Schulz-Kamm, E., Walters, E., & Grafenstein, M. V. (2017). Privacy and security in autonomous vehicles. In *Automated driving* (pp. 17–27). Springer.

Ramayah, T. J. F. H., Cheah, J., Chuah, F., Ting, H., & Memon, M. A. (2018). Partial least squares structural equation modeling (PLS-SEM) using smartPLS 3.0. *An updated guide and practical guide to statistical analysis*.

Ramirez-Peña, M., Sotano, A. J. S., Pérez-Fernandez, V., Abad, F. J., & Batista, M. (2020). Achieving a sustainable shipbuilding supply chain under I4. 0 perspective. *Journal of Cleaner Production*, *244*, 118789.

Reza, M. N. H., Jayashree, S., & Malarvizhi, C. A. (2020). Industry 4.0 and sustainability-A study on Malaysian MSC status companies. *Reza, MNH, Jayashree, S., and Malarvizhi, CA (2020).'Industry, 4*, 91–104.

Rutkowska, M., & Sulich, A. (2020). Green Jobs on the background of Industry 4.0. *Procedia Computer Science*, *176*, 1232–1240.

Sarstedt, M., & Cheah, J. H. (2019). Partial least squares structural equation modeling using SmartPLS: A software review. *Journal of Market Analysis, 7*, 196–202. https://doi.org/10.1057/s41270-019-00058-3

Sataloff, R. T., Johns, M. M., & Kost, K. M. (2019). Industry 4.0 and cybersecurity Managing risk in an age of connected production.

Schulz, S. A., & Flanigan, R. L. (2016). Developing competitive advantage using the triple bottom line: A conceptual framework. *Journal of Business & Industrial Marketing*, *31*(4), 449–458. https://doi.org/10.1108/JBIM-08-2014-0150

Serdar, M. Z., Koç, M., & Al-Ghamdi, S. G. (2022). Urban transportation networks resilience: Indicators, disturbances, and assessment methods. *Sustainable Cities and Society*, *76*, 103452. https://doi.org/10.1016/j.scs.2021.103452

Shackelford, S. J., Fort, T. L., & Charoen, D. (2016). Sustainable cybersecurity: Applying lessons from the green movement to managing Cyber Attacks. *University of Illinois Law Review* 1995.

Stock, T., & Seliger, G. (2016). Opportunities of sustainable manufacturing in industry 4.0. *Procedia CIRP*, *40*, 536–541. https://doi.org/10.1016/j.procir.2016.01.129

Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and sustainable development. *Procedia Computer Science*, *192*, 20–28. https://doi.org/10.1016/j.procs.2021.08.003

Swiatkowski, J., Roth, K., Veeling, B., Tran, L., Dillon, J., Snoek, J., & Nowozin, S. (2020). The k-tied normal distribution: A compact parameterization of gaussian mean field posteriors in bayesian neural networks. In *International Conference on Machine Learning* (pp. 9289–9299). .PMLR

Tabassum, A., Mustafa, M. S., & Al Maadeed, S. A. (2018). The need for a global response against cybercrime: Qatar as a case study [Paper presentation]. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1–6). IEEE. https://doi.org/10.1109/ISDFS.2018.8355331

Telukdarie, A., & Shisane, F. A. (2018). Investigating the factors, risk and challenges impacting cloud computing services adoption rate. In Proceedings of the International Annual Conference of the American Society for Engineering Management (pp. 1–11). American Society for Engineering Management (ASEM).

Tonn, G., Reilly, A., Czajkowski, J., Ghaedi, H., & Kunreuther, H. (2021). US transportation infrastructure resilience: Influences of insurance, incentives, and public assistance. *Transport Policy*, *100*, 108–119.

Tvaronavičienė, M., Plėta, T., Semaškaitė, V., Paulauskienė, T., & Vaičiūtė, K. (2020). Cold energy economy and cybersecurity of floating storage and regasification units: Emerging trends, challenges, and opportunities. *Journal of Security and Sustainability Issues*, *10*(1), 249–262.

Voorhees, C. M., Brady, M. K., Calantone, R., & Ramirez, E. (2016). Discriminant validity testing in marketing: An analysis, causes for concern, and proposed remedies. *Journal of the Academy of Marketing Science*, *44*(1), 119–134. https://doi.org/10.1007/s11747-015-0455-4

Vrchota, J., Pech, M., Rolínek, L., & Bednář, J. (2020). Sustainability outcomes of green processes in relation to industry 4.0 in manufacturing: Systematic review. *Sustainability*, *12*(15), 5968. https://doi.org/10.3390/su12155968

Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security*, *89*, 101659.

Wong, K. K. K. (2016). Mediation analysis, categorical moderation analysis, and higher-order constructs modeling in Partial Least Squares Structural Equation Modeling (PLS-SEM): A B2B Example using SmartPLS. *Marketing Bulletin*, *26*(1), 1–22.

Yadav, G., Kumar, A., Luthra, S., Garza-Reyes, J. A., Kumar, V., & Batista, L. (2020). A framework to achieve sustainability in manufacturing organizations of developing economies using industry 4.0 technologies' enablers. *Computers in Industry*, *122*, 103280. https://doi.org/10.1016/j.compind.2020.103280

Yadav, G., Luthra, S., Jakhar, S. K., Mangla, S. K., & Rai, D. P. (2020). A framework to overcome sustainable supply chain challenges through solution measures of industry 4.0 and circular economy: An automotive case. *Journal of Cleaner Production*, *254*, 120112. https://doi.org/10.1016/j.jclepro.2020.120112

Yang, Y., Ng, S. T., Zhou, S., Xu, F. J., Li, D., & Li, H. (2020). A federated pre-event community resilience approach for assessing physical and social sub-systems: An extreme rainfall case in Hong Kong. *Sustainable Cities and Society*, *52*, 101859. https://doi.org/10.1016/j.scs.2019.101859

Zhu, Q., Sarkis, J., & Lai, K-h (2008). Confirmation of a measurement model for green supply chain management practices implementation. *International Journal of Production Economics*, *111*(2), 261–273. https://doi.org/10.1016/j.ijpe.2006.11.029