Liana-Elena ANICA-POPA, PhD
liana.anica@cig.ase.ro
Bucharest University of Economic Studies, Romania

Corina PELĂU, PhD (corresponding author)
corina.pelau@fabiz.ase.ro
Bucharest University of Economic Studies, Romania

Sînziana-Maria RÎNDAȘU, PhD
sinziana.rindasu@cig.ase.ro
Bucharest University of Economic Studies, Romania

Gabriela SAVA, PhD
msava@bgsu.edu
Bowling Green State University, Bowling Green, USA

Nurturing Information Security Awareness in Work-from-Home Environments. Insights from Global Business Services Centres

Abstract. *Work-from-home (WFH) scenarios implemented during and after the pandemic boosted the cyber-threats and unexpectedly transformed the business environment. Our study investigates the relationship between employees' information security awareness (ISA) and WFH determinants within Global Business Services centres (GBS). The purpose is to provide insights useful to nurture the workforce's ISA in post-pandemic WFH approaches. We collected the data through a questionnaire sent to professionals from GBSs based in Romania. Using a partial least squares structural equation modelling analysis, we investigated the impact of Work Engagement and Internal Service Quality as ISA drivers. Deepening understanding beyond behaviour-based theories through such a construct is, to our knowledge, an original approach. Our results showed that Work Engagement components, Absorption and Dedication, influence ISA. The need for managers to acknowledge, as cybersecurity requirements, not only the IT infrastructure cyber-resilience, but also the employees ISA, was also stressed and argued.*

Keywords: *Information Security Awareness (ISA), Work from Home (WFH), cybersecurity, Global Business Service (GBS), engagement, Internal Service Quality (ISQ).*

JEL Classification: C30, M15, M54, O33, F23.

1. Introduction

The COVID-19 pandemic has forced organisations and employees to suddenly switch to working from home (WFH), but not all companies have been able to enforce cybersecurity policies in due time. According to Eurostat (2022), only 5.5%

DOI: 10.24818/18423264/58.4.24.10

of the employees worked from home in 2019. Therefore, the organisations cyber resilience depended on the employees 'cyber behaviour and their information security awareness (ISA) level achieved up to that point. In this new WFH context, researchers stress the need to promote adequate "cyber hygiene" of employees in order to reduce risks and losses from cyber attacks (Wong et al., 2022) and to foster ISA and cyber vigilance policies among employees.

By acknowledging the central role of people in ensuring cyber resilience, researchers emphasised that the cybersecurity awareness capabilities are shaped by personnel, management, and infrastructure dimensions (Lyon, 2024). Studies that have employed behaviour-based theories (the theory of reasoned action and the theory of planned behaviour) examine the factors that enhance employees' security awareness (Zwilling et al., 2022). Other researchers encompass intrinsic motivation factors based on the self-determination theory as drivers for ISA improvement in a training context (Alahmari et al., 2022). However, the determinants of such employee behaviour are underinvestigated in the literature. By trying to address this gap, we propose to explore how ISA can be nurtured in a WFH environment focusing on the perceived level of internal service quality (ISQ) and dimensions of engagement, such as absorption and dedication. Going beyond the behaviour-driven theories and towards a better understanding of the employees' ISA determinants in a triaxial ISQ-engagement-ISA factorial approach, this is, to our knowledge, an original study. It also aims to highlight how organisational leadership may intervene to increase staff awareness of information security and specific cyber vulnerabilities.

To capture real-world insights from an international business environment, our study investigates employees' information security awareness (ISA) in the WFH settings within Global Business Service Centres (GBS) based in Romania and offers new insights into WFH influences exerted on the individual's ISA and cybersecurity behaviour. Our goal is to assess whether the perceived ISQ level, absorption, and dedication influence the employees' ISA degree while working from home. The decision to choose GBS from Romania as our research scope was grounded on the following arguments: (1) according to the European Business Services Association - EBSA (2021), Romania is considered one of the "best-known business service destinations in the world", many companies bringing, at the time, new processes to this country; (2) regarding WFH, EBSA notes that 70% of multinational companies surveyed in 2021 considered WFH possible only in Romania, 22% allow work from anywhere, with certain restrictions, and 5% - without any constraints, 3 % have no WFH-specific policy; (3) searching for trends, we found that, in 2021, EBSA announced that 84% of companies were working from home; (4) GBS embrace an advanced digital mindset, prioritising an innovation culture over the next one to three years (Deloitte, 2021); (5) by directly interviewing managers in various GBSs, we were confirmed that cybersecurity procedures are disseminated and applied internationally, within all subsidiaries or business service provider partners of multinationals. Based on the questionnaire answers of 323 employees, our study conceptualises and tests a-priori a model focusing on determining the impact that perceived ISQ level and engagement dimensions have on employees' ISA. We also

mention that the approach to aspects regarding engagement contributes to a timely, yet underexplored, research topic.

The remainder of the paper is structured as follows. In Section 2, we present a brief literature review on cybersecurity, ISA, ISQ, and engagement in WFH settings within international business environment. In Section 3, we develop the model that describes the influence of work conditions on information security awareness and work engagement and elaborate the hypothesis to be tested. We also depict the data collection procedure and the modelling approach. In Section 4, we present our results and specify which of our hypotheses were supported by our data. In Section 5, we detail our contributions to the theory and management practice. Finally, in Section 6, we highlight the main outcomes, our research originality, the results usefulness in developing managerial policies dedicated to the improvement of ISA, we acknowledge the limitations of our study, and discuss further research directions.

2. Literature review

Responding to COVID-19 imperatives, organisations worldwide have compressed what would have been years of digital transformation into just a few months (PwC, 2022), the online workflows generating opportunities for a sharp increase in the number of cyber attacks. For the post pandemic era, scholars have predicted the fastest social changes, a much wider adoption of WFH in various forms, e.g., hybrid, across borders, from multiple locations (Caligiuri and Cieri, 2021), and a shift in focus from the place of work to the work itself, employee's role, and work procedures.

The presence and performance of a GBS in the market depend on the employees' knowledge, engagement and application of cybersecurity policies. Hence, the people may need additional training on awareness of information security risks their company is exposed to, as well as on the steps to secure online work, to report and address violations of applicable regulations.

2.1 Information Security Awareness

In the post-pandemic years, remote key operational areas in organisations are still largely supported by the human workforce serving as their backbones and influencing information security policies effectiveness (Wong et al., 2022). To build and evaluate an organisational cybersecurity culture and to inspire good security behaviours, constant communication and SETA parameters (security education, training and awareness) are reckoned pivotal success factors (Da Veiga et al., 2020). Information Security Awareness (ISA) has been defined as a state of cognisance in which the employee knows the rules, recognises the potential danger, understands the own information security responsibilities, and acts in accordance with the procedures in place (Ahlan et al., 2015). To address the ISA challenges, researchers have determined different ISA dimensions: personnel - knowledge, attitude and learning; management - training, culture, and strategic orientation; and infrastructure

- technology and data governance (Saeed et al., 2021). The core ISA role mainly refers to increasing the employees 'level of knowledge on the risks, vulnerabilities, cyber attacks, information security rules, and thus ensuring greater protection of information, systems and networks. Moreover, employees' lack of ISA and cyber-risks management in WFH conditions are considered critical vulnerabilities in the literature.

Defining employee behaviour in applying cybersecurity policies and procedures has been and remain challenges for both researchers and managers, especially after the transition to WFH during pandemic, when there was an increased proliferation of cyber attacks. A solution for encouraging more significant engagement in ISA activities is considered the continuous training, along with better methods of measuring behavioural change regarding the cyber resilience after implementing cybersecurity learning programmes (Khan et al., 2023).

In order to address ISA-related organisational needs by getting a current image of the ISA level and drivers in the WFH setting, we investigated the GBS employees' 'adherence to cybersecurity practices and the influence of individual decision-making styles on the compliance with organisational cybersecurity regulations.

2.2 Internal Service Quality and Engagement as determinants of Information Security Awareness

Internal Service Quality (ISQ) refers to the services provided to individuals (employees) within the organisation, being considered a key prerequisite for the companies' performance (Chen, 2022). As every employee is considered to be both a service provider and an utiliser, the perception about the provided ISQ could lead to an increase in employees 'commitment. This represents a vital aspect in the WFH context, where companies count on the employees to behave in a compliant manner.

While examining the mediating factors between job characteristics and extra-role behaviours, Sulea et al. (2012) found that work engagement exerts a significant influence in increasing organisational citizenship behaviours, while it decreases counterproductive work behaviours. The organisational climate seems to be a driver of work engagement and performance; therefore, a high level of perceived ISQ might contribute to an employees' engagement increase and lead to an ISA strengthening.

Dalal et al. (2022) highlighted that while the technological part of cybersecurity is a trending research topic, the human factor counterpart is less examined and researchers should focus more on the items that lead to counterproductive work behaviour. Rebolledo et al. (2021) pointed out the "Paradox of Working from Home", which describes the dichotomy between WHF advantages and WHF specific damages. The advantages, created by the individual and organisational dimensions, are personal work/life balance, organisational commitment, effort satisfaction, increased creativity, while the WHF specific damages refer to social isolation, material conditions existing at the employee's workplace, amplified effort required to perform tasks. The link between job performance and WFH infrastructure, employee responsibilities, and IT management in the WFH context was particularly

highlighted. Previous research emphasised that job performance is directly influenced by the perceived quality of internal services provided (Singh, 2016).

Since ISQ and engagement directly affect performance even in a WFH context, we therefore operate with these two concepts to investigate the impact on ISA.

3. Research methodology

The twofold objective of our research is, more specifically, to assess whether the perceived ISQ level, through absorption and dedication, influence the employees' ISA degree while working from home and then to provide some insights into the role of employees' ISA for organisational survival and performance in WFH settings, that may be useful guidelines to managers and researchers.

For this purpose, we have conducted a partial least squares structural equation modelling analysis to empirically test the impact of the equipment-related and social work conditions on the employees' absorption and dedication, and sequentially their impact on the ISA. Based on these concepts, we developed the model presented in Figure 1 and defined the following hypotheses, taking into consideration the dimensions of the analysed constructs:

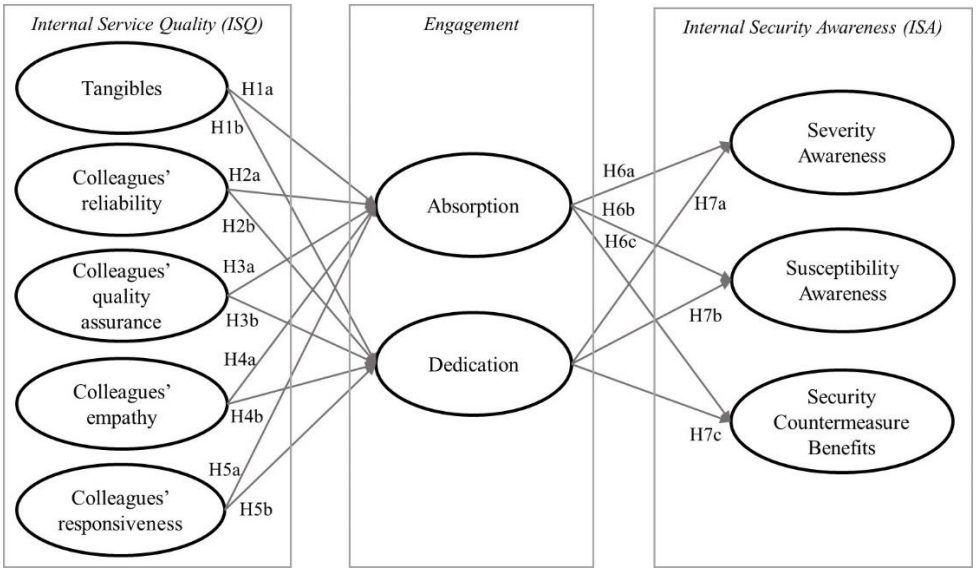

Figure 1. The influence of work conditions on work engagement and ISA
Source: Authors' own creation.

H1. The perceived quality of the tangible assets (equipment) provided has a positive impact on the employees' absorption (H1a) and dedication (H1b) during WFH.
H2. The perceived quality of colleagues' reliability has a positive impact on the employees' absorption (H2a) and dedication (H2b) during WFH.
H3. The perceived quality of assurance from colleagues has a positive impact on the employees' absorption (H3a) and dedication (H3b) during WFH.

H4. The perceived quality of the colleagues' empathy has a positive impact on the employees' absorption (H4a) and dedication (H4b) during WFH.
H5. The perceived quality of the colleagues' responsiveness has a positive impact on the employees' absorption (H5a) and dedication (H5b) during WFH.
Further, we are interested in testing the impact of the absorption and dedication on the ISA, which is characterised by three dimensions: (a) the severity awareness, (b) susceptibility awareness, and (c) security countermeasure benefits. To test the described relationships, the following hypotheses were developed:
H6: The employees' absorption during WFH has a positive impact on the perceived severity of noncompliance with security countermeasures (H6a), on the susceptibility regarding the noncompliance with security countermeasures (H6b), and on the perceived benefits of information security countermeasures (H6c).
H7: The employees' dedication during WFH has a positive impact on the perceived severity of noncompliance with security countermeasures (H7a), on the susceptibility regarding the noncompliance with security countermeasures (H7b), and on the perceived benefits of information security countermeasures (H7c).

Initial Questionnaire Development

To test the hypotheses developed above, we designed a questionnaire administered online to GBS employees who had WFH experience. The questionnaire was developed using concepts already validated by other studies, but never combined, as proposed in the model depicted in Figure 1.

To assess the equipment and social work conditions, we employed adapted items from the SERVQUAL survey by Kang et al. (2002), an instrument previously utilised to gauge employee satisfaction across various sectors, as reported by Fang et al. (2020). In order to assess work engagement, the Utrecht Work Engagement Scale (Schaufeli and Bakker, 2003) was used. This involved the selection of only the absorption and dedication dimensions, with vigour being excluded due to the potential distortions that may have been caused by the peak of the COVID-19 pandemic (Ruiz-Frutos et al., 2022). Furthermore, employees' ISA levels were assessed using adapted items proposed by Humaidi and Balakrishnan (2015). All the items used were measured using a 7-point Likert scale, where 1 represents strongly disagree and 7 signifies strongly agree.

Pilot Testing and Questionnaire Refinement

The questionnaire was tested and analysed by several managers and specialists from different GBS, with the aim of improving its effectiveness. The final questionnaire form included recurrent refinements of the structure and content suggested by participants in our pilot study phase.

Sampling and Participants

The questionnaire was sent by email or message on professional social media platforms (such as LinkedIn) to potential respondents employed by Multinational Business Services Centres from Romania, between September and November 2021.

A participant was eligible for our study if he/she worked at least one day per week from home and used equipment provided by the employer to perform the job duties.

Data Collection and Analysis

The dataset comprises 323 responses collected during September-November 2021, which coincided with Romania's fourth wave of the COVID-19 pandemic, when the majority of respondents were working from home. Out of 361 questionnaires, 38 were excluded due to non-compliance with the inclusion criteria.

The mean age of our respondents was 34 years, with a standard deviation of 8.54 years, 76.78% of the study's participants being female employees. Additionally, the respondents are distributed almost evenly between the execution (56.03%) and management (43.97%) roles. In addition, 52.32% of the respondents worked no day from home before the pandemic, while during the pandemic 71.52% of them reported working five days a week from home.

The collected data was processed using PAWS Statistics 18 for data management and data cleaning. To test the research hypotheses developed, we performed a covariance-based structural equation modelling (SEM) analysis based on the model defined in Figure 1. For the partial least squares structural equation modelling (PLS-SEM) analyses, we used SmartPLS 3 software (Ringle et al., 2015). As the study utilised a 7-point Likert scale, we tested for the presence of common method bias by employing the Harman's single factor test (Fuller et al., 2016). The test showed an average variance of 30.78%, indicating that common method bias is not a concern in our study.

4. Results

4.1 The measurement model

The measurement model presented in Figure 1 is used to evaluate the quality of the constructs, with the results presented in the Supplementary Appendix 1. The initial step involved the analysis of factor loadings with only one item, EMP_2, exhibited a loading below the 0.708 cut-off. Hair et al. (2017) propose that content validity should be analysed for loadings between 0.4 and 0.7 before any item is removed. Therefore, EMP_2 was removed due to its impact on discriminant validity.

To assess the reliability of the dataset, we used the Cronbach's Alpha and Composite reliability (CR). A reliable item has to have a Cronbach's Alpha greater than 0.7 and a CR greater than 0.8 (Hair et al., 2017). For our model, all the factor loadings have values between 0.677 and 0.939. Looking at the CR values, all of them range between 0.854 and 0.964, thus deemed suitable for the confirmatory analysis. By assessing the internal consistency using Cronbach's Alpha, the reliability is confirmed. In case of the exploratory analysis, the minimum accepted value is 0.6, while our measures range between 0.753 and 0.972. The average variance extracted (AVE) was used to measure the amount of variance from the constructs relative to

the variance of the measurement errors. In our model, the values for the dimensions' AVE vary between 0.615 and 0.870, all above the recommended threshold of 0.50.

To assess the discriminant validity, we used the Fornell-Larker criterion and the heterotrait–monotrait ratio (HTMT) of the correlations. The Fornell-Larker criterion tests whether the square root of AVE for the construct analysed is greater than its correlations with other constructs of the model (Fornell and Larker, 1981) (Table 1). In terms of HTMT, a value above the recommended threshold of 0.9 suggests a lack of discriminant validity; however, since PLS-SEM does not rely on any assumptions regarding the distribution, "researchers have to rely on a procedure called bootstrapping to derive a distribution of the HTMT statistic" (Hair et al., 2017, p. 119). In the original analysis performed, two of the HTMT ratio values exceeded the 0.9 threshold. To test whether there is any discriminant validity issue, we then performed a second analysis using a bootstrapping procedure with 5000 samples. Our bootstrapping results show that all intervals do not include 1, thus eliminating the possibility of discriminant validity issues (Hair et al., 2017).

Table 1. Discriminant validity using Fornell-Larker criterion

	ABS	ASU	BEN	DED	EMP	REL	RES	SEV	SUS	TAN
ABS	**0.813**									
ASU	0.195	**0.900**								
BEN	0.194	0.252	**0.876**							
DED	0.685	0.276	0.221	**0.846**						
EMP	0.267	0.798	0.219	0.311	**0.875**					
REL	0.171	0.820	0.279	0.268	0.765	**0.882**				
RES	0.253	0.819	0.232	0.336	0.849	0.747	**0.933**			
SEV	0.236	0.254	0.834	0.229	0.243	0.263	0.231	**0.914**		
SUS	0.189	0.333	0.793	0.178	0.245	0.330	0.248	0.846	**0.927**	
TAN	0.319	0.544	0.194	0.392	0.501	0.546	0.508	0.248	0.232	**0.784**

Source: Authors' processing.

4.2 The structural equation model analysis

To test the hypotheses defined, we run our structural equation model using bootstrapping with 5000 samples. We performed a one-tail testing with the confidence interval method bias-corrected and accelerated (BCa) bootstrap, having a significance level of 0.05. The results of our model are presented in Table 2 simultaneously with the decisions regarding the developed hypotheses.

Table 2. Structural equation modelling results

Hypothesis	Relationship	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values	Decision
H1a	*TAN -> ABS*	*0.294*	*0.295*	*0.067*	*4.380*	*0.000**	*Supported*
H1b	*TAN -> DED*	*0.323*	*0.328*	*0.060*	*5.435*	*0.000**	*Supported*
H2a	REL -> ABS	-0.182	-0.173	0.129	1.412	0.079	Rejected
H2b	REL -> DED	-0.038	-0.020	0.127	0.302	0.381	Rejected
H3a	ASU -> ABS	-0.099	-0.100	0.142	0.699	0.242	Rejected
H3b	ASU -> DED	-0.127	-0.138	0.134	0.944	0.173	Rejected

Hypothesis	Relationship	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values	Decision
H4a	*EMP -> ABS*	*0.224*	*0.227*	*0.116*	*1.928*	*0.027***	*Supported*
H4b	EMP-> DED	0.071	0.074	0.132	0.540	0.295	Rejected
H5a	RES -> ABS	0.121	0.117	0.115	1.052	0.146	Rejected
H5b	*RES -> DED*	*0.235*	*0.226*	*0.115*	*2.043*	*0.021***	*Supported*
H6c	ABS -> BEN	0.085	0.093	0.078	1.091	0.138	Rejected
H6a	*ABS -> SEV*	*0.154*	*0.162*	*0.071*	*2.190*	*0.014***	*Supported*
H6b	*ABS -> SUS*	*0.128*	*0.134*	*0.074*	*1.731*	*0.042***	*Supported*
H7c	*DED -> BEN*	*0.162*	*0.163*	*0.068*	*2.383*	*0.009**	*Supported*
H7a	*DED -> SEV*	*0.122*	*0.121*	*0.069*	*1.784*	*0.037***	*Supported*
H7b	DED -> SUS	0.091	0.089	0.067	1.354	0.088	Rejected

*p<0.01, **p<0.05, ***p<0.10

Source: Authors' processing.

Our results show that tangibles (TAN), such as equipment, are the most important condition to increase work engagement. Tangibles influence in a significant positive way both absorption (ABS) and dedication (DED). The social factors and the impact of the relation with the colleagues, such as the reliability of colleagues (REL) and their ability for quality assurance (ASU) does not impact dedication and absorption of the employees' work engagement. The empathy of colleagues (EMP) affects only the absorption component of work engagement, while the responsiveness of colleagues (RES) impacts only the dedication of employees.

In terms of how work engagement influences ISA, it can be observed that both absorption and dedication impact the severity (SEV) and susceptibility awareness of information security (SUS), as well as the security countermeasure benefits (BEN). The absorption component of work engagement mainly influences the severity (SEV) and susceptibility awareness of employees (SUS), but it does not influence the security countermeasure benefits (BEN). Dedication (DED) impacts severity awareness and security countermeasure benefits and not susceptibility awareness (SUS).

5. Discussion

5.1 Theoretical contributions

Our proposed model emphasises the influence of work engagement on ISA, as well as the factors that affect work engagement during WFH. Unlike previous studies that focus on developing a proactive cybersecurity behaviour based on attitudinal, organisational, and motivational factors (Alahmari et al., 2022), the current research highlights the items that can lead to an ISA increase, such as nurturing the employees' engagement as influenced by the ISQ. Hence, our results allow organisations to better understand which behavioural-related factors determine an increase of employees' engagement in ISA.

Based on our findings, the absorption during WFH affects severity and susceptibility awareness, showing that a deep concentration on work can trigger both

an intrinsic and extrinsic ISA. A more company-oriented view emerges from dedication's influences on severity awareness, generating also a more conscious reaction to security countermeasure benefits. The results also showed that the not all social aspects contribute to the employees' improvement in engagement, while surprisingly the tangibles, e.g., giving to the employees the appropriate equipment, seems to have a positive impact on both dimensions of engagement. The direct impact of responsiveness to the dedication dimension of the engagement highlights that improving individual commitment is not just a matter of intrinsic factors, but it is also determined by the quality of the interactions and colleagues' influence. Moreover, our study highlights that colleagues' perceived level of empathy improves employee absorption. Therefore, companies should focus more on motivating employees to have a better level of responsiveness in a WFH context.

From a theoretical perspective, our results provide a new understanding of the ISA and work engagement under WFH conditions and also during atypical work situations such as the pandemics. As employees' behaviour tends to change after a severe disruption and the number of remote employees worldwide increases, employers should focus more on how to improve the ISA of their personnel, especially given that technology continues to evolve, generating new settings for better supporting remote work (such as the metaverse).

5.2 Managerial implications

The research revealed two decisive pillars for ensuring the information security of organisations: the degree of ISA achieved by their employees and a high level of employee engagement. Our outcomes indicate that companies should provide adequate equipment to the employees to ensure a higher work engagement and thus an increased ISA level. Although not all ISQ dimensions directly impact engagement, organisations can leverage our results to define new ISA protocols. As in the WFH context, the engagement is negatively affected by family-work conflict, social isolation, and the distractions of the work environments, GBS may focus more on providing employees with the necessary tools to improve individual engagement. Therefore, the impact of the perceived quality of tangibles on the engagement dimensions has direct managerial implications. In addition to having up-to-date equipment, highly appreciated by the GBS employees, and thus contributing directly to the increase in engagement, they also value a comfortable and attractive work environment and a professional appearance of the colleagues.

Due to increasingly complex security threats in a currently expanding WFH setting, it is recommended both a change in the managers' vision regarding the need for a steadily high ISA degree and a shift to a praxeological approach in nurturing employees' ISA. Our insights are consistent with the Human Aspects of Information Security (HAIS) model (Riahi et al., 2024), highlighting distinct culture-driven patterns in shaping employees behaviours: in Sweden, ISA enhancement was dependent of the employees involvement in the ISA policy design process; in France, learning from past experiences and respecting hierarchical structures were found

pivotal factors in raising ISA, whereas in Tunisia, the ISA-spotting initiatives should consider the social and relational aspects. These results provide valuable guidance to managers in multinational organisations, enabling them to comprehend the underlying forces and dynamics in countries with similar characteristics.

Employers should also focus on designing and delivering training programmes tailored to individual WFH contexts and vulnerabilities. The same idea was promoted by Saritepeci et al. (2024), who stressed the crucial role of Digital Literacy in Digital Data Security Awareness and Online Privacy Concern. Anti-phishing training programmes, to help employees become more suspicious of potential attacks, and thus increase their ISA level, are also recommended. For example, Xu et al. (2023) include, among learning topics, the principles of theory of mind (ToM), the differences between mass phishing and spearfishing, or the use of embedded training programmes. By applying ToM reasoning in harnessing shared information to discover people's mental state, judgments, opinions, and feelings, the learners could better understand how cyber-attackers try to predict the behavioural response of targeted people. Moreover, by endorsing more engaging training methods, such as serious games or interactive storytelling, managers could foster learning in a simulated game environment about, for example, phishing and spear-phishing concepts. Also, it may be useful to track the effects of just-in-time employee awareness on the cyber-risks mitigation and thus to evaluate the ISA training effectiveness.

Ensuring a good ISA level becomes a managerial challenge focused *on the employee*, and not only on enforcing IT infrastructure security measures. Using our research, regardless of industry or area of expertise, managers may integrate actions (ISA training, employee engagement strengthening) into strategic information security policies, to ensure the continuity of WFH-delivered business services.

5.3 Research limitation

As the pandemic restrictions have caused a certain level of job insecurity, employees were reluctant to speak in favour of WFH, lest it be interpreted as a lack of dedication and commitment to work. This affected our questionnaire response rate.

6. Conclusions and future research corridors

In today’s business landscape, a revamped design of supportive workplaces, that empower sustainable people practices, represents equally a pivotal opportunity and need for leaders. Working from home positively affects staff’s discipline, but employees still need to increase their information security awareness (ISA). Investigating to which degree the GBS employees’ ISA is influenced, in a WFH setting, by internal service quality (ISQ) and dimensions of work engagement, new insights into the impact exerted by the WFH environment on the individual's behaviour concerning compliance with organisational cybersecurity policies were

provided. Our study addresses a gap in the literature by looking beyond behaviour-based theories to deepen the understanding of the factors that determine employees' ISA, being, to our knowledge, the first article that examines the role of engagement determined by the ISQ as a driver of ISA.

Our results highlight the noteworthy role of the GBS employees' work engagement in achieving a good ISA level, as well as the tangibles relevance during WFH. A practical research implication is the essential position the employees hold in the organisational strategy puzzle aimed at increasing the ISA degree and so ensuring business continuity in a WFH setting. This finding is in contrast with the view of many companies' board members and CEOs that confine cybersecurity strictly between technical boundaries (PwC, 2022). We would recommend that management teams consider a change in their praxeological vision about the perception and level of ISA in organisations resorting WFH business models. Since a dominant decision-making style has been proven to influence individual cybersecurity compliance behaviour, it can be concluded that a *pro-ISA managerial approach* could help to avoid information security breaches.

Our findings show that not only ISA training, but also having the proper tangibles, and thus ensuring a higher work engagement, could increase the GBS employees' ISA. This paper extends the previous studies by pointing out the key role of employees' work engagement and attitude in an atypical context such as the pandemics. Knowing employees' perception of cyber-risks under pandemic restrictions, forthcoming research should focus on configuring future work conditions suitable for WFH settings. Further, scholars may also look into the importance assigned by the employees to tangibles in the detriment of healthy social relations with their colleagues and the change of employees' attitudes towards it. Subsequently, the effect of technological disruptions on employees 'WFH-required equipment, work engagement, and ISA may be assessed. Additionally, investigating how to capitalise on ISA-enhancing knowledge acquired in a WFH context by designing and harnessing GBS organisational memory tools (Constantin and Anica-Popa, 2017) could reveal levers to improve organisations' competitiveness.

References

[1] Ahlan, A.R., Lubis, M., Lubis, A.R. (2015), *Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. Procedia Computer Science*, 72, 361-373.

[2] Alahmari, S., Renaud, K., Omoronyia, I. (2022), *Moving beyond cyber security awareness and training to engendering security knowledge sharing. Information Systems and e-Business Management*, 1-36.

[3] Caligiuri, P.M., Cieri, H.D. (2021), *Predictors of Employees Preference for Working from Home Post-Pandemic. Business and Economic Research*, 11(2), 1-19.

[4] Chen, W.J. (2022), *Innovative Service Behaviors of Hotel Employees: An Internal Service Perspective. Journal of Quality Assurance in Hospitality & Tourism*, 1-22.

[5] Constantin, R., Anica-Popa, L. (2017), *Enhancing Business Services' Performances by using Domain Ontologies. Quality-Access to Success*, 18(161), 99-102.

[6] Da Veiga, A., Astakhova, L.V., Botha, A., Herselman, M. (2020), *Defining organisational information security culture. Perspectives from academia and industry. Computers & Security*, 92, 101713.

[7] Dalal, R.S., Howard, D.J., Bennett, R.J., Posey, C., Zaccaro, S.J., Brummel, B.J. (2022), *Organizational science and cybersecurity: abundant opportunities for research at the interface. Journal of business and psychology*, 37(1), 1-29.

[8] Deloitte (2021), *2021 Deloitte Global Shared Services and Outsourcing Survey*, https://www2.deloitte.com/ro/en/pages/operations/articles/gx-shared-services-survey.html (accessed 15 December 2021).

[9] Eurostat (2022), *Rise in EU population working from home,* https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20221108-1 (accessed 15 December 2022).

[10] European Businesss Services Association (2021). *ABSL Romania Annual Report: 79% of companies say turnover will increase in 2022*, https://www.europeanbusinessservices.com/news/absl-romania-annual-report-79-of-companies-say-turnover-will-increase-in-2022 (accessed 15 December 2021).

[11] Fang, L., Lu, Z., Dong, L. (2020), *Differentiating service quality impact between the online and off-line context: an empirical investigation of a corporate travel agency*. *International Hospitality Review*, 35(1), 3-18.

[12] Fornell, C., Larcker, D.F. (1981), *Structural equation models with unobservable variables and measurement error: Algebra and statistics*, 18(3), 382-388.

[13] Fuller, C.M., Simmering, M.J., Atinc, G., Atinc, Y., Barry J.B. (2016), *Common methods variance detection in business research. Journal of Business Research*, 69(8), 3192-3198.

[14] Hair, Jr. J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M. (2017), *A primer on partial least squares structural equation modeling (PLS-SEM)*, SAGE Publications, USA.

[15] Humaidi, N., Balakrishnan, V. (2015), *Leadership styles and information security compliance behavior: The mediator effect of information security awareness. International Journal of Information and Education Technology*, 5(4), 311-318.

[16] Kang, G.D., Jame, J., Alexandris, K. (2002), *Measurement of internal service quality: application of the SERVQUAL battery to internal service quality*. *Managing Service Quality: An International Journal*, 12(5), 278-291.

[17] Khan, N.F., Ikram, N., Murtaza, H., Javed, M. (2023), *Evaluating protection motivation based cybersecurity awareness training on Kirkpatricks Model. Computers&Security*, 125, 103049.

[18] Lyon, G. (2024), *Informational inequality: the role of resources and attributes in information security awareness. Information and Computer Security*, 32(2), 197-217.

[19] PwC (2022), *Cyber Risks are top threats to growth in 2022 - Have we become too complex to secure?*, https://www.pwc.com/mu/en/services/advisory/consulting/blog/ cyber-threats.html (accessed 19 September 2022).

[20] Rebolledo, O.A., Vega, D.C., Belmar, R.S. (2021), *Learning to Work While Homebound– The Effects of Remote Work on Job Performance during the Covid-19 Pandemic. Journal of Economics, Finance and Management Studie*s, 4(6), 772-793.

[21] Riahi, E., Islam, M.S. (2024), *Employees information security awareness (ISA) in public organisations: insights from cross-cultural studies in Sweden, France, and Tunisia*. *Behaviour & Information Technology*, 1-23.

[22] Ringle, C.M., Wende, S., Becker, J.-M. (2015), *SmartPLS 3, Boenningstedt: SmartPLS*, https://www.smartpls.com (accessed 10 November 2021).

[23] Ruiz-Frutos, C., Adanaqué-Bravo, I., Ortega-Moreno, M., Fagundo-Rivera, J., Escobar-Segovia, K., Arias-Ulloa, C.A., Gómez-Salgado, J. (2022), *Work Engagement, Work Environment, and Psychological Distress during the COVID-19 Pandemic: A Cross-Sectional Study in Ecuador. Healthcare*, 10(7), 1330.

[24] Saeed, A., Alqahtani, M., Erfani, E. (2021), *Exploring the Relationship Between Technology Adoption and Cyber Security Compliance: A Quantitative Study of UTAUT2 Model. International Journal of Electronic Government Research*, 17(4), 40-62.

[25] Saritepeci, M., Durak, H.Y., Özüdoğru, G., Uslu, N.A. (2024), *The role of digital literacy and digital data security awareness in online privacy concerns: a multi-group analysis with gender. Online Information Review*, (ahead-of-print).

[26] Schaufeli, W.B., Bakker, A.B. (2003), *Test manual for the Utrecht Work Engagement Scale*, unpublished manuscript, Utrecht University, the Netherlands, https://www.wilmarschaufeli.nl/ (accessed 10 September 2021).

[27] Sulea, C., Virga, D., Maricutoiu, L.P., Schaufeli, W., Dumitru, C.Z., Sava, F.A. (2012), *Work engagement as mediator between job characteristics and positive and negative extra-role behaviors. Career Development International*, 17(3), 188-207.

[28] Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., Sohal, A. (2022), *The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. International Journal of Information Management*, 66, 102520.

[29] Xu, T., Singh, K., Rajivan, P. (2023), *Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. Applied Ergonomics*, 108, 103908.

[30] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., Basim, H.N. (2022), *Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems*, 62(1), 82-97.

Supplementary Appendix 1. The measurement model items evaluation

Table 1. The measurement model evaluation

Item	Factor loadings	Cronbach's Alpha	CR	AVE
Absorption (ABS_i, i = 1..3) (Adapted after Schaufeli and Bakker, 2003)				
ABS_1: I am immersed in my work	0.814	0.753	0.854	0.661
ABS_2: I get carried away when I'm working	0.835			
ABS_3: I feel happy when I am working intensely	0.790			
Assurance (ASU_i, i = 1..4) (Adapted after Kang et at., 2002)				
ASU_1: I can trust my coworkers	0.905	0.921	0.944	0.810
ASU_2: I feel safe in dealing with coworkers	0.909			
ASU_3: Coworkers are polite and kind	0.910			
ASU_4: Coworkers are knowledgeable	0.875			
Benefit of security countermeasures (BEN_i, i = 1..7) (Adapted after Humaidi and Balakrishnan, 2015)				
BEN_1: I am aware that using information security countermeasures is effective for reducing the number of security incidents in my organisation.	0.886	0.950	0.959	0.768
BEN_2: I am aware that information security countermeasures are effective for protecting my organisation's data.	0.813			
BEN_3: I am aware that using a strong password is effective for avoiding unauthorised access.	0.846			
BEN_4: I am aware that changing my password regularly is effective for avoiding unauthorised access.	0.860			
BEN_5: I am aware that using anti-virus regularly is effective for protecting my computer.	0.923			
BEN_6: I am aware that updating anti-virus regularly is effective for protecting my computer.	0.913			
BEN_7: I am aware that scanning files and devices before using them is effective for protecting my computer.	0.889			
Dedication (DED_i, i = 1..3) (Adapted after Schaufeli and Bakker, 2003)				
DED_1: I am enthusiastic about my job.	0.815	0.816	0.883	0.716
DED_2: My job inspires me.	0.864			
DED_3: I am proud of the work that I do.	0.859			
Empathy (EMP_i, i = 1..4) (Adapted after Kang et at., 2002)				
EMP_1: Coworkers are sincerely concerned about problems	0.825	0.897	0.929	0.765
EMP_2: (removed)	0.461*			
EMP_3: We have convenient working hours	0.870			
EMP_4: Coworkers give me individual attention	0.901			
EMP_5: Coworkers seem to have each other's best interests in mind	0.895			
Reliability (REL_i, i = 1..5) (Adapted after Kang et at., 2002)				
REL_1: Coworkers provide service that is promised	0.858	0.929	0.946	0.778
REL_2: Coworkers are dependable for handling my problems	0.853			

Item	Factor loadings	Cronbach's Alpha	CR	AVE
REL_3: Coworkers perform services right the first time, to avoid having to make corrections later	0.906			
REL_4: Coworkers provide correct and necessary information	0.924			
REL_5: Coworkers are reliable	0.866			
Responsiveness (RES_i, i = 1..4) (Adapted after Kang et at., 2002)				
RES_1: My communication with coworkers is appropriate, accurate, and clear	0.921	0.951	0.964	0.870
RES_2: Coworkers respond quickly and efficiently	0.939			
RES_3: to my request				
RES_4: Coworkers are willing to help me	0.937			
RES_5: Coworkers are willing to accommodate special requests and	0.934			
Severity (SEV_i, i = 1..4) (Adapted after Humaidi and Balakrishnan, 2015)				
SEV_1: If I do not follow information security policy, the penalty will be severe.	0.911	0.934	0.953	0.835
SEV_2: Failure to adopt information security behavior will worsen information security problem of my organisation	0.927			
SEV_3: Failure to adopt information security behavior will jeopardise my career.	0.894			
SEV_4: Failure to adopt information security behavior will harm my organisation's data.	0.924			
Susceptibility (SUS_i, i = 1..4) (Adapted after Humaidi and Balakrishnan, 2015)				
SUS_1: I am aware that if I do not adopt appropriate information security behavior, it will cause security incidents.	0.859	0.945	0.960	0.859
SUS_2: I am aware that it is a serious problem if I am not complying with information security policies in my organisation.	0.955			
SUS_3: I am aware that if I am not complying with information security policies, my organisation could be subjected to serious information security threats.	0.961			
SUS_4: I am aware that it is a serious problem if organisational data is stolen by unauthorised users.	0.928			
Tangibles (TAN_i, i = 1..4) (Adapted after Kang et at., 2002)				
TAN_1: We have up-to-date equipment	0.757	0.796	0.864	0.615
TAN_2: Working environment is comfort and attractive	0.867			
TAN_3: Coworkers have a neat, professional appearance	0.677			
TAN_4: The materials used in the workplace are visually appealing	0.813			
*The item EMP_2 has been removed due to the factor loading value. All the other values in the above table have been computed after the removal of the indicator				

Source: Authors' processing.