“Privacy concerns and protection behavior during the Covid-19 pandemic”

AUTHORS	Ranjany Sundaram Snehal Shetty
ARTICLE INFO	Ranjany Sundaram and Snehal Shetty (2022). Privacy concerns and protection behavior during the Covid-19 pandemic. *Problems and Perspectives in Management*, *20*(2), 57-70. doi:10.21511/ppm.20(2).2022.06
DOI	http://dx.doi.org/10.21511/ppm.20(2).2022.06
RELEASED ON	Wednesday, 20 April 2022
RECEIVED ON	Sunday, 21 November 2021
ACCEPTED ON	Friday, 08 April 2022
LICENSE	This work is licensed under a Creative Commons Attribution 4.0 International License
JOURNAL	"Problems and Perspectives in Management"
ISSN PRINT	1727-7051
ISSN ONLINE	1810-5467
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
92	4	1

BUSINESS PERSPECTIVES

LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine

www.businessperspectives.org

Ranjany Sundaram (India), **Snehal Shetty** (India)

PRIVACY CONCERNS AND PROTECTION BEHAVIOR DURING THE COVID-19 PANDEMIC

Received on: 21st of November, 2021
Accepted on: 8th of April, 2022
Published on: 20th of April, 2022

Ranjany Sundaram, Bachelor of Engineering, Amrita Vishwa Vidyapeetham University, India. (Corresponding author)

Snehal Shetty, Ph.D., Amrita Vishwa Vidyapeetham University, India.

Conflict of interest statement:
Author(s) reported no conflict of interest

Abstract

This paper aims to analyze the protection behavior of employees while working remotely during the Covid-19 pandemic using online video chat software. This pandemic changed the way organizations work, managers meet with employees, and employees communicate. An e-mail-based survey among computer users who use video chat software for remote working is employed in this study. Using 306 responses, structural equation modeling explores the relationship between privacy concerns, protection behavior, and antecedents. The technological changes induced due to Covid-19 influence privacy concerns and protection behavior. Privacy efficacy increases privacy concerns and protection behavior. Perceived vulnerability increases privacy concerns. Perceived effectiveness of organization software affects privacy concerns but does not affect protection behavior. There is a positive relationship between privacy concerns and protection behavior; however, this positive relation is negatively moderated by a propensity to trust. A finding of threat severity measure using Covid-19 factors concludes that both privacy concerns and protection behavior increased for online video chat software users. The theoretical model explicates 75% of variances in privacy concerns and 57% of variances in protection behavior. Every one-unit increase in Covid-19 induced changes regarding the work environment increases the privacy concern by 35%, and every one-unit increase in perceived effectiveness of organization software increases privacy concern by 22%. Every one-unit increase in the privacy concern increases the protection behavior by 48%, and every one-unit increase in privacy efficacy increases protection behavior by 59%.

Keywords privacy, Covid-19, threat, online, protection, Zoom, India

JEL Classification J28, M10, M15

INTRODUCTION

Human behavior is the feeblest link in any security chain (Crossler et al., 2013). Human errors cause one-quarter of cybersecurity attacks (Waldrop, 2016). It is important to understand users' protection behavior determinants when protecting their devices, computers, and networks. Several theories have been applied to study protection behavior. Protection motivation theory has been widely used in protecting against the viruses (Lee et al., 2008), spyware (Johnston & Warkentin, 2010), password leaks (Stanton et al., 2005), information leaks (Tsai et al., 2016), and social networking (Hoy & Milne, 2010).

Sudden changes imposed by the Covid-19 pandemic forced organizations to resort to remote working using the available tools (CDC, 2020).

The privacy risk portrayed by the media and the fact that users were suddenly forced to install online video chat software to facilitate office meetings prompted the paper to study the protection behavior in this context.

http://dx.doi.org/10.21511/ppm.20(2).2022.06

A new dimension to measure the effect of users' perception of the effectiveness of software chosen by the organization is introduced in this study. The theoretical basis is a meta-model using protection motivation theory (PMT) along with additional factors such as perceived effectiveness of software and propensity to trust to measure protection behavior mediated by privacy concerns.

1. LITERATURE REVIEW, HYPOTHESES, AND RESEARCH MODEL

Demand for online video meeting software rose very high after the pandemic lockdown. According to a news report, video conferencing software downloads rose to 62 million in March 2020. Google Meet, Zoom, Microsoft Teams, Cisco WebEx Teams, and GoTo meetings are popular online meeting software. After the pandemic imposed lockdown, organizations started using this software to conduct office meetings, universities for online classes, and home users for casual group video calls. This software is also created with program codes, posing a security risk and increasing privacy concerns. In addition, intruders hack the online meetings to show offensive content, marketing agencies use the background information seen in the video to advertise relevant products to users, and hackers look forward to stealing data during transit; thus, these incidents increase privacy concerns (John, 2020).

The online video chat software such as Zoom, Microsoft Teams, and Google Meet gave a quick platform for remote working and became a target for much negative news. There were numerous warnings against security threats posed by them. The Pentagon in the United States and the German Government warned against Zoom use and restricted this software (Singh & Awasthi, 2020). These warnings and bad news sparked disagreement and uncertainty over the choice of video chat software. The Covid-19 pandemic changed the organization's work routines and structure. Organizational changes affect the organization (Herold et al., 2008) if unplanned changes are not strategically and quickly handled (Shaw, 2017). Organizations had to set up remote working quickly, so they had to select one of the software without being able to plan or compare with better alternatives (Carroll & Conboy, 2020). That meant there was no time for understanding privacy implications. Employee compliance with organization security policies is a widely discussed topic. Employees' trust in their organization improves safety performance (Conchie et al., 2012). Unfortunately, employees often breach safety policies even if they are aware of the security risks (Kirlappos & Sasse, 2014).

The more concerned the employees are about the dangers of online information misuse, the more they should restrict the information. In other words, as privacy concerns of employees increase, protection behavior should also increase. Literature has different conclusions as to whether privacy concerns increase the protection behavior. Many argue that an increased concern for privacy does not lead to the corresponding protective behavior, defined as the privacy paradox (Acquisti & Gross, 2006; Taddei & Contena, 2013; Norberg et al., 2007). Social media users concerned about their privacy disclose information instead of limiting the information disclosure. Privacy calculus theory states that users calculate the expected loss of privacy and potential gain of disclosure. The benefit gained in the form of fulfilling their desire is stated to be one of the reasons for this risky behavior. However, several studies suggested a positive relationship between privacy concerns and protection behavior (Youn, 2009; Dienlin & Trepte, 2015). Another issue observed in the literature on the privacy paradox premise is that result varies depending on the methods employed and the inclusion of behavior intention instead of the actual protection behavior (Sheeran, 2002).

Four behavioral theories have been used for studying information security behavior (Lebek et al., 2014). They are:

1) Theory of Planned Behavior (TPB);
2) Technology Acceptance Model (TAM);
3) General Deterrence Theory (GDT); and
4) Protection Motivation Theory.

Among these four theories, TPB and PMT have been widely used to study employees' compliance.

http://dx.doi.org/10.21511/ppm.20(2).2022.06

PMT (Rogers, 1975, 1983) suggests people appraise the threat and the efficacy mechanisms when facing a threatening event. Protective behavior is motivated by these two appraisals – threat appraisal (TA) and coping appraisal (CA). Threat appraisal informs the users of the risks associated with the threat. Coping appraisal informs the necessary safety behavior to undertake. Protection behavior is also influenced by users' perception of how others think they should behave. This is called subjective norm.

Information privacy importance (Chai et al., 2009), perceived severity (Zhang & McDowell, 2009), and perceived vulnerability (Dinev & Hart, 2004) are the TA factors. On the other hand, privacy self-efficacy (Chai et al., 2009), response efficacy (Zhang & McDowell, 2009), perceived ability to control (Dinev & Hart, 2004), and personality traits (Junglas et al., 2008) are the CA factors.

Studies worthy of mentioning that have used protection motivation theory are Ifinedo (2012), Herath and Rao (2009b), Pahnila et al. (2007a), Siponen and Oinas-Kukkonen (2007), and Siponen et al. (2010). One common theme is that they have studied behavior intention as an outcome. Determinants of behavior intention using protection motivation theory are threat appraisal (Ifinedo, 2012; Pahnila et al., 2007a, 2007b; Siponen et al., 2010) and coping appraisal (Pahnila et al., 2007a). In addition, studies analyzed the protection behaviors of users while using a smartphone (Verkijika, 2018), desktop (Hanus & Wu, 2016), anti-virus software (Lee et al., 2008), wireless networks (Woon, 2005), and the internet (Van Bavel et al., 2019).

In an organizational context, PMT has been used to study the effectiveness of persuasive messaging to align users' security behavior with the organization's security policy. Using persuasive messaging increases the users' threat appraisal, which in turn improves their protection behavior (Johnston & Warkentin, 2010). Security tools alone cannot improve users' compliance with organizational security policies. It is affected by organizational, environmental, and behavioral factors. The possibility of security breaches (Herath & Rao, 2009a) is undermined by users. Protecting the resources of an organization is users' commitment to organizational wellbeing.

In summary, a review of relevant research puts forth two observations. First, a meta-model including the core constructs of PMT and perceived effectiveness of security software and Covid-19 induced changes in work in a single framework to measure the actual behavior is necessary. There is a need to measure actual technical protection behavior in an online video chat context rather than asking users to rate their protection behavior. As stated in prior literature, factors influencing protection behavior are privacy concern, perceived vulnerability, and privacy efficacy. Applying to organization setting, protection behavior of users may be influenced by the choice of the security software used in their organizations. Apart from this, external situations may induce changes in the way users work, which influences users' concern for privacy and the desire to protect information. Therefore, this study uses the following constructs to understand the influence of various factors on users' protection behavior.

Protecting information is essential when a user is connected via the internet, irrespective of the applications one uses. Adopting Rogers (1983) definition of protection behavior (PB), this construct measures how effectively a user adopts secure behavior to stop the intruder, avoid malicious software, stop unwanted participants from joining the meeting, and information protection mechanisms from marketing agencies to control the risk, threat, and danger in the context of an online video chat application. PB construct measures the necessary protection behaviors that are critical for stopping the threats imposed by video chat software.

The privacy concern measure adopted from Buchanan et al. (2007) was modified to suit the online video chat context addressing various privacy dimensions such as online presence, impersonation, identity theft, and email fraud. Privacy concern (PC) adopted from Buchanan et al. (2007) measures internet privacy concerns.

Perceived vulnerability measure was adopted from Workman et al. (2008). The likelihood of personal information loss in a user's computer when using online video chat is defined as perceived vulnerability. It is measured by the possibility of information violation threats expected by the user.

Measures of self-efficacy should apply to the task (Peterson & Arnn, 2005); hence, skills needed for online privacy adapted from Workman et al. (2008) are measured. In addition, studies suggested that the predicating power of privacy coping behavior is explained through privacy efficacy (Dinev & Hart, 2005, 2007; Yao & Linz, 2008). Privacy efficacy refers to the user's perceived ease of performing a particular behavior; thus, user's ease of applying preventative measures and stopping information security violations are measured.

The severity of the threat brought by the sudden changes that forced the user to carry out office meetings from home is measured. The threat exposure from carrying out office meetings from the computers and devices without office network protection is another threat component. CO measures the threat severity of users due to the changes caused by the Covid-19 pandemic. CO stands for Covid-19 measure. Item development, scale development, and scale evaluation of this new construct were performed as per the procedure listed for scale development (Boateng et al., 2018). To evaluate the scale items, interviews with twenty experts and twenty end-users were conducted. The original scale had eight items, and this was brought down to five with multiple rounds of testing.

How users perceive the effectiveness of software selected by their organization is a form of trust component. Past research has shown that trust increases users' compliance with security policy. However, employee compliance measurement using a new construct was found to be lacking in the literature review analysis (Lebek et al., 2014). A new construct for employee compliance is introduced in this study, measured through the perceived effectiveness of the organization's choice of software by following the scale development procedure (Boateng et al., 2018). OR measures the users' perception of their organization's choice of video chat software. OR stands for users' perceived effectiveness of software decided by their organizations.

Users who are highly concerned about privacy employ privacy-enhancing mechanisms as a means to avoid negative consequences. Concerns about online privacy result in protective behaviors such as removing personal information from marketable databases (Son & Kim, 2008), desisting from self-disclosure (Krasnova et al., 2010) in the e-commerce domain, and deleting cookies (Lutz & Strathoff, 2014). Protection in the video software context should be stopping the intruders who force their entry into meetings, not installing the app from malicious installation download sources, not displaying the background for others to misuse, and not transmitting unencrypted data to participants. Suppose the software is connected to the internet. In that case, invasion of privacy such as spam emails, offensive communication, creation of databases consisting of personal information, and misuse of that information is unavoidable. Any additional use of the software is an additional threat introduced to the existing online threats. "Knowledge" is the passive element of information privacy, and "control" is the active element; however, both are highly interrelated (Malhotra et al., 2004). Past research in e-commerce, social networking sites, Facebook, online, and with studies focusing on teens and adults groups showed that as concern for privacy increases, there would be more protective behaviors to guard their privacy (Sheehan & Hoy, 1999; Mohamed & Ahmad, 2012; Young & Quan-Haase, 2009; Moscardelli & Divine, 2007; Chen et al., 2017).

Pandemic brings many fundamental changes in mundane activity patterns, which provoke crime rates (Cohen & Felson, 1979). The Covid-19 pandemic brought sudden changes and forced people to work from home. A structural change in routine activities came in the form of using home computers for office work. Home computers and devices are not updated with the latest security patches, latest security policies, and do not have anti-virus or any other security protection an office computer would have. These changes further brought other changes in data storage; data had to be transferred to removable hard disks or flash memory cards, which are easily prone to hacking. Criminals take advantage of emergencies where individuals are vulnerable (Khan et al., 2020).

The pandemic period reported a significant increase in spam messages, malware attacks, and malicious links (Khan et al., 2020; Naidoo, 2020). In addition, vulnerable home PCs are targeted

http://dx.doi.org/10.21511/ppm.20(2).2022.06

for denial of service attacks, spam, and phishing emails (Furnell et al., 2007). Studies recommend a multifaceted protection approach called defense in depth (Schou & Trimmer, 2004). This means that if the perimeter layer of security is breached, additional layers provide defense and protection from attack. These additional layers of protection are missing for home computers, as there are no perimeter firewalls or security devices. These changes in security posture increase the perception of threats and concerns.

Employee organization relationship refers to the trust, commitment, and satisfaction with each other (Men & Stacks, 2014, p. 307). When there are changes in the organization, only if employees experience positive emotions about the changes at work, they cope with the changes effectively (Fugate et al., 2008). The Covid-19 pandemic created many changes and uncertainty for all organizations, employees, and humans. When an employee faces uncertainty, several negative consequences for contentment and welfare are bound to arise (Bordia et al., 2004).

Trust is one of the vital constructs in predicting users' acceptance of technology in uncertainty (Carter & Bélanger, 2005; Dhagarra et al., 2020). Employees adopt protection behaviors when they trust that their organization cares about their safety (Hofmann & Morgeson, 1999). Organizational practices that make employees view management as legitimate are the main factor that will encourage an employee to trust its choices. Only when an employee trusts the organization, he/she will be motivated to accept the organization's choice of software and follow compliance. Trust in an organization is integral to employees' perceptions of privacy.

Self-efficacy is "the belief in one's capabilities to execute the courses of action" (Bandura et al., 1999). Privacy efficacy is the user's mastery experiences in managing the security threats and protecting the system. Privacy efficacy has been shown to enhance the privacy-protecting behaviors of online consumers by restricting self-disclosure (LaRose & Rifon, 2007). Social network users with high privacy efficacy are found to limit profile visibility and self-disclosure while conducting online transactions (Chen & Chen, 2015). Only when the users are confident in their privacy-enhancing skills, they will undertake security measures (Jutla & Bodorik, 2005). Privacy efficacy paves the way for easy learning (Martocchio, 1994) of privacy technologies. With this learning, commitment to search for suitable alternatives for limiting the information disclosure increases (Latham et al., 2002).

Propensity to trust is a general inclination to display faith and trust others based on ongoing life experiences. In e-commerce, consumers with a high trust propensity form higher trust with selling parties (McKnight et al., 1998). Social media users with a high propensity to trust disclose more information online (Mesch, 2012). A lower privacy concern increases trust (Olivero & Lunt, 2004). Increased propensity to trust reduces the perception of the risk connected with privacy (Zimmer et al., 2010). Thus, the positive relation between privacy concern and protection behavior is negatively moderated by the propensity to trust.

This study aims to analyze whether privacy efficacy, perceived vulnerability, organization choice of software, and Covid-19 induced changes in the office work settings and increased protection behavior. Also, this study analyses whether privacy concerns positively influence protection behavior. With the aim of testing the impact of these factors on protection behavior and based on the review of prior findings, the following hypotheses were proposed (Figure 1):

H1: *Stronger privacy concern leads to stronger protection behavior.*

H2: *Covid-19 pandemic increases privacy concerns.*

H3: *Perceived effectiveness of an organization's choice of software increases protection behavior.*

H4: *Stronger privacy efficacy leads to stronger protection behavior.*

H5: *Privacy concern and protection behavior relation are negatively moderated by a propensity to trust.*

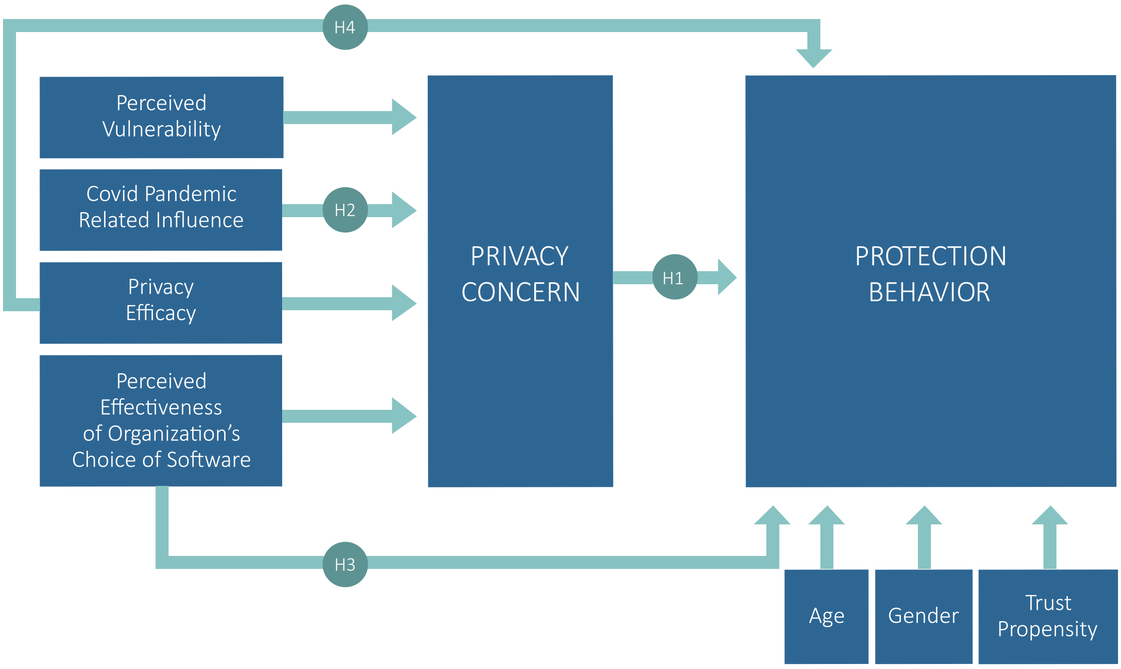

Figure 1. Hypothesized structural model

2. METHODS

An email requesting several computer users who use video chat software for remote working was sent to test the hypotheses. The email contained a link to the web-based questionnaire. Three hundred and fifteen responses were received.

Snowball sampling was used in this study to identify users who use video chat software for remote working. Forty primary contacts of authors helped forward the survey to the broader working audience through their contacts. The respondents were working professionals from India. The primary contacts explained the purpose of the survey and made sure only the working professionals who used video chat software for remote working participated in the survey. The survey has been conducted for six months. A survey was not restricted to a particular video chat software. This study considers all the video chat software used for remote working. The adversarial sentence was added as an attention check, and nine samples were removed that failed this attention check. Therefore, the total sample was three hundred and six.

2.1. Measures

The questionnaire consisted of 33 items, which included a variety of measures to assess protection behavior, privacy concern, perceived vulnerability, privacy efficacy, Covid-19 factors, and perceived effectiveness of organization's choice of software.

Propensity to trust, a control variable, is the inclination to believe in the positive attributes of others in general, and it is measured on a five-point Likert scale (Gefen, 2000; McKnight et al., 2002). Age (Miltgen & Peyrat-Guillard, 2014) and gender (Park, 2015) are also control variables.

The survey instruments have five items measured using a five-point Likert scale anchored by strongly disagree (1) to strongly agree (5). The questionnaire was pretested by ten knowledgeable cyber professionals, five IT professionals, and eighty regular video chat users. Test-retest reliability with two weeks intervals was .95. Internal consistency was measured using Cronbach's alpha. Ten cyber security experts checked face validity, content validity, and criterion validity. Factor loadings ranged from 0.885 to 0.946. Cronbach's alpha for OR construct is 0.885, CO construct is 0.898, and for PB construct is 0.946.

2.2. Sample

Male participants constitute 36% and females 63% of the sample. Age below 35 years accounts for 67%, and the age group between 35 to 56 years accounts for 33% of respondents.

Table 1. Results of protection behavior analysis

	Average variances extracted	Composite reliability coefficient	Perceived vulnerability	Privacy efficacy	Covid-19 pandemic	Perceived effectiveness	Privacy concerns	Protection behavior
Perceived vulnerability	0.747	0.936	0.864	–	–	–	–	–
Privacy efficacy	0.762	0.941	0.604	0.873	–	–	–	–
Covid-19 pandemic	0.714	0.925	0.721	0.561	0.845	–	–	–
Perceived effectiveness	0.685	0.916	0.693	0.706	0.770	0.828	–	–
Privacy concerns	0.746	0.936	0.758	0.650	0.790	0.767	0.863	–
Protection behavior	0.822	0.958	0.693	0.810	0.622	0.675	0.652	0.906

48% of the sample population are married. All respondents have an undergraduate degree, and all of them receive a monthly income.

2.3. Analysis

The reliability of the scales was checked using composite reliability (Fornell & Larcker, 1981) and coefficient alpha (Cronbach, 1951). Table 1 shows composite reliability for each of the scales, and it varies from 0.916 to 0.958. Coefficient alpha ranges from 0.828 to 0.906. These levels are within the range of levels suggested by Nunnally (1967).

The validity of the scales was examined using confirmatory factor analysis with covariance-based structural equation modeling. The total number of items equals 33.

Pairwise correlation between six factors was compared with average variance extracted to check discriminant validity recommended by Fornell and Larcker (1981). Average variance exceeded the square of the correlation between the factors thus proving discriminant validity.

The lowest average variance extracted is 0.685, and the lowest composite reliability is 0.916, so convergent validity is proved (Fornell & Larcker, 1981). The result is shown in Table 1.

3. RESULTS

Hypothesis 1 (the stronger the privacy concerns, the stronger the protection behavior) is supported with β = 0.48, $P < .01$ (Figure 2). Covid-19 pandemic increases privacy concerns thus supporting hypothesis 2 (β = 0.35, $P < .01$). Also, a finding worth mentioning here is that there is a positive relationship between Covid-19 pandemic and protection behavior (β = 0.12, $P = .01$). Covid-19 not only increases the privacy concerns but also the protection behavior.

Hypothesis 3 is not supported. The perceived effectiveness of organization software has a positive effect on privacy concerns (β = 0.22, $P < .01$). However, it does not have a relation with protection behavior.

Hypothesis 4 (the stronger the privacy efficacy, the stronger the protection) is also supported. Here β = 0.59, $P < .01$. This finding agrees with Floyd et al. (2000) and LaRose et al. (2005).

Hypothesis 5 (the propensity to trust negatively moderates privacy concerns and protection behavior relation) is supported. Here β = –0.13, $P < .01$. The result is shown in Figure 3. The moderator graph is shown in Figure 4.

Findings suggest that perceived vulnerability positively affects protection behavior (β = 0.21, $P < .01$). This finding contradicts Burns et al. (2017) and Mwagwabi et al. (2018) as they reported no relationship. A recent study that took both threat and coping appraisal reported that the latter impacted protection behavior more than the former (Van Bavel et al., 2019).

Analysis reported females having more protection behavior (β = –0.15, $P < .01$). There was a negative relationship between trust propensity and

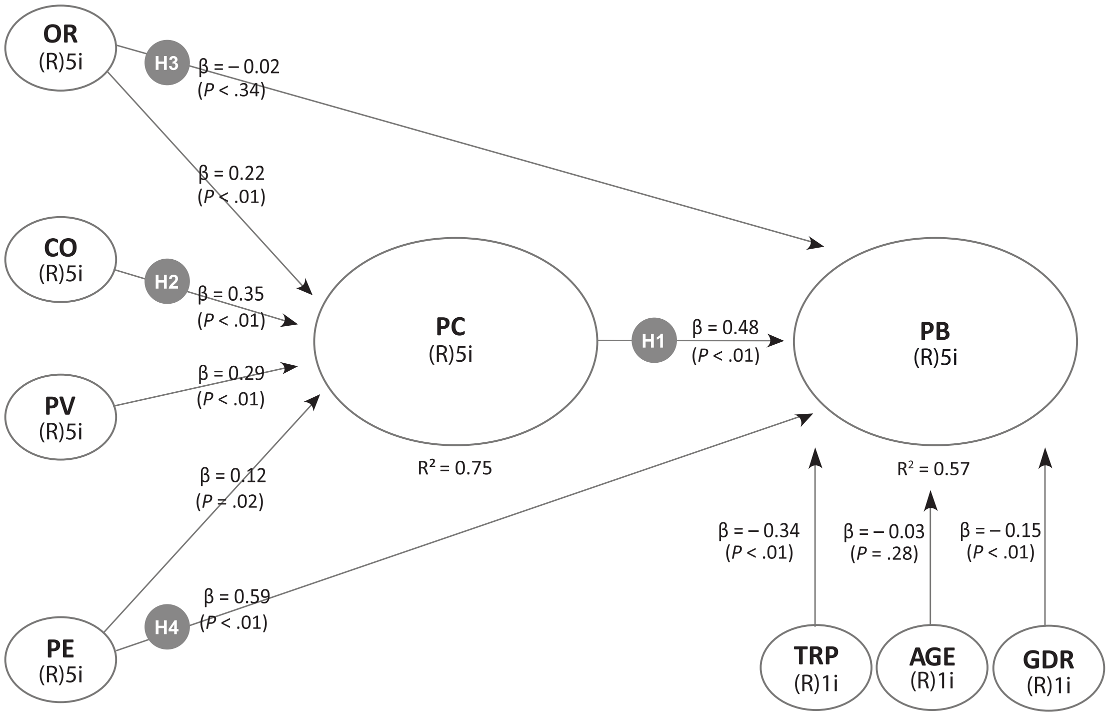

Figure 2. Structural model with the result

protection behavior (β = −0.34, P < .01). Age does not have a relation with protection behavior. This finding does not match Esposito et al. (2017) and Lunn and Lyons (2010), who reported that the elderly population has less protection behavior.

Regarding the explanatory power of this research model, the theoretical model explicates 75 percent of variances in privacy concerns and 57 percent of variances in protection behavior.

4. DISCUSSION

Positive relationship between privacy concerns and protection behavior agrees with past studies (Youn, 2009; Dienlin & Trepte, 2015). However, this finding contradicts Acquisti and Gross (2006) and Tufekci (2008), who reported no relationship. The privacy paradox states that privacy concerns and the corresponding protection behavior have no relation. The finding of this study suggests

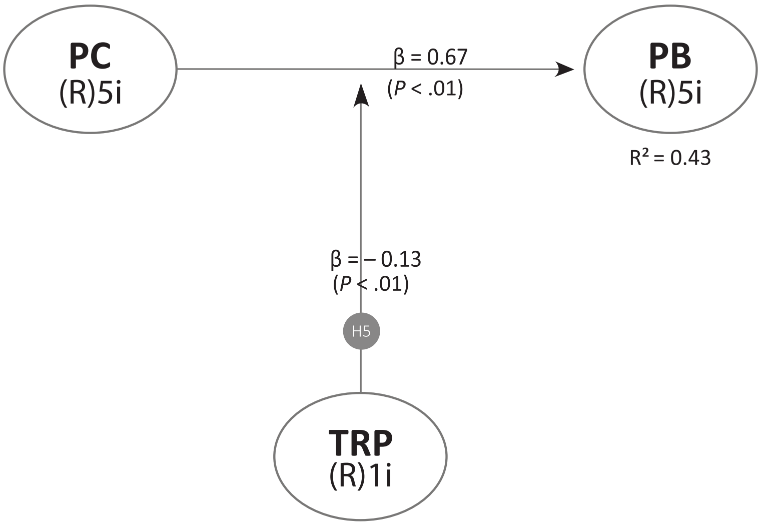

Figure 3. TRP as moderator

http://dx.doi.org/10.21511/ppm.20(2).2022.06

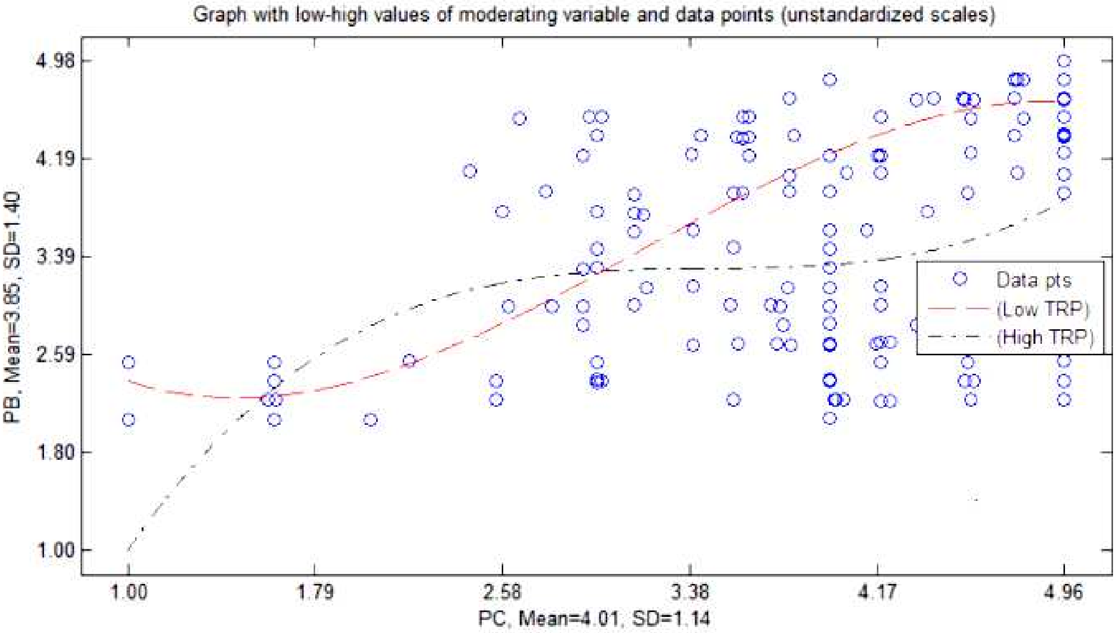

Figure 4. Graph of moderator analysis

there is no place for a privacy paradox. Dienlin and Trepte (2015) used regression analysis and structural equation modeling to find a relationship between privacy concerns and protection behavior. Only structural equation modeling supported the positive relationship between the two, whereas regression analysis supported the privacy paradox.

Similarly, Acquisti and Gross (2006) used regression analysis, and this must be the reason for not finding positive relation between privacy concerns and protection behavior. Another reason for not finding the positive relation is a selection of variables leading to the limitation of variance (Schmidt et al., 1976). The privacy literature yielded mixed findings on gender and privacy-protective behaviors. This result agrees with Milne and Culnan (2004).

The study demonstrated interesting implications from a practitioner's perspective. Privacy efficacy, perceived vulnerability, and Covid-19 induced changes in the office work settings increased protection behavior. Propensity to trust reduces protection behavior. Females employ more protection behavior than males.

CONCLUSION

This study aimed to analyze the influence of privacy efficacy, perceived vulnerability, organization choice of software, and Covid-19 induced changes on users' protection behavior in the office work settings. In addition, this study aimed to analyze whether privacy concerns positively influenced protection behavior. Findings illustrated the positive relationships among privacy efficacy, Covid-19 induced changes, and protection behavior. Privacy efficacy and Covid-19 induced changes increase protection behavior. In normal circumstances, users delegate the security responsibility to the IT team, but users had to take personal responsibility for securing data and devices during the pandemic. That is why Covid-19 induced changes in work settings increased protection behavior. Since privacy efficacy increases protection behavior when a particular threat situation is faced by an organization, the corresponding coping mechanism to tackle the threat should be imparted to the users. Organization choice of software is positively related to privacy concerns but not protection behavior. Another important finding is that privacy concerns increased protection behavior. Analysis of this study showed that there is no privacy paradox.

The study concludes with some important practical implications. Organizations that use online video chat software need to move the scope of their IT team from on-premises security behavior to securing their employee devices over the untrusted public internet. Implications for the research community are that the construct for measuring security threats induced by Covid-19 could be used in future studies. In addition, the protection behavior constructs created to measure the security behavior of online video software users can also be used by future studies.

AUTHOR CONTRIBUTIONS

Conceptualization: Ranjany Sundaram.
Data curation: Ranjany Sundaram.
Formal analysis: Ranjany Sundaram.
Investigation: Snehal Shetty.
Methodology: Snehal Shetty.
Software: Ranjany Sundaram.
Supervision: Snehal Shetty.
Validation: Snehal Shetty.
Visualization: Ranjany Sundarm.
Writing – original draft: Ranjany Sundaram.
Writing – review & editing: Snehal Shetty.

ACKNOWLEDGMENT

The assistance provided by Arun Thottath in reaching out to survey participants was greatly appreciated.

REFERENCES

1. Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies* (pp. 36-58). Springer, Berlin, Heidelberg.
2. Bandura, A., Freeman, W. H., & Lightsey, R. (1999). *Self-efficacy: The exercise of control*. New York: W.H. Freeman and Company.
3. Boateng, G. O., Neilands, T. B., Frongillo, E. A., Melgar-Quiñonez, H. R., & Young, S. L. (2018). Best practices for developing and validating scales for health, social, and behavioral research: a primer. *Frontiers in Public Health, 6*. https://doi.org/10.3389/fpubh.2018.00149
4. Bordia, P., Hobman, E., Jones, E., Gallois, C., & Callan, V. J. (2004). Uncertainty during organizational change: Types, consequences, and management strategies. *Journal of Business and Psychology, 18*(4), 507-532. https://doi.org/10.1023/B:JOBU.0000028449.99127.f7
5. 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. https://doi.org/10.1002/asi.20459
6. Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior, 68,* 190-209. https://doi.org/10.1016/j.chb.2016.11.018
7. Carroll, N., & Conboy, K. (2020). Normalising the "new normal": Changing tech-driven work practices under pandemic time pressure. *International Journal of Information Management, 55,* 102186. https://doi.org/10.1016/j.ijinfomgt.2020.102186
8. Carter, L., & Bélanger, F. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information Systems Journal, 15*(1), 5-25.
9. Centers for Disease Control and Prevention (CDC). (2020). *Interim clinical guidance for management of patients with confirmed coronavirus disease (COVID-19).* Retrieved from https://stacks.cdc.gov/view/cdc/89980
10. Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication, 52*(2), 167-182. https://doi.org/10.1109/TPC.2009.2017985
11. Chen, H. T., & Chen, W. (2015). Couldn't or wouldn't? The

influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 13-19. https://doi.org/10.1089/cyber.2014.0456

12. Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior, 70,* 291-302. Retrieved from http://hdl.handle.net/20.500.11990/2043

13. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608. https://doi.org/10.2307/2094589

14. Conchie, S. M., Taylor, P. J., & Donald, I. J. (2012). Promoting safety voice with safety-specific transformational leadership: The mediating role of two dimensions of trust. *Journal of Occupational Health Psychology, 17*(1), 105-115. https://doi.org/10.1037/a0025101

15. Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297-334. https://doi.org/10.1007/BF02310555

16. Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32,* 90-101. https://doi.org/10.1016/j.cose.2012.09.010

17. Dhagarra, D., Goswami, M., & Kumar, G. (2020). Impact of trust and privacy concerns on technology acceptance in healthcare: An Indian perspective. *International journal of medical informatics, 141,* 104164. https://doi.org/10.1016/j.ijmedinf.2020.104164

18. Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297. https://doi.org/10.1002/ejsp.2049

19. Dinev, T., & Hart, P. (2004). Internet Privacy Concerns and their Antecedents – Measurement Validity and a Regression Model. *Behavior and Information Technology, 23*(6), 413-422. https://doi.org/10.1080/01449290410001715723

20. Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29. https://doi.org/10.2753/JEC1086-4415100201

21. Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7). http://dx.doi.org/10.17705/1jais.00133

22. Esposito, G., Hernández, P., van Bavel, R., & Vila, J. (2017). Nudging to prevent the purchase of incompatible digital products online: An experimental study. *PloS One, 12*(3), e0173333. https://doi.org/10.1371/journal.pone.0173333

23. Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407-429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

24. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

25. Fugate, M., Kinicki, A. J., & Prussia, G. E. (2008). Employee coping with organizational change: An examination of alternative theoretical perspectives and models. *Personnel Psychology, 61*(1), 1-36. https://doi.org/10.1111/j.1744-6570.2008.00104.x

26. Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security, 26*(5), 410-417. https://doi.org/10.1016/j.cose.2007.03.001

27. Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega, 28*(6), 725-737. Retrieved from http://onemvweb.com/sources/sources/ecommerce_role_familiarity_trust.pdf

28. Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management, 33*(1), 2-16. https://doi.org/10.1080/10580530.2015.1117842

29. Herath, T., & Rao, H. R. (2009a). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

30. Herath, T., & Rao, H. R. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. https://doi.org/10.1016/j.dss.2009.02.005

31. Herold, D. M., Fedor, D. B., Caldwell, S., & Liu, Y. (2008). The effects of transformational and change leadership on employees' commitment to a change: A multilevel study. *Journal of Applied Psychology, 93*(2), 346-357. https://doi.org/10.1037/0021-9010.93.2.346

32. Hofmann, D. A., & Morgeson, F. P. (1999). Safety-related behavior as a social exchange: The role of perceived organizational support and leader-member exchange. *Journal of Applied Psychology, 84*(2), 286-296. Retrieved from http://www.morgeson.com/downloads/hofmann_morgeson_1999.pdf

33. Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10*(2), 28-45. https://doi.org/10.1080/15252019.2010.10722168

34. Ifinedo, P. (2012). Understanding information systems security

policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

35. John, A. S. (2020). *It's Not Just Zoom. Google Meet, Microsoft Teams, and Webex Have Privacy Issues, Too.* Retrieved from https://www.hawaii.edu/its/wp-content/uploads/sites/2/2020/05/Google-Meet-Microsoft-Teams-Webex-Privacy-Issues-Consumer-Reports.pdf

36. Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-566. https://doi.org/10.2307/25750691

37. Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387-402. https://doi.org/10.1057/ejis.2008.29

38. Jutla, D. N., & Bodorik, P. (2005). Sociotechnical architecture for online privacy. *IEEE Security & Privacy, 3*(2), 29-39. https://doi.org/10.1109/MSP.2005.50

39. Khan, N. A., Brohi, S. N., & Zaman, N. (2020). *Ten deadly cyber security threats amid COVID-19 pandemic.* TechRxiv. Retrieved from https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792

40. Kirlappos, I., & Sasse, M. A. (2014). What usable security really means: Trusting and engaging users. *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 69-78). Springer.

41. Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: why we disclose. *Journal of Information Technology, 25*(2), 109-125. https://doi.org/10.1057/jit.2010.6

42. LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs, 41*(1), 127-149. https://doi.org/10.1111/j.1745-6606.2006.00071.x

43. LaRose, R., Rifon, N., Liu, S., & Lee, D. (2005). Understanding online safety behavior: A multivariate model. *The 55th annual conference of the international communication association.* New York.

44. Latham, G. P., Locke, E. A., & Fassina, N. E. (2002). The high performance cycle: Standing the test of time. In S. Sonnentag (Ed.), *Psychological management of individual performance* (pp. 201-228). https://doi.org/10.1002/0470013419.ch10

45. Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review, 37*(12), 1049-1092. https://doi.org/10.1108/MRR-04-2013-0085

46. Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology, 27*(5), 445-454. https://doi.org/10.1080/01449290600879344

47. Lunn, P., & Lyons, S. (2010). *Behavioural economics and "vulnerable consumers": a summary of evidence.* London: Communications Consumer Panel. Retrieved from https://www.communicationsconsumerpanel.org.uk/Behavioural%20Economics%20and%20Vulnerable%20Consumers%20final%20report%20correct%20date.pdf

48. Lutz, C., & Strathoff, P. (2014). *Privacy concerns and online behavior – Not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses.* Retrieved from https://www.alexandria.unisg.ch/228096/1/Lutz_Strathoff.pdf

49. 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), 311-416. https://doi.org/10.1287/isre.1040.0032

50. Martocchio, J. J. (1994). Effects of conceptions of ability on anxiety, self-efficacy, and learning in training. *Journal of Applied Psychology, 79*(6), 819-825. https://doi.org/10.1037/0021-9010.79.6.819

51. McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The Journal of Strategic Information Systems, 11*(3-4), 297-323. https://doi.org/10.1016/S0963-8687(02)00020-3

52. McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review, 23*(3), 473-490. https://doi.org/10.5465/amr.1998.926622

53. Men, L. R., & Stacks, D. (2014). The effects of authentic leadership on strategic internal communication and employee-organization relationships. *Journal of Public Relations Research, 26*(4), 301-324. https://doi.org/10.1080/1062726X.2014.908720

54. Mesch, G. S. (2012). Is online trust and trust in social institutions associated with online disclosure of identifiable information online? *Computers in Human Behavior, 28*(4), 1471-1477. https://doi.org/10.1016/j.chb.2012.03.010

55. Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15-29.

56. Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems, 23*(2), 103-125. https://doi.org/10.1057/ejis.2013.17

57. Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior, 28*(6), 2366-2375. https://doi.org/10.1016/j.chb.2012.07.008

58. Moscardelli, D. M., & Divine, R. (2007). Adolescents' concern for privacy when using the Internet: An empirical analysis of predictors and relationships with privacy-protecting behaviors. *Family and Consumer Sciences Research Journal, 35*(3), 232-252. https://doi.org/10.1177/1077727X06296622

59. Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and long-term effects of fear appeals in improving compliance with password guidelines. *Communications of the Association for Information Systems, 42*(1).

60. Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems, 29*(3), 306-321. https://doi.org/10.1080/0960085X.2020.1771222

61. Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

62. Nunnally, J. (1967). *Psychometric theory.* New York: McGraw-Hill.

63. Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology, 25*(2), 243-262.

64. Pahnila, S., Siponen, M., & Mahmood, A. (2007a). Employees' behavior towards IS security policy compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 156b-156b). IEEE.

65. Pahnila, S., Siponen, M., & Mahmood, A. (2007b). Which factors explain employees' adherence to information security policies? An empirical study. *Pacis 2007 Proceedings,* 73.

66. Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in) equality in the Internet. *Computers in Human Behavior, 50,* 252-258. https://doi.org/10.1016/j.chb.2015.04.011

67. Peterson, T. O., & Arnn, R. B. (2005). Self-efficacy: The foundation of human performance. *Performance Improvement Quarterly, 18*(2), 5-18. https://doi.org/10.1111/j.1937-8327.2005.tb00330.x

68. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology, 91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

69. Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook,* 153-176.

70. Schmidt, F. L., Hunter, J. E., & Urry, V. W. (1976). Statistical power in criterion-related validation studies. *Journal of Applied Psychology, 61*(4), 473-485. https://doi.org/10.1037/0021-9010.61.4.473

71. Schou, C. D., & Trimmer, K. J. (2004). Information assurance and security. *Journal of Organizational and End User Computing, 16(3),* 123-145.

72. Shaw, D. (2017). Managing people and learning in organisational change projects. *Journal of Organizational Change Management, 30*(6), 923-935. https://doi.org/10.1108/JOCM-11-2016-0253

73. Sheehan, K. B., & Hoy, M. G. (1999). Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising, 28*(3), 37-51. https://doi.org/10.1080/00913367.1999.10673588

74. Sheeran, P. (2002). Intention – behavior relations: a conceptual and empirical review. *European Review of Social Psychology, 12*(1), 1-36. https://doi.org/10.1080/14792772143000003

75. Singh, R., & Awasthi, S. (2020). *Updated Comparative Analysis on Video Conferencing Platforms-Zoom, Google Meet, Microsoft Teams, WebEx Teams and GoToMeetings* (EasyChair Preprint No. 4026). Retrieved from https://easychair.org/publications/preprint_open/Fq7T

76. Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 38*(1), 60-80. https://doi.org/10.1145/1216218.1216224

77. Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71. https://doi.org/10.1109/MC.2010.35

78. Son, J. Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly, 32*(3), 503-529. https://doi.org/10.2307/25148854

79. Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133. https://doi.org/10.1016/j.cose.2004.07.001

80. Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior, 29*(3), 821-826. https://doi.org/10.1016/j.chb.2012.11.022

81. Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59,* 138-150. https://doi.org/10.1016/j.cose.2016.02.009

82. Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20-36.

83. Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies, 123,* 29-39. https://doi.org/10.1016/j.ijhcs.2018.11.003

84. Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security, 77,* 860-870. https://doi.org/10.1016/j.cose.2018.03.008

85. Waldrop, M. M. (2016). How to hack the hackers: The human side of cybercrime. *Nature, 533,* 164-167. https://doi.org/10.1038/533164a

86. Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *Association for Information Systems – 26th International Conference on Information Systems, ICIS 2005: Forever New Frontiers* (pp. 367-380). Retrieved from https://scholarbank.nus.edu.sg/handle/10635/42823

87. Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816. https://doi.org/10.1016/j.chb.2008.04.005

88. Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. *CyberPsychology & Behavior, 11*(5), 615-617. https://doi.org/10.1089/cpb.2007.0208

89. Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389-418. https://doi.org/10.1111/j.1745-6606.2009.01146.x

90. Young, A. L., & Quan-Haase, A. (2009). Information revelation and internet privacy concerns on social network sites: a case study of facebook. *Proceedings of the fourth international conference on Communities and technologies* (pp. 265-274). https://doi.org/10.1145/1556460.1556499

91. Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce, 8*(3-4), 180-197. https://doi.org/10.1080/15332860903467508

92. Zimmer, J. C., Arsal, R., Al-Marzouq, M., Moore, D., & Grover, V. (2010). Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure. *Decision Support Systems, 48*(2), 395-406. https://doi.org/10.1016/j.dss.2009.10.003