🏆 *reviewed paper*

Employee Behaviour as a Possible Corporate System Vulnerability when Implementing Digitalisation in Smart Cities

Lara Sehlmeyer, Hans Rüdiger Kaufmann

(Lara Sehlmeyer, BA, Hochschule der Wirtschaft für Management, Oskar-Meixner-Straße 4-6, lara.sehlmeyer@student.hdwm.org
(Prof. Dr. Hans Rüdiger Kaufmann, Hochschule der Wirtschaft für Management, Oskar-Meixner-Straße 4-6, hans-ruediger.kaufmann@hdwm.org

DOI: 10.48494/REALCORP2024.0055

1 ABSTRACT

Digitizing processes to improve the citizen centered performance is one of the key challenges for Smart Cities (Radchenko, 2023) This paper contends that, whilst resolving those challenges, the implemented strategies could cause undesired outcomes. Also, this intersects significantly with urban planning considerations, as it involves the integration of digital technologies, including infrastructure, service and governance. At first glance, innovative digital technologies might render more transparent processes saving time and money for organizations. However, people, too often, disregard the threats associated with them. The latter can be classified in external and internal threats. Interestingly, companies feel threatened more by the internal ones since they cannot entirely be eliminated (Boce, 2023). In more detail, the importance of the topic emerges from the following research gap: “From the general point of view of companies, there are no real structures for security management. Also, they do not design policies that will minimize internal threats, they have not yet understood the importance and influence of man as a threatening factor…” (Boce, 2023, p.76).

The research addresses the general question of how employee behavior contributes to internal vulnerabilities affecting the security and compliance governance of digitalization implementations in a Smart City context?

The aim of this research in progress is to address this ‘human threat’ via a comprehensive systematic literature review and a consecutive empirical research design.

Keywords: employees, digitisation, smart city, planning, vulnerability

2 METHODOLOGY

A systematic literature review on web of science and scopus indexed journals will investigate the existing categories of the internal threats and of human behaviors as well as their interactions. The abstract and journal inclusion criteria refer to relevant security management and administrative structure topics. Further the implementation of digital solutions in public institutions and the impact of human factors on security, compliance and governance in this context should be apparent. To offer data-driven insights, the studies should employ empirical methodologies such as surveys, case studies or mixed-methods approaches.

Furthermore, selected sources will include only recent research within the last 10 years to ensure reference to current trends of the smart city movement. Thus, real-world examples that take a holistic view, examining besides the technology aspects also the behavioral and governance factors are reviewed. To facilitate accessibility, English and German studies will be chosen. The systematic literature review will result in more detailed research questions and in an initial conceptualization to be presented at the conference. Based on the critical realism research philosophy, the methodology to conduct empirical research pursues a triangulation approach and will be suggested at the conference.

3 QUALITY ASSESSMENT

The criteria for paper selection and/or rejection are contingent upon pertinent reliability and validity measures. It needs to be ensured that the instruments which have been used for data collection are consistent and accurately measure the variables. Potential biases in the study will be diligently examined. Ultimately, the credibility of the research hinges on the coherence between the results and the research question and / or hypotheses. Ensuring ethical standards is crucial and includes elements such as obtaining informed consent and handling sensitive data responsibly. Equally noteworthy is the open acknowledgment of potential biases and limitations in the studies, a key measure to maintain the integrity of the research. The examination aims to determine the transferability of the conclusions drawn to different corporate contexts or if they are specific to certain conditions.

4 FLOW CHART OUTLINING THE IDENTIFIED ARTICLES

The following section explains the entire inclusion and exclusion process using a flow chart model.

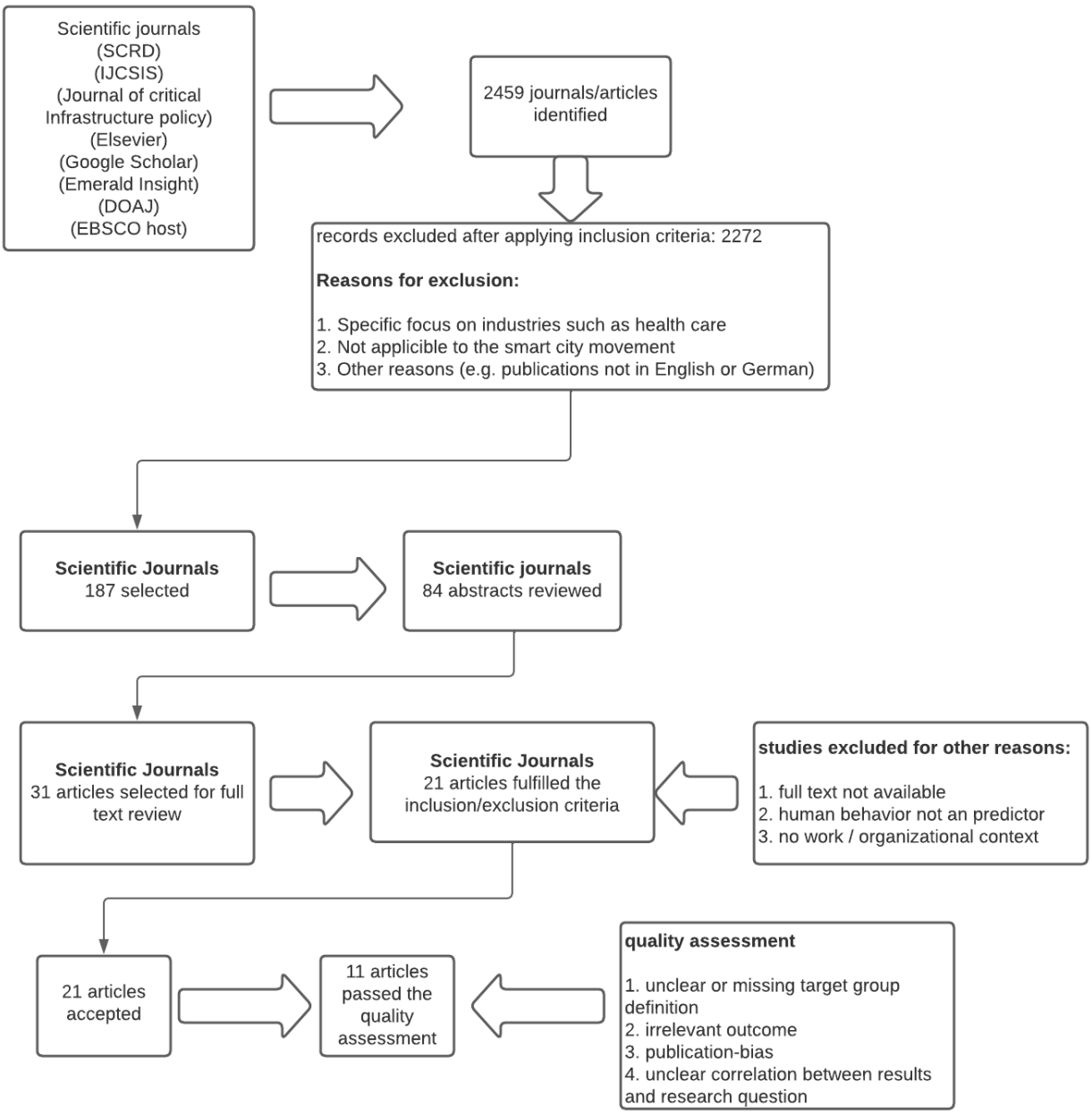

Figure 1: Flow Chart Model

5 DATA EXTRACTION FORM

The following table shows the articles that met the inclusion criteria. These were extracted on the basis of their data.

Number of study	Title	Author/s	Publication details	Year of publication	Methodology adopted	Population characteristics	Sample size	Key results
1	Analysis of the human factor as an internal threat to the security of an organization	Boce, Grigorina	Smart Cities and Regional Development Journal (V7. I2. 203) pp. 69-76	2023	Metaanalysis	employees	-	If there are not the right people to manage and use them, then the security objectives will not be achieved.
2	An information security risk-driven investment model for analysing human factors	Reza Alavi; Shareeful Islam; Haralambos Mouratidis	Information & Computer Security Vol. 24 No. 2, 2016 pp. 205-227	2016	Quantitative approach	employees	62	clear relationship between risks, incidents, and investment
3	SOFIT: Sociotechnical and Organizational Factors for Insider Threat	Greitzer, F. et al.	2018 IEEE Symposium on Security and Privacy Workshops	2018	Mixed Methods	organizations	5	Combination of behavioral and technical factors can identify threats earlier
4	Trust as a human factor in holistic cyber security risk assessment	Henshel ,D.; Cains,M. G.;Hoffman, B.;Kelley ,T.	Procedia Manufacturing 3 (2015) 1117-1124	2015	Literature analysis & Quantitative approach	User, Defender, Attacker	-	importance of trust in cybersecurity risk assessment
5	Human factor, a critical weak point in the information security of an organization's Internet of things	Hughes-Lartey, Kwesi; Li, Meng; Botchey, Francis; Qin, Zhen	Heliyon 7 (2021) e06522	2021	Quantitative approach (linear regression)	Employees familiar with IOT	1600	Framework should combine technological and social aspects
6	Moderne Arbeitswelten im Kontext fortschreitender Digitalisierung und Gefahren in der IT-Security	Kraml, Janina	Master-Thesis	2023	Qualitative approach	Manager	9	Need of security standards

7	Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses	Neetesh, Saxena et.al	Electronics 2020,9,1460 (mdpi)	2020	Qualitative approach	Public and private sector organizations	105	Challenge, emanating from various employee levels
8	A Human Factor Approach to Threat Modeling	Ferro, Lauren; Marella, Andrea; Catarci, Tiziana	HCI-CPT 2021, pp.139-157	2021	Human centered approach	employees	-	gap in traditional threat modeling and system security design
9	Human Individual Difference Predictors in Cyber-Security: Exploring an Alternative Scale Method and Data Resolution to Modelling Cyber Secure Behavior	Raywood-Burke, George; Bishop, Laura; Asquith, Phoebe; Morgan, Phillip	HCI-CPT 2021, pp.226-240	2021	Quantitative approach	Humans, no specification	189	Understanding individual vulnerabilities for interventions
10	Human factors in information leakage: mitigation strategies for information sharing integrity	Wong, Wai Peng; Tan, Hwee Chin; Tan, Kim Hua; Tseng, Ming-Lang	Industrial Management & Data Systems, Vol. 119 No. 6, pp. 1242-1267.	2019	Qualitative approach	Multinational enterprises/corporations	5	addressing information leakage involves for example human governance
11	Sicherheitsherausforderungen für Smart-City-Infrastrukturen	Zimmermann, Verena et.al	Wirtschaftsinformatik & Management 2022 • 14 (2): 119–126	2022	Mixed Methods	Experts	30 (online surveys),7 interviews with 10 experts	Challenges are complex (ethical, social), technological

Figure 2: Data Extraction Form

6 SYNTHESIS

The central theme revolves around three key aspects: digitalization in smart cities, the unintended consequences of digitalization strategies, and internal threats arising from employee behavior. These outlined focal points include certain categories.

- Digitalization in smart cities:

This segment delves into the challenges faced during the implementation of digitization processes in Smart Cities.

(1) Threat Modeling and System Security Design in Smart Cities

Examining the gap in traditional threat modeling approaches and system security design within the context of smart cities, emphasizing the need for innovative strategies that consider the unique challenges presented by the integration of digital technologies and human factors in urban environments.

(2) Integrated Security Framework

Developing a holistic security framework that integrates both technological solutions and social aspects, aiming to establish comprehensive security standards and address the complexity of contemporary security challenges.

- Undesired outcomes of digitalization strategies:

Despite the potential for innovative digital technologies to enhance transparency in processes, the argument is made that implemented strategies may result in unintended consequences.

(3) Risk and investment relationship

Examining how an organization's risks, incidents, and investments in security measures are interconnected, assessing the impact of resource allocation on overall risk, and exploring strategic investments to mitigate potential threats.

- Internal threats due to employee behavior

A substantial emphasis is placed on internal threats stemming from employee behavior as opposed to external threats

(4) Human Factor and Security Management

A lack of qualified personnel can hinder security goals, and it's crucial to understand individual vulnerabilities for specific interventions, considering challenges at different employee levels and addressing multifaceted issues like ethics, social dynamics, and technology in security management.

(5) Trust and Cybersecurity Risk Assessment

Exploring the influence of trust on cybersecurity risk assessment and decision-making and integrating trust-related factors for more robust risk evaluations.

Number	Factor description	Categories				
		1	2	3	4	5
1	Examine how employee behaviours impact risk, incidents and investment.			X		
2	Examine existing frameworks integrating technological and social aspecs from an employee perspektive.		X			
3	Gauge employee trust's significance in cybersecurity risk assessment.					X
4	Identify gaps in traditional threat modeling and system security design affecting employee compliance in Smart Cities.	X				
5	Identify and address individual employee vulnerabilities.				X	
6	Evaluate challenges across employee levels				X	
7	Assess security standards' impact on employee adherence.		X			
8	Address information leakage through human governance and trust-building.					X
9	Assess organizations' security personnel adequacy.				X	

Figure 3: Interplay of factors and criteria

7 FINAL RESEARCH GAPS

The challenge with current advancements lies in the fact that information security tends to focus on the technical effects and external factors rather than on the inclusion of human factors on the internet of things context. The diverse interest groups, each with distinct expectations and requirements for IT security lack a comprehensive analysis. The interaction between individuals and their surroundings is currently unexplored. Furthermore, the various forms of internal threats are not currently correlated with the company's subsystems.

It is noteworthy that there is no complete framework of quantifiable parameters for cyber security risk assessment. Additionally, there is a lack of a procedural model that consolidates the risks associated with the insider threats.

8 INITIAL CONCEPTUALISATION

The following model is intended to illustrate the employee as an internal threat, as well as the outcome when implementing digitalization in smart cities.

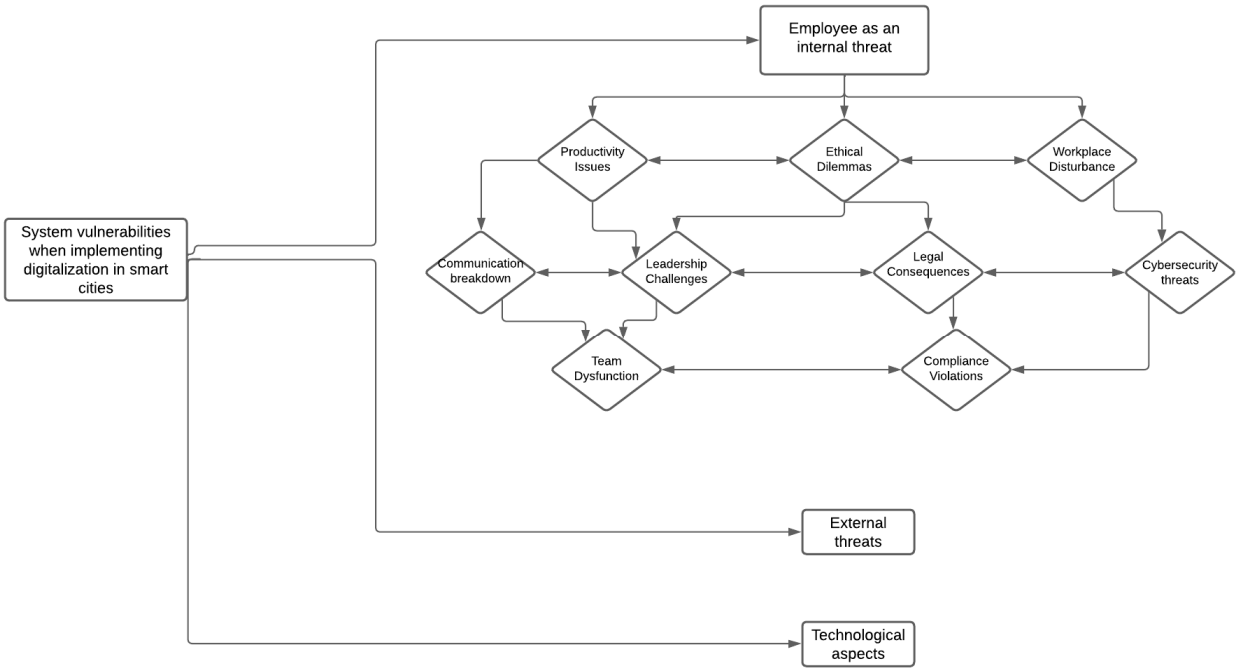

Figure 4: Illustration of the employee as an internal threat

9 RESARCH DESIGN TABLE

Table 1 is intended to show which research questions need to be explored and may have been addressed in the previously selected literature through interview questions

Research Objectives	Stage	Detailed research	Hypotheses	Interview/ Questionnaire questions	Sources
Objective 1: systematic literature review	Stage 1	Carry out a systematic literature review on employee behavior as a possible corporate system vulnerability.			see: data extraction form
Objective 2: Examine and propose effective strategies for companies to efficiently mitigate the impact of employee behavior on system deficits during the digitalization process in smart cities.	Stage 2	Carry out interviews with experts and project managers of the digitalization process in smart cities.	Implementing comprehensive employee behavior management strategies will effectively mitigate the impact of employee actions on system deficits during the digitalization process, resulting in enhanced system resilience and operational efficiency for companies.	What measures should companies take to improve their IT security in the course of digitization? How can companies ensure that their employees are informed about the risks associated with IT security and can respond accordingly? What role do IT security training and education play in enhancing IT security in companies?	Ferro, L., Marella, A. and Catarci, T. (2021) 'A Human Factor Approach to Threat Modeling Kraml, J. (2023) 'Moderne Arbeitswelten im Kontext fortschreitender Digitalisierung und Gefahren in der IT-Security'.
Objective 3: Investigate the specific behavioral factors that contribute to vulnerabilities in corporate systems during the digitalization process within smart cities.	Stage 2	Carry out interviews with experts and project managers of the digitalization process in smart cities.	Specific behavioral factors, such as lack of employee cybersecurity awareness, resistance to change, and inadequate training on digitalization processes, contribute significantly to vulnerabilities in corporate systems during digitalization in smart cities.	Does your company educate you about risky behaviors that could unintentionally leak data and information? In spite of such education, employees continue to show risky behaviors and put data at risks. Why is this so? What could change these risk behaviors? Do you and your friends or colleagues talk about work	Raywood-Burke, G. et al. (2021) 'Human Individual Difference Predictors in Cyber-Security: Exploring an Alternative Scale Method and Data Resolution to Modelling Cyber Secure Behavior' Wong, W.-P. et al. (2019) 'Human factors in information leakage: mitigation strategies for information sharing integrity

				(suppliers, contractors, and customers) during tea time and lunch hour?	
Objective 4: Examine how the above risks/ factors influence other smart cities and what known strategies they use to minimize the risk of danger from employees	Stage 3	Sending and evaluating questionnaires to smart cities	To be continued	To be continued	Kraml, J. (2023) 'Moderne Arbeitswelten im Kontext fortschreitender Digitalisierung und Gefahren in der IT-Security'. Saxena, N. et al. (2020) 'Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses Wong, W.-P. et al. (2019) 'Human factors in information leakage: mitigation strategies for information sharing integrity
Objective 5: To carry out an initial conceptualization	Stage 4	Comparison of the findings from the literature review, the interviews and the questionnaire			

Table 1: Research Design Table

10 OUTLINE OF RESEARCH METHODOLOGY

Later research is suggested. The methodology is briefly outlined in the following.

A non-probability sample, based on certain criteria, should be conducted in the form of a targeted selection of employees across diverse hierarchical levels within public administration organizations.

A mixed methods approach should be used as a research method. Therefore, a qualitative approach to gain in-depth knowledge about employee behaviors and motivations is recommended. An exploratory approach could be chosen to generate new insights and to understand specific aspects of behavior. Moreover, expert interviews can validate the findings obtained through observation.

For the quantitative aspect, company data offering insights into the weakest subsystems should be analyzed. Additionally, a survey may be administered to the entire workforce to capture attitudes towards employee behavior and organizational culture. This could be descriptively evaluated in the form of a cross tabulation, frequency analysis, significance, and correlation. Additionally, referring to explanatory cause-effect analysis could be conducted via factor analysis and multiple regression analysis.

11 CONCLUSION

The systematic literature review shows that companies actually tend to focus on the technological aspects and external threats rather than on the much closer danger, their own employees. Although the various internal threat types have been analyzed in the literature, this must always be viewed in the context of stakeholder interests and corporate culture. There is also a need for research into the interaction of employees with their environment, as well as the creation of a framework that includes quantifiable parameters for cyber security risk assessment. the interplay between risks and insider threats also needs to be examined more closely.

12 REFERENCES

BOCE, G. (2023) 'Analysis of the human factor as an internal threat to the security of an organization', SCRD, 7(no.2), pp. 69–76. Available at: https://doi.org/10.25019/pc270249.

FERRO, L., Marella, A. and Catarci, T. (2021) 'A Human Factor Approach to Threat Modeling', for Cybersecurity, Privacy and Trust2021, pp. 139–157. Available at: https://doi.org/10.1007/978-3-030-77392-2.

GREITZER, F., Purl, J. and Leong, Y.M. (2018) 'SOFIT: Sociotechnical and Organizational Factors for Insider Threat', IEEE Symposium on Security and Privacy Workshops [Preprint]. Available at: https://doi.org/10.1109/SPW.2018.00035.

HENSHEL, D. et al. (2015) 'Trust as a human factor in holistic cyber security risk assessment', Procedia Manufacturing, 3, pp. 1117–1124. Available at: https://doi.org/10.1016/j.promfg.2015.07.186.

HUGHES, L.-K. et al. (2021) 'Human factor, a critical weak point in the information security of an organization's Internet of things', Heliyon 7 (2021) e06522 [Preprint].

KRAMEL, J. (2023) 'Moderne Arbeitswelten im Kontext fortschreitender Digitalisierung und Gefahren in der IT-Security',Available at: https://netlibrary.aau.at/obvuklhs/download/pdf/9257324?originalFilename=true

RADCHENKO, K. (2023) 'The economic and social impacts of smart cities: multi- stakeholder pre-study results', SCRD, 7(2), pp. 25–38. Available at: https://doi.org/10.25019/71fq6q53.

RAYWOOD-BURKE, G. et al. (2021) 'Human Individual Difference Predictors in Cyber-Security: Exploring an Alternative Scale Method and Data Resolution to Modelling Cyber Secure Behavior', HCI for Cybersecurity, Privacy and Trust, pp. 226–240. Available at: https://doi.org/10.1007/978-3-030-77392-2.

REZA, A., Shareeful, I. and Haralambos, M. (2016) 'An information security risk-driven investment model for analysing human factors', Information & Computer Security, 24(2), pp. 205–227.

SAXENA, N. et al. (2020) 'Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses', Electronics 2020, 9(1460). Available at: https://doi.org/10.3390/electronics9091460.

WONG, W.-P. et al. (2019) 'Human factors in information leakage: mitigation strategies for information sharing integrity', Industrial Management & Data Systems, 119(6), pp. 1242–1267. Available at: https://doi.org/10.1108/IMDS-12-2018-0546.

ZIMMERMANN, V. et al. (2022) 'Sicherheitsheraus- forderungen für Smart- City-Infrastrukturen', Wirtschaftsinformatik & Management 2022, 14, pp. 119–126. Available at: https://doi.org/10.1365/s35764-022-00396-5.