Computers in Human Behavior Reports 8 (2022) 100240

Contents lists available at ScienceDirect

Computers in Human Behavior Reports

journal homepage: www.sciencedirect.com/journal/computers-in-human-behavior-reports

The Workplace Information Sensitivity Appraisal (WISA) scale

John Blythe [a], Richard Brown [b,*], Lynne Coventry [c]

[a] Immersive Labs, Bristol, United Kingdom
[b] Psychology Department at Northumbria University, Newcastle, United Kingdom
[c] Abertay cyberQuarter, Abertay University, Dundee, United Kingdom

ARTICLE INFO

Keywords:
Cyber security
Information sensitivity
Behavior change
Employee behaviors
Information security
Organizational security culture

ABSTRACT

Human error in security plays a significant role in the majority of cyber-attacks on businesses. Security behaviours are impacted by numerous factors, including individual perceptions of information sensitivity. However, there is currently a lack of empirical measurement of information sensitivity and its role in determining security behaviours. This research presents a measure of information sensitivity appraisal that predicts security behaviour. We outline the design, development and validation of the Workplace Information Sensitivity Appraisal scale. The psychometric properties were assessed with data from an online sample of 326 employees in the UK. The scale comprises of five subscales: Privacy, Worth, Consequences, Low proximity interest by others and High proximity interest by others. The final 16-item WISA scale, alongside its five subscales, represents a comprehensive measure of information sensitivity appraisal in the workplace. The WISA scale has been found to have strong factorial validity, confirmed across eight information types, strong content validity, good criterion-related validity, adequate discriminant validity, and high internal reliability. This research utilised the WISA scale to explore sensitivity differences across eight information types: four concerning living individuals (Personal, Health, Financial & Lifestyle) and four organisationally-focused information types (IP, day to day, commercial & HR). Financial information was found to have the highest ratings for overall sensitivity followed by health and HR. Finally, scores for the WISA scale predicted a range of security behaviours including password usage, secure Wi-Fi usage, physical security and avoiding security risks. This demonstrates the potential role for information sensitivity appraisal as a determinant of security behaviours.

Background

Organisations are under constant attack from internal and external threats that put the integrity, availability and confidentiality of their information at risk. In the UK, four in ten businesses (39%) and a quarter of charities (26%) reported cyber attacks in 2021 (Department for Digital, Culture, Media, & Sport, 2021). This was highest among medium businesses (65%), large businesses (64%) and high-income charities (51%). The implications of security breaches are vast, including service disruption, reputational damage, and extensive financial damage. Recent findings suggest that cyber attacks are growing in frequency and severity (Hiscox, 2019), and are projected to account for a global cost of $6 trillion by the end of 2021 (Cybersecurity Ventures, 2019; Lallie et al., 2021). Organisations adopt technical, procedural and human defences to protect against security threats. Employees play a large role in cyber security as their behaviour is estimated to account for a considerable portion of security breaches (Dhillon & Moores, 2001; Mitnick & Simon, 2003; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005; Vroom & Von Solms, 2004). An analysis of data published by the UK Information Commissioner's Office identified that 64% of reported information security incidents and breaches across all sectors were likely to be the result of human error (Evans, He, Maglaras, Yevseyeva, & Janicke, 2019). There is a need to understand the role that improved employee security behaviours can play in the defence of organisational information security.

It is important that research looks to understand the range of factors that can influence the security behaviours of employees. One such approach is to study the relationship between information sensitivity and security behaviours in the workplace (Blythe, 2015). Securely guarding sensitive information is a goal of all organisations in order to minimize the threat of data breaches. Although there has been limited research exploring the direct link between information sensitivity and security in the workplace, Adams and Sasse (1999) found that employees perceived sensitive information as requiring more protection

* Corresponding author. Department of Psychology, Northumberland Building, Northumbria University, Newcastle, NE1 8SG, United Kingdom.
E-mail address: richard6.brown@northumbria.ac.uk (R. Brown).

https://doi.org/10.1016/j.chbr.2022.100240
Received 12 May 2022; Received in revised form 3 October 2022; Accepted 5 October 2022
Available online 9 October 2022

and security than other types. They found that confidential information about individuals (personnel files and emails) were rated as sensitive, whereas commercially-orientated information (such as customer databases and financial data) were often seen as less sensitive and consequently needing less protection. These perceptual differences can impact security behaviours. For example, the sensitivity of data has been found to have an impact on password re-use (Grawemeyer & Johnson, 2011), suggesting that users do consider the sensitivity of the data stored on a service and adjust their security behaviour accordingly.

A significant challenge in the study of perceptual differences in information sensitivity is that there is no clear consensus as to what constitutes sensitive information. In the UK, the protection of citizen's information is regulated by the Information Commissioner's Office and governed by the Data Protection Act (DPA; 2018). This is the UK's implementation of the General Data Protection Regulation (GDPR). The act seeks to control how individuals' personal data is used by businesses and specifies different levels of protection for sensitive personal data. Personal data means any information relating to an identified or identifiable living individual. The act goes on to describe how the processing of personal data would be considered sensitive where it relates to the following factors: racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, or of biometric data, for the purpose of uniquely identifying an individual, data concerning health, data concerning an individual's sex life or sexual orientation. However, despite the breadth of this categorisation, the legal framework for sensitive information does not easily translate into a theoretical account of the central constructs that encompass the nature of sensitive information.

Within the research domain, the majority of studies do not provide a clear theoretical account of what may be driving individual appraisals of information sensitivity. However, there are two clear divides in the way that research has conceptualised information sensitivity. Some accounts focus on the privacy and intimacy of information as a basis for evaluating sensitivity. For example, Weible (1993) defines information sensitivity as "*the level of privacy concern an individual feels for a type of data in a specific situation.*" Sheehan and Hoy (2000) present a broader definition and argue that information sensitivity is simply the distinction between what is private and what is not private. Other researchers consider sensitivity to relate to intimate self-disclosures. For example, Lwin, Wirtz, and Williams (2007) define information sensitivity as the perceived intimacy level of information and Moon (2000) defines intimate self-disclosures as those information types that are high-risk and heighten vulnerability if disclosed. The second type of definition focuses more on the vulnerability and potential exploitative nature of information as a basis for evaluating sensitivity. For example, Gandy Jr (1993) argues that some people view sensitive information as any information that if disclosed would likely cause them harm. Mothersbaugh, Foxx, Beatty, and Wang (2012) also define perceived sensitivity as potential losses associated with disclosing information. More recently Sun, Liu, and Wang (2017) have defined information sensitivity as the extent to which information is perceived as sensitive due to the potential for loss as a result of its disclosure. In summary, the range of potential definitions for information sensitivity broadly reflects the following two dimensions: 1) the perceived *privacy* that an individual ascribes to data in a given context, and 2) the anticipated negative *consequences* that an individual associates with the potential disclosure of information.

There is currently a lack of empirical studies investigating information sensitivity and its role in employee security behaviour. A lack of conceptual consensus in the literature has resulted in a shortage of scales measuring how individuals appraise information sensitivity. This absence of empirical measurement is likely the reason that information sensitivity is considered a neglected construct within the privacy and security domain (Kokolakis, 2017). This is unfortunate, as it has further been suggested that information sensitivity may play an important role in explaining privacy behaviours and related phenomena, such as the privacy paradox (Mothersbaugh et al., 2012). Since individuals process information differently based on distinct perceptions of informational qualities, it may be appropriate to measure sensitivity of information by scaling users' perceptions rather than indiscriminately dividing levels of sensitivity based on general information types (Sun et al., 2017).

There is currently no widely accepted scale that measures information sensitivity within the workplace. Previous studies exploring information sensitivity have largely used scales investigating willingness to disclose (Cranor, Reagle, & Ackerman, 2000) or privacy concerns (Buchanan, Paine, Joinson, & Reips, 2007; Preibusch, 2013). However, none of these directly investigate how individuals evaluate information sensitivity in the workplace. In this article, we attempt to address this gap in the security literature by returning to previous doctoral research: *Information Security in the Workplace: A Mixed-Methods Approach to Understanding and Improving Security Behaviours* (Blythe, 2015). Given the growing threat of cyber attacks faced by organisations, and the central role of human error in security, we believe that repositioning the previous findings of Blythe (2015) presents the opportunity for researchers to employ a useful scale for measuring workplace information sensitivity. By presenting the merits of the scale as a standalone contribution to the literature, we hope that it may be used to better understand the relationship between the appraisal of information sensitivity and subsequent security behaviours. Therefore, this research will: 1) describe the development and validation of a measure aimed at capturing employees' assessment of information sensitivity, the Workplace Information Sensitivity Appraisal (WISA) scale (Blythe, 2015), and 2) discuss the application of the WISA scale to investigating differences in sensitivity by information type, and as a predictor of multiple security behaviours.

Method

Item generation and reduction

Existing literature on information sensitivity was first consulted to aid item generation. This highlighted the central components of information sensitivity as being the degree of privacy concern experienced by the individual (Sheehan & Hoy, 2000; Weible, 1993) and the potential for negative consequences associated with the disclosure of specific information (Gandy Jr, 1993; Mothersbaugh et al., 2012; Sun et al., 2017). This deductive approach for generating scale items outlined by Hinkin (1998) is deemed most suitable when there are sufficient theoretical grounds on which to base the generation of items. However, given the discussed lack of previous research on information sensitivity, specifically in the workplace, this approach was not used in isolation. Therefore, the current study used a combination of inductive and deductive approaches to enhance item generation. Items were also generated using verbal extracts from a qualitative study exploring factors that most influence workplace security behaviours (Blythe, 2015). This qualitative study used a semi-structured approach of vignette based one-to-one interviews, followed by a framework analysis to suggest a range of factors that influence security behaviours. This qualitative study involved a purposeful sample of 20 participants recruited from two organisations (a university & industry research institution) from the North of England and South of Scotland. This qualitative analysis allowed the research team to identify four themes of information sensitivity: *the private nature of information*, *the potential consequences associated with information*, *the value of information*, and *the perceived (third party) interest in information*. The four themes informed the creation of the initial survey items and would subsequently be used to help define extracted scale factors. An initial 22 items were generated with respect to these four dimensions (see Table 1 for initial 22 items). These items were devised in accordance with recommendations from Hinkin (1998) to ensure the use of short and simple questions and to avoid the use of double-barrelled statements and leading questions. Reverse-scored items were also included to help reduce response bias. A consistent rating scale from "*strongly disagree to strongly agree*" was implemented across the initial four areas of the WISA appraisal in

Table 1
Factor loadings for each item (factor loadings lower than 0.30 are suppressed).

Item	Rotation Factor Loadings				
"I think [information type] is …"	Factor 1: *Privacy*	Factor 2: *Worth*	Factor 3: *Consequences*	Factor 4: *Low proximity interest*	Factor 5: *High proximity interest*
• Confidential	.897				
• Private	.898				
• Secret	.850				
• Restricted	.761				
• Privileged	.656				
• Insignificant[a]		.834			
• Meaningless[a]		.895			
• Worthless[a]		.890			
• Embarrassing			.869		
• Compromising			.753		
• Discreditable			.656		
• Humiliating			.866		
• Of interest to my friends					.941
• Of interest to my family					.946
• Of interest to business competitors				.895	
• Of interest to criminals				.861	
• Of interest to fellow employees				.755	.360
Eigenvalues	4.89	3.37	2.72	1.52	1.06
• Sensitive	.723	.451			
• Valuable	.433	.733			
• Important	.553	.685			
• Exploitable		.359	.601	.359	
• Of interest to the general public				.670	.514

[a] Reversed scored.

response to previous research that has highlighted prior difficulties in combining scores from different rating scales (Gliem & Gliem, 2003).

Study design

A non-experimental survey design was employed to validate the WISA scale (see Fig. 1). The following approach was used to explore the validity and reliability of the scale in accordance with previous recommendations for developing novel measures (Hinkin, 1995, 1998).

Participants

An opportunity sample of 326 (Age, M = 31.75, SD = 11.51) individuals were recruited online between August and November 2014. All recruited participants were in full-time or part-time employment or unemployed for less than three months. Our sample included 87 males and 217 females (22 participants chose not to disclose their gender), with an average (mean) organisational tenure of 5.23 years (SD = 6.66) and job tenure of 3.18 years (SD = 4.7). Of our sample, 11% (34) were from a microenterprise (less than ten staff), 13% from a small enterprise (less than 50 staff), 9.2% from a medium-sized enterprise (less than 250 staff) and 61% from a large organisation (more than 250 staff). Participants were recruited using a variety of platforms based on recruitment recommendations from Branley, Covey, and Hardey (2014) which included dedicated participation sites (e.g. callforparticipants.com), social media (e.g. Facebook, Twitter, LinkedIn), mailing lists, student participation pools and websites and forums. A snowballing sampling technique was employed in order to maximise recruitment. As compensation for study completion, participants were entered into a prize draw to win an iPad or, if they were university students, they received institutional participation points.

Information types

The WISA scale was validated across eight information types. Potential information types were suggested by the lead researcher and

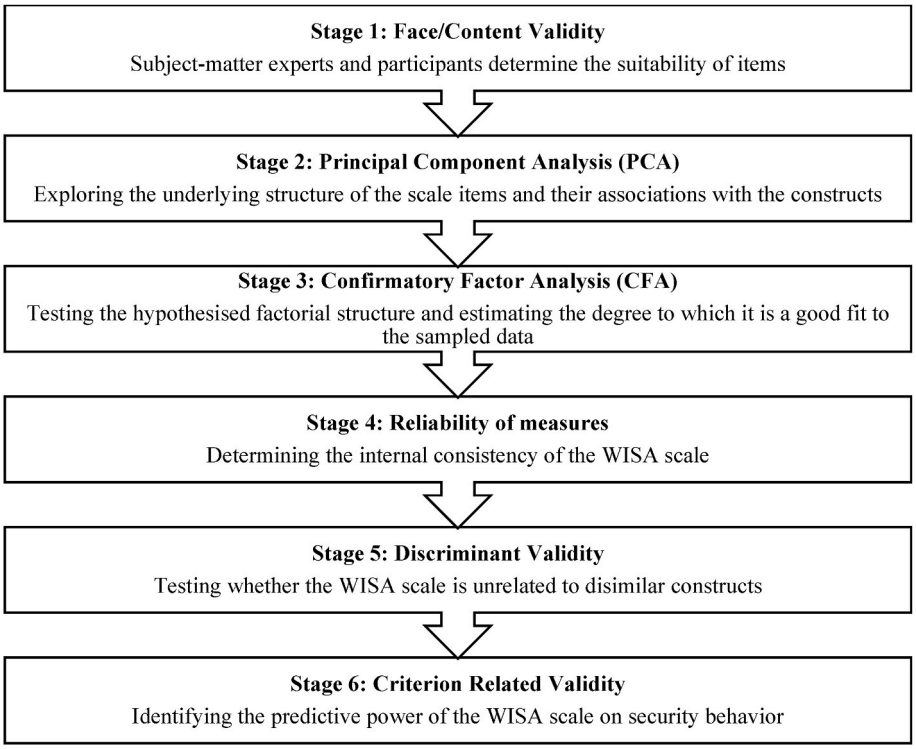

Fig. 1. The process of assessing the validity and reliability of the WISA scale.

reviewed and modified by other members of the research team. The resulting categorisation distinguishes between two general types of information. The first is information about living individuals, replicating the four information types proposed by Little, Briggs, and Coventry (2011): *personal information* (e.g. address, gender, date of birth, marital status), *health information* (e.g. physical and mental health history, weight, family medical history), *financial information* (e.g. banking details, credit rating, loan history) and *lifestyle information* (e.g. shopping habits, hobbies, interests). The focus of the items refers to other individuals' information, rather than the employee's own information to capture the broader perceived sensitivity information. The second general information type refers to organisationally-owned information: *intellectual property* (e.g. trade secrets, creative ideas that could lead to patents, copyrights, new products), *day-to-day business information* (e.g. current customer & supplier details, quotes, purchase history, call records), *commercial information* (e.g. strategic plans, business financial data) and *personnel/HR information* (e.g. appraisal, disciplinary information, salary, sickness records). Participants were asked to respond to each of the proposed items of the WISA scale for all eight information types.

The WISA scale and participant instructions are shown in Fig. 2 below (note that during the validation of the WISA scale participants responded to six items that were subsequently removed from the final scale, identified as 'removed items').

Instructions

- *The following statements are about different types of information that may be stored by your organisation.*
- *Read each statement carefully and please rate the extent to which you agree with the statements using a rating scale from 'strongly disagree' to 'strongly agree'.*

Information types

- Personal information about other people (e.g. address, gender, date of birth, marital status)
- Health information about other people (e.g. physical and mental health history, weight, family medical history)
- Lifestyle information about other people (e.g. shopping habits, hobbies, interests)
- Financial information about other people (e.g. banking details, credit rating, loan history)
- Information about or relating to intellectual property (e.g. trade secrets, creative ideas that could lead to patents, copyrights, new products)
- Day-to-day business operation information (e.g. current customer & supplier details, quotes, purchase history, call records)
- Commercial business information (e.g. strategic plans, financial business data)
- Personnel / HR information (e.g. appraisal, disciplinary info, salary, sickness records)

WISA Scale Survey Task

"I think [information type] is…"	*Strongly Disagree*	*Disagree*	*Neither Agree nor Disagree*	*Agree*	*Strongly Agree*
• Secret	☐	☐	☐	☐	☐
• Private	☐	☐	☐	☐	☐
• Insignificant	☐	☐	☐	☐	☐
• Humiliating	☐	☐	☐	☐	☐
• Of interest to fellow employees	☐	☐	☐	☐	☐
• Meaningless	☐	☐	☐	☐	☐
• Worthless	☐	☐	☐	☐	☐
• Of interest to business competitors	☐	☐	☐	☐	☐
• Of interest to criminals	☐	☐	☐	☐	☐
• Embarrassing	☐	☐	☐	☐	☐
• Discreditable	☐	☐	☐	☐	☐
• Confidential	☐	☐	☐	☐	☐
• Of interest to my family	☐	☐	☐	☐	☐
• Of interest to my friends	☐	☐	☐	☐	☐
• Restricted	☐	☐	☐	☐	☐
• Compromising	☐	☐	☐	☐	☐
Removed Items					
• ~~Privileged~~	☐	☐	☐	☐	☐
• ~~Sensitive~~	☐	☐	☐	☐	☐
• ~~Valuable~~	☐	☐	☐	☐	☐
• ~~Important~~	☐	☐	☐	☐	☐
• ~~Exploitable~~	☐	☐	☐	☐	☐
• ~~Of interest to the general public~~	☐	☐	☐	☐	☐

Fig. 2. WISA Scale and participant instructions.

Additional measures

Organisational Citizenship Behaviour. The Organisational Citizenship Behaviour (OCB) scale was used to assess the discriminant validity of the WISA scale. We used the OCB-O subscale by Lee and Allen (2002). The OCB-O scale was found to have strong internal reliability, Cronbach's α = .89. The importance of OCB has been demonstrated in occupational psychology literature and has been found to have many positive consequences for organisations, such as increased job performance (MacKenzie, Podsakoff, & Ahearne, 1998; Podsakoff & MacKenzie, 1997). The scale consists of eight items and all items were measured on a seven-point scale that ranged from one (never) to seven (always) in which participants indicated the extent to which they perform the citizenship behaviours.

Security behaviour. A measure of security behaviour was used to assess the criterion validity of the WISA scale. Security behaviour was measured using a 16 item self-developed scale based on best practice security behaviours identified in a report for the Department for Business, Innovation and Skills (Coventry, Briggs, Blythe, & Tran, 2014). Behaviours were worded to explicitly target the workplace setting (e.g. "*I share passwords with other people at work*"). The behaviours comprised access control, software updates, *anti*-malware, physical behaviours and reporting behaviours. The scope of the scale was broad to encompass the different working conditions employees may face. The security behaviour scale had strong internal reliability, Cronbach's α = 0.85. All items were measured on a seven-point scale that ranged from one (never) to seven (always) in which participants indicated the extent to which they perform security behaviours in a workplace setting.

Results

We present the following results for 1) an assessment of the validity and reliability of the Workplace Information Sensitivity Appraisal (WISA) scale, and 2) the application of the WISA scale to investigate differences in sensitivity by information type, and as a predictor of multiple security behaviours.

Assessing the validity and reliability of the WISA scale

Stage 1: Face/Content validity. The content validity of the scale was assessed using subject-matter experts as well as naïve participants to evaluate the suitability and comprehensibility of selected items. A workshop with subject-matter experts revealed that the items were suitable for measuring the construct of information sensitivity. Ten participants were recruited as naïve subjects to assess the items. In a card sorting activity, they were presented with the questionnaire items and asked to sort the items into clusters they felt most represented the items. This procedure was informed by previous research (MacKenzie, Podsakoff, & Fetter, 1991). This confirmed that the generated items were representative of the qualitatively identified themes of information sensitivity taken from the previously described vignette-based interviews and theoretical background. Participants were asked to define their categories. Definitions were not initially provided to participants in order to gain a deeper understanding of how participants interpreted the items. This procedure allowed for a more thorough analysis of the initial items and dimensions beyond what is typically produced by a simple cognitive sorting task akin to traditional card sorting with definitions (Anderson & Gerbing, 1991). Participants were also asked to comment on the clarity and complexity of the questionnaire instructions and initial items. Finally, participants were asked to provide additional examples of types of information they would classify under the eight target information types. The results showed that 60% of participants indicated that survey items were representative of the same themes of information sensitivity as those identified by the research team, this falls below the acceptable agreement index of 75% (Hinkin, 1998). This was to be expected as participants were not provided with the definitions. Therefore, another four participants were recruited to conduct a simple card sorting task with definitions in which 100% sorted them into their respective themes. Changes were made to the instructions and definitions of the information types following the one-to-one sessions to improve the usability and comprehensibility of the questionnaire.

Stage 2: Principal Component Analysis. To explore the factor structure of information sensitivity appraisal, Principal Component Analysis (PCA) was performed using varimax with Kaiser normalization. The initial 22 items were entered into the analysis and factor loadings lower than 0.30 were suppressed (see Table 1). The findings from the PCA revealed that five factors (eigenvalues were above 1) could explain the data accounting for 79.73% of the variance. This complied with the minimum acceptable level of 60% variance and recommendations of eigenvalues above one for factors (Hinkin, 1998). All items loaded onto their designated factor above the accepted .40 criterion level. The four previously identified qualitative themes of information sensitivity were used to label the proposed factors: *the private nature of information*, *the potential consequences associated with information*, *the value of information*, and *the perceived (third party) interest in information*. The fourth theme *"interest by others"* was considered relevant to two distinct factors. Factor four from the PCA was assigned to those recipients of information that may be considered to be low proximity to individuals (i.e. business competitors, criminals and fellow employees). Factor five, on the other hand, was assigned to those recipients of information which are in high proximity to individuals (i.e. family and friends). The PCA also revealed five items that cross-loaded onto multiple factors and these were removed (see Table 1) as their values were above 0.4 (Hinkin, 1998). "*I think < information type> is of interest to fellow employees*" was left in the analysis as the cross-loading was less than 0.40 on the second factor (Hinkin, 1998). Overall, the PCA revealed that five factors explained a large amount of the variance in the data and the items had strong factor loadings (above 0.40).

Stage 3: Confirmatory factor analysis. CFA was carried out on the data using AMOS (version 22) to explore the factor structure and estimate the degree to which the model was a good fit to the data. The five factors were presented as latent variables within AMOS and were permitted to co-vary. The items for each factor were only allowed to load onto their respective factor. Covariance between error terms was only allowed where items were related to the same factor, pursuant to advice from modification indices within AMOS. The item "*privileged*" was removed as it shared too much covariance across factors, had the lowest factor loadings and was deemed non-specific within the privacy factor. Fig. 3 shows the average standardised item loadings for the hypothesised model.

Maximum likelihood estimation methods were used and the input for each analysis was the covariance matrix of the items. The goodness-of-fit for the models was evaluated with the following absolute goodness-of-fit indices: 1) the X^2 goodness-of-fit statistic, 2) the Root Mean Square Error of Approximation (RMSEA), 3) the Goodness of Fit Index (GFI), and 4) the Adjusted Goodness of Fit Index (AGFI). Non-significant X^2 values indicate that the hypothesised model fits the data and RMSEA values smaller than or equal to 0.08 are indicative of acceptable fit. However, values above 0.1 should lead to model rejection (Browne & Cudeck, 1992). GFI values greater than 0.95 are indicative of good fit and values greater than 0.90 are indicative of an acceptable fit (Marsh & Grayson, 1995). AGFI values of 0.90 are indicative of a good fit and values greater than 0.85 may be considered an acceptable fit (Hu, Bentler, & Hoyle, 1995). The final model indicated an acceptable level of fit for three of the four fit indices and this was evident across all eight information types (see Table 2). The fit indices for GFI and AGFI were all above 0.9 and 0.85 and the RMSEA were all below 0.08. The chi-square indicated that the model was not a good fit to the data for all information types, however, chi-squared has been criticised for being too sensitive to large sample sizes, especially for samples over 200 (Hoe, 2008), as in the current study. The model had the best fit for intellectual property and the least best fit for financial information. However, it was an acceptable

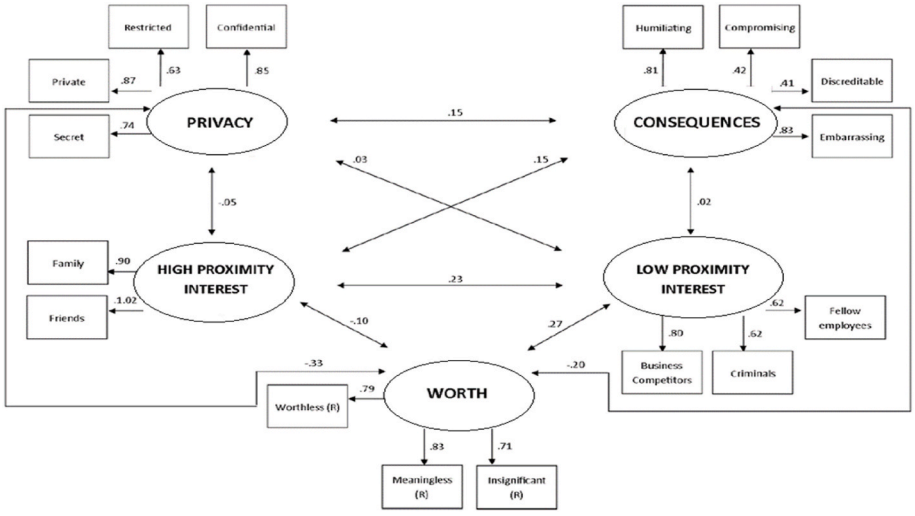

Fig. 3. WISA Appraisal Confirmatory Factor Analysis with average Item Loadings.

Table 2
Goodness-of-fit indices for WISA appraisal for eight target information types.

Information type	X^2	RMSEA	GFI	AGFI
Personal	x^2 (92) = 201.456, p < .001	.061	.926	.890
Health	x^2 (92) = 211.818, p < .001	.065	.921	.883
Lifestyle	x^2 (92) = 216.460, p < .001	.065	.928	.893
Financial	x^2 (92) = 252.166, p < .001	.073	.907	.862
Intellectual Property	x^2 (92) = 179.095, p < .001	.054	.939	.910
Day to Day	x^2 (92) = 170.270, p < .001	.051	.941	.913
Commercial	x^2 (92) = 223.679, p < .001	.066	.923	.887
HR	x^2 (92) = 189.792, p < .001	.057	.931	.898

fit for all types. Therefore, the WISA appraisal was considered to be an acceptable model to explain the data.

Stage 4: Internal Reliability. The final WISA scale comprises of 16 items. The majority of WISA subscales across the eight information types demonstrated an acceptable alpha level normally deemed to be 0.70 or above (Hinkin, 1998; Kline, 2013). A small number of subscales fell short of this 0.70 level, however these items were still above the 0.65 level considered to be at the lower end of the acceptable level for new scales (Hair, Black, Babin, Anderson, & Tatham, 2006) (see Supplement Table S3 for full reliability statistics for each WISA subscale across eight information types).

Stage 5: Discriminant validity. The findings revealed that three of the five aspects of the WISA scale were statistically unrelated to organisational citizenship behaviour, therefore, providing partial support for discriminant validity for the WISA scale. Correlations between WISA factors and organisational citizenship behaviour were all either low or statistically insignificant: Privacy ($r = .14$, $p < .05$), Worth ($r = 0.15$, $p < .05$), Consequences ($r = 0.02$, $p > .05$), High Proximity ($r = -0.04$, $p > .05$), and Low Proximity ($r = 0.04$, $p > .05$). See Supplement Tables S1–2 for descriptive statistics for organisational citizenship and security behaviour, and correlations between WISA components and OCB.

Stage 6: Criterion-related validity. Multiple regressions were performed to explore the predictive validity of the WISA scale in explaining security behaviour. The multiple regression model revealed that $r^2 = 0.089$, F(5, 287) = 5.586, p < .001 indicating that the WISA scale accounts for 8.9% of the variance in the composite measure of security behaviour. Three of the five WISA components (Worth, Consequences & Low proximity) were found to significantly contribute to the model (see Table 3). Further analyses were conducted to estimate the degree to which the WISA scale predicts individual security behaviours (discussed below, see Table 4). Overall, the WISA scale explains some of the variance in security behaviour, therefore, demonstrating reasonable criterion-related validity.

Table 3
Tests of significance for the predicted variable of security behaviour from the predictors of the WISA appraisal.

Predictor variable	*β*	*B*	*SE B*	*p*
WISA Privacy	.100	1.454	.918	p = .114
WISA Worth	.143	2.562	1.138	p < .05[a]
WISA Consequences	−.125	−1.887	.906	p < .05[a]
WISA High Proximity	.075	−.729	.578	p = .208
WISA Low Proximity	.140	1.616	.692	p < .05[a]

[a] p < .05; **p < .01.

Table 4
Regressions with specific security behaviours and the variance explained by WISA scale results.

Behaviour	Regression	Variance explained
• I use complex passwords at work	r^2 = .106, F(5, 287) = 6.807, p < .01.	10.6%
• I use different passwords for different work accounts	r^2 = .056, F(5, 287) = 1.115, p < .01.	5.6%
• I use trusted and secured connections, and devices (including Wi-Fi) when at work	r^2 = .086, F(5, 286) = 5.361, p < .01	8.6%
• I use trusted and secure websites and services at work and connect securely	r^2 = .075, F(5, 287) = 4.670, p < .01	7.5%
• I stay informed about security risks online and in the workplace	r^2 = .050, F(5, 287) = 3.019, p < .05	5%
• I avoid security risks online and in the workplace	r^2 = .068, F(5, 286) = 4.198, p < .05	6.8%
• I am aware of my physical surroundings when online at work	r^2 = .099, F(5, 287) = 6.281, p < .01	9.9%
• I adjust account settings on websites that I use at work	r^2 = .040, F(5, 287) = 2.384, p < .05	4%
• I lock my computer when I leave my workstation	r^2 = .032, F(5, 287) = 1.897, p = .095.	3.2%

Findings from the application of the WISA scale

Sensitivity appraisal differences by information type. An eight (information type) by five (WISA appraisal) repeated measures ANOVA was conducted to explore differences in ratings for the eight information types. There was a significant main effect of WISA appraisal on

sensitivity ratings ($F(3.17, 994.48) = 438.924$, $p < .001$) with Greenhouse-Geisser correction. Post-hoc analyses indicated that there was a significant difference in ratings between all WISA types. Worth had the highest ratings ($M = 4.12$), followed by privacy ($M = 3.94$), low proximity interest ($M = 3.24$), consequences ($M = 2.81$) and finally, high proximity interest ($M = 2.35$). There was also a significant main effect of information type on rating ($F(5.73, 1799.27) = 92.435$. $p < .001$) with Greenhouse-Geisser correction. Post-hoc analyses indicated that financial information had the highest ratings ($M = 3.49$), followed by health information ($M = 3.48$), HR information ($M = 3.44$), intellectual property ($M = 3.34$), commercial information ($M = 3.24$), personal information ($M = 3.18$), day to day business information was second lowest for sensitivity ratings ($M = 3.14$), and lifestyle information was the lowest for ratings ($M = 3.04$; see supplement, Table S5).

There was a significant interaction effect of information type and WISA appraisal on ratings ($F(16.46, 5169.106) = 110.43$. $p < .001$) with Greenhouse-Geisser correction. Fig. 4 suggests that there appears to be a consistent trend in the order of the information types across privacy, worth and consequences. This ordering appears to change for high and low proximity interest, particularly for the information types of financial and HR for high proximity interest, and commercial and day to day for low proximity interest. Financial, HR and health were the three information types to be amongst the highest for privacy, worth and consequences dimensions whereas commercial, day to day, and personal are amongst the lowest for these three dimensions. Intellectual Property is amongst the highest for privacy and worth, and lifestyle amongst the lowest. However, this observation reverses for the consequences dimension. Intellectual property is considered to be highly private and has high worth but consequences of its disclosure are not perceived as severe. Lifestyle information is not perceived as highly private and having high worth, but it may have consequences if disclosed. For perceived interest in information, intellectual property is the only information type to be amongst the highest for high and low proximity interest. Health, lifestyle and personal information were considered to be of interest to high proximity groups whereas commercial, day to day and financial were perceived to be of interest to low proximity groups (see Supplement Figs. S1–5 for mean sensitivity ratings for each WISA subscale by information type).

Predicting specific security behaviours. The results from our sample found that employees reported engaging in some security behaviours more than others. For example, employees reported high adherence with not sharing passwords with others, and using trusted and secured connections when at work. However, employees reported low adherence with security behaviours such as scanning for available software updates, and running anti-virus and *anti*-spyware software at work (see supplement, Table S1, for descriptive statistics for individual security behaviours). Further analyses were conducted to estimate the degree to which the WISA scale predicts individual security behaviours. Table 4 shows that the WISA scale best predicts security behaviours relating to access control and physical security. Specifically, WISA scale scores predicted 11% of the variance in the reported use of complex passwords in the workplace and 10% of the variance of the perceived awareness of physical surroundings when online at work.

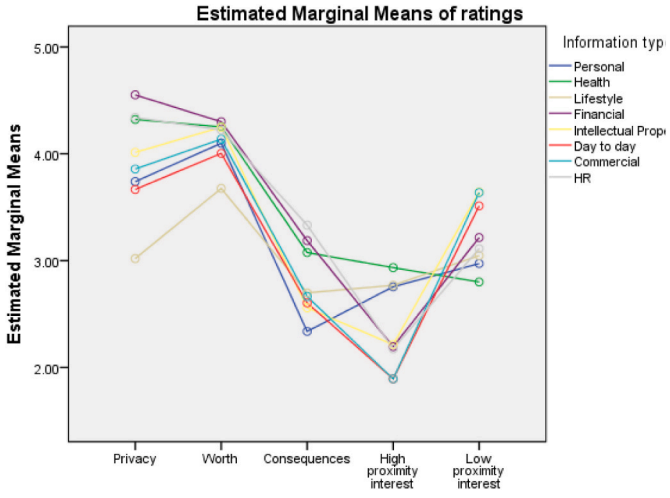

Fig. 4. Line graph of ratings for each information type.

Discussion

This article is an attempt to address the lack of scales measuring information sensitivity by returning to previous doctoral research: *Information Security in the Workplace: A Mixed-Methods Approach to Understanding and Improving Security Behaviours* (Blythe, 2015). We highlight the development and validation of a measure for information sensitivity to be used within a workplace setting. The resulting 16-item scale has five sub-scales: *privacy*, *worth*, *consequences*, *low proximity interest* and *high proximity interest*. The WISA scale, alongside its five subscales was found to have strong factorial validity which was confirmed across eight information types. The scale also had good criterion-related validity and was found to significantly predict security behaviour. Finally, the scale was found to have adequate discriminant validity as three of the five aspects of the WISA scale were found to be unrelated to organisational citizenship behaviour. This research sought to add further understanding to defining information sensitivity. The revised WISA structure was found to be a strong fit to the data for the eight target information types which suggests that this definition of information sensitivity provides a valuable contribution to the literature. This knowledge might be useful for how we conceptualise information sensitivity in future research and within government legislation such as the Data Protection Act (2018). Finally, scores for the WISA scale were found to predict a range of specific security behaviours including password usage, secure Wi-Fi usage, physical security and avoiding security risks. This demonstrates the potential role of information sensitivity appraisal as a determinant of protective actions in the workplace. We discuss our findings alongside early applications of the WISA scale in recent research.

Information sensitivity differences by type

Financial information was found to have the highest ratings for sensitivity followed by health and HR. These aspects were also found to be the highest for three of the five sensitivity ratings: privacy, worth and consequences. Previous qualitative findings have reported that employees typically rate information about individuals to be more sensitive than organisational information (Blythe, 2015). The findings from the application of the WISA scale support these qualitative findings, however not all information types are considered sensitive. For example, lifestyle information overall had the lowest ratings for sensitivity. This difference in information sensitivity with regards to individuals' data supports previous research by Cranor et al. (2000) which found that individuals were willing to disclose lifestyle information but not willing to disclose financial information. Further research by Mothersbaugh et al. (2012) on information disclosure found that sensitivity works along a continuum with demographic and lifestyle factors being the information people are most willing to disclose and personal identifiable and financial information as least willing to disclose. Our research supports this literature, however, it adds a further level of understanding by exploring how individuals make this appraisal of sensitivity by considering its perceived privacy, worth, consequences and perceived interest by high and low proximity others and if it affects security behaviour.

The development of the WISA scale allows one of the first investigations of how individuals appraise the sensitivity of organisationally-focused information. Previously, the findings by Adams

and Sasse (1999), highlighted that people rate some information about individuals as more sensitive than organisational information. Information regarding health and financial data is consistently viewed as sensitive across the dimensions of privacy, worth and consequences. Likewise, HR information about individuals is also considered sensitive across these dimensions. Personal and lifestyle information, whilst they refer to individuals' information are not considered sensitive for privacy, worth and consequences. Commercial and day to day organisationally-focussed information were consistently low for privacy, worth and consequences. Intellectual property was the only information type that did not relate to individuals but was highly rated for privacy, worth, high proximity and low proximity interest. Intellectual Property was not highly rated for consequences and this was the same for other organisational information. There are a number of possible reasons for this finding; firstly this study defines consequences as humiliating, compromising, discreditable, and embarrassing, which individuals may not associate with information that is not about people. This could reflect the decline in sensitivity rating for consequences when comparing the two broad information types of organisational-focussed and individual-focussed. A second potential explanation could be that individuals lack awareness of consequences associated with organisational information and, therefore, rate them lower. Our research confirms both the findings from Adams and Sasse (1999), as well as previous qualitative research into factors that influence security behaviours (Blythe, 2015), and shows that employees do consider some forms of organisational-focussed information to be sensitive i.e. intellectual property. This suggests that a binary judgement is not sufficient for understanding how information sensitivity is appraised and therefore recommends the use of the WISA scale to capture the five components shown to reflect information sensitivity.

The main difference between individually-focussed information and organisational-focussed is the perceived high or low proximity interest. High proximity and low proximity interest revealed some interesting findings with regards to differences in the two broad information types. Information about individuals (e.g. personal, health and lifestyle) was considered to be of interest to employees' high proximity interest groups (i.e. family and friends) in comparison to organisational-focussed information as well as financial and HR information. For low proximity interest, the opposite effect is apparent with organisational-focussed information (intellectual property, commercial and day to day) perceived to be of interest to low proximity groups (i.e. criminals, fellow employees & business competitors). There is limited previous research that looks at this form of sensitivity appraisal, the inclusion of which was driven by previous qualitative findings which suggested that employees consider the audience (or interest) in information that they work with and use this as a basis to evaluate the sensitivity of the information (Blythe, 2015). The current study contributes novel findings that suggest that future research may need to further explore perceived interest in information sensitivity conceptualisations.

Information sensitivity predicts security behaviours

The WISA scale was shown to significantly predict security behaviours, explaining approximately 10% of the variance in the composite security behaviour measure. When exploring the role of information sensitivity on individual security behaviours, the WISA scale was found to explain between 8 and 10% of the variance for use of complex passwords, secure Wi-Fi and awareness of physical surroundings when at work. This indicates that the WISA scale may be more effective in accounting for some security behaviours in comparison to others, and that further research may help to identify those behaviours most closely associated with appraisals of information sensitivity. This is promising as it suggests that using the WISA scale as a measure of information sensitivity may help to increase our understanding of the determinants of multiple security behaviours.

The WISA scale has been further used to study factors that influence employee *anti*-malware behaviours (Blythe & Coventry, 2018). An online cross-sectional survey of 526 employees was used to identify factors that influence intentions to perform three *anti*-malware behaviours. The consequences factor of the WISA scale was reported to predict unique variance in behaviour and was a significant predictor of Anti-malware software behaviour (scanning USB sticks with *anti*-malware software). This suggests that employees who have a greater perception that the disclosure of the data they work with may lead to negative consequences (such as compromising and discreditable) intend to scan USB sticks with *anti*-malware software to protect the information. This was the first study to specifically explore the role of workplace information sensitivity appraisal for a specific security threat and sub-set of behaviours. The WISA scale has also been adapted to capture the perceived sensitivity of health and lifestyle data in a study concerning the sharing of health data by 250 UK participants living with long-term health conditions (Brown, Coventry, et al., 2022). The WISA scale was implemented as part of broader efforts to understand patient perceptions and behaviours surrounding health and lifestyle data (Brown, Sillence, et al., 2022; Simpson et al., 2021). Total WISA scale scores were moderately associated with greater perceived risk, as well as increased concern for trust, identity, privacy and security issues related to the sharing of health and lifestyle data. WISA scale scores were also significantly higher among participants who reported having experienced stigma as a result of their condition. Of the individual WISA factors, privacy was negatively associated with overall willingness to share health and lifestyle data with others. The consequences factor was strongly associated with overall perceived risk from sharing health and lifestyle data with others. Finally, higher scores on the 'high proximity interest' factor were associated with more frequent sharing of health data with others and greater overall willingness to share. This study suggests that the WISA scale provides a useful measure for capturing perceptions of information sensitivity relevant to self-generated health and lifestyle data. Further validation of the scale will provide more evidence for its potential utility for use within the workplace setting and beyond, and for future research focussing on information sensitivity.

Limitations

A limitation of the current study is that it is dependent on data and analysis from previous doctoral research (Blythe, 2015) that did not sufficiently explore the influence of personal characteristics on the appraisal of information sensitivity. It is possible that the gender imbalance in our sample (87 males and 217 females) may have influenced our findings. Further research may look to recruit population representative samples (as opposed to our use of snowball sampling) in order to investigate the potential role that features such as age, gender and additional personal characteristics may play in assessing the sensitivity of workplace information.

Convergent validity could not be assessed. Convergent validity is important as it measures the degree to which the current scale is correlated with scales that claim to measure the same construct (i.e. information sensitivity) (Onwuegbuzie, Daniel, & Collins, 2009). Previous research (Cranor et al., 2000; Malhotra, Kim, & Agarwal, 2004) have used related measures of information sensitivity. However, these were not considered adequate as they had not been under validation assessment nor did they measure information sensitivity in the workplace or were related to assessing information that is not about oneself. Furthermore, they measure the information sensitivity of consumers'

own information and there are potential ownership and framing issues when used in comparison to the construct measured within the current study. However, despite this limitation, the current study provides a solid basis for further scale refinement and development for measuring information sensitivity within the workplace.

Finally, it is noted that the 'Worth' factor of the WISA scale consisted of the three items that were reverse scored. It is possible that these items loaded onto the same factor due to their scoring structure. Future iterations of the WISA scale may chose to not use reverse scoring with respect to these three items to explore whether or not they still load onto the same 'Worth' factor.

Conclusion

There is currently no consensus on defining information sensitivity within the security literature. The WISA scale was developed in response to this gap in the literature and to present a novel measure of information sensitivity (Blythe, 2015). The development and application of the WISA scale is one of the first attempts to explore how individuals rate the sensitivity of information in a workplace setting. Due to a growing need to understand the role that workplace information appraisals have on security behaviours, this article sought to revisit the work of Blythe (2015) to combine insights from previous literature and to identify the relevant dimensions of perceptions of information sensitivity. The final information sensitivity structure of the WISA scale was found to comprise of privacy, worth, consequences, high and low proximity interest. This structure was found to be a strong fit to the data for the eight target information types. This suggests that this theoretical account of information sensitivity is a strong explanation of the data and provides a valuable step forward for understanding and defining information sensitivity. The WISA scale was also shown to predict security behaviours in the workplace and early findings have reported how individual dimensions of the scale are predictive of specific employee security behaviours. This demonstrates the utility of the WISA scale for understanding employee security behaviours and for defining information sensitivity. Further research may look to apply the WISA scale to a broader range of security behaviours to develop our understanding and definition of information sensitivity in a security context.

Conflicting interests

The authors declare that there are no conflicts of interest.

Funding

This work is funded by the EPSRC, grant number EP/R 033900/1.

Ethical approval

This study was approved by the Department of Psychology Ethics Committee at Northumbria University.

Guarantors

JB, RB and LC shall act as guarantors, taking responsibility for the contents of this article.

Data availability

The authors do not have permission to share data.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.chbr.2022.100240.

References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40–46.

Anderson, J. C., & Gerbing, D. W. (1991). Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. *Journal of Applied Psychology, 76*(5), 732.

Blythe, J. (2015). *Information security in the workplace: A mixed-methods approach to understanding and improving security behaviours*. Northumbria University.

Blythe, J., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior, 87*, 87–97. https://doi.org/10.1016/j.chb.2018.05.023

Branley, D., Covey, J., & Hardey, M. (2014). *Online surveys: Investigating social media use and online risk*. SAGE Publications, Ltd.

Brown, R., Coventry, L., Sillence, E., Blythe, J., Stumpf, S., Bird, J., et al. (2022). Collecting and sharing self-generated health and lifestyle data: Understanding barriers for people living with long-term health conditions–a survey study. *Digital health, 8*, Article 20552076221084458.

Browne, M. W., & Cudeck, R. (1992). Alternative ways of assessing model fit. *Sociological Methods & Research, 21*(2), 230–258.

Brown, R., Sillence, E., Coventry, L., Simpson, E., Tariq, S., Gibbs, J., et al. (2022). Understanding the attitudes and experiences of people living with potentially stigmatised long-term health conditions with respect to collecting and sharing health and lifestyle data. *Digital health, 8*. https://doi.org/10.1177/20552076221089798

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157–165.

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). *Using behavioural insights to improve the public's use of cyber security best practices*. Gov. UK report.

Cranor, L. F., Reagle, J., & Ackerman, M. S. (2000). Beyond concern: Understanding net users' attitudes about online privacy. *The Internet upheaval: Raising Questions, Seeking Answers in Communications Policy*, 47–70.

Department for Digital, Culture, Media, & Sport. (2021). *Cyber security breaches survey 2021*. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021.

Dhillon, G., & Moores, S. (2001). Computer crimes: Theorizing about the enemy within. *Computers & Security, 20*(8), 715–723.

Evans, M., He, Y., Maglaras, L., Yevseyeva, I., & Janicke, H. (2019). Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. *International Journal of Medical Informatics, 127*, 109–119.

Gandy, O. H., Jr. (1993). *The panoptic sort: A political economy of personal information. Critical studies in communication and in the cultural industries*.

Gliem, J. A., & Gliem, R. R. (2003). *Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales*.

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers, 23*(3), 256–267.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. (2006). *Multivariate data analysis*. Uppersaddle River: Pearson Prentice Hall. NJ.

Hinkin, T. R. (1995). A review of scale development practices in the study of organizations. *Journal of Management, 21*(5), 967–988.

Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. *Organizational Research Methods, 1*(1), 104–121.

Hiscox. (2019). *The hiscox cyber readiness report 2019*. Retrieved from https://www.hiscox.co.uk/cyberreadiness.

Hoe, S. L. (2008). Issues and procedures in adopting structural equation modelling technique. *Journal of Quantitative Methods, 3*(1), 76.

Hu, L.-T., Bentler, P. M., & Hoyle, R. H. (1995). Structural equation modeling: Concepts, issues, and applications. *Evaluating model fit, 54*, 76–99.

Kline, P. (2013). *Handbook of psychological testing*. Routledge.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., et al. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cybercrime and cyber-attacks during the pandemic. *Computers & Security, 105*, Article 102248. https://doi.org/10.1016/j.cose.2021.102248

Lee, K., & Allen, N. J. (2002). Organizational citizenship behavior and workplace deviance: The role of affect and cognitions. *Journal of Applied Psychology, 87*(1), 131.

Little, L., Briggs, P., & Coventry, L. (2011). *Who knows about me? An analysis of age-related disclosure preferences*.

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science, 35*(4), 572–585.

MacKenzie, S. B., Podsakoff, P. M., & Ahearne, M. (1998). Some possible antecedents and consequences of in-role and extra-role salesperson performance. *Journal of Marketing, 62*(3), 87–98.

MacKenzie, S. B., Podsakoff, P. M., & Fetter, R. (1991). Organizational citizenship behavior and objective productivity as determinants of managerial evaluations of salespersons' performance. *Organizational Behavior and Human Decision Processes, 50*(1), 123–150.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355.

Marsh, H. W., & Grayson, D. (1995). *Latent variable models of multitrait-multimethod data*.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.
Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research, 26*(4), 323–339.
Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research, 15*(1), 76–98.
Onwuegbuzie, A. J., Daniel, L. G., & Collins, K. M. (2009). A meta-validation model for assessing the score-validity of student teaching evaluations. *Quality and Quantity, 43*(2), 197–209.
Podsakoff, P. M., & MacKenzie, S. B. (1997). Impact of organizational citizenship behavior on organizational performance: A review and suggestion for future research. *Human Performance, 10*(2), 133–151.
Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies, 71*(12), 1133–1143.
Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy and Marketing, 19*(1), 62–73.
Simpson, E., Brown, R., Sillence, E., Coventry, L., Lloyd, K., Gibbs, J., … Durrant, A. C. (2021). Understanding the barriers and facilitators to sharing patient-generated health data using digital technology for people living with long-term health conditions: A narrative review. *Frontiers in Public Health, 9*(1747). https://doi.org/10.3389/fpubh.2021.641424
Sun, Y., Liu, D., & Wang, N. (2017). A three-way interaction model of information withholding: Investigating the role of information sensitivity, prevention focus, and interdependent selfconstrual. *Data and Information Management, 1*(1), 61–73.
Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24*(6), 472–484.
Cybersecurity Ventures. (2019). 2019 official annual cybercrime report. In *Recuperado el*.
Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191–198.
Weible, R. J. (1993). *Privacy and data: An empirical study of the influence of types of data and situational context upon privacy perceptions*. Mississippi State University.