Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1547–1558
DOI : 10.47974/JDMSC-2153

Cybersecurity meets HR : A decade of trends, challenges, and best practices

Sonal Khandelwal [†]
Amity Business School
Amity University Rajasthan
SP-1, Kant Kalwar, RIICO Industrial Area, NH-11C
Jaipur 303002
Rajasthan
India

Aanyaa Chaudhary *
Department of Management
Manipal University Jaipur
Jaipur Ajmer Express Highway
Jaipur 303007
Rajasthan
India

Abstract

This systematic literature review (SLR) examines the convergence of cybersecurity and human resource management (HRM), aiming to understand the dynamic landscape, uncover key trends, address challenges, and highlight best practices. The ever-increasing reliance on digital technologies has necessitated robust cybersecurity measures, making it imperative for HRM to adapt and integrate these practices into organizational strategies. The review synthesizes findings from numerous studies published over the past decade, emphasizing HR's pivotal role in cultivating a cybersecurity-conscious culture, examining how cybersecurity affects employee behavior and organizational performance, and outlining strategies for managing cybersecurity risks. The insights are invaluable for HR professionals, cybersecurity specialists, and organizational leaders, underscoring the essential function of HR in protecting digital assets and ensuring the organization's resilience in a highly interconnected world.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Cybersecurity, Cybercrime, Human resource management, SLR, Employees, Culture, Organizations.*

[†] *E-mail:* **sonal.khandelwal.sharma@gmail.com**
* *E-mail:* **aanyaa1912@gmail.com (Corresponding Author)**

1. Introduction

In today's digitally driven organizational setting, the threat environment has become more complicated, with cybersecurity breaches and cybercrime which are detrimental on operations, reputation, and financial stability. Thorough cybersecurity measures are vital; yet the efficacy of these defenses is significantly influenced by the human element within businesses. As people become accustomed to improved vigilant employment of technology the sentiments were more neutral or positive towards cyber threats [1]. HRM plays a major role in enhancing cybersecurity resilience by increasing awareness, implementing training programs, and developing rules for safety. Despite this important relationship, the academic literature on the topic of cybersecurity and human resource management is largely scattered. Using the PRISMA approach, this SLR attempts to synthesize research on the relationship between cybersecurity and HRM, guaranteeing a thorough and transparent review process. R Studio was used in this SLR to facilitate effective data analysis and visualization. The review seeks to pinpoint important developments, difficulties, and best practices at the nexus of HRM and cybersecurity.

The results of this SLR will provide insightful information for cybersecurity specialists, HR specialists, and organizational leaders, highlighting the critical role that HR plays in safeguarding digital assets and maintaining resilience.

2. Methodology

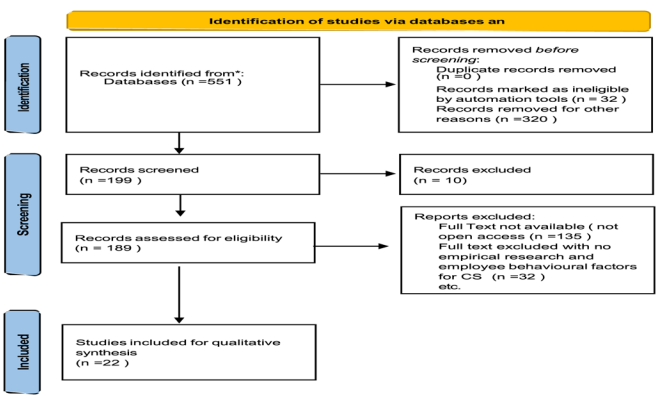


Figure 1

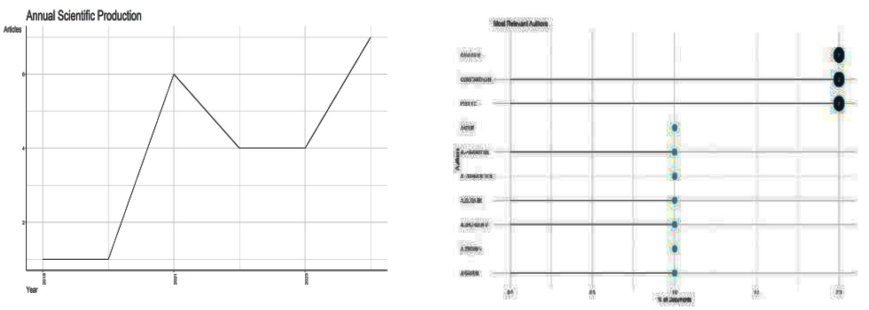
PRISMA Flowchart used for SLR

The research adapts Preferred Reporting Items for Systematic Reviews and Meta- Analyses (PRISMA) technique [2], for conducting a structured literature review (SLR). This provides a clear direction for SLR [3]. The exclusion and inclusion criterion has been explained in figure 1. The first database based comprised of identification stage of literature from Scopus database based on the keywords related to research keywords related to research namely, "Cybersecurity" OR " Cybercrime") AND ("HR" OR "Human Resource Management" OR "Employee" OR called filtering stage "Employees") AND ("Organization" OR "Organization"). They were further filtered in the second stage based on years from 2014 -2024, were included. Furthermore, only those studies which were in English and from the subject area "Social Sciences", " Business, Management " and "Accounting "were included. In the screening stage, only those articles that were open access were included. In the final stage, the eligibility stage those articles that were empirical studies and highlighted the factors impacting cybersecurity behavior were selected and the factors were identified that promoted cybersecurity behavior amongst employees. The bibliometric analysis of the literature thus obtained was done using Biblioshiny software with R studio 'Bibliometrix' tool and the SLR was done by reading each article in depth.

3. Results

3.1 *Bibliometric Analysis*

Figure 2 depicts that there has been increase in research centered around employee-related factors that enhance cybersecurity behavior since 2019 Though there was small fall in the publication between 2021



2(a) 2(b)

Figure 2

(a) Annual Scientific Production & 2(b) Most Relevant Authors

3(a) 3(b)

Figure 3

Word Cloud of Bigrams in abstract and Trend Topics

and 2023. Figure 2 (b) also highlights Canham, Constantino and Posey as most prolific authors in the field since 2019.

Figure 3 (a) reflects the word cloud of bigrams of abstract of the research studies. It is evident from the word cloud the proliferation of cybersecurity issues and studies about the employees' behavioral factors to protect against cybercrime. Words like multi-factor authentication, information processing, and time pressure highlight the factors that influence employees' CS behavior. This is reinforced by the trend graph in 3(b) which depicts the growing topics of the research in the area including terms like 'cybersecurity awareness", and "technology protection". Trend analysis shown in figure 4 shows that amongst the 4 quadrants, the upper right quadrant with high centrality and high density shows the topics that are most developed from 2019-2024 with increasing studies in the field. These topics are "time pressure", "cybersecurity awareness" and "information processing".

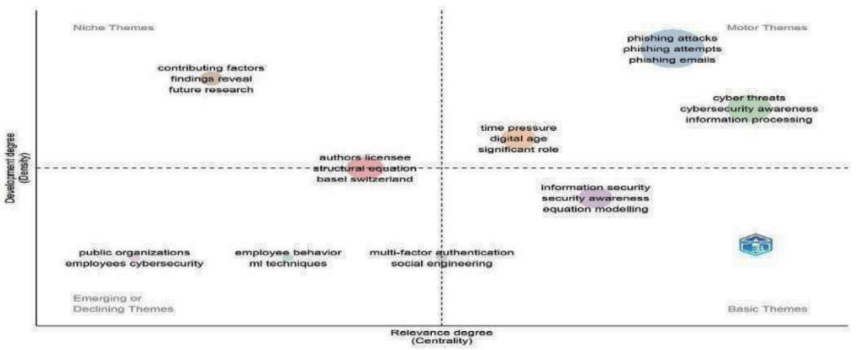


Figure 4

Thematic Map

3.2 *SLR on Employee Cybersecurity (CS) Behaviour*

Table 1 summarizes the factors identified that impacted employee CS behavior. It categorizes the factors as intrinsic /(individual-level) factors and extrinsic (organization-level) factors. Intrinsic factors include an employee's personality, stress, time pressure, normative belief, information processing and awareness. Extrinsic factors are the factors controlled by organization like training to educate employees, incentive, multifactor authentication and single platform usage.

Table 1

Studies on Factors Impacting Employees' Cybersecurity Behavior

Author	Title	Factors Identified	Intrinsic / Extrinsic
Chaudhary [4]	"Driving Behavior Change with Cybersecurity Awareness"	senior management support and participation, cultivate and spread 'cybersecurity' as a norm in the organization; iv) encourage cybersecurity activities and behaviors through incentives, regular updating of CS awareness, incentives to promote CS behavior	Extrinsic
Saeed [5]	"Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia"	Effective password management, Appropriate email management, Organizational security policy	Extrinsic
Strang [6]	"Cybercrime Risk Found in Employee Behavior Big Data Using Semi-Supervised Machine Learning with Personality Theories"	neuroticism was associated with a greater organizational cybercrime risk, openness to new experiences was inversely related to cybercrime risk	Intrinsic

Contd...

Nepal et al. [7]	"Burnout in Cybersecurity Incident Responders: Exploring the Factors that Light the Fire"	Increased workload, limited control, poor teamwork, and inadequate recognition Which increased burnout that leads to CS risks	Extrinsic
Spithoven and Drenth [8]	"Who will take the bait? Using an embedded, experimental study to chart organization-specific phishing risk profiles and the effect of a voluntary microlearning among employees of a Dutch municipality"	Senior and middle-aged employees have higher CS risk; offline training reduces CS risk	Extrinsic
Daengsi, Pornpong-techavanich, and Wuttidit-tachotti, [9]	"Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks"	Knowledge transfer decreased cybersecurity risk and it was also impacted by gender.	Extrinsic
Whitty, Moustafa, and Grobler [10]	"Cybersecurity when working from home during COVID-19: considering the human factors"	psychological (e.g. stress, anxiety, confidence, motivation)	Intrinsic
		sociological (e.g. sharing physical spaces, digital divide) factors influence cybersecurity behavior	Extrinsic
Beu et al. [11]	"Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation"	lower employee satisfaction and loyalty predicted increasingly unsafe behavior	Intrinsic

Contd...

Waqas [12]	"Enhancing Cybersecurity: The Crucial Role of Self-Regulation, Information Processing, and Financial Knowledge in Combating Phishing Attacks"	systematic information processing and financial knowledge	Intrinsic
Gerdenitsch, Wurhofer, and Tscheligi [13]	"Working Conditions and Cybersecurity: Time Pressure, Autonomy and Threat Appraisal Shaping Employees' Security Behavior"	security knowledge, perception of severity, increased cybersecurity behavior while time pressure reduced it	Intrinsic
Tariq et al. [14]	"How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks"	detect function, multifactor authentication	Extrinsic
Baltuttis and Teubner [15]	"Effects of visual risk indicators on phishing detection behavior: An eye-tracking experiment"	visual risk indicators enhanced cybersecurity behavior	Extrinsic
Sumner [16]	"Examining Factors Impacting the Effectiveness of Anti-Phishing Trainings"	Personality	Intrinsic
		Training	Extrinsic
Canham et al. [17]	"Phishing for Long Tails: Examining Organizational Repeat Clickers and Protective Stewards"	"Gaffes," "Beacons," "Spectators," and "Gushers."-four categories of employees that impacted cybersecurity behavior	Intrinsic
Buil-Gil and Barrett [18]	"The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention"	Cybersecurity training increases cybersecure behavior	Extrinsic

Contd...

Williams, Maharaj, and Ojo [19]	"Employee behavioural factors and information security standard compliance in Nigeria banks"	normative belief, security awareness, perception biases and certainty of detection influence compliance to CS policies	Intrinsic
Donald, Bumpus, and Zhang [20]	"A case study in selection and deployment of a multi-factor authentication solution"	multi-factor authentication implementation	Extrinsic
Heering [21]	"Ensuring cybersecurity in shipping: Reference to Estonian shipowners"	Education & Training of potential threats	Extrinsic
Park, Yoo, and Lee [22]	"7s model for technology protection of organizations"	shared values impacted the Cs behavior most than other factors in 7s model	Intrinsic
Canham, Posey, and Constantino [23]	"Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks"	Learning goal orientation, past performance	Intrinsic
		Age (Older employees showed more cybersecure behavior), single platform usage	Extrinsic
Leering, Wijngaert, and Nikou [24]	"More honour'd in the breach: predicting non-compliant behaviour through individual, situational and habitual factors"	Bad habits, lack of self-efficacy, time pressure	Intrinsic
Mihailović [25]	"Covid-19 and beyond: Employee perceptions of the efficiency of teleworking and its cybersecurity implications"	Employee Perception, namely, perception of organizational efficiency and the extent to which the digital information security of their organizations has been threatened	Intrinsic

4. Discussion

The above results clearly depict the growth in the field of identification of factors that promote cybersecure behavior in organizations. The trend topics and thematic maps depict that cybersecurity can be enhanced by creating awareness and training employees to identify phishing attacks and prevent them from being detrimental for the organization. The SLR points out that apart from extrinsic factors there are intrinsic factors within individual employees that determine their cybersecure behavior. These include perception of severity, personality of the employees, internal information processing, normative behavior and bad habits. The identification of the factors both internal and external will help organizations to educate the employees and craft policies that will equip employees to identify cybercrime and protect organizations from cyber-attacks which is a major challenge faced globally.

5. Conclusion

This research study is based on PRISMA method of SLR as it is most preferred method for identification and selection of articles for SLR. As the world moves towards digital transformation the concerns of cybersecurity are also on the rise. This study uniquely contributes to the identification of intrinsic and extrinsic factors that organizations should consider for creating a cyber secure workplace. Future research may be taken to empirically study the factors and create digitally secure workplace.

References

[1] S. Khandelwal and A. Chaudhary, "COVID-19 pandemic & cyber security issues: Sentiment analysis and topic modeling approach," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 25, no. 4, pp. 987–997 (May 2022).

[2] M.J. Page, J.E. McKenzie, P.M. Bossuyt, I. Boutron, T.Hoffmann, C.D. Mulrow, L. Shamseer, and D. Moher , "Mapping of reporting guidance for systematic reviews and meta-analyses generated a comprehensive item bank for future reporting guidelines", *Journal of clinical epidemiology,* 118, pp. 60-68 (2020), https://doi.org/10.1016/j.jclinepi.2019.11.010,

[3] E. Stovold, D. Beecher, R. Foxlee, and A. Noel-Storr, "Study flow diagrams in Cochrane systematic review updates: An adapted PRISMA flow diagram," *Systematic Reviews*, vol. 3, p. 54 (2014).

[4] S. Chaudhary, "Driving behaviour change with cybersecurity awareness," Computers & Security, Article ID 103858 (2024).

[5] S. Saeed, "Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia," *Sustainability*, vol. 15, no. 7, p. 6019 (2023).

[6] K. D. Strang, "Cybercrime Risk Found in Employee Behavior Big Data Using Semi-Supervised Machine Learning with Personality Theories," *Big Data and Cognitive Computing*, vol. 8, no. 4, p. 37 (2024).

[7] S. Nepal, J. Hernandez, R. Lewis, A. Chaudhry, B. Houck, E. Knudsen, R. Rojas, B. Tankus, H. Prafullchandra, and M. Czerwinski, "Burnout in Cybersecurity Incident Responders: Exploring the Factors that Light the Fire," Proceedings of the ACM on Human-Computer Interaction, vol. 8, no. CSCW1, pp. 1–35 (2024).

[8] R. Spithoven and A. Drenth, "Who will take the bait? Using an embedded, experimental study to chart organization-specific phishing risk profiles and the effect of a voluntary microlearning among employees of a Dutch municipality," *Journal of Cybersecurity*, vol. 10, no. 1 (2024).

[9] T. Daengsi, P. Pornpongtechavanich, and P. Wuttidittachotti, "Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks," *Education and Information Technologies*, vol. 27, no. 6, pp. 7975–7995 (2022).

[10] M. T. Whitty, N. Moustafa, and M. Grobler, "Cybersecurity when working from home during COVID-19: considering the human factors," *Journal of Cybersecurity*, vol. 10, no. 1, Article ID tyae001 (2024).

[11] N. Beu, A. Jayatilaka, M. Zahedi, M. A. Babar, L. Hartley, W. Lewinsmith, and I. Baetu, "Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a natu-

ralistic phishing simulation," *Computers & Security*, vol. 131, Article ID 103313 (2023).

[12] M. Waqas, A. Hania, F. Yahya, and I. Malik, "Enhancing Cybersecurity: The Crucial Role of Self-Regulation, Information Processing, and Financial Knowledge in Combating Phishing Attacks," SAGE Open, vol. 13, no. 4, Article ID 21582440231217720 (2023).

[13] C. Gerdenitsch, D. Wurhofer, and M. Tscheligi, "Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 17, no. 4 (2023).

[14] E. Tariq, I. Akour, N. Al-Shanableh, E. Alquqa, N. Alzboun, S. Al-Hawary, and M. Alshurideh, "How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks," *International Journal of Data and Network Science*, vol. 8, no. 1, pp. 69–76 (2024).

[15] D. Baltuttis and T. Teubner, "Effects of Visual Risk Indicators on Phishing Detection Behavior: An Eye-Tracking Experiment," *Computers & Security*, Article ID 103940 (2024).

[16] A. Sumner, X. Yuan, M. Anwar, and M. McBride, "Examining factors impacting the effectiveness of anti-phishing trainings," *Journal of Computer Information Systems*, vol. 62, no. 5, pp. 975–997 (2022).

[17] M. Canham, C. Posey, D. Strickland, and M. Constantino, "Phishing for long tails: Examining organizational repeat clickers and protective stewards," *SAGE Open*, vol. 11, no. 1, Article ID 2158244021990656 (2021).

[18] D. Buil-Gil and E. Barrett, "The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention," in The New Technology of Financial Crime, Abingdon, UK: Routledge, pp. 5–34 (2022).

[19] A. S. Williams, M. S. Maharaj, and A. I. Ojo, "Employee behavioural factors and information security standard compliance in Nigeria

banks," *International Journal of Computing and Digital Systems*, vol. 8, no. 4, pp. 387–396 (2019).

[20] E. C. Donald, M. A. Bumpus, and X. Zhang, "A case study in selection and deployment of a multi-factor authentication solution," *Issues in Information Systems*, vol. 22, no. 3 (2021).

[21] D. Heering, "Ensuring cybersecurity in shipping: Reference to Estonian shipowners," *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 14, no. 2 (2020).

[22] H. Park, Y. Yoo, and H. Lee, "7s Model for technology protection of organizations," *Sustainability,* vol. 13, no. 13, p. 7020 (2021).

[23] M. Canham, C. Posey, and M. Constantino, "Phish derby: Shoring the human shield through gamified phishing attacks," in *Frontiers in Education*, vol. 6, p. 807277, Frontiers Media SA (Jan. 2022).

[24] A. Leering, L. van de Wijngaert, and S. Nikou, "More honour'd in the breach: predicting non-compliant behaviour through individual, situational and habitual factors," *Behaviour & Information Technology*, vol. 41, no. 3, pp. 519–534 (2022).

[25] A. Mihailović, J. Cerović Smolović, I. Radević, N. Rašović, and N. Martinović, "COVID-19 and beyond: employee perceptions of the efficiency of teleworking and its cybersecurity implications," *Sustainability,* vol. 13, no. 12, p. 6750 (2021).