Winter 10-14-2023

The Interplay of Human Factors and Cybersecurity: An Organizational Outlook

Paolo Bernardi
University of Campania "L. Vanvitelli", paolo.bernardi@unicampania.it

Raffaele Cecere
University of Campania "L. Vanvitelli"

Marcello Martinez
Univeristy of Campania Luigi Vanvitelli, marcello.martinez@unicampania.it

The Interplay of Human Factors and Cybersecurity: An Organizational Outlook

Paolo Bernardi[1][0000-0002-0567-4229], Raffaele Cecere[2] and Marcello Martinez[3]

[1] Dept. of Economics, University of Campania 'L. Vanvitelli', Capua (CE), Italy
[2] Dept. of Economics, University of Campania 'L. Vanvitelli', Capua (CE), Italy
[3] Dept. of Economics, University of Campania 'L. Vanvitelli', Capua (CE), Italy
paolo.bernardi@unicampania.it

Abstract. This paper critically examines the role of human factors in organizational cybersecurity through a bibliometrics approach supported by qualitative analyses. In an evolving digital landscape, cyber threats have outpaced the capacity of organizations to secure their operations, with economic and psychological implications escalating. While technology-based defenses are essential, the paper posits that cybersecurity strategy should also account for human behaviors and vulnerabilities. The results highlight individuals' critical role as potential weak links or safeguards within the digital realm. Bibliometric analysis conducted on a pool of 200 papers extracted from Web of Science (WoS) database. Findings consolidate the idea of cybersecurity as a sociotechnical domain and underscore the need for a comprehensive cybersecurity strategy, transcending purely technological defenses, to incorporate aspects of human behavior, emotions, and organizational culture. This work also stresses the efficacy of strategies such as deterrence, fear appeal, continuous education, and sector-specific policies in improving Information Security Policy (ISP) compliance. The paper concludes by suggesting some potential future research to bolster both theory and practice.

Keywords: organizational cybersecurity, information system security, organizational behavior, human factor.

1 Introduction

In recent years, the global landscape of cybersecurity has drastically shifted, becoming an integral part of our digital reality, and impacting practically every sector of industry. As the digital realm continues to evolve, the scale and nature of cyberthreats have escalated, often outpacing the capacity of organizations to safeguard their operations [1]. In fact, the economic implications of cybercrime have now surpassed those of many traditional illicit industries such as the drug trade and human trafficking. According to various estimates, cybercrime was responsible for an annual worldwide loss of US$1 trillion in the 2010s, a figure that is predicted to escalate to US$5 trillion by 2024 [2].

Moreover, these costs may be underestimated as they frequently do not encompass the full spectrum of associated expenses. Such overlooked costs include the damage and destruction of data, lost productivity, theft of intellectual property, personal and

financial data, disruptions post-breach, forensic investigations, restoration of hacked data and systems, and company devaluations resulting from reputational harm [3]. If these ancillary costs are taken into consideration, the estimated cost of cybercrime in 2015 was a staggering US$3 trillion, with forecasts suggesting an increase to US$6 trillion annually by 2021.

The study of cybersecurity within organizational settings necessitates a holistic perspective that encompasses not only technological components, but also human factors. Indeed, cybercrimes can be categorized based on the tools employed: attacks/crimes that are primarily technology-based, and attack/crimes that leverage human elements through social engineering [4].

While social engineering forms a significant portion of cybercrimes that exploit human factors, this category also includes other strategies that leverage human vulnerabilities. A common example beyond social engineering is Insider Threats. Insider threats originate from individuals who have legitimate access to an organization's systems and data, such as employees, contractors, or business partners. They pose a unique risk as they can bypass security measures more easily due to their inherent access privileges. These attacks can occur due to a variety of reasons - from disgruntled employees acting out of spite, to individuals who unintentionally expose sensitive information due to lack of awareness or negligence.

On July 30, 2021, amid the Covid-19 pandemic, the Lazio Region in Italy suffered a ransomware attack that paralyzed various health services, including the anti-covid vaccination system and the release of the “Green Pass”, causing disruptions that lasted for more than a month. Access to the system was obtained through an employee of a service company, but it is not clear whether he was a victim of a phishing attack or inadvertently downloaded the ransomware [5].

This demonstrates that while technology-based defenses are crucial in cybersecurity, a comprehensive strategy also needs to account for human behaviors and vulnerabilities that can be exploited by both external actors and insiders. For this reason, this paper aims to respond to the following research question:

RQ: “*How do individuals’ behaviors, vulnerabilities and characteristics influence organizational cybersecurity? What strategies could employ in order to mitigate that?*"

To answer the research question, this paper will employ a bibliometric approach, analyzing patterns and trends in scholarly publications on the intersection of organizational cybersecurity and the human factor. It is also complemented by qualitative insights based on authors' study of relevant papers. Following a detailed overview of the utilized methodology, the paper will proceed to show main results and discuss them, with a particular focus on recent years. Finally, the paper closes with conclusions, some future research perspectives, and major limitations.

2 Methodology

This paper adopted a bibliometrics analysis, supported by qualitative assessments based on the analyzed literature [6]. Through this method, we've quantitatively analyzed the

breadth and patterns of scholarly publications in the chosen domain. Moreover, bibliometric analysis is an effective method for achieving a transparent and replicable review process, centered on the quantitative measure of scientific activity [7] [8]. The application adopted is based on Aria and Cuccurullo's software [9]: Bibliometrix (version 4.1.1).

The research method comprises five phases: study design, data collection, data analysis, data visualization, and interpretation.

In the study design phase, we establish our primary objective: a systematic analysis of the diverse facets of existing literature at the intersection of human factors and organizational cybersecurity. Subsequently, we develop a search strategy accordingly to the research question examining keywords and main terms of a selected numbers of papers [10] [11]. The research focused on the following search string:

TS = (("cyber securit" OR "cyber-securit*" OR "cybersecurit*" OR "information* securit*" OR "information*-securit*" OR "information* system* securit*" OR "data* securit*" OR "IT securit*") AND ("people" OR "human" OR "employe*" OR "workforc*" OR "manager*" OR "individual*") AND ("error*" OR "failure*" OR "fault*" OR "mistake*" OR "flaw*" OR "omission*" OR "violation*" OR "breach*" OR "leak*" OR "attack*" OR "threat*"))*

The search for the stock of knowledge was carried out on 14 May 2023 on the Web of Science (WoS) database. Wos was selected for data collection since it contains a wealth of high-impact journals and articles in our research field and requires less data-cleaning procedures [12] [13].

Initially, the search returned 5334 documents. The dataset was then refined:

- by including Web of Science categories: Management, Business;
- by including only English language;
- by including only Articles, and excluding Conferences proceedings, book chapters, in consideration of a lower impact on the production of knowledge;
- by including citations Indexes: SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH, ESCI.

The final dataset consists of 200 articles.

Data analysis was conducted using a bibliometric approach, providing a quantitative evaluation of scientific publications [14]. It incorporates general descriptive statistics and more sophisticated methods such as document co-citation, collaboration, and co-occurrence analyses [15].

Bibliometrix facilitates co-word analysis [16] through multiple correspondence analysis [17] and hierarchical agglomerative clustering [18]. Data visualization aids in generating a science map and displaying the results of data analysis.

The final phase is interpretation, which combines an objective methodology with a subjective one, a qualitative analysis based on relevant papers emerged. In this way, the bibliometric analysis is rounded off with a qualitative assessment [6].

3 Results

The dataset consists of 200 documents from 74 sources. The main information about the dataset are presented in Table 1. Since the number of total authors exceeds the number of papers, the co-authors per doc is 2.96 while the collaboration index is 2.54, that is obtained by dividing the number of authors of multi authored documents and the multi authored documents. This indicates a fairly strong collaboration, and it also characterized by a fair degree of internationalization, denoting that the topic is very cross-country.

Table 1. Main information about data. Authors' elaboration.

Description	Results
MAIN INFORMATION ABOUT DATA	
Timespan	1992:2023
Sources (Journals, Books, etc)	74
Documents	200
Annual Growth Rate %	9.36
Document Average Age	5.49
Average citations per doc	41.83
References	11258
DOCUMENT CONTENTS	
Keywords Plus (ID)	579
Author's Keywords (DE)	882
AUTHORS	
Authors	475
Authors of single-authored docs	22
AUTHORS COLLABORATION	
Single-authored docs	22
Co-Authors per Doc	2.96
International co-authorships %	31
DOCUMENT TYPES	
article	186
article; early access	14

The first article on this topic was written in 1992. Loch et al. [10] investigates the threats to information systems and resident data, and which of these are the most serious threats. The study categorizes threats by source and perpetrator, distinguishing between internal and external threats, and human versus non-human perpetrators, highlighting

that understanding these threats and their relative importance can help organizations better manage their information security. As can be seen in Figure 1, from that point onward, there was no significant activity until 2008, when the digitization process started to gain increasing importance. Simultaneously, cybersecurity risks amplified, particularly in the wake of conspicuous incidents such as the Yahoo's Data breach in 2014 or Ukraine power grid hack in 2015. The COVID-19 pandemic further accelerated the digitization process, highlighting the necessity to mitigate cybersecurity risks [19]. The scientific production reflected this trend, as the most significant peaks were observed in 2015, 2021, and 2022.

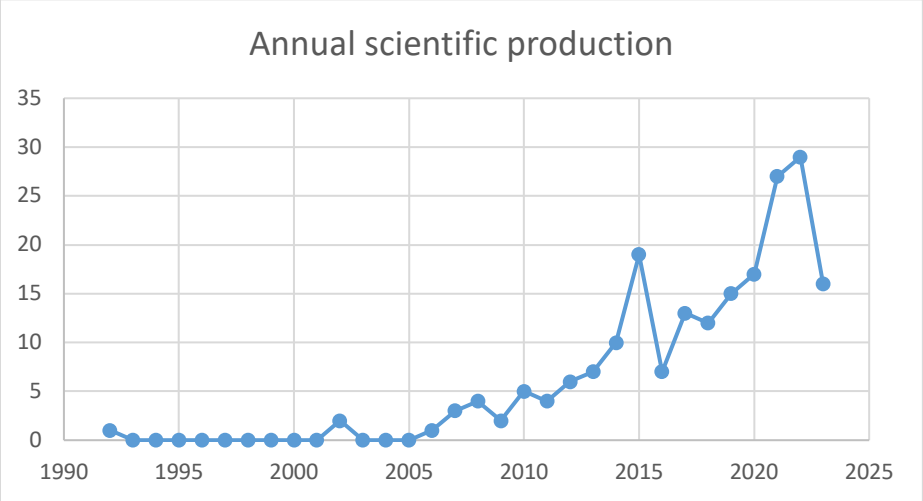

Fig. 1. Annual scientific production. Authors' elaboration

For example, Johnston et al. [20] explored the effectiveness of fear-based messages in encouraging compliance with information security policies, emphasizing the importance of social forces over formal sanctions in promoting compliance with recommended security policies and procedures. Vance et al. [21] stated moral beliefs and cultural factors play a significant role in in explaining employees' intentions to violate information system security policies. Kobis et Karyy [22] notes that the pandemic has forced enterprises to adapt to rapid changes in work organisation. This rapid transition, particularly for those with no previous remote work experience, resulted in a weakening of IT security infrastructure, particularly where the human factor was concerned.

In the Table 2 and Table 3 are shown most relevant journals and top authors. Figure 2 presents the principal nations in terms of citations. The United States stands out as the most significant contributor, responsible for over 80% of the citations. European countries, on the other hand, lag significantly behind.

Table 2. Most relevant sources

Sources	Articles
INFORMATION & MANAGEMENT	24
MIS QUARTERLY	18
INFORMATION SYSTEMS RESEARCH	14
EUROPEAN JOURNAL OF INFORMATION SYSTEMS	12
JOURNAL OF MANAGEMENT INFORMATION SYSTEMS	11
EUROPEAN JOURNAL OF OPERATIONAL RESEARCH	6
JOURNAL OF ENTERPRISE INFORMATION MANAGEMENT	6
TECHNOLOGY INNOVATION MANAGEMENT REVIEW	6
IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT	5
BUSINESS HORIZONS	4

Table 3. Most relevant authors

Authors	Articles	Articles Fractionalized
LOWRY PB	10	2,43333333
VANCE A	9	2,68333333
WANG JG	8	2,66666667
POSEY C	6	1,26666667
RAO HR	6	2,08333333
SIPONEN M	6	2,08333333
WARKENTIN M	6	2,16666667
D'ARCY J	5	1,91666667
ROBERTS TL	5	1,1
BENNETT RJ	4	0,81666667

Figure 3 shows most frequents keywords, adopting Keyword plus term provided by Wos [23]. The most common keywords in the data are “impact”, “deterrence”, “threats, and “model”, following “fear appeals” and “policy compliance”. This frames the trend that sees many cybersecurity issues related to the need to follow company policies in terms of Information Security Policy (ISP), using the strategy of deterrence or fear appeal from an organizational behavior perspective [20]. The former is based on the principle that people will be dissuaded from committing cybercrimes or violating information security policies if the potential cost or punishment outweighs the perceived benefits while the latter relies on generating a sense of fear or apprehension to motivate behavior change [24] [25]. The idea is to highlight the potential negative outcomes of

certain behaviors to encourage individuals to adopt safer practices, through training or awareness campaigns.

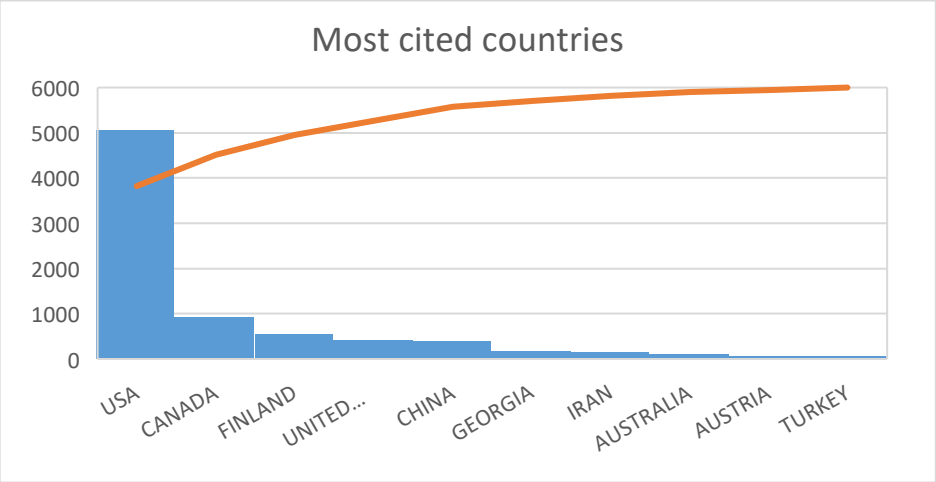

Fig. 2. Most cited countries

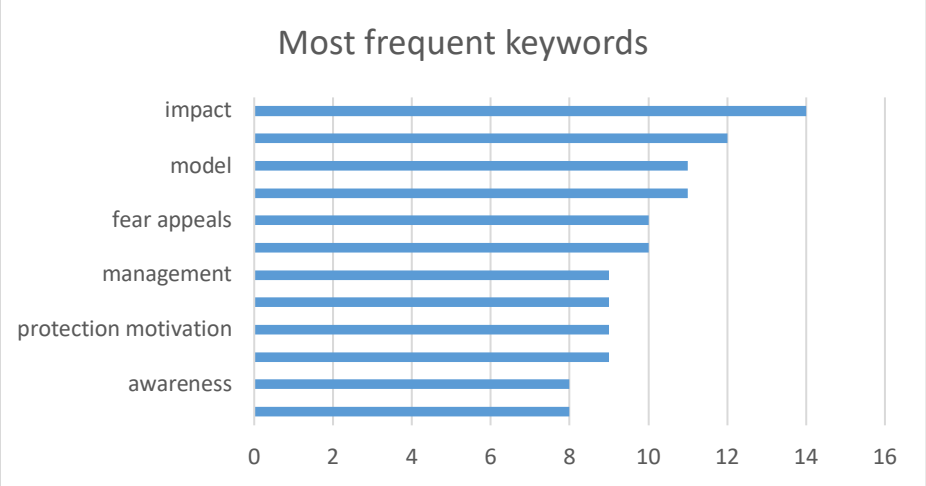

Fig. 3. Most frequent keywords

Table 4 and Table 5 show the top 10 most locally cited papers related to the entire dataset and a subset of the last 5 years of scientific production, respectively. The choice to highlight the most locally cited papers helps identify the most influential documents within a specific dataset. These are the works that have had the most impact on the set of documents analyzed and understanding them can provide valuable insights into the core ideas driving the area of interest.

Table 4. Most local cited papers (complete dataset / from 1992)

Document	Year	Local.Citations	Global.Citations
HERATH T, 2009, EUR J INFORM SYST	2009	45	664
SIPONEN M, 2010, MIS QUART	2010	45	568
JOHNSTON AC, 2010, MIS QUART	2010	40	651
BOSS SR, 2015, MIS QUART	2015	28	315
WILLISON R, 2013, MIS QUART	2013	27	280
JOHNSTON AC, 2015, MIS QUART	2015	27	227
VANCE A, 2012, INFORM MANAGE-AMSTER	2012	21	376
D'ARCY J, 2014, J MANAGE INFORM SYST	2014	20	247
LOCH KD, 1992, MIS QUART	1992	15	176
POSEY C, 2013, MIS QUART	2013	15	130

It's worth commenting on the most local cited papers from the last five years (Table 5) in order to capture the most recent trends and emerging issues. It was identified three themes among them.

Emotion, Personality, and Behavior

Vance et al. [26] contribute to understanding security warnings habituation in information systems by measuring the decline in attention and warning adherence over time using neurobiological tools and field experiments. It illustrates that frequent exposure to security warnings results in reduced adherence. However, the use of polymorphic warnings - those changing in appearance - can effectively reduce habituation. Johnston et al. [27] explore the effectiveness of information security fear appeal messages in inducing employees to comply with security policies. It finds that such messages are more effective when they align with the personality characteristic adaptations of the recipients. Good alignment leads to higher perceptions of threat severity and self-efficacy, and lower perceived cost, leading to better compliance behavior. Poor alignment, conversely, results in failure to influence behavior. The primary distinction between successful and unsuccessful messages was the rhetoric employed, suggesting the need to personalize security communications for maximum effectiveness. The study also stresses the importance of measuring actual behavior, not just behavioral intentions. Liang et al. [28] provide new insights into the role of emotions in IT security management. The study delves into personal IT users' coping strategies when faced with security threats, focusing on Emotion-Focused Coping (EFC) and Problem-Focused Coping (PFC). It reveals that different types of EFC (inward and outward) have contrasting effects on PFC behavior - the former discourages PFC actions, whereas the latter encourages them. The research enhances the understanding of users' response to perceived threats and perceived avoidability, informing how these perceptions impact EFC and, subsequently, PFC. Schuetz et al. [29] investigate the effectiveness of fear appeals in Information Security (ISec) contexts. It finds concrete fear appeals to be more successful in provoking fear-based outcomes than abstract appeals. Surprisingly, organizational users demonstrated higher fear and protection motivation levels than personal

users. The research suggests that the mixed findings in prior literature may be due to message abstractness and audience differences, offering significant insights for constructing fear appeals in ISec. D'Arcy et Teh [30] examine the relationship between Security-Related Stress (SRS) and compliance with Information Security Policies (ISP). It finds that SRS events provoke feelings of frustration and fatigue within individuals. These emotions can lead to an increased tendency to justify (neutralize) ISP violations, subsequently reducing ISP compliance. Frustration and fatigue serve as key intermediaries in the relationship between SRS and rationalizations of ISP violations. These findings underscore the need to account for emotional reactions when assessing ISP compliance, and the dynamic nature of neutralization.

Sanctions, Awareness, and Training

Chen et al. [31] conducted research to understand how formal (e.g., written rules) and informal (e.g., social or unwritten rules) sanctions affect compliance with an organization's Information Security Policy (ISP), particularly in a public university setting. Surprisingly, they found that formal rules or sanctions did not directly encourage people to follow the ISP while informal sanctions and an individual's ability or capability played a more significant role in ensuring people adhered to the ISP. Moreover, the type of organization, particularly public ones, might influence how compliant people are, possibly because of factors like wanting to take responsibility or gain recognition.

Burns et al. [32] explored the role of Security Education, Training, and Awareness (SETA) in shaping how internal members of an organization approach information security. They relied on expectancy theory, a psychological principle suggesting people will act based on what they expect as a result. They found that does SETA affects how much employees value security (security valence), believe that following security measures will have desired outcomes (security instrumentality), and expect that their efforts will ensure security (security expectancy). The authors point out that SETA does not just address basic motivations but also deeper, more intrinsic ones, since it promotes both lower and higher-order motivation-driving mechanisms in employees. It is important because the study also differentiates between just following security policies because it's a rule and genuinely wanting to protect an organizational informations. In this vein, SETA can be a powerful tool for organizations, pushing internal members to be more proactive and invested in maintaining information security.

Professional Subcultures and Security Compliance in Healthcare

Sarkar et al [33] reveal the influence of professional subcultures on Information System Policy (ISP) compliance in healthcare. Three subcultures: physicians, nurses, and support staff showed different ISP violation behaviors, highlighting an unspoken authority hierarchy despite a formal lack thereof. Notably, the concept of pseudocompliance, "window-dressing" without real security enhancement, emerged as a significant type of ISP violation. This behavior often stems from a desire to maintain patient care workflow, suggesting the need to streamline authentication processes. The research underscores the importance of considering professional subcultures when addressing ISP violations and designing user interfaces. Kwon & Johnson [34] investigate how meaningful-use attestation, a certification mechanism in U.S. healthcare aimed at promoting electronic health record (EHR) adoption and data protection, influences data breaches.

Findings reveal that attestation impacts external and accidental internal breaches differently over time. Hospitals attesting to Stage 1 meaningful-use standards experience fewer external breaches in the short term, but the improvement doesn't sustain over the next year. Accidental internal breaches initially increase in attesting hospitals but see long-term reductions. However, no connection was found between attestation and malicious internal breaches. The study provides insights for effective design of certification mechanisms. Kim & Kwon [35] found that the risk of breaches is rooted in digitized data and processes, rather than in the technological components themselves. The study found that the deployment of Electronic Health Records (EHRs) and undertaking Meaningful Use (MU) initiatives increases the risk of patient information breaches, primarily accidental rather than malicious. This suggests that such breaches occur due to user inattentiveness and lack of awareness rather than deliberate intent. It was observed that larger hospitals face higher risks of accidental breaches. Interestingly, the scale of malicious breaches was larger in hospitals that implemented EHRs. The study further discovered that the risk of breaches is rooted in digitized data and processes, rather than in the technological components themselves.

Table 5. Most local cited papers (2018-2023)

Document	Year	Local.Citations	Global.Citations
VANCE A, 2018, MIS QUART	2018	6	54
JOHNSTON AC, 2019, DECISION SCI	2019	6	28
CHEN XF, 2018, INFORM MANAGE-AMSTER	2018	5	43
BURNS AJ, 2018, DECISION SCI	2018	4	26
KWON J, 2018, MIS QUART	2018	4	19
LIANG HG, 2019, MIS QUART	2019	4	67
SCHUETZ SW, 2020, J MANAGE INFORM SYST	2020	3	19
D'ARCY J, 2019, INFORM MANAGE-AMSTER	2019	2	36
KIM SH, 2019, INFORM SYST RES	2019	2	17
SARKAR S, 2020, INFORM SYST RES	2020	2	16

Thematic map

Figure 4 shows the thematic map of keywords. The goal of constructing a thematic map is to discern the current landscape of a field and to anticipate its future direction. The methodology of thematic analysis involves examining clusters of keywords used by authors and their interconnections to establish themes. These themes are defined by two characteristics: density and centrality. The vertical axis represents the density, which gauges the cohesiveness among nodes. On the other hand, centrality is depicted on the horizontal axis and refers to the correlation degree among various topics. Both properties, as described by Esfahani et al. [36], provide measures of the development status

and importance of specific topics within the thematic framework. The upper right quadrant (“Motor”) represents driving themes, the lower right quadrant (“Basic”) is underlying themes, the upper left quadrant (“Niche”) is the very specialized themes, and the lower left quadrant (“Emerging/Declining”) is emerging or disappearing themes.

It's noticeable that themes are broadly scattered across all dimensions, with none having reached such magnitude as to represent a central theme in terms of contributions. Among the "motor themes", we can highlight the theme of information security in the healthcare sector [33]; the role of organizational culture, awareness, and motivational leverage in ensuring cybersecurity [37] [38]; the ability of top management to mitigate the effects of a cybersecurity incident through disclosure and apologies [39] [40]; the search for models, strategies, and practices to influence behavior to adhere to the Information Security Policy (ISP) [41] [42] [31].

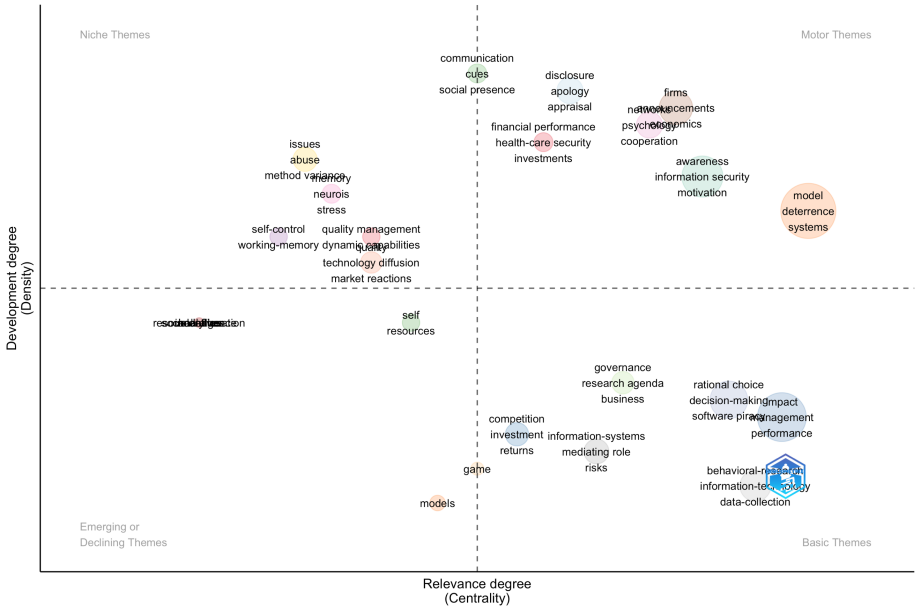

Fig. 4. Thematic map

The "niche themes" are less explored research trends that may offer interesting development perspectives. Some leverage frontier topics, such as neuroscience, for example: a research into non-malicious Information Security Policies violations reveals that reducing neuronal excitability in the left dorsolateral prefrontal cortex can lower endorsement of such violations, highlighting a neurobiological aspect of cybersecurity behaviors [43]. Another study exposes the "privacy paradox," demonstrating that low-effort information processing due to cognitive depletion or positive mood weakens the relationship between stated privacy concerns and disclosure behaviors, highlighting that the paradox's existence is contextually dependent [44]. Also, a study linked self-control to information security decisions, with individuals of lower self-control showing reduced neural activity in decision-making regions [45]. Another theme involves applying the lens of organizational learning to cybersecurity issues. Ghahramani et al.

[46] reveal that absorptive capacity affects an organization's continuous improvement in information security management, with this effect mediated through adaptability to security threats and dependent on the organization's competitive pressure.

4 Discussion

The intricate connections between human factors and cybersecurity outcomes emerge as a key theme across the literature. As digital technologies become further embedded into organizational operations, it is apparent that generic cybersecurity strategies are not sufficient to address the dynamic challenges of today considering the various cognitive, emotional, and professional dynamics involved.

A notable concern in cybersecurity literature is the phenomenon of habituation to security warnings. Over time people tend to become less compliant with these warnings [47]. One potential solution is to introduce variability in how these warnings appear which could help reduce habituation and promote a dynamic approach to security communications. Furthermore, there's a growing emphasis on personalization, premised on the idea that tailoring security messages to align with individual traits can lead to better compliance, underscoring the importance of moving away from one size fits all strategies. In this way, it's important to develop security messages that are congruent with individual characteristics rather than relying on generic approaches. At the same time, emotional responses significantly influence security behaviors. Different coping mechanisms, whether introspective or extrospective, can have an impact on how individuals respond to perceived threats. The ramifications of emotional strain from security stressors, such as frustration and fatigue, are instrumental in shaping compliance. Thus, efficacious strategies necessitate an understanding of the individual’s emotional context.

However, based on the analysis conducted it appears that the effectiveness of cybersecurity strategies is also impacted by professional subgroups. These can have their own culture, skill set, language, and *modus operandi* that may differ from other subgroups within the same organization [48]. Professional subgroups play a role in shaping the dynamics of an organization by establishing standards, practices, and expectations related to their area of expertise. Although there is evidence in the healthcare sector [33], these issues can likely also be transferred to other contexts. For instance, different subgroups may perceive risks and priorities differently due to their use of technologies, systems and workflows which have distinct vulnerabilities. Moreover, each subgroup can influence the development of cybersecurity policies and conflicts may arise when one groups needs clash with anothers. In this sense, the presence of professional subcultures introduces an additional layer of complexity, suggesting that strategies need to be tailored not just to individuals but also to entire professional groups [49].

Conversely, initiatives focused on training and increasing awareness (SETA) are particularly promising avenues, in strengthening organizational cybersecurity. By influencing the motivations and behaviors of employees these initiatives can bridge the gap between policy and practice. However, it's essential to differentiate between intentions to comply with security policies and intentions to protect organizational information. On one hand, there's the intention to comply with set policies due to mandates

such as following password guidelines without grasping their importance. On the other, there is an intrinsic motivation to genuinely protect organizational data and information driven by a deep understanding of its value and the risks posed by breaches [50]. Each type of intention requires an approach in terms of training and awareness. For the first, it might be about clarity on rules and potential consequences of non-compliance. For the latter, it's about fostering a culture of security and instilling a genuine understanding of the risks and repercussions of security breaches. Several aspects related to the technical aspects of cybersecurity organizational readiness yielded encouraging results, which could be attributed to the IT skills of employees working in the ICT sector [51]. However, areas such as training activities and implementation of cybersecurity policies require improvement as they form the foundation, for cybersecurity awareness and culture. This highlights that both human factors and organizational elements are weak points that require attention.

5 Conclusions

The findings of this paper emphasize the critical role of human factors in organizational cybersecurity [52] [53]. The review highlights the pivotal position of individuals within the digital realm - not merely as users, but also as potential weak links or safeguards in the cybersecurity landscape. Our analysis demonstrates that a robust cybersecurity strategy requires an approach that go beyond relying on purely technological defenses and consider aspects such as human behavior, emotions and organizational culture. This further supports the notion that cyber risk is primarily rooted in people and processes than the technological components themselves [35]. Consequently there is a need for work that can strengthen both theoretical foundations and practical applications in this critical field.

This paper shows that interplay between human factors and cybersecurity outcomes is crucial across all organizational settings. Standardized approaches to cybersecurity often fail to address the complexities arising from cognitive, emotional, and professional dynamics. Dealing with responses to security alerts poses challenges, however personalized and dynamic security communications tailored to characteristics can enhance compliance. Emotions, like frustration and fatigue significantly influence security behaviors. Furthermore, the presence of professional subgroups and different workflows introduces additional layers of complexity. This calls for strategies that resonate with both individual and group-specific cultural contexts and characteristics. While technical aspects of cybersecurity readiness show promise, it is crucial to prioritize training and policy implementation to emphasize compliance and genuine data protection motivations.

According with Dalal et al. [54], this study highlights the evolving perspective on cybersecurity, clarifying that technology alone cannot safeguard organizations. Instead, the nexus between human factors and cybersecurity emerges as the central issue [55]. The literature clearly states that comprehending cybersecurity requires an understanding of emotional and professional dynamics within organizations. As such, this paper contributes to the theory by emphasizing the limitations of standardized cybersecurity

approaches. It accentuates the importance of adaptive strategies which take into account the human complexities, diverse professional subgroups, and their respective organizational cultures. The findings consolidate the idea of cybersecurity as a sociotechnical domain, urging the integration of organizational science insights to foster both practical applications and theoretical advancements in cybersecurity.

6 Further research

Considering recent advancements and findings, the landscape of cybersecurity continues to evolve, uncovering gaps that require further exploration. This section focuses on areas that can provide insights for improving organizational security measures and gaining a deeper understanding of vulnerabilities centered around human behavior.

The emotional aspects within cybersecurity offer an avenue for research. It is crucial to develop an understanding of how individuals emotionally respond to security warnings and breaches as well as their coping mechanisms. Examining the impact of emotions such as trust, anxiety, and overconfidence can yield significant insights. Excessive trust might lead to inertia, while increased anxiety could hinder responses during crises. Concurrently, it is important to understand how stress affects cognitive abilities like attention and decision making. In a stressful situation, an employee might overlook critical signs of a cyberattack or misinterpret the severity of an incident due to impaired judgment, particularly when time pressure comes into play [56]. Investigating how stress-induced cognitive disruptions amplify vulnerabilities and developing real time interventions to mitigate these challenges would greatly contribute to both theory and practice.

Moreover, the influence of professional subcultures on security compliance seems a promising avenue of research. This calls for ongoing investigation across diverse industries. While it has been observed that distinct dynamics within healthcare, extending this line of research across other industries like finance, education, and defense could provide a comprehensive understanding. By examining how the characteristics and requirements of different industries shape cybersecurity policies and practices, it could help to develop targeted strategies that cater to specific sectors. For instance, exploring potential tensions between productivity pressures and security best practices within specific industries could unveil key insights.

Finally, the development of a framework focused on human behavior and organizational cybersecurity is crucial. This framework would serve as a foundation for addressing vulnerabilities systematically guiding interventions and identifying areas for future research. For instance, Rasmussen [57] presented a human error taxonomy that identified three primary categories of errors: skill-based, rule-based, and knowledge-based. Each type of error is rooted in a distinct cognitive process. Skill-based errors arise from actions performed almost automatically due to repetition and familiarity. Rule-based errors emerge when individuals misapply standardized procedures or learned rules in certain contexts. Conversely, knowledge-based errors surface in uncharted territories, where individuals navigate unfamiliar challenges without pre-established rules or ex-

periences, relying primarily on problem-solving skills. Applying Rasmussen's taxonomy to organizational cybersecurity offers a fresh perspective to identify and understand vulnerabilities. For instance, skill-based errors may manifest when employees undertake habitual cybersecurity measures, leading to oversight due to over-familiarity. Rule-based errors arise in scenarios where pre-established security protocols are either misunderstood or wrongly implemented. Finally, knowledge-based errors arise when individuals face unfamiliar challenges without a set playbook and they are not sufficiently prepared to uncertainty.

This structured approach offers a method for guiding future research and integrating new organizational routines and policies. By examining training programs and distinct organizational designs we can address specific human errors in the context of organizational cybersecurity. This advancement in both theory and practice could contribute to strengthening cybersecurity practices by addressing the inherent human vulnerabilities in cyber incidents.

7 Limitations

The present study, though comprehensive in examining the association between human factors and organizational cybersecurity, possesses several limitations. First, the confined scope of the literature review may have potentially affected the all-inclusiveness of the study. The literature review was exclusively grounded in research articles from Web of Science databases, deliberately excluding any meaningful information from conference papers, books, chapters, and monographs. Furthermore, the keyword selection, though supported by prior studies, could have inadvertently omitted pertinent articles that employed different terms and keywords to describe analogous concept.

References

1. Global cyber risk perception survey. Marsh (2019).
2. Business losses to cybercrime data breaches to exceed $5 trillion by 2024. Juniper Research. Retrieved from https://www.juniperresearch.com/press/press-releases/business-losses-cybercrime-data-breaches, last accessed 2023/05/10.
3. Cybercrime damages $6 trillion by 2021. Cybersecurityventures. Retrieved from https://cybersecurityventures.com/annual-cybercrime-report-2017/, last accessed 2023/05/10.
4. Gordon, S., & Ford, R.: On the definition and classification of cybercrime. Journal in computer virology 2, 13-20 (2006).
5. La Stampa: “Regione Lazio ostaggio degli hacker, ecco come è stato organizzato l’attacco”, https://www.lastampa.it/cronaca/2021/08/02/news/regione-lazio-ostaggio-degli-hacker-ecco-come-e-stato-organizzato-l-attacco-1.40561532/ last accessed 2023/05/10.
6. Zupic, I., & Čater, T.: Bibliometric methods in management and organization. Organizational research methods 18(3), 429-472 (2015).
7. Broadus, R. N.: Toward a definition of “bibliometrics”. Scientometrics 12, 373-379 (1987).
8. Crane, D.: Invisible colleges: Diffusion of knowledge in scientific communities.
9. Aria, M., & Cuccurullo, C.: bibliometrix: An R-tool for comprehensive science mapping analysis. Journal of informetrics 11(4), 959-975 (2017).

10. Loch, K. D., Carr, H. H., & Warkentin, M. E.: Threats to information systems: today's reality, yesterday's understanding. Mis Quarterly, 173-186 (1992).
11. Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K.: A systematic literature review on the cyber security. International Journal of scientific research and management 9(12), 669-710 (2021).
12. Hicks, D., & Wang, J.: Coverage and overlap of the new social sciences and humanities journal lists. Journal of the American Society for Information Science and Technology 62(2), 284-294 (2011).
13. Ball, R., & Tunger, D.: Science indicators revisited–Science Citation Index versus SCOPUS: A bibliometric comparison of both citation databases. Information Services & Use 26(4), 293-301 (2006).
14. Verbeek, A., Debackere, K., Luwel, M., & Zimmermann, E.: Measuring progress and evolution in science and technology–I: The multiple uses of bibliometric indicators. International Journal of management reviews 4(2), 179-211 (2002).
15. Briner, R. B., & Denyer, D.: Systematic review and evidence synthesis as a practice and scholarship tool. (2012)
16. Callon, M., Courtial, J.P., Turner, W.A., & Bauin, S.: From translations to problematic networks: An introduction to co-word analysis. Social Science Information 22(2), 191-235 (1983).
17. Lebart, L., Morineau, A., & Warwick, K.M.: Multivariate Descriptive Statistical Analysis (Correspondence Analysis and Related Techniques for Large Matrices). Wiley, Chichester (1984).
18. Rousseeuw, P. J.: Silhouettes: a graphical aid to the interpretation and validation of cluster analysis. Journal of computational and applied mathematics 20, 53-65 (1987).
19. Pranggono, B., & Arabo, A.: COVID-19 pandemic cybersecurity issues. Internet Technology Letters 4(2), e247 (2021).
20. Johnston, A. C., Warkentin, M., & Siponen, M.: An enhanced fear appeal rhetorical framework. MIS quarterly 39(1), 113-134 (2015).
21. Vance, A., Siponen, M. T., & Straub, D. W.: Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. Information & Management 57(4), 103212 (2020).
22. Kobis, P., & Karyy, O.: Impact of the human factor on the security of information resources of enterprises during the COVID-19 pandemic. Polish Journal of Management Studies 24(2), 210-227 (2021).
23. Garfield, E., & Sher, I. H.: Key words plus [TM]-algorithmic derivative indexing. Journal-American Society For Information Science 44, 298-298 (1993).
24. Li, Y., Pan, T., & Zhang, N.: From hindrance to challenge: How employees understand and respond to information security policies. Journal of enterprise information management 33(1), 191-213 (2020).
25. Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P.: What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS quarterly 39(4), 837-864 (2015).
26. Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., & Kirwan, C. B.: Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments (2018).
27. Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M.: Speak their language: Designing effective messages to improve employees' information security decision making. Decision Sciences 50(2), 245-284 (2019).

28. Liang, H., Xue, Y., Pinsonneault, A., & Wu, Y. A.: What users do besides problem-focused coping when facing IT security threats: An emotion-focused coping perspective. MIS quarterly 43(2), 373-394 (2019).
29. Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J.: The effectiveness of abstract versus concrete fear appeals in information security. Journal of Management Information Systems 37(3), 723-757 (2020).
30. D'Arcy, J., & Teh, P. L.: Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. Information & Management 56(7), 103151 (2019).
31. Chen, X., Wu, D., Chen, L., & Teng, J. K.: Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. Information & Management 55(8), 1049-1060 (2018).
32. Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F.: Intentions to comply versus intentions to protect: A VIE theory approach to understanding the influence of insiders' awareness of organizational SETA efforts. Decision Sciences 49(6), 1187-1228 (2018).
33. Sarkar, S., Vance, A., Ramesh, B., Demestihas, M., & Wu, D. T.: The influence of professional subculture on information security policy violations: A field study in a healthcare context. Information Systems Research 31(4), 1240-1259 (2020).
34. Kwon, J., & Johnson, M. E.: Meaningful healthcare security: Does meaningful-use attestation improve information security performance?. MIS Quarterly 42(4), 1043-1068 (2018).
35. Kim, S. H., & Kwon, J.: How do EHRs and a meaningful use initiative affect breaches of patient information?. Information Systems Research 30(4), 1184-1202 (2019).
36. Esfahani, H., Tavasoli, K., & Jabbarzadeh, A.: Big data and social media: A scientometrics analysis. International Journal of Data and Network Science 3(3), 145-164 (2019).
37. Tejay, G. P., & Mohammed, Z. A.: Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. Information & Management 60(3), 103751 (2023).
38. Kumah, P., Yaokumah, W., & Buabeng-Andoh, C.: Identifying HRM practices for improving information security performance: an importance-performance map analysis. In: Research Anthology on Business Aspects of Cybersecurity, pp. 326-348. IGI Global (2022).
39. Kim, N., & Lee, S.: Cybersecurity breach and crisis response: An analysis of organizations' official statements in the United States and South Korea. International Journal of Business Communication 58(4), 560-581 (2021).
40. Demek, K. C., & Kaplan, S. E.: Cybersecurity breaches and investors' interest in the firm as an investment. International Journal of Accounting Information Systems 49, 100616 (2023).
41. Herath, T., & Rao, H. R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of information systems 18, 106-125 (2009).
42. Siponen, M., Mahmood, M. A., & Pahnila, S.: Employees' adherence to information security policies: An exploratory field study. Information & management 51(2), 217-224 (2014).
43. Turel, O., He, Q., & Wen, Y.: Examining the neural basis of information security policy violations: a noninvasive brain stimulation approach. MIS Quarterly 45(4), 1715-44 (2021).
44. Alashoor, T., Keil, M., Smith, H. J., & McConnell, A. R.: Too Tired and in Too Good of a Mood to Worry About Privacy: Explaining the Privacy Paradox Through the Lens of Effort Level in Information Processing. Information Systems Research (2022).
45. Hu, Q., West, R., & Smarandescu, L.: The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. Journal of Management Information Systems 31(4), 6-48 (2015).

46. Ghahramani, F., Yazdanmehr, A., Chen, D., & Wang, J.: Continuous improvement of information security management: an organisational learning perspective. European Journal of Information Systems, 1-22 (2022).
47. Reeves, A., Delfabbro, P., & Calic, D.: Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. SAGE open 11(1), 21582440211000049 (2021).
48. Bechky, B. A.: Sharing meaning across occupational communities: The transformation of understanding on a production floor. Organization science 14(3), 312-330 (2003).
49. Rangachari, P.: Knowledge sharing networks in professional complex systems. Journal of Knowledge Management 13(3), 132-145 (2009).
50. Alzahrani, A., Johnson, C., & Altamimi, S.: Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organisation. In: 2018 4th International Conference on Information Management (ICIM), pp. 125-132 (2018)
51. Neri, M., Niccolini, F., & Martino, L.: Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. Information & Computer Security (2023).
52. Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D.: Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work 24(2), 371-390 (2022).
53. Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z.: Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon 7(3) (2021)
54. Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J.: Organizational science and cybersecurity: abundant opportunities for research at the interface. Journal of business and psychology 37(1), 1-29 (2022).
55. Lu, Y.: Cybersecurity research: A review of current research topics. Journal of Industrial Integration and Management 3(04), 1850014 (2018).
56. Chowdhury, N. H., Adam, M. T., & Teubner, T.: Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. Computers & Security 97 (2020).
57. Rasmussen, J.: The definition of human error and a taxonomy for technical system design. In: New technology and human error, pp. 23-30. Wiley (1987).