ISSN 2409-2665
Journal of Logistics, Informatics and Service Science
Vol. 13 (2026) No. 11, pp.132-156
DOI:10.33168/JLISS.2026.1106

Privacy Concern, Cognitive Trust and Employee Well-Being in Digital Workplace Information Systems

Vy Phan Khanh Tran, Quynh Phuong Pham, Tham Thi Hong Trinh*, Thuy Thanh Thi Le, Huyen Thu Le Nguyen

School of Advanced Study, Ho Chi Minh City Open University, Ho Chi Minh City, Viet Nam
2354010396tham@ou.edu.vn (Corresponding author)

Abstract. In the context of rapid digital transformation, the application of technology in management and internal communication has led to the increasing popularity of corporate social networks and online work platforms. Besides the benefits of connectivity, this also poses significant risks regarding privacy and impacts employee morale. This study analyzes the extent to which privacy concern affects employee psychological well-being and identifies the moderating role of cognitive trust. Data collected from 339 employees at various organizations were analyzed using structural equation modeling (PLS-SEM) and ANN methods to determine the relationship between research variables and predictive ability, thereby enhancing the theoretical validity, reliability, and applicability of the study. The results show that privacy concern significantly influences risk perception and self-disclosure behavior, thereby indirectly impacting psychological well-being. Furthermore, cognitive trust plays a moderating role, helping to mitigate the negative impact of privacy concern. Based on these findings, the study proposes governance implications and practical solutions to enhance trust, protect personal data, and improve mental health for workers in the digital workplace.

Keywords: Psychological well-being, perceived risk, cognitive trust, privacy concern, self-disclosure.

1. Introduction

Information and information management are among the top strategies for sustainable and stable organizational operation. When evaluating modern digital workplace systems, the reality shows that the digital internal service channels and feedback systems that businesses currently deploy are often ineffective, thereby reducing the effectiveness of information management and organizational operational control (Chen et al., 2026). In essence, these digital internal reporting systems function as employee-centric service systems designed to streamline bottom-up information flow management (Dalati, 2025). However, the technical and administrative architecture of these systems directly triggers critical privacy concerns and perceived risks regarding data security. While operational problems often arise at the root level, front-line employees lack the structural power to protect themselves when raising concerns due to the risk of strict scrutiny or even retaliation from affected interest groups. Consequently, these heightened privacy concerns heavily restrain employee self-disclosure. Although organizations want employees to actively share critical internal updates, staff members choose silence over openness due to the clear risk of their mental state becoming unstable and their psychological well-being significantly diminished. According to recent literature on sustainable system designs (Alsaedi, 2022), systemic vulnerability in information sharing channels remains a crucial barrier to organizational transparency. Indeed, the fear that provided information may be stored and weaponized as a tool for evaluation or judgment rather than triggering constructive organizational responsiveness directly causes employees to protect themselves through silence (Glavin et al., 2024). When privacy concerns are not secured through a robust management system, employee psychological well-being is threatened, transforming the digital workspace into an environment rife with apprehension. Hence, when an organization seeks to balance top-down information extraction with positive psychological well-being, understanding privacy concerns, associated risks, and their final impact on well-being becomes a critical necessity, pointing directly toward unresolved research gaps.

Studies in the context of organizational management and human resources have extensively evaluated the relationship between privacy concern and well-being, as well as self-disclosure and well-being (Kundi et al., 2021; Wuersch et al., 2024), and simultaneously yielded many noteworthy results. However, studies such as those by Chan (2021) aim to examine the interaction between these concepts within the context of social media (Hossain et al., 2023), when employees' emotions are assessed from the perspective of sharing those emotions on a third-party platform. On the other hand, organizational digital systems, such as social media monitoring and mental health programs, may offer limited support because organizations often lack the resources and capacity to continuously monitor employees' interactions on external platforms. Meanwhile, the reflections by internal digital communication system self-disclosure are actually a valuable source of information for providing the most accurate, and even up-to-date, reflection on issues at the bottom-up viewpoint (Wuersch et al., 2024). Unlike public voices, which reflect reality, the true problems of an organization often involve vested interests and a range of internal relationship issues (Soerjoatmodjo, 2025), these issues are further masked by the collective culture of Asian organizations. Therefore, when self-disclosure in this context requires a very high level of security, the risk of leakage is high (perceived risk) and concerns about the level of security and system administration are reflected (privacy concern), which restrains self-disclosure again and simultaneously reduces well-being. The feeling of knowing a secret but not being able to share it increases anxiety and lowers well-being, and releasing the secret through safely designed channels will keep well-being strong (Bedrov & Gable, 2024). These issues lead us to two precise research gaps regarding theoretical omissions in prior literature. First, existing literature offers a limited understanding of how privacy concerns within organizational digital communication systems structurally damage employee self-disclosure and psychological well-being specifically through the mechanism of perceived risk. This gap leads to the limitations of the theory in assessing whether system prefixes such as information flow management flaws or poor organizational responsiveness will hinder or promote well-being as information becomes increasingly valuable in organizational management, yet sharing

encounters too many barriers and diminishes employee morale. The second research gap focuses on the specific theoretical mechanisms linking privacy concern to self-disclosure and privacy concern to perceived risk within this digitally mediated framework, which currently lacks clear empirical evidence. While research on measures to encourage open employee feedback is extensive, explanations for why self-disclosure remains ineffective despite being considered safer, and studies explaining how privacy concern related to system design specifically influences perceived risks, remain unclear. A lack of understanding of this relationship leads managers to overlook the potential harms of privacy concern and technical flaws in technical feedback quality, thereby limiting their responses to improve information quality and feedback based on systems (Frener et al., 2024).

In this context, we apply Privacy Calculus Theory (PCT) to explain information-sharing behavior by considering the potential risks and benefits (Smith et al., 2011). However, PCT is too focused on pure data trading (Cloarec et al., 2024; Meier & Krämer, 2024), particularly in the context of organizational behavior, applying PCT purely in terms of information sharing will inadvertently equate the image of the information sharing system with the organizational culture and even the organization's reputation among employees. Meanwhile, employees themselves possess cognitive trust, which reflects their reasonable expectations of the organization's ability to manage and operate personal information systems safely (Gill et al., 2024), this will govern the extent to which privacy concern influences perceived risk and self-disclosure. While privacy concern stems from employee forecasts regarding system vulnerabilities, cognitive trust itself is formed based on observations and assessments of the clear performance, robust privacy protection, and transparent governance of the system. Therefore, when cognitive trust is high, privacy concern are less stressful and psychological well-being is protected in a context of uncertain data; conversely, when cognitive trust is low, privacy concern are more stressful and risk sensitivity increases because the technical capabilities of information flow management and feedback quality are deemed unreliable. Based on the above arguments, we identify cognitive trust as a potential moderating variable for the relationship between privacy concern, self-disclosure, and perceived risk in the context of employee well-being research. This is a novel approach, as previous studies have often viewed cognitive trust as a variable that directly or indirectly influences data-sharing behavior, rarely considering its moderating role (Chua & Banerjee, 2017; Masood et al., 2023). This research gap needs to be addressed to shed light on how employees overcome psychological fears and how organizations indirectly build a positive internal image through their digital infrastructure. By shifting the focus from behavior to mental health within the framework of informatics, cognitive trust becomes a clear regulatory mechanism, separating those who maintain psychological stability from those who are vulnerable, thereby highlighting its crucial role in explaining the impact of privacy concern on sharing behavior and ultimately promoting well-being.

With the research gaps already identified, this study aims to examine the influence of privacy concern, self-disclosure, and perceived risk on psychological well-being under the moderating lens of cognitive trust. By conceptualizing self-disclosure not merely as a rational data exchange but as a voluntary psychological process of emotional release mediated by digital service channels, the study hopes to shed light on the mechanisms protecting employees' mental health in a digital environment (Chu et al., 2023). Simultaneously, applying PCT within the context of digital workplace information systems and extending the discussion of employee well-being within digitally mediated organizational communication will provide a comprehensive theoretical framework to explain how organizations can indirectly influence risk perception through concrete service system elements such as privacy protection mechanisms, high feedback quality, and swift organizational responsiveness. Thus, the research not only contributes to the academic body on PCT but also offers practical solutions for the IT and service science industries to create a psychologically safe environment where system design and transparency become a shield protecting the psychological well-being of employees (Chu et al., 2023).

2. Literature Review

2.1. Psychological well-being

Psychological well-being is a state that reflects an individual's level of positive thinking and feeling, including subjective factors (Groenestein et al., 2024) and the ability to maintain inner balance in the face of environmental influences (Chu et al., 2023). According to Alsaedi et al. (2022), psychological well-being is formed from independence, strong relationships, and self-acceptance, all of which contribute to the successful development of each individual. In the context of HRM and the era of rapid digital transformation, personal well-being has become a key factor in helping employees maintain performance, adaptability, and psychological stability. Within organizational digital communication systems, psychological well-being also reflects employees' perceptions of psychological safety and emotional stability when interacting with internal information-sharing platforms. Furthermore, psychological well-being helps employees reinforce their sense of work meaning, enhance self-control, and thus foster long-term commitment to the organization. In this study, psychological well-being reflects the level of happiness and psychological adaptability of employees in the workplace.

2.2. Privacy calculus theory (PCT)

Smith et al. (2011) explain Privacy Calculus Theory as a classic framework for explaining the mechanisms of individual information disclosure. According to PCT, the voluntary disclosure of workplace issues is seen as the result of a psychological calculation, where employees weigh the benefits of transparency against potential risks such as retaliation or identity exposure (Chatterjee et al., 2022). In this study, self-disclosure is understood as the proactive act of disclosing problems arising in the workplace; meanwhile, perceived risk and privacy concern act as psychological barriers that determine employees' openness to wrongdoing or negativity in the workplace. Therefore, sharing behavior is no longer simply a matter of assessing gains and losses, but is also strongly influenced by power and organizational culture (Gal et al., 2020). Simultaneously, this study expands on PCT by making cognitive trust a driving factor that directly impacts how employees interpret risk. Instead of simply balancing the benefits and drawbacks of disclosure, the organizational context will determine whether employees feel secure enough to voluntarily disclose misconduct and internal conflicts or choose to remain silent to protect themselves.

2.3. Hypothesis development

Self-disclosure is the process by which an individual assesses and decides whether to disclose information they possess (Nabity-Grover et al., 2022). In a business context, self-disclosure is manifested through the disclosure and sharing of personal opinions, perspectives, and information that employees possess in order to reflect organizational issues (Guarin et al., 2025). As organizations increasingly adopt digital HRM and organizational digital communication systems, self-disclosure behavior is also shifting from face-to-face interaction to communication through online business platforms and collaboration tools. With a digital environment for HRM, employees can share feedback, concerns, or sensitive work-related experiences to support organizational improvement and address internal issues (Wuersch et al., 2024). Based on PCT, employees typically weigh the potential risks against the benefits of providing information to the organization before deciding to disclose it (McIlwraith, 2021; Solove, 2022).

In a business environment, the more appropriate the level of self-disclosure, the less risk anxiety and psychological stress will be experienced (Ostendorf et al., 2022). Wuersch et al. (2024) have shown that when employees have good control over the sensitive information they disclose, they feel more confident in internal communication and maintain their motivation. Agreeing with this view, Chu et al. (2023) also argued that self-disclosure can promote psychological well-being through a sense of security and emotional release when employees are allowed to voluntarily share sensitive aspects of their work under strict control of personal information.

H1: Self-disclosure has positive impacts on psychological well-being

Perceived risk (PR) is the degree of uncertainty an individual feels when engaging in a behavior, encompassing both cognitive and emotional factors (Yadav et al., 2024). The study by Xu et al. (2011) suggests that perceived risk is formed from an assessment of the likelihood and severity of adverse consequences. Studies show that perceived risk is often associated with data leaks, privacy breaches, and security attacks (Garas, 2024). In an organization's digital communication environment, perceived risk reflects employees' awareness of the potential negative consequences associated with using internal information-sharing systems, including concerns about traceability, unauthorized access, or misuse of disclosed content.

Previous research has indicated that when employees engage in information-disclosing behaviors in the workplace, they tend to be more sensitive to privacy risks (Tolsdorf et al., 2022; Ostendorf et al., 2022). This becomes apparent when employees proactively disclose sensitive issues to relieve emotional stress but do not fully trust the system's security capabilities. As risk perception increases, employees are more likely to develop anxiety and lose control over the sensitive information they have shared through organizational information systems (Reeves et al., 2020). In the context of organizations operating multiple digital internal information channels, any indication of a lack of transparency in data management can increase employee risk perceptions (Kröger et al., 2021). When perceived risk reaches a high level, it generates negative emotional responses such as anxiety, stress, or fear of retaliation, thereby undermining employees' psychological well-being instead of providing them with the expected psychological relief (Srivastava & Dhir, 2024).

H2: Perceived risk has negative impacts on psychological well-being

Privacy concern is defined as "*a user's anxiety about the risk of losing privacy due to the disclosure of personal information to a specific third party.*" (Xu et al., 2011). As organizations increasingly utilize digital communication systems to support information sharing and interaction among employees, privacy concerns also become more apparent (Bhave et al., 2020). In management, disclosing sensitive issues through internal platforms causes employee anxiety due to the risk of unintended information leaks, leading to tighter control over privacy (Tirtayani et al., 2023). With the increasing need to share information to relieve stress in the workplace, employees have growing concerns about privacy if these information sharing systems are not operated transparently and effectively to build trust in the system from their perspective.

As privacy concern in the workplace increases, employees tend to reduce the freqency of self-disclosure (Rodríguez-Priego et al., 2023). Specifically, employees who are highly concerned about the security of their sensitive information tend to share little or no information about the hidden aspects of their work (Tolsdorf et al., 2022). Furthermore, Saffarizadeh et al. (2017) and Koohang et al. (2018) argue that security concerns lead users to tightly control the content they disclose or even provide information that does not accurately reflect reality for fear of retaliation.

H3: Privacy concern has negative impacts on self-disclosure.

Furthermore, privacy concern in the modern workplace directly impacts employees' perceived risk (Cheng et al., 2022). The greater the privacy concern, the more strongly these risks are perceived by employees, and the higher the risk they assess (Xueyun et al., 2023). From the fear of a lack of control over sensitive information that has been voluntarily disclosed (Koohang et al., 2021), the process of perceived risk formation is strongly driven by employees' assessment and response to factors that raise concerns about system security (Li, 2025). Van Ooijen et al. (2024) also pointed out that privacy concern increases perceived risk, thereby influencing employees' decisions to share information through internal digital communication channels to alleviate their emotions.

H4: Privacy concern has positive impacts on perceived risk.

Although some argue that privacy concern can drive protective strategies, this study highlights the negative consequences of privacy concern on mental health (Frener et al., 2024; Tirtayani et al., 2023). Within the framework of psychological well-being, the constant need to maintain strict personal

boundaries and suppress the need to express sensitive issues through digital workplace systems creates a significant psychological burden, undermining inner balance (Chu et al., 2023). When employees experience high levels of concern, they often fall into a state of anxiety and resort to complex coping strategies such as selective self-disclosure or silence in the face of injustice to protect themselves (Soerjoatmodjo, 2025). Constantly being on alert to control the flow of information and striving to mitigate risks when the system lacks the necessary security causes fatigue and a loss of natural control (Tolsdorf et al., 2022). The constant pressure to manage risk and establish overly rigid boundaries, instead of being able to express and relieve stress, disrupts the psychological environment of safety, thereby negatively impacting the psychological well-being of employees in the context of digital transformation.

H5: Privacy concern has negative impacts on psychological well-being.

Cognitive trust (CT) is a form of belief formed based on a rational, logical, and well-founded assessment of an organization's competence, professionalism, and reliability in operating systems (Ozturk et al., 2014). This concept is expressed through the degree to which employees believe the organization has sufficient capacity to secure data, operate systems transparently, control access to information effectively, and use information appropriately (Saffarizadeh et al., 2017). Cognitive trust is developed based on employees' rational evaluations of past performance, professional competence, and the reliable signals the organization demonstrates (Su & Mattila, 2020). In organizational information systems and digital internal service channels, cognitive trust is demonstrated through employees' perceptions of professional system management and administration, as well as secure and reliable information protection.

Numerous studies indicate that cognitive trust strongly influences individuals' self-disclosure behavior in the digital environment (Chen et al., 2021), while privacy concern tends to undermine trust and reduce willingness to disclose sensitive issues (Saffarizadeh et al., 2017; Kose, 2019). From the perspective of PCT, the decision to share information reflects a balance between the benefits of psychological relief and the potential risks. In an organizational environment, self-disclosure depends on belief in the transparency, security, and operational capabilities of the organization's information systems (Mutimukwe et al., 2020). Employees often worry that sensitive information, when disclosed, may be misused or lead to retaliation if the system is not sufficiently secure (Ramasundaram et al., 2024). These concerns increase privacy concern, causing employees to limit sharing to avoid risks and to assess the risks to their occupational health more highly (Atalay & Yücel, 2024). Conversely, confidence in the competence, transparency, and fairness of the organization's governance system helps to mitigate these concerns: when security procedures and whistleblower protection mechanisms are clear, employees have a rational basis to believe that the organization will act appropriately and protect their interests (Ebert et al., 2021; Klimchak et al., 2020). These signals help them feel that the risks mentioned above are lower, leading to the following hypotheses:

H6: As a moderator, cognitive trust weakens the negative impact of privacy concern on individual self-disclosure.

H7: As a moderator, cognitive trust weakens the positive relationship between privacy concern and perceived risk.

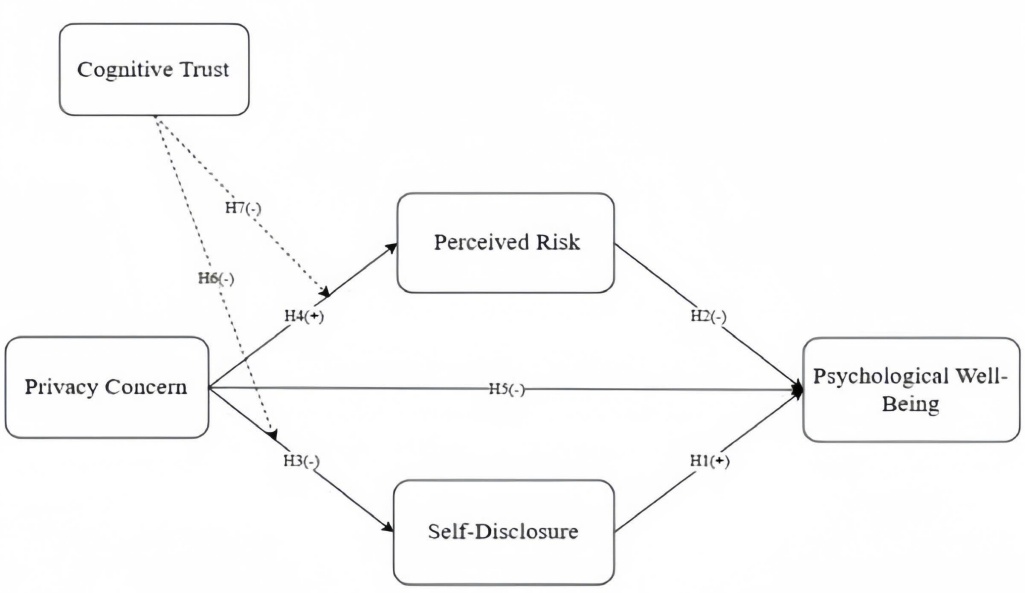


Fig. 1: Proposed Research Model

3. Methodology

3.1. Scale

This study focuses on internal information systems that manage and process data in the form of anonymous reporting, which allows employees to self-disclosure workplace issues, unethical behavior, or policy violations without revealing their identity. Therefore, after conducting a literature review, this study selected and constructed appropriate scales for each concept in the model (See Appendix). Specifically, the psychological well-being scale includes 8 items developed by Diener et al. (2009) to assess the mental health of employees. To capture individuals' concerns about controlling information disclosed in workplace communication, the privacy concern scale was inherited and modified from Snyder (2010) with 5 items. Next, the perceived risk scale was modified from Xu et al. (2011) with 4 items to measure perceived risk associated with sharing personal or sensitive information.

Furthermore, the self-disclosure scale with 7 items is inherited and developed from the research of Guarin et al. (2025). This scale captures an individual's willingness to voluntarily share opinions, concerns, and personal experiences through various voice mechanisms. This concept is suitable for anonymous reporting formats, where employees voluntarily disclose workplace-related concerns and sensitive information. Finally, the cognitive trust scale developed by Ozturk et al. (2014) was used to capture employees' trust in those responsible for handling the disclosed information. At the same time, to ensure accurate measurement and reflect the respondents' level of perception, the study used a 7-point Likert scale, ranging from level 1 ("Strongly disagree") to level 7 ("Strongly agree").

The model was tested using PLS-SEM and an artificial neural network (ANN) to improve the accuracy of estimates and the robustness of the analysis. This integrated approach is particularly suitable in the context of online work platforms, where employee responses do not follow a purely linear relationship. First, the measurement model was evaluated through outer loadings (λ), Cronbach's alpha (α), composite reliability (CR), the average variance extracted (AVE), and the heterotrait-monotrait ratio (HTMT) to ensure the reliability and validity of the scales.

Table 1. Bootstrapping execution settings.

Parameter	Setting
Complexity	Most important (faster)
Confidence interval method	Percentile bootstrap
Parallel processing	Yes
Samples	5000
Save results per sample	No
Seed	Fixed seed
Significance level	0.05

Next, the structural model was tested using bootstrapping to estimate path coefficients, while considering multicollinearity (VIF) and predictability (Q^2) to ensure the stability and fit of the model (Hair et al., 2019). The Bootstrapping process was performed using SmartPLS software with 5,000 replicate samples, the Percentile Bootstrap confidence interval method, and a significance level of 0.05. The detailed settings of the Bootstrapping process are presented in Table 1.

In contrast, because PLS-SEM is primarily based on the assumption of linearity (Haji-Othman et al., 2024; Subhaktiyasa, 2024), this method may not fully reflect the complex interactions in human behavior. Therefore, ANNs are deployed as an additional analytical step to capture non-linear relationships. The significant constructs identified through PLS-SEM, including privacy concern, perceived risk, and self-disclosure, were subsequently incorporated as input variables in the ANN analysis to ensure that the machine learning process remained theoretically grounded (Wu & Feng, 2018). Data are split into training and testing sets to evaluate out-of-sample predictions through RMSE, combined with sensitivity analysis to determine the importance of predictive variables (Albahri et al., 2022). Finally, by comparing the PLS-SEM path coefficients with the normalized relative importance (NRI) in the ANN, the variables were ranked based on their influence on the outcome variable (Albahri et al., 2022). This approach allows for the combination of the explanatory power of PLS-SEM and the predictive power of ANN, thereby enhancing both the theoretical validity, reliability, and applicability of the study.

3.2. Data Collection and Descriptive Statistics

Data were collected from October to December 2024 using a non-probability-based convenience sampling method. An online survey was used due to the difficulty in reaching employees across multiple organizations. The survey was distributed through professional networks, social media platforms, and online communities targeting employees working in diverse professions. Before proceeding to the questionnaire round, respondents were informed of the study's purpose and asked to confirm whether they had experience with, awareness of, or exposure to anonymous reporting systems within their organizational environment. The data were then screened to remove incomplete responses, ultimately resulting in 339 valid samples retained for further analysis.

In terms of gender, women accounted for a higher proportion at 53.6%, while men accounted for 46.4%. The survey sample focused on early and mid-career stages, with the highest percentage of participants belonging to the Employee group (45.6%). Regarding industry, the majority of participants came from the economics sector (47.6%), followed by social sciences (23.7%), science (20.1%), and healthcare (8.6%), ensuring the diversity of the research sample and the ability to cover many different occupational groups (see Table 2).

Table 2. Descriptive Statistics (N=339)

Sample size N=339		Frequency	Percentage %
Gender	Male	157	46.4
	Female	181	53.6
Working experience	Employee	154	45.6
	Junior	98	29.0
	Senior	86	25.4
Industry	Economics and Management	161	47.6
	Social Sciences and Humanities	80	23.7
	Natural Sciences and Engineering	68	20.1
	Health and Medical Sciences	29	8.6

4. Results

4.1. Measurement Model Evaluation

Reliability is determined via Cronbach's alpha and composite reliability. These values must exceed the threshold of 0.7. According to Hair et al. (2019), this value shows high stability and consistency between the observed variables in each scale. Additionally, AVE helps assess the extent to which each observed variable accounts for the latent construct, and this value must be greater than 0.5. Table 3 shows that all values are above the cut-offs, indicating that the convergent validity is satisfied.

At the same time, the outer loadings are all in the range of 0.727 to 0.890, indicating a strong and clear association between the observed variables and the corresponding concepts (Hair et al., 2017). Overall, these results demonstrate that the constructed scale has high reliability and effectively measures the research concepts, creating a strong premise for assessing discriminant validity in the next step through HTMT.

Table 3. Results of Reliability and Convergent Validity Assessment

Constructs	Items	λ	α	CR	AVE
Cognitive trust	CT1	0.863	0.889	0.919	0.694
	CT2	0.858			
	CT3	0.838			
	CT4	0.757			
	CT5	0.846			
Privacy concern	PC1	0.813	0.893	0.921	0.701
	PC2	0.870			

	PC3	0.867			
	PC4	0.876			
	PC5	0.754			
Perceived risk	PR1	0.825	0.882	0.918	0.738
	PR2	0.880			
	PR3	0.890			
	PR4	0.839			
Self-disclosure	SD1	0.818	0.916	0.933	0.665
	SD2	0.843			
	SD3	0.829			
	SD4	0.834			
	SD5	0.812			
	SD6	0.841			
	SD7	0.727			
Psychological well-being	PWB1	0.775	0.917	0.932	0.632
	PWB2	0.804			
	PWB3	0.817			
	PWB4	0.767			
	PWB5	0.825			
	PWB6	0.822			
	PWB7	0.749			
	PWB8	0.797			

Discriminant validity is estimated using HTMT. Among discriminant evaluation methods, HTMT is recommended due to its more efficient assessment ability (Henseler et al., 2015). HTMT identifies that scales are measuring distinct, non-overlapping concepts, thereby improving the reliability and validity of the scale. In contrast, other indices, such as the Fornell & Larcker criteria, are considered less accurate, possibly missing cases of lack of discrimination. The above HTMT values are all below the threshold of 0.85, indicating that strict discrimination is ensured (see Table 4).

Table 4. Discriminant Validity Results

	CT	PC	PR	PWB	SD
CT	-				

PC	0.158	-			
PR	0.066	0.407	-		
PWB	0.297	0.346	0.566	-	
SD	0.548	0.107	0.245	0.339	-

Note: CT = Cognitive trust, PC = Privacy concern, PR = Perceived risk, SD = Self-disclosure, PWB = Psychological well-being

4.2. Structural Model Evaluation

According to Table 5, the data do not exhibit major problems with multicollinearity when the variance inflation factors (VIFs) are lower than the warning level of 3 (Hair et al., 2019). The variables in the model can be effectively used in the analysis process, providing reliable and accurate results.

On the other hand, the model provided the best explanation for psychological well-being, with 34.8% of the main factors related to psychological well-being identified (see Table 5). For self-disclosure behavior, this concept explained 27.1% of its variation through independent concepts, reflecting a relatively high level of explanation. In contrast, perceived risk explained only 17.8%, suggesting that there are many factors outside the model that influence this variable (Henseler & Sarstedt, 2013).

According to Sarstedt et al. (2021), the Q^2 Predict indices are positive, indicating that the model predicts and explains all three factors of psychological well-being, perceived risk, and self-disclosure. Among them, self-disclosure stands out with the highest predictive ability, demonstrating the model's superior performance in capturing factors related to this behavior.

Table 5. Structural Model Evaluation Results

	VIF	R^2	Adjusted R^2	Q^2
CT	1.823 - 2.673	-	-	-
PC	1.755 - 2.903	-	-	-
PR	2.125 - 2.610	0.186	0.178	0.053
SD	1.733 - 2.830	0.277	0.271	0.305
PWB	2.023 - 2.559	0.354	0.348	0.076

To evaluate the overall fit of the structural model with the empirical data, two standard indicators, SRMR and NFI, are analyzed in Table 6. According to statistical criteria, a model demonstrates a good fit when the SRMR value is below 0.08 (Hu & Bentler, 1999). In terms of the Normed Fit Index (NFI), while a value closer to 1 is traditionally preferred (Bentler & Bonett, 1980), foundational methodological literature indicates that NFI is highly sensitive to model parameters. Specifically, as demonstrated by Bentler (1990), NFI has a well-documented downward bias and tends to underestimate the true model fit in complex structural models or under specific sample constraints.

The empirical results show that the SRMR value of 0.069 meets the recommended threshold of 0.08, indicating a good model fit. Although the NFI value of 0.848 falls below the conventional cutoff, it remains acceptable for exploratory and complex models due to the index's conservative nature (Bentler, 1990). Overall, the model demonstrates an acceptable fit with the empirical data, supporting subsequent hypothesis testing.

Table 6. Structural Model Fit Assessment Indicators

Conformity Assessment Index	Estimated model
SRMR	0.069
NFI	0.848

The study conducted bootstrapping (N = 5000) and found that all hypotheses were statistically significant at a 95% confidence level ($P < 0.05$), except for H6 which was rejected. The results showed that perceived risk had a negative impact on psychological well-being ($\beta = -0.460$; $p = 0.000$). Privacy concern increased perceived risk ($\beta = 0.434$; $p = 0.000$) and decreased self-disclosure ($\beta = -0.137$; $p = 0.025$), causing privacy concern to tend to inhibit information sharing, thereby suppressing pressure, anxiety, and insecurity, leading to a decline in mental state ($\beta = -0.144$; $p = 0.031$). Furthermore, self-disclosure is considered a positive indicator of psychological well-being ($\beta = 0.268$; $p = 0.000$), providing timely feedback on the work environment helps employees feel understood, thereby promoting their psychological well-being. In addition, cognitive trust has a significant moderating effect on the relationship between privacy concern and perceived risk ($\beta = -0.143$; $p = 0.015$). This implies that organizational transparency and trust in data management can help weaken employees' perceived risk, even if they still have privacy concern (see table 7).

Table 7. Hypothesis Testing Results

Hypothesis	β	T-value	P-value	f^2	2.5%	97.5%	Result
H1: SD → PWB	0.268	5.657	0.000	0.106	0.173	0.357	Accepted
H2: PR → PWB	-0.460	5.658	0.000	0.211	-0.533	-0.250	Accepted
H3: PC → SD	-0.137	2.240	0.025	0.024	-0.263	-0.022	Accepted
H4: PC → PR	0.434	6.672	0.000	0.214	0.297	0.551	Accepted
H5: PC → PWB	-0.144	2.164	0.031	0.028	-0.284	-0.021	Accepted
H6: CT * PC → SD	-0.060	1.188	0.235	0.010	-0.159	0.041	Rejected
H7: CT * PC → PR	-0.143	2.444	0.015	0.049	-0.248	-0.020	Accepted

Based on the Full Collinearity Assessment by Kock (2015), Common Method Bias (CMB) is controlled if all Inner VIF values are less than or equal to 3.3. The results in Table 8 show that the Inner VIF values for all paths are very low, ranging from 1.049 to 1.210, which are well below the 3.3 threshold. Therefore, the model fully meets the statistical criteria, confirming that the collected data is free from Common Method Bias (CMB) and serious multicollinearity issues.

Table 8. Inner VIF Results for Common Method Bias Assessment

Path	Inner VIF
SD → PWB	1.049
PR → PWB	1.210
PC → SD	1.081

PC → PR	1.081
PC → PWB	1.161
CT * PC → SD	1.061
CT * PC → PR	1.061

4.3. Artificial Neural Network (ANN)

In this study, an ANN model was implemented using SPSS to enhance the ability to predict nonlinear relationships between variables (Soomro et al., 2025), thereby serving as an effective complement to the PLS-SEM method (Haji-Othman et al., 2024).

To predict the value of the dependent variable (psychological well-being) based on the independent variables (privacy concern, perceived risk and self-disclosure), this study deploys a multilayer perceptron (MLP) neural network. The dataset is randomly partitioned into two independent sets: the training set accounts for 90% of the total samples to optimize the weights, while the remaining 10% is allocated to the test set to objectively evaluate forecasting performance and prevent overfitting (Soomro et al., 2025).

The network architecture (illustrated in Fig. 2) consists of three interconnected layers: the input layer containing 3 standardized covariates (privacy concern, perceived risk, self-disclosure); the output layer containing the target variable (psychological well-being); and one hidden layer in between, with the number of hidden units automatically computed by the software. Regarding the activation mechanism, the model applies the Sigmoid function at the hidden layer to capture non-linear relationships, combined with the Identity function at the output layer to optimize the regression for continuous value prediction (Zhang & Qi, 2022). The network undergoes batch training utilizing the Scaled conjugate gradient algorithm to accelerate convergence. The entire process is executed with parallel processing on IBM SPSS Statistics and automatically terminates via early stopping when the test error reaches its minimum threshold.

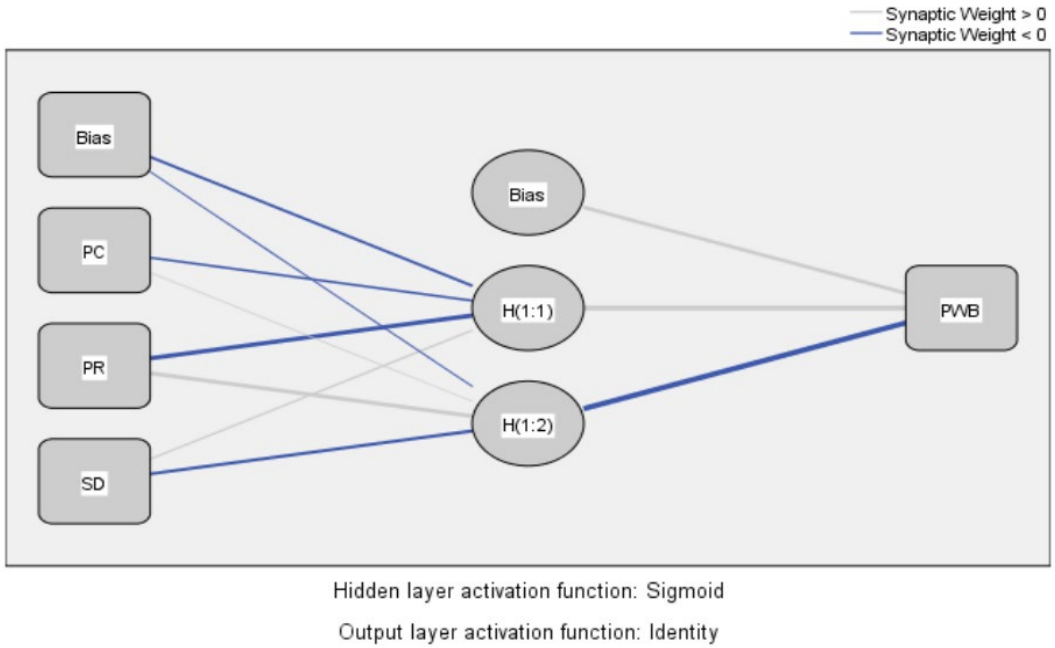


Fig. 2: Artificial Neural Network Diagram

The results in Table 9 show that the average RMSE of the training set is 0.421 (SD = 0.020), while that of the testing set is 0.410 (SD = 0.072). The model shows no signs of overfitting and has good

generalizability. Simultaneously, sensitivity analysis showed that the perceived risk variable had the greatest influence with a normalized importance of 98.0%, followed by self-disclosure (75.1%) and privacy concern (55.3%) (Table 10). The clear difference in importance levels between the variables indicates that the ANN model is capable of differentiating the role of each factor in predicting the outcome (Albahri et al., 2022).

Table 9. RMSE Values

Training			Testing			Total samples
N	SSE	RMSE	N	SSE	RMSE	
301	102.462	0.428	38	14.334	0.473	339
308	103.847	0.433	31	4.149	0.245	339
307	111.768	0.450	32	17.977	0.503	339
301	93.888	0.411	38	8.972	0.361	339
296	88.412	0.397	43	14.416	0.478	339
308	91.341	0.403	31	9.229	0.386	339
299	87.155	0.394	40	10.179	0.405	339
306	112.158	0.448	33	11.065	0.413	339
299	107.377	0.439	40	14.706	0.465	339
303	92.812	0.407	36	8.697	0.372	339
Mean	99.122	0.421	Mean	11.373	0.410	
Standard deviation	9.040	0.020	SD	3.795	0.072	

Table 10. Sensitivity Analysis

Neural network (NN)	PC	PR	SD
ANN (1)	0.492	1.000	0.710
ANN (2)	0.132	1.000	0.397
ANN (3)	0.822	0.971	1.000
ANN (4)	0.392	1.000	0.698
ANN (5)	0.614	1.000	0.987
ANN (6)	0.541	1.000	0.707

ANN (7)	0.753	1.000	0.779
ANN (8)	0.415	1.000	0.538
ANN (9)	0.882	0.833	1.000
ANN (10)	0.483	1.000	0.698
Average importance	0.553	0.980	0.751
Normalized importance (%)	55.3%	98.0%	75.1%

5. Discussion

Within an organization, privacy concern becomes particularly vulnerable within digital internal service channels and organizational information systems, especially when employees are not fully familiar with data governance mechanisms, information processing procedures, or internal security protocols. Consequently, in hypothetical scenarios involving workplace misconduct or negative issues, employees might choose to passively comply by remaining silent or providing superficial reports rather than voluntarily exposing the problems. This stems from the fear that their identity is not protected, leading to a defensive mindset due to concerns about retaliation or negatively impacting their personal standing in the group environment. They are prone to stress and a decline in psychological well-being (β = -0.460), which in turn reduces performance and engagement levels (Glavin et al., 2024). Personal information not only increases perceived risk (β = 0.434) but also makes employees more cautious about sharing information or emotions, especially when organizational systems lack transparency about how personal information is handled and protected. Therefore, privacy concern is not only linked to personal risks but also reflects the level of employee trust in the information systems and information management practices within the organization.

According to Luo and Hancock (2020), self-disclosure is often seen as an expression of openness and positive communication. When considering complex workplace environments, a system's capability to protect individuals from sensitive issues (such as potential workplace bullying or misconduct) can serve as a conceptual safety net to alleviate personal frustration (Glavin et al., 2024). Interacting with a reputable and professional system helps employees avoid bearing work pressures or feelings of isolation on their own. Thus, instead of repression, implementing self-disclosure through a secure system that respects individual voices helps employees effectively relieve stress (Srivastava & Dhir, 2024), thereby promoting psychological well-being (β = 0.268).

Contrary to initial expectations, cognitive trust did not moderate in the relationship between privacy concern and self-disclosure (β = -0.060; p = 0.235), but significantly moderated the relationship between privacy concern and perceived risk (β = -0.143), reflecting two different levels of impact. At the cognitive level, cognitive trust acts as a risk reinterpretation mechanism (Xia et al., 2023), significantly weakening the impact of privacy concern on perceived risk. With high cognitive trust, individuals reduce uncertainty because they have sufficient rational information about how the organizational system collects, uses, and protects data; the less they guess, the less they exaggerate risks (Saveljeva, 2025). Signals of organizational competence and transparency, such as security certifications, access control mechanisms, or public reporting practices, reinforce the belief that information is managed securely (Haider, 2024), making privacy concern appear more manageable and weakening its relationship with perceived risk (Atalay & Yücel, 2024).

However, at the behavioral level, the statistical rejection of H6 (β = -0.060; p = 0.235) indicates that this rational trust is still not strong enough to motivate employees to proactively speak up through the system when incidents or misconduct occur. Although cognitive trust reinforces the belief that data

is handled professionally (Gill et al., 2024), privacy barriers still prevent them from taking specific actions such as suggesting improvements or reporting sensitive issues through official channels. This dichotomy occurs because a reduction in perceived risk does not automatically equate to a feeling of absolute psychological safety. This suggests that transparency policies alone may not be enough to give employees a stronger sense of anonymity, control, and peace of mind; they still perceive internal reporting systems as fraught with risks. Furthermore, when encountering deep-seated organizational dynamics, cognitive assurances regarding data governance are often overshadowed by non-technical anxieties. Fears of misjudgment, surveillance, or disadvantage in future career opportunities continue to deter them from reporting sensitive issues, even when formal privacy protections are in place (Bhave et al., 2020). Even with transparent organizations, skepticism about the true purpose of monitoring systems persists (Hasan et al., 2021). As a result, despite public policies, feelings of lack of control and psychological insecurity (Russo & Terraneo, 2020), along with factors such as power, performance evaluation, or supervision, remain more prevalent (Ramasundaram et al., 2024). Consequently, while cognitive trust can convince an employee's intellect that the system is secure, it cannot overcome the structural and social vulnerabilities that govern the high-stakes decision to disclose sensitive workplace information.

Table 11. PLS-SEM and ANN Results Comparison

Construct	Coefficient	NRI (%)	Ranking (PLS-SEM)	Ranking (ANN)
PR → PWB	-0.460	98.0	1	1
SD → PWB	0.268	75.1	2	2
PC → PWB	-0.144	55.3	3	3

The results in Table 10 show a high degree of consistency between PLS-SEM and ANN in identifying factors influencing psychological well-being. Serving as a complementary predictive analysis for the direct antecedents of well-being, the ANN model focuses exclusively on predicting psychological well-being using privacy concern, perceived risk, and self-disclosure, without testing the full structural framework or moderating effects. Regarding the mechanism of impact, perceived risk emerged as the strongest predictor of employee psychological state (β = -0.460; NRI = 98.0%). For employees, there is often a fear of privacy risks associated with disclosing sensitive workplace issues (Yadav et al., 2024). The predictive contribution in ANN highlights that as perceived risk increases, the negative impact on psychological well-being becomes overwhelming. From an information systems perspective, weaknesses in governance and identity protection within digital platforms significantly undermine employee well-being. This suggests that addressing specific, contextual fears (such as potential retaliation or identity fears) is crucial, rather than relying on general reassuring messages.

Regarding the role of voluntary self-disclosure, proactive sharing is key to improving psychological well-being (β = 0.268; NRI = 75.1%). When employees openly express their concerns, they feel more connected and understood (Heaphy et al., 2021). On the other hand, within the ANN predictive ranking, the positive impact of self-disclosure on psychological well-being ranks second and may be significantly weakened in contexts characterized by high perceived risk levels. Therefore, encouraging self-disclosure is only effective when risk barriers are appropriately managed (Chu et al., 2023). Meanwhile, although privacy concern has the lowest impact, both PLS-SEM and ANN analysis show that general privacy concerns continue to diminish psychological well-being. While perceived risk is tied to specific risks, privacy concern reflects the foundational level of employee trust in the organization's data security mechanisms, requiring long-term control alongside immediate perceived risk reduction.

6. Conclusion

This study has realized the objectives set out in the introduction by providing deeper insights into the mechanisms of interaction between cognitive trust, privacy concern, perceived risk, and self-disclosure on an employee's psychological well-being, rather than definitively decoding them, given the inherent constraints of the current research design. This study also explains and shapes employee engagement in digital internal reporting systems and its impact on the efficiency of information flow within the organization. Results from PLS-SEM confirm that the relationships are statistically significant, and the moderating role of cognitive trust shows a separation between two levels of impact; at the cognitive level, belief in the fairness and security of the system helps to minimize perceived risk through transparency in operational processes. However, at the behavioral level, this belief is still not strong enough to encourage self-disclosure, which is understood as employees voluntarily disclosing sensitive information to relieve psychological pressure on internal technical reporting systems. This suggests that, aside from factors such as organizational power, transparency, and the perceived quality of information system governance, decisions about sharing confidential information remain strongly influenced. Furthermore, the combination of PLS-SEM and ANN showed that the influence levels of the variables were not only statistically stable but also strengthened in terms of their predictive power, with potential non-linear relationships also reflected and integrated into the results. Therefore, in practice, organizations should prioritize building a safety reporting system and mitigate the risk of retaliation before expecting employees to voluntarily share information to improve participation and mental health in the workplace.

6.1. Theoretical Implications

Theoretically, this research contributes important insights to the body of academic knowledge on human resource management, organizational information systems and organizational psychology in the digital age. First, the research challenges and expands on the traditional assumptions of PCT. The results show that purely rational logic is insufficient to explain the consequences of self-disclosure in highly monitored organizational information environments. Instead of viewing self-disclosure as merely a rational decision based on a risk-benefit analysis (Dinev & Hart, 2006), this study also indicates that sharing sensitive organizational information through digital internal communication channels is influenced by employees' perceptions of system transparency, privacy protection, and organizational governance mechanisms. Research demonstrates that as privacy concern increases, it not only inhibits behavior but also reduces willingness to participate in information-sharing systems and puts direct pressure on psychological well-being, forcing employees to confront the conflict between the need to express themselves and the fear of retaliation and misuse of sensitive information (Anand et al., 2020).

Secondly, research establishes a new role for cognitive trust (Jalees et al., 2023; Qureshi et al., 2024), not as a driver of sharing, but as a mechanism to mitigate perceived risk. By reinterpreting system security signals, cognitive trust helps employees feel more secure when facing privacy concerns. This clarifies the regulatory role of systemic beliefs; it does not eliminate privacy concern but it lessens the weight of perceived risk, creating a more secure informational environment for employees' participation and to move toward self-disclosure. Finally, by demonstrating that privacy concern impacts psychological well-being, the study clarified a novel coping mechanism: when employees face privacy concerns, they not only passively endure but also actively engage in self-disclosure behavior as a way to release emotions through internal systems. The research fills a theoretical gap by asserting that self-disclosure is not the provision of data on demand by the system, but rather a voluntary process of disclosing sensitive information. This is a strategic behavior that allows employees to free themselves from inner anxieties, helping to explain how digital internal reporting systems influence employee behavior, thereby directly strengthening their own mental health in a volatile work environment (Luo & Hancock, 2020; Brinson et al., 2024).

Finally, by combining PLS-SEM and ANN, the study confirms the existence of a dynamic equilibrium mechanism. perceived risk and self-disclosure operate as two opposing yet complementary forces, transmitting directly and reliably, and this balance reflects and explains how privacy concern is transformed and impacts psychological well-being. This combination of methodologies reveals that relationships are not limited to linear interactions but also encompass complex non-linear interactions. Thus, the research contributes to repositioning PCT from a framework for explaining behavior to a mechanism for balancing risk, privacy governance, and information interaction and psychological adaptation in the digital workplace.

6.2. Practical Implications

In practical terms, the research offers important managerial implications for business leaders in balancing data management and employee mental health within digital internal communication systems. Organizations need to recognize that building genuine perceived trust is far more valuable than simply establishing formal security policies. To achieve this, managers should combine information transparency with concrete and verifiable actions, such as conducting periodic security assessments, publicly disclosing the purpose of data use, and adopting international standards like GDPR or ISO/IEC 27001 to strengthen trust (Qusef & Alkilani, 2022). When systems operate transparently, employees will be less hesitant to proactively engage with the organization.

Furthermore, businesses need to create a psychologically safe digital environment where internal reporting channels, from formal (HR platforms, anonymous misconduct reporting systems) to informal (internal communities), operate based on the principles of confidentiality and non-retaliation. Instead of forcing employees to open up through coercive group activities, organizations should focus on designing secure and privacy-preserving communication infrastructures where employees have the right to voluntarily report problems such as procedural violations to relieve frustration without fear of professional consequences. Finally, organizations should promote a data culture where employees are educated about their right to disclose information and their responsibility to protect information. Training programs should not only focus on theoretical knowledge but also provide practical guidance on how internal information systems collect, manage, and secure employee data. When employees understand that they have complete control over the information they share and that disclosure is a right to protect their personal mental health, they will reduce anxiety and insecurity. Such systems not only support employees' psychological well-being but also improve the quality and reliability of information flow within the organization.

7. Limitations and Future Directions

The use of a cross-sectional survey sample does not accurately reflect changes in behavior over time. Subjective factors such as privacy concern may be influenced by immediate emotions and context at the time of the survey, reducing the accuracy of the results. Furthermore, while ANN improved predictive performance, its black-box nature limits the interpretability of the results. Additionally, the initial research design primarily focused on core behavioral variables, leaving the exploration of broader demographic dynamics as an open direction for future exploration. Future studies should employ longitudinal designs, integrate more diversified demographic profiles to expand the analytical scope, validate adapted scales across contexts, and combine ANN with more interpretable analytical approaches.

Acknowledgements

We would like to thank all the participants who voluntarily and anonymously participated in our survey. Their valuable responses provided the essential foundation for the completion of this research.

References

Albahri, A. S. Alnoor, A. Zaidan, A. A. Albahri, O. S. Hameed, H. Zaidan, B. B. Peh, S. S. Zain, A. B. Siraj, S. B. Masnan, A. H. B. & Yass, A. A. (2022). Hybrid artificial neural network and structural equation modelling techniques: a survey. *Complex & Intelligent Systems,* 8, 1781-1801.

Alsaedi, T. Sherief, N. Phalp, K. & Ali, R. (2022). Online social transparency in enterprise information systems: a risk assessment method. *Information Technology and Management*, 23, 95-124.

Anand, A. Centobelli, P. & Cerchione, R. (2020). Why should I share knowledge with others? A review-based framework on events leading to knowledge hiding. *Journal of Organizational Change Management*, 33, 379-399.

Atalay, H. N. & Yücel, Ş. (2024). Decoding privacy concerns: the role of perceived risk and benefits in personal health data disclosure. *Archives of Public Health*, 82, 180.

Bedrov, A. & Gable, S. L. (2024). How much is it weighing on you? Development and validation of the secrecy burden scale. *Personality and Social Psychology Bulletin,* 50, 1332-1347.

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin*, 107, 238.

Bentler, P. M. & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin,* 88, 588–606.

Bhave, D. P. Teo, L. H. & Dalal, R. S. (2020). Privacy at work: A review and a research agenda for a contested terrain. *Journal of Management*, 46, 127-164.

Brinson, N. Amini, B. Lemon, L. & Bawole, C. (2024). Electronic performance monitoring: The role of reactance, trust, and privacy concerns in predicting job satisfaction in the post-pandemic workplace. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 18.

Chan, T. K. (2021). Does self-disclosure on social networking sites enhance well-being? The role of social anxiety, online disinhibition, and psychological stress. In *Information technology in organisations and societies: Multidisciplinary perspectives from AI to technostress* (pp. 175-202). Emerald Publishing Limited.

Chatterjee, S. Chaudhuri, R. Vrontis, D. & Siachou, E. (2022). Examining the dark side of human resource analytics: an empirical investigation using the privacy calculus approach. *International Journal of Manpower*, 43, 52-74.

Chen, D. Ma, Y. Sun, W. & Liu, F. (2026). Network security risk management for artificial intelligence service platforms: An AI-based assessment framework. *Journal of Logistics, Informatics and Service Science,* 13*,* 1-16.

Chen, R. (2013). Living a private life in public social networks: An exploration of member self-disclosure. *Decision Support Systems*, 55, 661-668.

Chen, S. J. Waseem, D. Xia, Z. R. Tran, K. T. Li, Y. & Yao, J. (2021). To disclose or to falsify: The effects of cognitive trust and affective trust on customer cooperation in contact tracing. *International Journal of Hospitality Management*, 94, 102867.

Cheng, H. Ye, Q. & Liang, J. (2022). A review: the safety risk perception of the workplace. *Economics & Management Information*, 1-9.

Chu, T. H. Sun, M. & Crystal Jiang, L. (2023). Self-disclosure in social media and psychological well-being: A meta-analysis. *Journal of Social and Personal Relationships*, 40, 576-599.

Chua, A. Y. & Banerjee, S. (2017). To share or not to share: The role of epistemic belief in online health rumors. *International Journal of Medical Informatics*, 108, 36-41.

Cloarec, J. Meyer-Waarden, L. & Munzel, A. (2024). Transformative privacy calculus: Conceptualizing the personalization-privacy paradox on social media. *Psychology & Marketing*, 41, 1574-1596.

Dalati, S. (2025). Industry 5.0 as a pathway for Syria's economic and social reconstruction: A human-centered conceptual framework for sustainable development. *Journal of Service, Innovation and Sustainable Development*.

Diener, E. Wirtz, D. Biswas-Diener, R. Tov, W. Kim-Prieto, C. Choi, D. W. & Oishi, S. (2009). New measures of well-being. In *Assessing well-being: The collected works of Ed Diener* (pp. 247-266). Dordrecht: Springer Netherlands.

Dinev, T. & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17, 61-80.

Ebert, I. Wildhaber, I. & Adams-Prassl, J. (2021). Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection. *Big Data & Society*, 8, 20539517211013051.

Frener, R. Dombrowski, J. & Trepte, S. (2024). Development and validation of the Need for Privacy Scale (NFP-S). *Communication Methods and Measures*, 18, 48-71.

Gal, U. Jensen, T. B. & Stein, M. K. (2020). Breaking the vicious cycle of algorithmic management: A virtue ethics approach to people analytics. *Information and Organization*, 30, 100301.

Garas, S. R. R. (2025). Susceptibility to social influence the mediating role of perceived risk and attitudes when considering a counterfeit purchase choice. *EuroMed Journal of Business*, 20, 1119-1148.

Gill, H. Vreeker-Williamson, E. Hing, L. S. Cassidy, S. A. & Boies, K. (2024). Effects of cognition-based and affect-based trust attitudes on trust intentions. *Journal of Business and Psychology*, 39, 1355-1374.

Glavin, P. Bierman, A. & Schieman, S. (2024). Private eyes, they see your every move: workplace surveillance and worker well-being. *Social Currents*, 11, 327-345.

Groenestein, E. Willemsen, L. van Koningsbruggen, G. M. Ket, H. & Kerkhof, P. (2024). The relationship between fear of missing out, digital technology use, and psychological well-being: A scoping review of conceptual and empirical issues. *Plos One*, 19, e0308643.

Guarin, A. D. Edwards, M. R. Townsend, K. & Wilkinson, A. (2025). Using a process model to develop and expand employee voice scales. *Human Resource Management Journal,* 35, 783-801.

Haider, H. M. (2024). Analysis of the impact of organizational transparency on trust and loyalty of employees in health institutions. *International Journal of Operations and Quantitative Management*, 30, 200-213.

Hair Jr, J. F. Matthews, L. M. Matthews, R. L. & Sarstedt, M. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, 1, 107-123.

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, 2-24.

Haji-Othman, Y. Yusuff, M.S. & Hussain, M.N.M. (2024) Data analysis using partial least squares structural equation modeling (PLS-SEM) in conducting quantitative research. *International Journal of Academic Research in Business and Social Sciences*, 14, 2380–2388.

Hasan, Z. Zehra, N. Ahmed, S. & Wamiq, M. (2021). Factors Influencing Fear and its subsequent effects on Self Confidence: An analysis on HR Perspective. *KASBIT Business Journal*, 14, 142-152.

Heaphy, E. D. Lilius, J. M. & Feldman, E. (2021). Moved to speak up: How prosocial emotions influence the employee voice process. *Human Relations,* 75, 1113 - 1139.

Henseler, J. & Sarstedt, M. (2013). Goodness-of-fit indices for partial least squares path modeling. *Computational Statistics*, 28, 565-580.

Henseler, J. Ringle, C. M. & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43, 115-135.

Hossain, M. M. Islam, K. Z. Al Masud, A. Hossain, M. A. & Jahan, N. (2023). Antecedents and consequences of self-disclosure in subjective well-being: A Facebook case with a social support mediator. *Sage Open*, 13, 21582440231179925.

Hu, L. T. & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, 6, 1-55.

Jalees, T. Mubashir, A. Anwar, A. Ahmed, S. & Kanwal, N. (2023). Mediating Impact Of Transformational Leadership With Moderating Effects Of Employees' Psychological Wellbeing And Cognitive Trust In Leadership On The Relation Of Emotional Intelligence and Job Performance. *Journal of Positive School Psychology*, 7.

Klimchak, M. Ward Bartlett, A. K. & MacKenzie, W. (2020). Building trust and commitment through transparency and HR competence: A signaling perspective. *Personnel Review*, 49, 1897-1917.

Kock, N. (2015). *Common method bias in PLS-SEM: A full collinearity assessment approach. International Journal of E-Collaboration,* 11, 1–10.

Koohang, A. Floyd, K. Yerby, J. & Paliszkiewicz, J. (2021). Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument. *Issues in Information Systems*, 22, 133-145.

Koohang, A. Paliszkiewicz, J. & Goluchowski, J. (2018). Social media privacy concerns: trusting beliefs and risk beliefs. *Industrial Management & Data Systems*, 118, 1209-1228.

Kose, J. (2019). Privacy Concerns of Smartphone Technology. *ISSA Journal*, 17.

Kröger, J. L. Miceli, M. & Müller, F. (2021). How data can be used against people: A classification of personal data misuses. *Available at SSRN 3887097*.

Kundi, Y. M. Aboramadan, M. Elhamalawi, E. M. & Shahid, S. (2021). Employee psychological well-being and job performance: exploring mediating and moderating mechanisms. *International Journal of Organizational Analysis*, 29, 736-754.

Li, W. (2025). A study on factors influencing designers' behavioral intention in using AI-generated content for assisted design: Perceived anxiety, perceived risk, and UTAUT. *International Journal of Human–Computer Interaction*, 41, 1064-1077.

Luo, M. & Hancock, J. T. (2020). Self-disclosure and social media: motivations, mechanisms and psychological well-being. *Current Opinion in Psychology*, 31, 110-115.

Masood, A. Zhang, Q. Ali, M. Cappiello, G. & Dhir, A. (2023). Linking enterprise social media use, trust and knowledge sharing: paradoxical roles of communication transparency and personal blogging. *Journal of Knowledge Management*, 27, 1056-1085.

McIlwraith, A. (2021). *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Routledge.

Meier, Y. & Krämer, N. C. (2024). The privacy calculus revisited: an empirical investigation of online privacy decisions on between-and within-person levels. *Communication Research*, 51, 178-202.

Mutimukwe, C. Kolkowska, E. & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly*, 37, 101413.

Nabity-Grover, T. Thatcher, J. B. & Johnston, A. C. (2022). Contextualizing self-disclosure to the online environment: An assessment of the literature. *Communications of the Association for Information Systems*, 50, 39.

Ostendorf, S. Meier, Y. & Brand, M. (2022). Self-disclosure on social networks: more than a rational decision-making process. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 16.

Ozturk, A. B. Hancer, M. & Wang, Y. C. (2014). Interpersonal trust, organizational culture, and turnover intention in hotels: A cross-level perspective. *Tourism Analysis*, 19, 139-150.

Qureshi, E. Shehri, F. A. Malik, A. & Saif, O. B. (2024). Unravelling the interplay of servant leadership, cognitive trust, and employee wellbeing: A case of an emerging economy. *The Asian Bulletin of Green Management and Circular Economy,* 4, 154–162.

Qusef, A. & Alkilani, H. (2022). The effect of ISO/IEC 27001 standard over open-source intelligence. *PeerJ Computer Science*, 8, e810.

Ramasundaram, A. Gurusamy, R. & George, A. (2024). Employees and workplace surveillance: Tensions and ways forward. *Journal of Information Technology Teaching Cases*, 14, 2-6.

Reeves, A. Parsons, K. & Calic, D. (2020, July). Whose risk is it anyway: how do risk perception and organisational commitment affect employee information security awareness ? In *International Conference on Human-Computer Interaction* (pp. 232-249). Cham: Springer International Publishing.

Rodríguez-Priego, N. Porcu, L. Pena, M. B. P. & Almendros, E. C. (2023). Perceived customer care and privacy protection behavior: The mediating role of trust in self-disclosure. *Journal of Retailing and Consumer Services*, *72*, 103284.

Russo, C. & Terraneo, M. (2020). Mental well-being among workers: a cross-national analysis of job insecurity impact on the workforce. *Social Indicators Research*, 152, 421-442.

Saffarizadeh, K. Boodraj, M. & Alashoor, T. M. (2017). Conversational assistants: Investigating privacy concerns, trust, and self-disclosure. In *Proceedings of the 38th International Conference on Information Systems: Transforming Society with Digital Innovation (ICIS 2017)*. Association for Information Systems.

Sarstedt, M. Ringle, C. M. & Hair, J. F. (2021). Partial least squares structural equation modeling. In *Handbook of market research* (pp. 587-632). Cham: Springer International Publishing.

Saveljeva, J. (2025). Trust and Risk Management Interplay: A Review in the Digital Context. *FEMIB*, 189-196.

Smith, H. J. Dinev, T. & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, 989-1015.

Snyder, J. L. (2010). E-mail privacy in the workplace: A boundary regulation perspective. *The Journal of Business Communication (1973)*, 47, 266-294.

Soerjoatmodjo, G. W. L. (2025). Support over Safety? Rethinking How Organizational Support Empowers Gen Z in The Workplace. *Indonesian Psychological Research,* 7, 156-164.

Solove, D. J. (2022). The limitations of privacy rights. *Notre Dame L. Rev.*, *98*, 975.

Soomro, R. B. Al-Rahmi, W. M. Dahri, N. A. Almuqren, L. Al-Mogren, A. S. & Aldaijy, A. (2025). A SEM–ANN analysis to examine impact of artificial intelligence technologies on sustainable performance of SMEs. *Scientific Reports*, 15, 5438.

Srivastava, S. & Dhir, S. (2024). Do workplace practices really matter? Role of ostracism and dehumanization at the workplace and psychological well-being of employees. *International Journal of Organizational Analysis*, 32, 1574-1593.

Su, N. & Mattila, A. S. (2020). Does gender bias exist? The impact of gender congruity on consumer's Airbnb booking intention and the mediating role of trust. *International Journal of Hospitality Management*, 89, 102405.

Subhaktiyasa, P. G. (2024). PLS-SEM for multivariate analysis: A practical guide to educational research using SmartPLS. *EduLine: Journal of Education and Learning Innovation*, 4, 353-365.

Tirtayani, I. G. A. Wardana, I. M. Setiawan, P. Y. Widagda K, I. G. N. J. A. Kustina, K. T. & Arlita, I. G. D. (2023, May). The Privacy Paradox on Social Media: Balancing Privacy Concerns, Perceived Value, and Purchase Intentions with Habit Moderation. In *International Conference on Business and Technology* (pp. 357-366). Cham: Springer Nature Switzerland.

Tolsdorf, J. Reinhardt, D. & Iacono, L. L. (2022). Employees' privacy perceptions: exploring the dimensionality and antecedents of personal data sensitivity and willingness to disclose. *Proceedings on Privacy Enhancing Technologies*.

Van Ooijen, I. Segijn, C. M. & Opree, S. J. (2024). Privacy cynicism and its role in privacy decision-making. *Communication Research*, 51, 146-177.

Wu, Y. C. & Feng, J. W. (2018). Development and application of artificial neural network. *Wireless Personal Communications*, 102, 1645-1656.

Wuersch, L. Neher, A. Maley, J. F. & Peter, M. K. (2024). Using a digital internal communication strategy for digital capability development. *International Journal of Strategic Communication*, 18, 167-188.

Xia, H. Lu, D. Lin, B. Nord, J. H. & Zhang, J. Z. (2023). Trust in Fintech: Risk, governance, and continuance intention. *Journal of Computer Information Systems*, 63, 648-662.

Xu, H. Dinev, T. Smith, J. & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 12, 1.

Xueyun, Z. Al Mamun, A. Masukujjaman, M. Rahman, M. K. Gao, J. & Yang, Q. (2023). Modelling the significance of organizational conditions on quiet quitting intention among Gen Z workforce in an emerging economy. *Scientific Reports*, 13,15438.

Yadav, N. Verma, S. & Chikhalkar, R. (2024). Online reviews towards reducing risk. *Journal of Tourism Futures*, 10, 299-316.

Zhang, Y. & Qi, E. (2022). Happy work: Improving enterprise human resource management by predicting workers' stress using deep learning. *Plos One*, 17, e0266373.

Appendix

Concept	Code	Items	Source
Privacy Concern	PC1	I am concerned that I do not have complete control over who can access the information I choose to disclose at work.	Snyder (2010)
	PC2	I feel that the way information I disclose may be accessed or shared could violate my privacy.	
	PC3	I feel uneasy about how the information I disclose may be used by others.	
	PC4	I do not have enough control over who is able to access the information I disclose at work.	
	PC5	It makes me uncomfortable to know that information I disclose may remain available for others to view or revisit.	
Perceived Risk	PR1	In general, it would be risky to disclose personal or sensitive information through my organization's internal communication systems.	Xu et al. (2011)
	PR2	There would be a high potential for privacy loss associated with disclosing personal or sensitive information through my organization's internal communication systems.	
	PR3	The information I disclose could be used inappropriately by my organization or by individuals who have access to the system.	
	PR4	Disclosing personal or sensitive information through my organization's internal communication systems could lead to unexpected negative consequences.	
Self-disclosure	SD1	I actively come forward through the system to disclose issues and relieve stress.	Guarin et al. (2025)
	SD2	I always speak up through the system to freely disclose unfair treatments.	
	SD3	I always speak up through the system if I feel favoritism to clear my mind.	
	SD4	I always speak up through the system to voluntarily disclose workplace secrets.	
	SD5	I communicate my concerns through the system to freely disclose injustice.	

	SD6	I speak through the system if I have concerns about organizational bias.	
	SD7	I raise concerns through the system about any injustice to feel better.	
Psychological well-being	PWB1	When I work at this organization, I feel that I lead a purposeful and meaningful life.	Diener et al. (2009)
	PWB2	When I work at this organization, I feel that my social relationships are supportive and rewarding.	
	PWB3	When I work at this organization, I feel engaged and interested in my daily activities.	
	PWB4	When I work at this organization, I feel that I actively contribute to the happiness and well-being of others.	
	PWB5	When I work at this organization, I feel that I am a good person and live a good life.	
	PWB6	When I work at this organization, I feel competent and capable in the activities that are important to me.	
	PWB7	When I work at this organization, I feel optimistic about my future.	
	PWB8	When I work at this organization, I feel respected by others.	
Cognitive Trust	CT1	I can rely on my executive not to make issues related to my disclosed information more difficult by handling that information carelessly.	Ozturk et al. (2014)
	CT2	My executive demonstrates professionalism and dedication when handling information shared by employees.	
	CT3	My executive approaches tasks related to personal information or required disclosures with professionalism and dedication.	
	CT4	Other colleagues of mine who also need to provide or exchange information with my executive consider him/her to be trustworthy.	
	CT5	Most people, even those who are not close to my executive, trust and respect him/her in matters related to information handling.	