Computers & Security 131 (2023) 103301

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Would US citizens accept cybersecurity deresponsibilization? Perhaps not

Karen Renaud[a,b,c,*], Karl van der Schyff[b], Stuart MacDonald[d]

[a] University of Strathclyde, Glasgow, UK
[b] Abertay University, Dundee, UK
[c] University of South Africa, Pretoria, RSA
[d] Seric Systems, Glasgow, UK

ARTICLE INFO

Article history:
Received 9 December 2022
Revised 20 March 2023
Accepted 21 May 2023
Available online 23 May 2023

Keywords:
Cybersecurity Responsibilization
Cybersecurity deresponsibilization
Government competence and benevolence

ABSTRACT

Responsibilizing governments provide advice about how to manage a variety of risks. If citizens do not heed the advice and things go wrong, they are expected to accept the adverse consequences without complaint. However, in some cases, citizens are unable or unwilling to embrace these government-assigned responsibilities and to act on the advice, for a variety of valid reasons. It may be appropriate for governments to provide more direct support: in essence, *deresponsibilizing* citizens who struggle to embrace the responsibility. In this paper, we explore whether US citizens would be willing to accept more help from their government in the cyber realm. Using two studies, we find that perceptions related to the government's competence and benevolence are necessary pre-requisites for a willingness to be deresponsibilized, and also that many respondents did not have confidence that either of these were sufficient. This deficiency might well render governments' well-intended deresponsibilization endeavours futile. We conclude by proposing deresponsibilization strategies that acknowledge and accommodate this.

1. Introduction

Cybercrime poses a global threat to online safety and security (Hernandez-Castro & Boiten, 2014; Jewkes, 2013; Nasser Alshabib & Tiago Martins, 2021). Notably, cybercrime attacks have increased in intricacy, requiring sophisticated practical skills to prevent and resist them (Cascavilla et al., 2021; Phillips et al., 2022). However, despite this, neoliberal governments often "responsibilize" their citizens in this regard (Renaud et al., 2020), expecting them to take care of their own cyber-safety and security. Responsibilization entails giving citizens a great deal of sound advice for managing some particular risk, and then expecting them to shoulder the burden and reduce the risk to themselves by following the advice (Giesler & Veresiu, 2014), or accept the consequences.

Responsibilization ostensibly demonstrates government commitment to individual freedom (Biebricher & Johnson, 2012). Masquelier (2017) explains that: "*a range of legal, economic and cultural resources are mobilized in an effort to compel individuals to regard themselves and/or others as personally responsible for their actions*" (p. 47). Neoliberal governments expect their citizens to be independent and self-steering, arguing that this respects their need for autonomy and adulthood. The aim is to produce "*self-reliant citizens who do not make too many demands on government services*" (p.2) (Trnka & Trundle, 2017). In essence, responsibilization allows the neoliberal state to "govern from a distance" (Bellamy, 2022).

Some believe that this stance goes back to politicians like Margaret Thatcher (Masquelier, 2017), who famously believed that there was no such thing as society, only individuals who ought to accept personal responsibility for all aspects of their lives. Her aim was to cut back state provisions (Harvey, 2005). One could go back even further to Milton Friedman (1962), who considered state interference a bar to self-determination. Whatever the provenance of the ideology, responsibilization is something of a long-standing strategy that is embraced by many Western governments. With the emergence of the cyber domain threats, governments chose to apply this familiar strategy, responsibilizing citizens to manage the cybersecurity risk themselves (Renaud et al., 2020).

Avigur-Eshel argues that responsibilization focuses on "'*how*' *questions, while questions of 'who' and 'why' are considered secondary at best*" (Avigur-Eshel, 2018, pp.512). In particular, some citizens (*the who*) are unable to accept the assigned responsibility by implementing the advice (*the how*), for a variety of reasons (*the why*). In fact, Brown (2019) found that responsibilization could be counterproductive, actually working *against* a sense of personal au-

* Corresponding author at: University of Strathclyde, Glasgow, UK.
E-mail address: karen.renaud@strath.ac.uk (K. Renaud).

https://doi.org/10.1016/j.cose.2023.103301

tonomy in situations where people experienced insuperable difficulties embracing their government-imposed responsibilities.

Clarke (2016) points out that responsibilization can also imply abandonment of citizens. In many cases, responsibilization can lead to anxiety and unwarranted guilt and, in the cybersecurity domain, breaches by cyber criminals. Gray (2009) makes the point that responsibilization affects people differently, especially when power issues are not acknowledged. Ekendahl et al. (2019) explain that responsibilization often myopically focuses on a person's behaviours instead of considering *why* people behave in a particular way. As such, it is a particularly naïve strategy because it does not address causatives, enablers and barriers to acting upon government-issued advice, however comprehensive and valuable it is. This applies particularly to the cybersecurity domain, given that people's insecure behaviours, or lack of precautionary behaviours, are likely to be symptoms of other issues which will not be solved by bombarding people with copious advice and leaving them to get on with it (Renaud & Coles-Kemp, 2022).

In other domains, it has latterly been acknowledged that disasters have occurred because responsibilities have been inappropriately assigned to individual citizens. For example, Pellandini-Simányi and Conte (2020) explain that after the widespread slump of 2008, the over borrowing was blamed on Hungarian banks' unethical behaviours rather than on people failing to embrace their fiduciary responsibilities.

In this paper, we contemplate cyber-related responsibilization. Renaud et al. (2018) argue that a responsibilization strategy is likely to fail when: (1) citizens need to possess exceptional skills to manage the risk, and (2) a citizen's failure to act in accordance with their assigned responsibilities impacts other citizens. Renaud et al. point to cybersecurity as a prime example of this kind of risk, an instantiation of Bergström's (2018) assertion that responsibilizing governments often decentralise responsibility for personal safety and security. When this responsibilization strategy fails, the risk is not managed, and harms result both for the citizen and others in their community.

Certainly, it seems that responsibilizing governments implicitly expect everyone to be cybersecurity experts, based on the existence of their cybersecurity responsibilization strategy. This is undoubtedly unrealistic. In the first place, cybersecurity skills are relatively rare in the general population (John et al., 2020). This is a consequence of the widespread specialisation approach, which is the order of the day in the 21st century (Sowell, 2022). In the second place, computer viruses demonstrate viral qualities, so a failure by one person to take precautions is likely to endanger other people's devices and information (Camp et al., 2019). It is natural for cyber criminals to exploit those who do not, or cannot, shoulder their assigned responsibilities. Given the global success rates of cyber criminals (Zaharia, 2023), it seems appropriate to question the wisdom of governmental cybersecurity responsibilization across the entire population.

Indeed, Renaud et al. (2018) argue for a cybersecurity deresponsibilization of citizens, given the required expertise and epidemiologic nature of cyber compromises. Such deresponsibilization has occurred in other domains, where governments have re-accepted responsibility to protect their citizens from risks related to: slave traders (Rodger, 2004), fire fighting (Mohun, 2013), and the impacts of prostitution (van Wijk & Mascini, 2019), to mention only three examples. These areas epitomise Renaud et al.'s two dimensions: (1) the risks require specialist skills to address, and (2) a citizen's failure to act in accordance with their assigned responsibilities can lead to calamitous or contagious consequences for others.

However, Bredewold et al. (2018) argue against government intervention, claiming that responsibilized citizens ought to be supported in coming up with their own solutions, with the help of family, friends, neighbours and informal carers. Ronald Reagan famously said[1] that the nine most terrifying words in the English language are: '*I'm from the government and I'm here to help*.' This quote might be used by those who would oppose citizen deresponsibilization of cybersecurity, perhaps believing that it would constitute government over reach.

If governments *do* decide to provide more direct cybersecurity-related support to their citizens, we cannot assume that such deresponsibilization would be acceptable to citizens. The purpose of this paper is to explore the acceptability of cybersecurity deresponsibilization to US citizens. As such, we seek to answer the following questions:

RQ1: which factors influence US citizen acceptance of cybersecurity deresponsibilization by government. (Study 1)
RQ2: what are citizens' subjective opinions of the significant factors that emerged from the first study? (Study 2)

We discuss our findings, as well as their research and practical implications, before concluding. Additionally, and given our use of abbreviations during the process of theory development and analysis, we refer readers to the glossary of abbreviations which can be located in the appendix (Table A.5).

2. Theoretical foundationS

2.1. Responsibilization

Hache (2007) explains that responsibilization is a new way of thinking and behaving that is encouraged by governments. In the first place, they make certain kinds of behaviours undesirable (e.g., being on welfare) and other kinds of behaviour desirable (e.g., taking personal responsibility). The government essentially: "*calls for self-transformation, for a change in behavior and way of thinking*" (Hache, 2007), thereby promoting self-sufficiency, under the mantle of self-empowerment. A great deal of research has been published to capture the nature and dimensions of responsibilization (Birk, 2017; Trnka & Trundle, 2017).

However, Hache cites Stengers (2003) to argue that empowerment is a collective rather than an individual process. In effect, the State fails in its duties and then assigns responsibilities to individuals and labels them *irresponsible* if they are unwilling or unable to shoulder these. Hache concludes by asking "*Who has the means for this responsibility*?" Hache cites Castel and Haroche (2001) to argue that responsibilization leads to a 'dual society' where there are those who are able to be responsibilized, and those who are not. The latter are weakened even further by each added responsibility and have to face the consequences of their incapacity to do something that was unfairly imposed on them in the first place.

Under the banner of responsibilization, citizens can have their rights compromised, and their welfare provisions withdrawn (Masquelier, 2017). Some researchers have investigated contexts where responsibilization fails e.g., medical treatment (Dent, 2007) and criminals being released from jail without support (Hart, 2016). Masquelier (2017) points out that responsibilization strategies do not take account of structural inequalities and explains that a responsibilization strategy merely legitimises unequal power relations. The core assumption underlying responsibilization is that individual capacity to embrace such responsibilities is universal (Bauman, 1997). It is hardly necessary to point out that when it comes to cybersecurity, this is naïve.

When responsibilization's underlying assumptions crumble, other institutions will step in to fill the gap. Those stepping in naturally charge for their services, so it is likely that those who need

[1] https://www.professorbuzzkill.com/reagan-terrifying-words/.

support and assistance most will not receive it. In general, leaving citizens at the mercy of profit-seeking organizations tends not to work well in high-risk domains (Renaud et al., 2018).

Pellandini-Simányi and Conte (2020) explain that "*de-responsibilization operates through a top-down, sovereign form of governance. It does not replace, yet constrains the fields of neoliberal governmentality and responsibilization, constituting a hybrid governance system of 'controlled freedom'* " (p.1). Some researchers consider how deresponsibilization could be achieved (Brisman & South, 2015; Pellandini-Simányi & Conte, 2020), but the cybersecurity domain is not directly addressed, apart from Renaud et al. (2021), who suggest that uncertainty might play a role in deterring deresponsibilization efforts. However, these authors did not empirically confirm the role of uncertainty in deterring the acceptance of cybersecurity deresponsibilization.

2.2. Cybersecurity: Current Landscape

Cybercrime is an escalating problem for individuals globally, and in the United States. In 2020, the Internet Crime Complaint Center (IC3) received a record number of complaints of suspected internet crime, with 791,790 complaints and total reported losses exceeding $4.1 billion (IC3, 2020). While organisations are undeniably targeted, so are individuals (Cyber Security Intelligence, 2022). By 2018, one in four Americans had fallen victim to cybercrime (Reinhart, 2018). Individuals are compromised via phishing, vishing, cyber stalking, credit card skimming, intellectual property crimes and identity theft (Cyber Security Intelligence, 2022). This can be devastating for victims (Rochester's News Talk, 2023; TNW, 2019; Her Money Moves, 2019; BBC, 2020). Some demographics, such as the elderly, are particularly vulnerable to cybercrime (Action Fraud, 2019). It is clear that cybercriminals are having unacceptable levels of success in carrying out their nefarious activities.

Now, consider that many governments cyber responsibilize their citizens (Renaud et al., 2020), which means that they are given advice to prevent them from falling victim, and then left to get on with managing the risk. Government reasoning in adopting this strategy appears to be based on three underlying and implicit assumptions: (1) the right advice can be agreed upon, (2) every citizen is able to follow such advice, and (3) one citizen's failure to follow advice will not expose other citizens to harm. These are flawed assumptions. Consider that:

(1) Even experts disagree about the most important precautions that the average computer user ought to implement (Ion et al., 2015; Redmiles et al, 2020), which confirms the elusiveness of a "one truth" set of cybersecurity precautions to implement.
(2) Strawser and Joy (2015) argue that it is unreasonable to assume that the average citizen will have the skills to embrace their cybersecurity responsibilities i.e. to follow technical advice. Renaud et al. (2018) argue that the general public often does not have the skills required to apply the recommended precautions. It is important to note that it is acknowledgement of this facet that often leads to deresponsibilization of citizens in particular risk domains (Pellandini-Simányi & Conte, 2020).
(3) Cyber-attacks tend to spread across networks. Computer viruses demonstrate the same contagion as viruses that infect humans (Camp et al., 2019). This means that one person's misfortune in falling victim is likely to impact others as well. As an example, consider the WannaCry ransomware attack of 2017, which quickly spread across the UK's national health service, crippling some health boards and preventing surgeries and treatments until the ransomware's spread had been halted.

2.3. Cybersecurity Deresponsibilization Acceptability

We wanted to understand what would make deresponsibilization acceptable and effective if governments came to the realisation that their cybersecurity responsibilization strategy was unworkable, at least for particular sectors of society.

Deresponsibilization relies on citizen willingness to accept assistance from governments. This will only happen if they trust their government, given that trust is a necessary prerequisite for acceptance to occur (Salvi & Spagnoletti, 2020). The notion of trust, according to Schoorman et al. (2007), is the willingness of a trustee (the recipient of trust or the party to be trusted – the government) to perform a particular function important to the trustor (the party that trusts the target party – the citizen). Such trust is based on a trustor's prior experience of the entity asking for trust (Liang et al., 2021).

Grimmelikhuijsen and Knies (2015) explain that trust can be measured on three dimensions: benevolence, competence and integrity. In exploring deresponsibilization acceptance factors, we will thus measure: (1) perceived government cybersecurity-related benevolence and (2) perceived government cybersecurity-related benevolence. Integrity is defined as: "*the extent to which a citizen perceives a government organization to be sincere, to tell the truth, and to fulfill its promises*" (p. 587). Cybersecurity deresponsibilization is likely to involve installation of government-issued or -recommended software, or to permit government bodies to access their devices in order to "clean" them of malware. Acceptance of deresponsibilization will require citizens to trust in the integrity of government issued software. Hence, we also measure: (3) trust in technology as a proxy for integrity in this context.

(1) Perceived Governmental Cybersecurity Benevolence

The Snowden revelations shook Americans' faith in the benevolence of their government (Byman & Wittes, 2014; Chen, 2016). This is relevant to the cybersecurity deresponsibilization agenda, because people might be concerned about allowing the government to gain control over their devices. Indeed, Degli-Esposti et al. (2021) make a direct link between perceived governmental benevolence and acceptance of surveillance technologies. A lack of government oversight might compromise perceptions of government benevolence (Moore, 2011). It is this aspect that Snowden attempted to highlight with his activities.

Hence, we argue that:

Hypothesis 1 (H1)**.** Perceived governmental cybersecurity benevolence will positively influence citizens' willingness to be deresponsibilized. In other words, the more benevolent citizens perceive their government to be, the more likely they are to accept cybersecurity deresponsibilization.

(2) Perceived Governmental Cybersecurity Competence

According to Berger and Calabrese's definition (p.41) uncertainty about another party is an "(in)ability to predict and explain their actions". Even though their study dealt with individuals and their behaviours, the principles are relevant to the cybersecurity deresponsibilization of citizens. In particular, existing trust in government competence, based on their previous performance in other domains, is likely to carry over when new trust needs to be established. For example, Liang et al. (2021) found that perceptions of provider competence exerted a significant positive influence on the adoption of mobile government cloud services whereas there was no demonstrable impact of perceived risk. Given that these researchers are reporting on a government cloud service, we can conclude that government-based deresponsibilization is also likely to depend on perceived competence.

We therefore argue that:

Hypothesis 2 (H2)**.** Perceived cybersecurity competence will positively influence citizens' willingness to be deresponsibilized. In other words, the more competent citizens perceive their government to be, the more likely they are to accept cybersecurity deresponsibilization.

(3) Trust in Technology

Establishing trust in technology is likely to be central to the deresponsibilization discourse because it will introduce a measure of interdependence into the relationship between the citizen and the government in a risk-laden context. In particular, deresponsibilization in the cybersecurity domain would require citizens to be willing to trust the government to manage their cybersecurity for them to a certain extent.

The same applies from a cybersecurity perspective, where trust in technology, as endorsed or used within the context of government systems, also likely influences citizens' willingness to be deresponsibilized wrt. cybersecurity. For example, Dewi et al. (2022) found trust in technology significantly influenced user satisfaction within the context of a governmental sustainability system. In particular, the authors found trust in technology (together with trust in government) to significantly influence the benefits users perceive. Abdulkareem et al. (2022) modelled trust in technology as a formative indicator of trust in e-government which, in turn, significantly influenced e-participation – both as a causal and direct antecedent. Similarly, Jasimuddin et al. (2017) reported that citizens' intention to use smart government services was significantly influenced by trust in technology. This was confirmed by a study carried out by Habib et al. (2019) where trust in technology acted as a significant direct antecedent of behavioural intention – albeit within the context of smart city responsibilisation and acceptance. Leroux and Pupion (2022) found that trust in technology was significantly related to citizens' intended adoption of IoT applications. Within the context of cybersecurity, Apau and Koranteng (2020) found that trust predicted adoption of e-commerce.

Based on the theory reviewed above, we argue that:

Hypothesis 3 (H3)**.** Trust in technology will positively influence citizens' willingness to be deresponsibilized with respect to cybersecurity. In other words, the more citizens trust technology, the more likely they are to accept cybersecurity deresponsibilization.

3. Methodology: Study 1

To collect quantitative data, we conducted a cross-sectional survey after receiving ethical clearance from the primary author's ethics review board. Potential respondents had to be registered users of the Prolific survey platform. Prolific is a crowdsourcing survey platform that has been successfully used in similar (and recent) behavioural research (Eyal et al., 2021; Geldsetzer, 2020; Schodt et al., 2021; Stanton et al., 2022) enabling researchers to enhance the demographic diversity of their study samples (Palan & Schitter, 2018). Having said this, it is advisable to use specific techniques to improve data quality when using platforms such as Prolific. Such techniques include the provision of clear instructions and definitions, removal of responses with missing values, and attention checks (Abbey & Meloy, 2017; Gummer et al., 2018; Hauser & Schwarz, 2016; Lowry et al., 2016). We used all of these techniques in addition to obtaining informed consent from all the respondents.

3.1. Data Collection

Our quantitative data was collected in 2022, resulting in an initial dataset containing 325 ($n = 325$) responses. These responses were reduced to 315 ($n = 315$) after filtering unsuitable responses. To be considered suitable, a response had to fulfil the following criteria:

- The response had to be complete with all the questions answered and no missing values.
- The two attention trap questions' answers had to be correctly answered. In this case, we asked people to choose a particular response to a question e.g., "choose strongly agree".

Table 1
Demographic distribution of sample ($n = 315$).

Variable	Frequency	Percentage (%)
Gender		
Male	153	48.57
Female	153	48.57
Non-binary / third gender	6	1.90
Prefer not to say	3	< 1
Age		
18–30	96	30.47
31–40	95	30.15
41–50	56	17.77
51–60	43	13.65
Over 60	23	7.30
Prefer not to say	2	< 1
Level of education		
No degree or up to high school	116	36.83
Bachelor's degree or equivalent	134	42.54
Master's degree and above	57	18.09
Prefer not to say	8	2.54

As per Table 1, a near equal number (48.57%) of males and females completed our questionnaire. Moreover, 60.62% of the respondents were under 41 years of age, with most having obtained at least a bachelor's degree (60.63%). Notably, nearly equal numbers of respondents fell into the 18-30 and 31-40 age groups (30.47% and 30.15% respectively).

3.2. Measures Used

Perceived Governmental Cybersecurity Benevolence (PGCB). Respondents' perceptions with regards to their government's cybersecurity benevolence were evaluated by adapting established items used in studies with similar conceptual contexts (Gefen & Straub, 2004; McKnight et al., 2002). These items all made use of five-point Likert scale responses (1 = *strongly disagree* and 5 = *strongly agree*).

Perceived Governmental Cybersecurity Competence (PGCC). To capture respondents' perceptions regarding their government's cybersecurity competence, we used items adapted from Grimmelikhuijsen and Porumbescu (2013). In short, these items focused on how capable, effective, skilful and professional governments are perceived to be in relation to cybersecurity matters. The same five-point Likert scale responses were used as with PGCB.

Trust in Technology (TTECH). Respondent's level of trust in technology was measured by making use of three items adapted from Lankton et al. (2015). Like those items associated with PGCB and PGCC, five-point Likert scale response options were used.

Willingness to be Deresponsibilized (WDR). To capture respondent's willingness to be deresponsibilized from a cybersecurity perspective, we had to adapt and recontextualise select items from Wu et al. (2016). We were particularly interested in understanding to what extent respondents (i.e., US citizens) are willing to accept their government's assistance when it comes to cybersecurity matters. This included to what extent they would agree to allow the government to perform certain cybersecurity tasks for them. Given the novelty of this phenomenon (cybersecurity deresponsibilization), we had to develop two new items – all of which loaded

above the acceptable threshold of 0.7. The same five-point Likert scale responses were used as outlined above.

3.3. Analysis and Results – Study 1

To analyse our results, we used a variance-based estimator for structural equation modelling (Benitez et al., 2020). In particular, partial least squares path modelling (PLS-PM). PLS-PM is particularly adept at estimating models with low structure making it a good choice amongst recent research within the information systems discipline (Jaeger & Eckhardt, 2021; Sarkar et al., 2020; van der Schyff et al., 2020). When used to investigate behavior-centric models, theoretical concepts are often operationalized by a measurement model – either reflective or causal-formative. However, it is the former of these measurement models used within the context of this study.

3.4. Evaluating the Measurement Model

Before investigating the structural properties of our model, we had to ensure that it was both valid and reliable. This required us to inspect various thresholds related to the latent variables within the research model. Unlike emergent variables, latent variables enable researchers to measure that which cannot be directly observed. This often includes variables which are behavioural in nature such as those contained within our research model (e.g., citizen perceptions and trust).

Within the context of PLS path models, researchers are typically required to investigate both convergent and discriminant forms of validity. Only if both of these are proven can it be said that the measurement model is valid. According to Hair et al. (2017) convergent validity enables researchers to assess the extent to which the items associated with a particular latent variable actually measure that variable. To assess our model from a convergent perspective, we used three criteria. *First*, we ensured that all the items associated with our latent variables exhibited outer loadings in excess of 0.7. *Second*, we inspected the significance (and magnitude) of the outer loadings. In particular, the *t*-statistics (also referred to as the *t*-values) of these outer loadings. These had to exceed 1.96 to be deemed significant at the 95% confidence interval (see Table A.1 in the Appendix). *Third*, we ensured that all the latent variables exhibited an average variance extracted (AVE) value in excess of 0.5 (see Table 2 below). All the values we inspected satisfied the above, enabling us to conclude that our measurement model is valid from a convergent perspective (Benitez *et al.*, 2020).

According to Benitez et al. (2020), discriminant validity entails proving that a research model's latent variables are statistically different. To prove this, we used three criteria. *First*, and using the Fornell-Larcker criterion, we ensured that the square root of each latent variables' AVE was larger than all the correlations between all the latent variables. These square root values are underlined and presented in bold within Table 2 below. *Second*, we ensured that all the items associated with a particular latent variable loaded highest on that variable (i.e., no apparent crossloading) (see Table A.2 in the Appendix). *Third*, we used the heterotrait-monotrait (HTMT) ratio values of our model's latent variables (Table A.3). Literature suggests that the HTMT values should be lower than 0.85 (Hair et al., 2017; Hair et al., 2019). Our measurement model statistics satisfied all of the above criteria, enabling us to conclude that our model is valid from a discriminant perspective.

We also assessed two additional aspects of our measurement model namely, multicollinearity and common method bias. To eliminate multicollinearity all the items within our questionnaire had to exhibit variance inflation factor (VIF) values below 5.0 (Hair et al., 2019). Given that the items' VIF values were well below the critical threshold of 0.5 (Table A.1), we concluded that the measurement model did not exhibit signs of multicollinearity. To evaluate common method bias we used a method pioneered by Ned Kock (2017), which argues that a model is devoid of common method bias if the VIF value of a latent variable is lower than 3.3. All of our latent variables' VIF values were below this threshold enabling us to eliminate common method bias (see Table A.4 in the Appendix).

In addition to the above, we also assessed the reliability of our measurement model. Here, we used two criteria namely, Cronbach's alpha (CA) and composite reliability (CR). Literature suggest that each latent variable should exhibit a CA and CR value above the threshold of 0.7 (Benitez et al., 2020; Peterson & Kim, 2013). Our model's latent variables' CA and CR values were well above this threshold enabling us to conclude that our measurement model is reliable (see Table 2 below).

3.5. Evaluating the Structural Model

The research literature suggests that a structural evaluation should focus on path coefficient estimates, effect sizes (f^2), and R^2 (coefficient of determination) (Benitez et al., 2020; Hair et al., 2019). Notably, researchers should also evaluate overall model fit. Given the explanatory (as opposed to confirmatory) nature of this study, we focused on our model's path coefficients, R^2 values, and relevant effect sizes. Path coefficient estimates are an indication as to the change in an endogenous variable measured in terms of standard deviation (SD). Specifically, when an exogenous variable's SD is increased by one. The assumption here being that all other exogenous variables remain constant. Using our measurement model as an example, if *trust in technology* (an exogenous variable) increases by one SD it will increase *willingness to deresponsibilize* (our model's endogenous variable) by 0.398 SDs. Collectively, our path coefficient estimates are presented in Table 3 below, indicating that two of the three paths in our model are statistically significant.

As stated, we also evaluated the effect sizes associated with the paths tested. Notably, these are measures of effect without taking the sample size into consideration and are generally categorised into one of three ranges. These effect size ranges are: 0.020 – 0.150 (a weak effect), 0.150 – 0.350 (a medium effect), and effects larger than 0.350 (a large effect) (Cohen, 1988). As per Table 3, it is clear that respondents' perceptions of their government's level of cybersecurity benevolence exerts the largest effect when considering cybersecurity deresponsibilization. Interestingly, respondent's level of trust in technology does not have a significant influence on cybersecurity deresponsibilization.

Next, we evaluated our model's in-sample predictive power (i.e., R^2). In this regard, Benitez et al. (2020) suggests that researchers

Table 2
Measurement model statistics.

Latent Variable	CR	CA	AVE	1	2	3	4
perceived governmental cybersecurity benevolence (1)	0.917	0.880	0.735	0.858			
perceived governmental cybersecurity competence (2)	0.939	0.918	0.754	0.669	0.869		
trust in technology (3)	0.908	0.849	0.768	0.448	0.414	0.877	
willingness to be deresponsibilized (4)	0.936	0.909	0.786	0.672	0.578	0.398	0.887

Table 3
Path coefficient estimates (*** significant at p < 0.01; ** significant at p < 0.05; ns = not significant).

Hypothesis	Path tested	β	f ^{2}	*t*-statistic	Supported
H1	PGCB → WDR	0.503	0.246 (medium effect)	7.562***	Yes
H2	PGCC → WDR	0.201	0.043 (small effect)	3.293***	Yes
H3	TTECH → WDR	0.094	0.015 (no effect)	1.916 ns	No

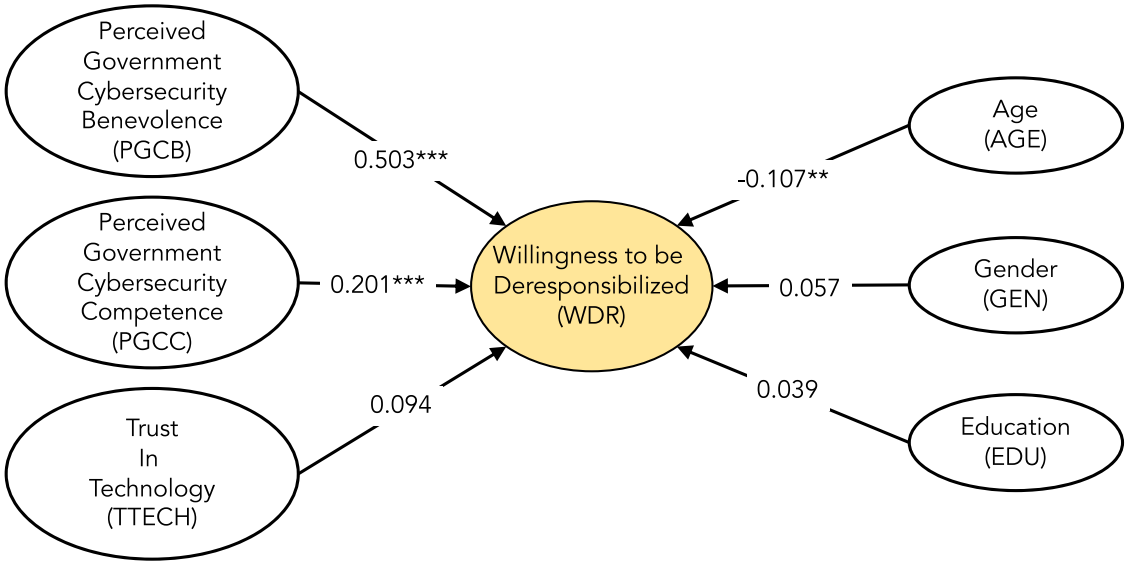

Fig. 1. Research Model (*** significant at p < 0.01; ** significant at p < 0.05).

should not attempt to judge the R^2 value based solely on their magnitude. Instead, an analysis of similar models should be conducted to ascertain what an acceptable R^2 value might be within that field of interest. Given the novelty of our study (and research model), we found it difficult to locate studies that measured deresponsibilization. Not to mention cybersecurity deresponsibilization. For example, the study by Wu et al. (2016) was deemed relevant given it use of the word *willing* within the context of measuring a desired behavior – albeit respondents' willingness to wear smart watches. Interpretations aside, we obtained a R^2 value of 0.503. This means that our chosen exogenous variables explain 50.3% of the variance in our endogenous variable (*willingness to be deresponsibilized*). Given the novelty of our phenomenon of interest (and our research model), we concluded that our R^2 value is of an acceptable magnitude. To complement our R^2 analysis we evaluated the out-of-sample predictive power of our model, commonly referred to as Stone-Geisser's Q^2. Given that the Q2 value of our endogenous variable (37.7%) far exceeded 0, we concluded that our out-of-sample predictive power was adequate.

Finally, and to obtain empirical evidence of our theoretical position, we evaluated the overall model fit. In this regard, our model exhibited a SRMR value (0.04) far below the acceptable threshold of 0.08 (Benitez et al., 2020). Based on the results of the measurement and structural evaluations we concluded that our research model is sound, enabling us to formally test our hypotheses.

Using the results presented in Table 3, we reject our third hypothesis (H3). As such, our results indicate that trust in technology does *not* play a significant role in influencing perceptions about cybersecurity deresponsibilization. Our results do, however, provide support for the first and second hypotheses (H1 and H2) indicating that the more respondents perceived their government to be benevolent and competent (in terms of cybersecurity matters), the more willing they are to accept cybersecurity deresponsibilization. It is worth noting that we found no evidence to suggest any significant interaction between PGCB and PGCC. Although not directly explored here, the absence of such an interaction is also interesting. It may be indicative that even though a government means well in its interaction with citizens (i.e., is benevolent), this may not directly translate to being perceived competent in the cybersecurity domain. The converse is also true in that a high degree of perceived competence does not necessarily imply that they are using such competence for the greater good (Degli-Esposti et al., 2021). We also evaluated the influence of several control variables; in particular gender, education, and age with only the latter significantly influencing deresponsibilization willingness (β = -0.107, p <0.05) Fig. 1.

Having identified the influential factors, we now proceeded to gauge subjective opinions of these factors by US citizens, as described in the next section.

4. Methodology: Study 2

To assess subjective perceptions of the influence of the significant factors identified in Study 1 on willingness to be deresponsibilized wrt. cybersecurity, we used Q-methodology, as proposed by Stephenson (1935). This mechanism is designed to study subjectivity systematically. Q-methodology is an instantiation of Cultural Consensus Theory (Weller, 2016), which provides a framework for the measurement of beliefs as cultural phenomena. It allowed us to assess the perceptions shared by groups of US citizens and informed as to what people consider to be the culturally appropriate answers to a series of related questions (the overriding theme, in our case, being cybersecurity deresponsibilization).

The findings are not representative of the general population. Study 1 was designed to give some indication of this. Our second study, however, sought to reveal the nature of subjectivity related to deresponsibilization. Not '*how are people thinking about being deresponsibilized?*', but rather: '*what is the nature of their think-*

ing about being deresponsibilized?' This focus on revealing different perspectives renders the issue of large participant numbers 'unimportant' (Brown, 1993). The Q-methodology method serves to reveal correlations between subjects across a sample of variables, referred to as the Q-set, composed of Q-statements. Factor analysis isolates the most influential "factors" representing cultural ways of thinking. The method's strengths are that it applies sophisticated factor analysis, but also supports a qualitative analysis by eliciting responses which explain people's ranking of different statements. This exploratory technique is not designed to prove hypotheses. What it can do is provide insights into 'potentially complex and socially contested' issues (Watts & Stenner, 2005). In our case, these issues were related to the findings of Study 1.

Participants sort statements into a fixed quasi-normal distribution, ranging from -4 (strongly disagree) to +4 (strongly agree). Participants are then allowed to amend and confirm their rankings and then asked for open-ended comments for the statement they agreed and disagreed with most (ranked +4 and -4 respectively). This serves to gain an insight into the range of perceptions related to deresponsibilization in the USA (Brown, 1993).

4.1. Deriving Statements

Based on our findings from Study 1, we derived statements from the research literature that would help us to explore subjectivity about these factors. These are listed in Table 4 below.

4.2. Recruitment

Three pilot tests were undertaken and timed, to get a sense of the time needed for the Q-Sort. Based on feedback from the pilot testers, unclear statements were subsequently refined and clar-

Table 4
Q statements.

	Cybersecurity Governmental Benevolence (PGCB)		
1	My government does not want to spend money to help its citizens with cyber related matters	Adapted from Arnal (2020)	No Benevolence (no monetary assistance)
2	I believe my government wants what is best for me in terms of my cyber well-being		Benevolent (best interest at heart)
3	My government is concerned about my cyber welfare and would not knowingly do anything to hurt me	Adapted from Mayer and Davis (1999)	Benevolent (concern for cyber welfare)
4	My government only really looks out for themselves	Mayer and Davis (1999)	No benevolence (government selfishness)
5	If I were to have cyber-related problems with my devices, my government would want to offer assistance and support	Adapted from Grayson et al. (2008)	Benevolent (will help)
	Perceived Governmental Cybersecurity Competence (PGCC)		
6	My government would be capable at making informed cyber related decisions on my behalf	Adapted from Etzioni (2018)	Competent (informed decision making)
7	I am uncertain about how capable my government would be at managing my cyber well-being (i.e., online safety and security)	Adapted from Renaud and Weir (2016)	Incompetent (uninformed decision making)
8	Governments these days have fantastic cyber abilities – they are definitely capable of helping citizens		Competent (capable at cyber assistance)
9	Government units are always being hacked – not that capable		Incompetent (low cyber self-efficacy)
10	I feel the current government, all in all, is competent and doing a very good job.	Kay et al. (2008)	Competent (doing well)
	Willingness to be Deresponsibilized (WDR)		
11	I would trust my government to have my best interests in mind and to secure my devices for me	Beldad et al. (2012)	Willing (best interest at heart)
12	I am not confident with IT, so cybersecurity is a real challenge	Johnstone (2007)	Willing (lack of self-efficacy)
13	I am not confident with IT so I need more support with my cybersecurity	Birk (2017)	Willing (lack of self-efficacy)
14	When an important cyber issue or problem arises, I would feel comfortable depending on my government	McKnight et al. (2002)	Willing (accept government dependence)
15	Based on my experience with my government in the past, I know they provide good services.	Hsieh et al. (2010)	Willing to deresponsibilise (best interest at heart)
	(Un)willingness to be Deresponsibilized (WDR)		
16	If I fail to secure my online information and devices, it is no one else's fault	Giesler and Veresiu (2014)	Autonomy (high cyber self-efficacy)
17	If I were to experience a cyber-attack I would blame myself	Gray (2009)	Autonomy (high cyber self-efficacy)
18	I am not a child – I do not need someone else to help me with my cyber well-being (i.e., online safety and security)	Brisman and South (2015)	Autonomy (high cyber self-efficacy)
19	My government wants to place its citizens under surveillance, so why would I let them take responsibility for my cyber well-being (i.e., online safety and security)?	Preibusch (2015); Bredewold et al. (2018)	Unwilling (surveillance concerns)
20	My government tells so many lies that I would not let them onto my devices	Adapted from Hsieh et al. (2010)	Unwilling (government lies)
	Cyber Risk Perceptions & Influences		
21	Children learn about cybersecurity at school but senior citizens need more government support	new statements	Age is relevant
22	Everyone is vulnerable to cyber attacks regardless of age		Age is irrelevant
23	The underlying technology is insecure – my government needs to hold technology providers accountable		Trust in technology (technology inherently insecure)
24	We need to incentivise technology providers to make our devices more secure – they are the ones who can do it		Trust in technology (incentivise security of technology)
25	I am not interested in cybersecurity		Trust in technology (lack of interest in cyber)

ity improved. Forty US-based participants were recruited on the Prolific platform, balancing genders (https://www.prolific.co/). This is consistent with recommended Q-methodology participant group sizes (Watts & Stenner, 2005). We paid participants £3 for 12 minutes of labour, exceeding the UK minimum wage. Ethical approval was obtained from the University of Strathclyde ethical review board. Participants did not provide any personal data beyond age and gender, ensuring that participation was anonymous.

4.3. Analysis

We extracted factors using the centroid technique and applied a varimax procedure for factor rotation. Factors with an eigenvalue in excess of 2.00 having at least three significantly-loading participants were retained for interpretation.

4.4. Findings

It is interesting that all respondents, irrespective of the factor they fell into, agreed or strongly agreed with statement 22 ("*Everyone is vulnerable to cyber attacks regardless of age"*), suggesting that they appreciated the existence and extent of the cybersecurity threat.

Factor A: Do not trust the government's benevolence nor their competence

This factor explains 32% of the variance with 18 respondents (12M/6F) aged 19 to 66. One participant said, related to statement 19: "*My government regularly talks about stripping away my right to privacy online to fight criminals when their bills wouldn't affect the criminals at all. They only care about watching every person in the world at all times to prevent any threat to their incestuous power*". Another echoed this: "*Well with technology and data being weaponized these days I'm just over the government trying to tell me it's for my safety when the harsh reality is just so they can have more data and control over the populace*". They were also scathing about government competence in disagreeing with statement 10: "*I don't think they are competent and I don't think they're doing a very good job due to their prior track record and history*" and "*I do not feel that the current government is competent at all, nor very good at doing its job. Its job should be to help and protect its citizens, but instead it profits the wealthy*". Finally, one said: "*The government is more interested in having access to people's private information than securing it from outside attacks*". One cannot see these respondents ever accepting government cybersecurity deresponsibilization.

Factor B: Trust in government's benevolence and competence

This factor explains 13% of the variance with 6 respondents (2M/3F/1 no response) aged 28 to 50. This group clearly believes in the competence of their government: In agreeing with statement 2, they say: "*This trust builds over time, whenever I or our community faces any unwanted situation including online matter our government handle it very swiftly and smoothly and we are happy for it*" and "*This trust builds over time, whenever I or our community faces any unwanted situation including online matter our government handle it very swiftly and smoothly and we are happy for it*". This group might well accept cybersecurity deresponsibilization.

Factor C: Unsure about government competence and thinks technology providers have a role to play

This factor explains 12% of the variance with 7 respondents (2M/4F/1 no response) aged 24 to 41. This group did not feel that help from the government would infantilise them, in commenting on Statement 18: "*I am not an expert on cyber security, so I would welcome any assistance*". They would like to see technology providers step up to make technology more resilient: "*People who are most familiar with the technology should be more scrutinized with regulation and held to the highest standards*". There are doubts about the government's ability to secure online services: "*The internet is still such a new thing– it's difficult for anyone to navigate it safely or to prepare for every negative thing*". They are also not convinced that governments care about their cybersecurity: "*The government doesn't seem all that concerned about the average person's cyber-security. I almost never hear politicians talk about this subject*".

Factor D: Do not think their government is trying to spy on them and happily accept cybersecurity responsibilities.

This factor explains 9% of the variance with 3 respondents (1M/2F) aged 37 to 60. This group were minded to trust the government with their devices: "*I trust mostly on the Government on certain devices, so I would want them to help out only when needed*" and "*Most government officials are well-educated and experienced*". They also disagreed with statement 19: "*I don't think that this is true. I don't think that big brother is watching. we're not there yet*". Yet, they accepted responsibility for their own cybersecurity: "*It's always a little bit my fault, but I'm pretty sure the people doing the hacking are the most at fault*" and "*currently there is no larger protection beyond what you implement yourself*".

5. Research Questions & Discussion

In answering RQ1, the objective of the first study was to examine the factors that influence citizens' willingness to accept cybersecurity assistance and support from their government, i.e., deresponsibilization. We found that perceived government benevolence and competence were significant predictors of being willing to be deresponsibilized in the cyber realm. Age, too, emerged as a significant factor.

Our second study revealed subjective opinions of the benevolence and competence of the US government in the cyber domain, answering RQ2. We did not find evidence of widespread faith in the benevolence nor the competence of the US government in the context of cybersecurity. Our findings suggest that the majority of our respondents would not welcome cybersecurity deresponsibilization by US government bodies. This is not because they did not believe that in the cybersecurity risk to themselves; they are well aware of the threats. It is primarily because there is little faith in the benevolence and competence of the government – probably based on experience of government bodies' performance in other domains. Moreover, given that we have just emerged from two years of pandemic, which many believe has been poorly managed (Gallo et al., 2022), trust in government might have diminished as a consequence.

If we view responsibilization through the lens of government failure, rather than individually-assigned responsibility, our findings become important. Three of our factor groups had doubts about government competence, as well they should, given our discussion of the motivations for cybersecurity responsibilization. Two groups were concerned about giving governments control over their personal devices – evidencing a lack of trust that came to the fore during the pandemic. Moreover, there were clear concerns about government over-reach, which is echoed by Myers (2019).

Although we found respondents to be averse to cybersecurity deresponsibilization overall, when considering the respondents' age groups, matters become even more interesting. Our results suggest that the older an individual becomes, the *less* likely they would be to accept cybersecurity deresponsibilization. This contradicts the findings of gerontological studies focused on technology use where extant research indicates that older individuals are *more* likely to require (and request) technological support (Marler & Hargittai, 2022; Özsungur, 2019; Yap et al., 2022). Our findings suggest that older individuals are more distrustful of their government (and the technologies they use) than younger individuals. Research indicates that in some (extreme) cases, older adults may

consistently reject digital technologies (Knowles & Hanson, 2018). We conclude that older individuals would rather be responsible for their own online safety and security; despite any (technical) difficulties they might experience in doing so. Although not directly related to all aspects of cybersecurity, extant research on information privacy indicates that apathetic forms of privacy protective behavior (e.g., acceptance of information security defaults) are higher for younger individuals (van Ooijen et al., 2022), despite their greater ability to configure information privacy settings. This further substantiates the claim that older individuals are not as willing to be deresponsibilized as their younger counterparts, who seemingly have no objection to this, despite probably needing help more than younger citizens.

5.1. Practical Implications

The status quo is no longer feasible – too many are falling victim to cyber criminals. They are not being given any direct support either in securing their devices or in reporting and recovering from attacks. If governments want to take a more proactive role in supporting their citizens in the cybersecurity realm, they will have to re-think their responsibilization strategies, as well as the mechanisms they could use to reverse them, even partially. Given that genuine empowerment is a societal construct, it might be preferable for charities and other third-party community support sectors to play an active role in supporting those who are unable to embrace cybersecurity responsibilities, perhaps using volunteers to provide such support (Ilcan & Basok, 2010). It might be preferable to engage society and local communities to fill the gap that governments have created with their cybersecurity responsibilization strategies (McCorry & Fuller, 2021). As such, we strongly dispute Margaret Thatcher's arguments suggesting that there is no such thing as society (Masquelier, 2017), and suggest that it is members of society who can best support each other in defeating cyber criminals. We suggest a fourfold strategy.

First, cybersecurity events, such as workshops, seminars, and conferences, could raise awareness. Hackathons, in particular, have proven an effective way to educate individuals about cybersecurity (Workman, 2021).

Second, local communities could foster online discussions on a variety of platforms to share experiences. Such forms of communication, especially via social media, have been proven effective at updating individuals about current (and possibly localized) cybersecurity threats (Labuschagne et al., 2011; Pham et al., 2021). Social media platforms provide direct lines of communication between cybersecurity experts and platform users. This facilitates timely distribution of information about emergent threats as well as informing people how to protect themselves. The latter also ties in with cybersecurity awareness campaigns. Cybersecurity posters could be displayed in libraries and other venues where people meet. Such posters could be complimented by social media-based cybersecurity awareness which are particularly effective at reaching younger individuals (Corallo et al., 2022; Quayyum et al., 2021). Given our age-related findings such an approach is likely to be be particularly impactful.

Third, local communities could offer formal localised cybersecurity training in way that is more accessible to community members. Language barriers become less of a problem as the training could be tailored to suit the needs of that community (Chang & Coppel, 2020).

Lastly, and to tie in with the formal government structures, local communities should collaborate with local authorities and law enforcement.

However, this has to be adequately resourced (Swyngedouw, 2009). Governments responsibilizing should fund external entities to provide essential support, ensuring that a dual society is not perpetuated in the cyber domain. This, then, would be true empowerment of individual citizens, and would lead to less success for cybercriminals preying on vulnerable individuals who are not able to follow government advice.

5.2. Research Impact and Implications

Cybersecurity deresponsibilization is a topical and important area which is ripe for more research, especially as its wisdom is being questioned due to the increasing success of cyber criminals. We have proposed some factors here which are clearly significant, in terms of accepting cybersecurity-related support, and finding the best way of identifying these people. Future research ought to investigate how best to support them, and also to flesh out the mechanisms by which charities could support citizens – achieving third-party deresponsibilization, as it were, in a rigorous and effective way. Future research may wish to provide respondents with a specific scenario before completing surveys. Moreover, and given the multidimensional nature of the theoretical constructs we studied, multiple scenarios could be developed and evaluated, enabling researchers to gain a more holistic (and somewhat context-sensitive) view of cybersecurity deresponsibilization.

Developing a multidimensional research instrument would assist in this regard as it would enable researchers to replicate studies which would aid comparative work going forward. Having said this, such an approach would require conducting these studies using larger probabilistic samples, especially, if one were to stratify across various age groups, which would be advisable given our age-related findings. Our results therefore imply that further gerontological cybersecurity studies are warranted. This would hep us to understand why older individuals are less likely to accept cybersecurity deresponsibilization, but also to understand why younger individuals are more likely to accept deresponsibilization. Understanding this disparity is particularly important if one considers the fact that espoused beliefs and values may become entrenched as the youth grow older. As such, if the youth's acceptance of cybersecurity deresponsibilization is grounded in a sense of apathy, as opposed to cybersecurity awareness and knowledge, we may eventually end up with a society that sees no value in cybersecurity awareness and education, with a learned helplessness and over reliance on others. Studies focused on the above should, however, focus on these issues by recruiting participants from several countries as our results are US specific. Inclusion of developing countries is desirable, not to mention more socialist countries, as opposed to the capitalist approach adopted by the US.

This would require conducting these studies larger sample sizes in a longitudinal manner so as to isolate (as much as possible) the consequences of citizen perceptions post COVID-19. To further enhance data subjectivity, a third means of data collection could be added by means of focus groups or semi-structured interviews. Such forms of qualitative data collection will enable researchers to further examine those statements which seemingly played a significant role when considering cybersecurity deresponsibilization. Specifically, those with which participants strongly agreed or disagreed.

5.3. Limitations and Future Research

We carried out this study with US citizens, given that the US prizes individual responsibility (Brewer & Stonecash, 2010). It would be important to replicate this study in other countries, perhaps more socialist countries such as Canada and the UK, to give us greater insights into the acceptance of deresponsibilization endeavours. The issue of trust in governments is likely to pervade in

other countries too, but their perspective on government support might differ given the socialist nature of their governance.

Second, our study was conducted in the aftermath of the COVID-19 pandemic. Given the central role played by governments during the pandemic, it is likely that citizens' reduced perceptions of government competence (Telesca, 2021) and of their benevolence (van Oost et al., 2022) have been coloured by the challenging period they have lived through. It is likely to take some time for perceptions to return to pre-pandemic levels, if indeed they go back to pre-pandemic levels.

6. Conclusion

In these studies, we investigated the feasibility of cybersecurity deresponsibilization in the US. First, we objectively investigated the influence of factors on citizens' willingness to accept cybersecurity deresponsibilization. Having identified the influential factors, we gauged subjective perceptions using statements related to the significant factors. We conclude that citizens will be willing to be cybersecurity deresponsibilized if they believe that their government is both competent and benevolent *in the cybersecurity domain*. It is unfortunate that many of our respondents were unconvinced. This might well be a consequence of the way the US government handled the COVID-19 pandemic. Predicting how these beliefs might be restored, post-pandemic, is out of scope for our paper. We do conclude, however, that if more support is to be provided to citizens to improve their cybersecurity, it might be best for governments to fund charities to provide direct support and assistance to those who are unable to embrace their cybersecurity responsibilities without assistance.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Karen Renaud: Conceptualization, Methodology, Investigation, Data curation, Writing – original draft, Writing – review & editing. **Karl van der Schyff:** Methodology, Investigation, Data curation, Formal analysis, Writing – original draft, Writing – review & editing. **Stuart MacDonald:** Writing – original draft, Writing – review & editing.

Data availability

Data will be made available on request.

Acknowledgments

We acknowledge funding from the South African National Research Foundation for this research.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.cose.2023.103301.

References

Abbey, J.D., Meloy, M.G., 2017. Attention by design: Using attention checks to detect inattentive respondents and improve data quality. J. Oper. Manag. 53, 63–70. doi:10.1016/j.jom.2017.06.001.

Abdulkareem, A.K., Abdulkareem, Z.J., Ishola, A.A., Akindele, I.T., 2022. Does e-government impact e-participation? The influence of trust in e-government. Int. Rev. Public Adm. 27 (2), 91–110. doi:10.1080/12294659.2022.2071540.

Action Fraud, 2019. Most Vulnerable In Society Are More At Risk Of Falling Victim To Fraudsters [Internet]. Action Fraud [cited 2023 Mar. 18] Available from: https://www.actionfraud.police.uk/news/most-vulnerable-in-society-are-more-at-risk-of-falling-victim-to-fraudsters.

Apau, R., Koranteng, F.N., 2020. Impact of cybercrime and trust on the use of e-commerce technologies: an application of the theory of planned behavior human factors in information and cyber security view project social networking, knowledge sharing & user behavior view project. Artic. Int. J. Cyber Criminol. 13 (2), 228–254. doi:10.5281/zenodo.3697886.

Arnal, M., 2020. The transformations of medicalization of pain relief in the organization of perinatal care system in Quebec. Soc. Theory Health 19 (3), 220–245. doi:10.1057/S41285-020-00133-1.

Avigur-Eshel, A., 2018. Synthesizing depoliticization and responsibilization: The case of financial education in Israel. Compet. Change 22 (5), 509–528. doi:10.1177/1024529418798115.

Bauman, Z., 1997. Postmodernity and its Discontents. Polity, Cambridge.

BBC, 2020. Woman loses £320,000 in 'Romance Fraud' Scam [Internet]. BBC [cited 2023 Mar. 18. Available from: https://www.bbc.co.uk/news/uk-england-somerset-54613937.

Beldad, A., van der Geest, T., De Jong, M., Steehouder, M., 2012. A cue or two and I'll trust you: determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online. Gov. Inf. Q. 29 (1), 41–49. doi:10.1016/J.GIQ.2011.05.003.

Bellamy, M.J., 2022. Business against drunk driving: The neoliberal state, Labatt Brewery, and the creation of the "responsible drinker. Enterp. Soc. 1–24. doi:10.1017/ESO.2021.60.

Benitez, J., Henseler, J., Castillo, A., Schuberth, F., 2020. How to perform and report an impactful analysis using partial least squares: guidelines for confirmatory and explanatory IS research. Inf. Manag. 57 (2), 103168. doi:10.1016/J.IM.2019.05.003.

Bergström, J., 2018. An archaeology of societal resilience. Saf. Sci. 110, 31–38. doi:10.1016/J.SSCI.2017.09.013.

Biebricher, T., Johnson, E.V., 2012. What's wrong with neoliberalism? New Political Sci. 34 (2), 202–211. doi:10.1080/07393148.2012.676398.

Birk, R.H., 2017. Making responsible residents: on 'responsibilization' within local community work in marginalized residential areas in denmark. Sociol. Rev. 66 (3), 608–622. doi:10.1177/0038026117738148.

Bredewold, F., Duyvendak, J., Kampen, T., Tonkens, E., Jansen Verplanke, L., 2018. De Verhuizing Van de Verzorgingsstaat. Hoe de Overheid Nabij Komt. Van Gennep.

Brewer, M., Stonecash, J.M., 2010. The battle over personal responsibility: the evolution of American liberalism and the conservative response. SSRN Electron. J. 1–49. doi:10.2139/SSRN.1661287.

Brisman, A., South, N., 2015. 'Life-stage dissolution', infantilization and antisocial consumption: Implications for de-responsibilization, denial and environmental harm. Young 23 (3), 209–221. doi:10.1177/1103308815584876.

Brown, B., 2019. Responsibilization and recovery: Shifting responsibilities on the journey through mental health care to social engagement. Soc. Theory Health 19 (1), 92–109. doi:10.1057/S41285-019-00097-X.

Brown, S.R., 1993. A primer on Q methodology. Operant Subj. 16, 91–138. https://www.researchgate.net/publication/244998835.

Byman, D., Wittes, B., 2014. Reforming the NSA: how to spy after snowden. Foreign Aff. 93, 117–127. http://www.jstor.org/stable/24483412.

Camp, L.J., Grobler, M., Jang-Jaccard, J., Probst, C., Renaud, K., Watters, P., 2019. Measuring human resilience in the face of the global epidemiology of cyber attacks. In: Proceedings of the 52nd Hawaii International Conference on System Sciences doi:10.24251/HICSS.2019.574.

Cascavilla, G., Tamburri, D.A., Van Den Heuvel, W.J, 2021. Cybercrime threat intelligence: a systematic multi-vocal literature review. Comput. Secur. 105, 102258. doi:10.1016/J.COSE.2021.102258.

Castel, R., Haroche, C., 2001. Propriété Privée, Propriété Sociale, Propriété de soi—Entretiens sur la Construction de L'individu. Fayard, Paris.

Chang, L.Y., Coppel, N., 2020. Building cyber security awareness in a developing country: lessons from Myanmar. Comput. Secur. 97, 101959. doi:10.1016/j.cose.2020.101959.

Chen, K., 2016. No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state. Intell. Natl. Secur. 32 (6), 868–871. doi:10.1080/02684527.2016.1254142.

Clarke, J., 2016. New labour's citizens: Activated, empowered, responsibilized, abandoned? Crit. Soc. Policy 25 (4), 447–463. doi:10.1177/0261018305057024.

Cohen, J., 1988. Statistical power analysis for the behavioral sciences. Lawrence Erlbaum Associates.

Corallo, A., Lazoi, M., Lezzi, M., Luperto, A., 2022. Cybersecurity awareness in the context of the industrial internet of things: a systematic literature review. Comput. Ind. 137, 103614. doi:10.1016/j.compind.2022.103614.

Cyber Security Intelligence, 2022. Cyber Crime Against Individuals [Internet]. Cyber Security Intelligence [cited 2023 Mar. 18]. Available from: https://www.cybersecurityintelligence.com/blog/cyber-crime-against-individuals-6500.html.

Degli-Esposti, S., Ball, K., Dibb, S., 2021. What's in it for us? Benevolence, national security, and digital surveillance. Public Adm. Rev. 81 (5), 862–873. doi:10.1111/PUAR.13362.

Dent, M., 2007. Patient choice and medicine in health care. Public Manag. Rev. 8 (3), 449–462. doi:10.1080/14719030600853360.

Dewi, A.A., Hasibuan, H.T., Paramadani, R.B., Visvizi, A., Alhalabi, W., Assem, S., Razek, A., Gerli, P., Troisi, O., Ariyanto, D., Dewi, A.A., Hasibuan, H.T., Paramadani, R.B, 2022. The success of information systems and sustainable informa-

tion society: measuring the implementation of a village financial system. Sustainability 14 (7), 3851. doi:10.3390/SU14073851.
Ekendahl, M., Månsson, J., Karlsson, P., 2019. Risk and responsibilization: resistance and compliance in swedish treatment for youth cannabis use. Drugs Educ. Prev. Policy 27 (1), 60–68. doi:10.1080/09687637.2018.1544224.
Etzioni, A., 2018. Happiness Is the Wrong Metric: A Liberal Communitarian Response to Populism. Springer, Cham.
Eyal, P., David, R., Andrew, G., Zak, E., Ekaterina, D., 2021. Data quality of platforms and panels for online behavioral research. Behav. Res. Methods 1–20. doi:10.3758/S13428-021-01694-3/TABLES/13.
Friedman, M., 1962. The interpolation of time series by related series. J. Am. Statist. Assoc. 57 (300), 729–757. doi:10.1080/01621459.1962.10500812.
Gallo, H.B., Kobayashi, L.C., Finlay, J.M., 2022. Older Americans' perceptions of the federal government's pandemic response: voices from the COVID-19 coping study. Res. Aging 44 (7-8), 589–599. doi:10.1177/01640275211062111.
Gefen, D., Straub, D.W., 2004. Consumer trust in B2C e-commerce and the importance of social presence: experiments in e-products and e-services. Omega 32 (6), 407–424. doi:10.1016/J.OMEGA.2004.01.006.
Geldsetzer, P., 2020. Use of rapid online surveys to assess people's perceptions during infectious disease outbreaks: a cross-sectional survey on COVID-19. J. Med. Internet Res. 22 (4), e18790. doi:10.2196/18790.
Giesler, M., Veresiu, E., 2014. Creating the responsible consumer: Moralistic governance regimes and consumer subjectivity. J. Consum. Res. 41 (3), 840–857. doi:10.1086/677842.
Gray, G.C., 2009. The responsibilization strategy of health and safety neo-liberalism and the reconfiguration of individual responsibility for risk. Br. J. Criminol. 49 (3), 326–342. doi:10.1093/BJC/AZP004.
Grayson, K., Johnson, D., Chen, D.F.R., 2008. Is firm trust essential in a trusted environment? How trust in the business context influences customers. J. Mark. Res. 45 (2), 241–256. doi:10.1509/JMKR.45.2.241.
Grimmelikhuijsen, S., Knies, E., 2015. Validating a scale for citizen trust in government organizations. Int. Rev. Adm. Sci. 83 (3), 583–601. doi:10.1177/0020852315585950.
Grimmelikhuijsen, S., Porumbescu, G., Hong, B., Im, T., 2013. The effect of transparency on trust in government: a cross-national comparative experiment. Public Adm. Rev. 73 (4), 575–586. doi:10.1111/PUAR.12047.
Gummer, T., Roßmann, J., Silber, H., 2018. Using instructed response items as attention checks in web surveys: properties and implementation. J. Consum. Res. 50 (1), 238–264. doi:10.1177/0049124118769083.
Habib, A., Alsmadi, D., Prybutok, V.R., 2019. Factors that determine residents' acceptance of smart city technologies. Behav. Inf. Technol. 39 (6), 610–623. doi:10.1080/0144929X.2019.1693629.
Hache, É., 2007. La responsabilité, une technique de gouvernementalité néolibérale? Raisons Polit. 28 (4), 49–65. doi:10.3917/RAI.028.0049.
Hair, J.F., Risher, J.J., Sarstedt, M., Ringle, C.M., 2019. When to use and how to report the results of PLS-SEM. Eur. Bus. Rev. 31 (1), 2–24. doi:10.1108/EBR-11-2018-0203.
Hair, J., Hult, T., Ringle, C., Sarstedt, M., 2017. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 2nd ed. Sage.
Hart, E.L., 2016. Women prisoners and the drive for desistance: Capital and responsibilization as a barrier to change. Women Crim. Justice 27 (3), 151–169. doi:10.1080/08974454.2016.1217814.
Harvey, D., 2005. A Brief History of Neoliberalism. Oxford University Press.
Hauser, D.J., Schwarz, N., 2016. Attentive Turkers: MTurk participants perform better on online attention checks than do subject pool participants. Behav. Res. Methods 48 (1), 400–407. doi:10.3758/S13428-015-0578-Z/TABLES/1.
Hernandez-Castro, J., Boiten, E., 2014. Cybercrime prevalence and impact in the UK. Comput. Fraud Secur. 2014 (2), 5–8. doi:10.1016/S1361-3723(14)70461-0.
Hsieh, J.J.P.A., Rai, A., Keil, M., 2010. Addressing digital inequality for the socioeconomically disadvantaged through government initiatives: forms of capital that affect ICT utilization. Inf. Syst. Res. 22 (2), 233–253. doi:10.1287/ISRE.1090.0256.
IC3, 2020. 2020 Internet Crime Report [Internet]. IC3 [cited 2023 Mar. 18]. Available from: https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics.
Ilcan, S., Basok, T., 2010. Community government: Voluntary agencies, social justice, and the responsibilization of citizens. Citizsh. Stud. 8 (2), 129–144. doi:10.1080/1362102042000214714.
Ion, L., Reeder, R., Consolvo, S.Google, 2015. "...No one can hack my mind": Comparing expert and non-expert security practices. Symp. Usable Priv. Secur. 327–346.
Jaeger, L., Eckhardt, A., 2021. Eyes wide open: The role of situational information security awareness for security-related behaviour. Inf. Syst. J. 31 (3), 429–472. doi:10.1111/ISJ.12317.
Jasimuddin, S.M., Mishra, N.A., Saif Almuraqab, N., 2017. Modelling the factors that influence the acceptance of digital technologies in e-government services in the UAE: A PLS-SEM approach. Prod. Plan. Control 28 (16), 1307–1317. doi:10.1080/09537287.2017.1375144.
Jewkes, Y., 2013. Crime Online. Taylor & Francis, London doi:10.4324/9781843925828.
John, S., Noma-Osaghae, E., Oajide, F., Okokpujie, K., 2020. Cybersecurity education: the skills gap, hurdle! In. In: Innovations in Cybersecurity Education. Springer, Cham, Switzerland, pp. 361–376.
Johnstone, J., 2007. Technology as empowerment: A capability approach to computer ethics. Ethics Inf. Technol. 9 (1), 73–87. doi:10.1007/S10676-006-9127-X.
Kay, A.C., Gaucher, D., Napier, J.L., Callan, M.J., Laurin, K., 2008. God and the government: Testing a compensatory control mechanism for the support of external systems. J. Pers. Soc. Psychol. 95 (1), 18–35. doi:10.1037/0022-3514.95.1.18.
Knowles, B., Hanson, V.L., 2018. The wisdom of older technology (non)users. Commun. ACM 61 (3), 72–77. doi:10.1145/3179995.
Kock, N., 2017. Common method bias: a full collinearity assessment method for PLS-SEM. In: Partial Least Squares Path Modeling. Springer, Cham, pp. 245–257. doi:10.1007/978-3-319-64069-3_11.
Labuschagne, W.A., Burke, I., Veerasamy, N., Eloff, M.M., 2011. Design of Cyber Security awareness Game Utilizing a Social Media Framework. Information Security for South Africa IEEE, pp. 1–9.
Lankton, N.K., Harrison Mcknight, D., Tripp, J., 2015. Technology, humanness, and trust: rethinking trust in technology. J. Assoc. Inf. Syst. 16 (10), 880–918. doi:10.17705/1jais.00411.
Leroux, E., Pupion, P.C., 2022. Smart territories and IoT adoption by local authorities: a question of trust, efficiency, and relationship with the citizen-user-taxpayer. Technol. Forecast. Soc. Change 174, 121195. doi:10.1016/J.TECHFORE.2021.121195.
Liang, Y., Wang, W., Dong, K., Zhang, G., Qi, G., 2021. Adoption of mobile government cloud from the perspective of public sector. In: Mob. Inf. Syst., pp. 1–20. doi:10.1155/2021/8884594.
Lowry, P.B., D'Arcy, J., Hammer, B., Moody, G.D, 2016. Cargo Cult" science in traditional organization and information systems survey research: a case for using nontraditional methods of data collection, including Mechanical Turk and online panels. J. Strateg. Inf. Syst. 25 (3), 232–240. doi:10.1016/j.jsis.2016.06.002.
Marler, W., Hargittai, E., 2022. Division of digital labor: partner support for technology use among older adults. New Media Soc. 1–17. doi:10.1177/14614448211068437.
Masquelier, C., 2017. Personal responsibilization. In: Critique and Resistance in a Neoliberal Age. Palgrave Macmillan, London, pp. 47–60. doi:10.1057/978-1-137-40194-6.
Mayer, R., Davis, J., 1999. The effect of the performance appraisal system on trust for management: a field quasi-experiment. J. Appl. Psychol. 84 (1), 123–136.
McCorry, T., Fuller, P.C., 2021. We take responsibility!": governing the neighborhood—governing the self. Ethnography 1–20. doi:10.1177/14661381211038927.
McKnight, D.H., Choudhury, V., Kacmar, C., 2002. Developing and validating trust measures for e-commerce: an integrative typology. Inf. Syst. Res. 13 (3), 334–359. doi:10.1287/ISRE.13.3.334.81.
Mohun, A.P., 2013. Risk. Johns Hopkins University Press.
Moore, A.D., 2011. Privacy, security, and government surveillance: Wikileaks and the new accountability. Public Aff. Q. 25 (2), 141–156. https://www.jstor.org/stable/23057094.
Myers, N.M., 2019. Jailers in the community": Responsibilizing private citizens as third-party police. Can. J. Criminol. Crim. Justice 61 (1), 66–85. doi:10.3138/CJCCJ.2017-0040.
Nasser Alshabib, H., Tiago Martins, J., 2021. Cybersecurity: Perceived threats and policy responses in the gulf cooperation council. IEEE Trans. Eng. Manag. 1–12. doi:10.1109/TEM.2021.3083330.
Özsungur, F., 2019. A research on the effects of successful aging on the acceptance and use of technology of the elderly. Assist. Technol. 34 (1), 77–90. doi:10.1080/10400435.2019.1691085.
Palan, S., Schitter, C., 2018. Prolific.ac—A subject pool for online experiments. J. Behav. Exp. Finance 17, 22–27. doi:10.1016/J.JBEF.2017.12.004.
Pellandini-Simányi, L., Conte, L., 2020. Consumer de-responsibilization: changing notions of consumer subjects and market moralities after the 2008–9 financial crisis. Consum. Mark. Cult. 24 (3), 280–305. doi:10.1080/10253866.2020.1781099.
Peterson, R.A., Kim, Y., 2013. On the relationship between coefficient alpha and composite reliability. J. Appl. Psychol. 98 (1), 194–198. doi:10.1037/A0030767.
Pham, H.C., Ulhaq, I., Nguyen, M., Nkhoma, M., 2021. An exploratory study of the effects of knowledge sharing methods on cyber security practice. Australas. J. Inf. Syst. 25.
Phillips, K., Davidson, J.C., Farr, R.R., Burkhardt, C., Caneppele, S., Aiken, M.P., Dinis-Oliveira, F., Alves, C., Barone, P.M., Phillips, K., Davidson, J.C., Farr, R.R., Burkhardt, C., Caneppele, S., Aiken, M.P, 2022. Conceptualizing cybercrime: definitions, typologies and taxonomies. Forensic Sci. 2 (2), 379–398. doi:10.3390/FORENSICSCI2020028.
Quayyum, F., Cruzes, D.S., Jaccheri, L., 2021. Cybersecurity awareness for children: a systematic literature review. Int. J. Child Comput. Interact. 30, 100343. doi:10.1016/j.ijcci.2021.100343.
Preibusch, S., 2015. Privacy behaviors after Snowden. Commun. ACM 58 (5), 48–55. doi:10.1145/2663341.
Redmiles, E.M., Warford, N., Jayanti, A., Koneru, A., Kross, S., Morales, M., ... Mazurek, M.L., 2020. A comprehensive quality evaluation of security and privacy advice on the web. In: Proceedings of the 29th USENIX Security Symposium (USENIX Security 20), pp. 89–108.
Reinhart, R.J., 2018. One in Four Americans Have Experienced Cybercrime [Internet]. Gallup [cited 2023 Mar. 18]. Available from: https://news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx.
Renaud, K., Coles-Kemp, L., 2022. Accessible and inclusive cyber security: a nuanced and complex challenge. SN Comput. Sci. 3 (5), 1–14. doi:10.1007/s42979-022-01239-1.
Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., Orgeron, C., 2018. Is the responsibilization of the cyber security risk reasonable and judicious? Comput. Secur. 78, 198–211. doi:10.1016/J.COSE.2018.06.006.

Renaud, K., Weir, G., 2016. Cybersecurity and the unbearability of uncertainty. In: Proceedings of the Cybersecurity and Cyberforensics Conference, pp. 137–143.
Renaud, K., Flowerday, S., van der Schyff, K., 2021. Uncertainty in cyber de-responsibilisation. Comput. Fraud Secur. 2021 (8), 13–19. doi:10.1016/S1361-3723(21)00086-5.
Renaud, K., Orgeron, C., Warkentin, M., French, P.E., 2020. Cyber security responsibilization: an evaluation of the intervention approaches adopted by the Five Eyes countries and China. Public Adm. Rev. 80 (4), 577–589. doi:10.1111/PUAR.13210.
Rochester's News Talk, 2023. Elderly Rochester Man Scammed out of Nearly $20k [Internet]. Rochester's News Talk [cited 2023 Mar. 18]. Available from: https://krocnews.com/elderly-rochester-man-scammed-out-of-nearly-20k/.
Rodger, N., 2004. The Safeguard of the Sea: a Naval History of Britain. Penguin, UK.
Salvi, A., Spagnoletti, P., 2020. Digital enabled mission command and control systems in military operations. In: Proceedings of the Conference of the Italian Chapter of AIS. Springer, Cham, pp. 204–215.
Sarkar, S., Vance, A., Ramesh, B., Demestihas, M., Wu, D.T., 2020. The influence of professional subculture on information security policy violations: A field study in a healthcare context. Inf. Syst. Res. 31 (4), 1240–1259. doi:10.1287/ISRE.2020.0941.
Schodt, K.B., Quiroz, S.I., Wheeler, B., Hall, D.L., Silva, Y.N., 2021. Cyberbullying and mental health in adults: The moderating role of social media use and gender. Front. Psychiatry 12, 954. doi:10.3389/FPSYT.2021.674298/BIBTEX.
Schoorman, F.D., Mayer, R.C., Davis, J.H., 2007. An integrative model of organizational trust: past, present, and future. Acad. Manag. Rev. 32 (2), 344–354. doi:10.5465/AMR.2007.24348410.
Sowell, T., 2022. Knowledge and Decisions. Basic Books USA.
Stanton, K., Carpenter, R.W., Nance, M., Sturgeon, T., Villalongo Andino, M., 2022. A multisample demonstration of using the prolific platform for repeated assessment and psychometric substance use research. Exp. Clin. Psychopharmacol. doi:10.1037/PHA0000545.
Stengers, I., 2003. afterword to Starhawk, Femmes, magie, et politique. Les Empêcheurs de Penser en Rond, Paris.
Stephenson, W., 1935. Correlating persons instead of tests. J. Pers. 4 (1), 17–24. doi:10.1111/J.1467-6494.1935.TB02022.X.
Strawser, B.J., Joy, D.J., 2015. Cyber security and user responsibility: Surprising normative differences. Procedia Manuf. 3, 1101–1108. doi:10.1016/J.PROMFG.2015.07.183.
Swyngedouw, E., MacCallum, D., Moulaert, F., Haddock, S.V., 2009. Civil society, governmentality and the contradictions of governance-beyond-the-state: the Janusface of social innovation. Social Innovation and Territorial Development. Ashgate Publishing, Ltd doi:10.4324/9781315609478.
Telesca, G., 2021. Crisis and competence the politics of competence: Covid-19 and the ERM. Renew. J. Soc. Democr. 29 (1), 28–37.
TNW, 2019. How an Engineer at a Crypto-Security Startup Lost $100K in a SIM-Swapping Hack. [Internet]. TNW [cited 2023 Mar. 18]. Available from: https://thenextweb.com/news/cryptocurrency-security-coinbase-hack-sim.
Trnka, S., Trundle, C., 2017. Reckoning personal responsibility, care for the other, and the social contract in contemporary life. In: Competing Responsibilities: The Ethics and Politics Of Contemporary Life. Duke University Press, pp. 1–26.
van der Schyff, K., Flowerday, S., Lowry, P.B., 2020. Information privacy behavior in the use of facebook apps: a personality-based vulnerability assessment. Heliyon 6, e04714. doi:10.1016/j.heliyon.2020.e04714.
van Ooijen, I., Segijn, C.M., Opree, S.J., Ooijen, I., Segijn, C.M., 2022. Privacy cynicism and its role in privacy decision-making. Commun. Res. 1–32. doi:10.1177/00936502211060984.
van Oost, P., Yzerbyt, V., Schmitz, M., Vansteenkiste, M., Luminet, O., Morbée, S., Van den Bergh, O., Waterschoot, J., Klein, O., 2022. The relation between conspiracism, government trust, and COVID-19 vaccination intentions: the key role of motivation. Soc. Sci. Med. 301, 114926. doi:10.1016/J.SOCSCIMED.2022.114926.
van Wijk, E., Mascini, P., 2019. The responsibilization of entrepreneurs in legalized local prostitution in the Netherlands. Regul. Gov. doi:10.1111/REGO.12273.
Weller, S.C., 2016. Cultural consensus theory: applications and frequently asked questions. Field Methods 19 (4), 339–368. doi:10.1177/1525822X07303502.
Workman, M.D., 2021. An exploratory study of mode efficacy in cybersecurity training. J. Cybersecur. Educ. Res. Pract. 1 (2), 1–14.
Wu, L.H., Wu, L.C., Chang, S.C., 2016. Exploring consumers' intention to accept smartwatch. Comput. Hum. Behav. 64, 383–392. doi:10.1016/J.CHB.2016.07.005.
Yap, Y.Y., Tan, S.H., Tan, S.K., Choon, S.W., 2022. Integrating the capability approach and technology acceptance model to explain the elderly's use intention of online grocery shopping. Telemat. Inform. 72, 101842. doi:10.1016/J.TELE.2022.101842.
Zaharia, A., 2023. 300+ Terrifying Cybercrime and Cybersecurity Statistics (2023 EDITION) [Internet]. Comparitech [cited 2023 Mar. 18]. Available from: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/.

Karen Renaud is a Scottish Computing Scientist at the University of Strathclyde in Glasgow, working on all aspects of Human-Centred Security and Privacy. She was educated at the Universities of Pretoria, South Africa and Glasgow. She is particularly interested in deploying behavioural science techniques to improve security behaviours, and in encouraging end-user privacy-preserving behaviours. She collaborates with academics in five continents and incorporates findings and techniques from multiple disciplines in her research.

Karl van der Schyff Karl (Ph.D. Rhodes University) is a Lecturer at Abertay University in Dundee, Scotland. His research interests include behavioural information security, information privacy, quantitative methods and cyberpsychology.

Stuart MacDonald Stuart is CEO of Seric Systems, Glasgow. Seric Systems helps start-ups, scale-ups and enterprises to improve their cyber security.