The Employee Cybersecurity Awareness Framework

Laura M. Bishop[1,2,3], , Phoebe M. Asquith[1], Phillip L. Morgan[1,2,3,4]

School of Psychology, Human Factors Excellence Research Group, Cardiff University, Wales, UK [1]

Cardiff University Centre for Artificial Intelligence, Robotics and Human-Machine Systems (IROHMS) [2]

Airbus Central R&T, Newport, Wales, UK [3]

Luleå University of Technology - Psychology, Division of Health, Medicine & Rehabilitation, Sweden[4]

Corresponding Author

Phillip L Morgan

School of Psychology, 70 Park Place

Cardiff University

Cardiff, UK, CF10 3AT

morganphil@cardiff.ac.uk

The Employee Cybersecurity Awareness Framework

Abstract

With cyber-attack methods becoming increasingly sophisticated and end-users of targeted technology continuing to be the weakest link, it is crucial to develop more optimal ways to measure and better understand human cybersecurity behavior risk. Across three studies, a tool consisting of a battery of established questionnaires and other measures to investigate employee cybersecurity vulnerability factors was tested and developed. Study 1 determined key correlating factors including security- self-efficacy, experience and involvement, awareness and organisational policy, with large effect sizes. A refined tool was deployed in Study 2 amongst a larger sample of employees within a multinational organisation. Exploratory factor analysis determined two latent factors – *cybersecurity awareness* and *psychological ownership*. However, 55% of variance within a regression model was explained by cybersecurity awareness alone. Study 3 included an even larger sample employed by multiple organisations – with cybersecurity awareness accounting for 60% of variance. We propose the *Employee Cybersecurity Awareness Framework (ECAF)* with cybersecurity awareness at its core and containing six underlying factors: threat appraisal, information security self-efficacy, information security awareness, information security attitude, information security operation policy and cybersecurity experience and involvement. The ECAF can be deployed by organisations to optimally measure employee cybersecurity risk factors and determine optimal interventions tailored to risk profiles.

1. Introduction

Organisations are increasingly relying on connected technology solutions, with the main goal of affording seamless communication, increased productivity, and almost infinite information sourcing. However, cyber criminals are often intent on beaching such systems; often by exploiting employee vulnerabilities to gain entry. In 2021, ~24,000 (rising to 30,458 in 2024) cyber security incidents were reported by organisations globally (Verizon, 2022), and 82% linked to humans (mostly employees). In 2024, this figure was at 76% when including those involving malicious actors within organizations (Verizon, 2024). Attacks are increasing in number with growing sophistication, especially with an increase in the use of artificial intelligence (AI) by malevolent actors. Despite a surge in research on individual and sometimes combined human cybersecurity risk factors over the past two decades in particular, and attempts at intervention, human susceptibility remains high. Though our understanding of human susceptibility remains low, with many studies often focussing on one or very few factors when it is highly likely that multiple factors are at play. There is an urgent need for a more holistic approach and a universally applicable tool for measuring factors that relate to risky cybersecurity behaviors such that more effective interventions can be developed and tailored towards key vulnerabilities. Developing and testing such a tool is the key aim of this paper.

Many (especially larger) organisations offer some form of security education, training and awareness (SETA), although success is questionable, especially over the longer term. It can be difficult to transfer content of training programmes into work practices (Alshaikh et al., 2018; Bada et al., 2019; Scholl et al., 2018; Skinner et al., 2018). Limited success may also be due to focusing on one (e.g. impulsivity, risk propensity) or a limited number of factors, when there are likely multiple factors and individual differences that collectively – rather than in isolation – underpin cyber risky behaviors. The main aim of the current paper is to present the development and testing of a comprehensive theoretically and pragmatically informed human cybersecurity vulnerability measurement tool that can best account for engagement in non-desirable cybersecurity behaviors[1]. From this, a human cybersecurity risk framework can be created in order to develop more optimal interventions.

To generate such a tool, we draw on relevant behavior change theories and models. We also evaluate individual differences, socio-psychological factors, technology interaction factors, and organizational specific reasons that appear most predictive of cybersecurity behavior. The key theoretical and empirical literatures on each as well as their links are considered below.

2. Theoretical Frameworks

There are major theoretical frameworks and models with associated research studies that speak to our aims and can inform predictions. These are presented and discussed in the subsections that follow.

2.1 Protection Motivation Theory (PMT: Rogers, 1975; McGill & Thompson, 2017)

PMT appears particularly applicable to human cybersecurity behavior. According to PMT, two appraisal systems are activated when assessing threat: (1) threat appraisal - where probability and severity are considered, and (2) coping appraisal - where judgements are made on *response efficacy*: how effective a person believes they will be in applying the response (i.e. *self-efficacy*) and associated costs to its application (i.e. *response costs*). Together, these impact the intention to adopt a behavior or indeed avoid it. For example, if risk of threat is appraised to be low, and chance of response success also low, motivation to exhibit the behavior will deplete (Rogers, 1975).

[1] The research was conducted as part of a PhD (awarded 2024 to the first author) entitled The Employee Experience in Cybersecurity and How to Mitigate Risk (Bishop, 2024)

Many cybersecurity studies have drawn upon PMT and its parameters in relation to cybersecurity attitudes and behavior, e.g. to examine fear appeals and coping messaging (e.g. Boehmer et al., 2015; Johnston & Warkentin, 2010; Kahn, Ikram, Murtaza, & Javid, 2023). Fear appeals tend to involve messages communicating probability and severity of a threat to increase threat appraisal. Coping messages provide information on how to be secure and can improve coping appraisals. Individually, they can effectively improve cybersecurity behavior (Shillair & Dutton, 2016; van Bavel et al., 2019) although combining them tends to be better, and can stronger ethically (Dupuis & Renaud, 2021; Witt & Allen, 2000).

A key issue is that humans are not always optimal at appraising threat. For example, we often tend to perceive risk to be lower than actual threat (e.g. in the wake of dangerous weather fronts that seem to be increasing in frequency and severity); possibly due to decision making biases (e.g. ‘things were not that bad last time a storm hit, and as such they might not be next time’). *The availability bias* manifests as an inaccurate perception of the probability of an event occurring, determined by how readily past instances can be brought to mind (Taylor-Gooby & Zinn, 2006; Tversky & Kahneman, 1973). Taking the weather example above, the sheer frequency and severity of storms, hurricanes and typhoons over the past few years in particular is likely shifting peoples threat appraisals about them. In the workplace however, if employees are shielded from security breaches, they will have fewer examples to draw upon, assume occurrences are rare, and possibly appraise threat to be low.

Often coinciding with availability is *saliency*, where prominent information dominates attentional focus (Schenk, 2011). Salience is higher if e.g. information is verbally spoken than silently read (Tversky & Kahneman, 1973) or concretely imagined (Carroll, 1978). It can increase through threat appraisal via the *affect bias* (Kahneman, 2011); where a decision is made based on emotion rather than rational thought (Loewenstein & Lerner, 2002; Pfleeger & Caputo, 2012). Affect can impact a decision via: anticipated emotion if an action is chosen, and, immediate emotions experienced about the decision, including irrelevant information (Loewenstein & Lerner, 2002). It can increase risk perception, particularly in relation to fear (Keller, et al., 2006; Pfleeger & Caputo, 2012; Slovic et al., 2007).

Fear is an emotion characterized by high arousal and negative valence (how positive, negative or neutral something is perceived to be)resulting in the cognition of threat; and often motivating people to try and avoid harm (Rogers, 1975; Witte & Allen, 2000). Findings on fear appeals to increase risk perception are mixed. Some meta-analyses provide support for increasing perceptions of susceptibility and severity and adaptive danger control actions such as message acceptance (Lowry et al., 2023; Tannenbaum et al., 2015; Witte & Allen, 2000). Though effectiveness can be limited in cybersecurity contexts, most likely because cybersecurity is often viewed as a secondary task within most workplaces at least (Briggs et al., 2017; Dupuis & Renaud, 2021; Schuetz et al, 2020).

Linked to threat appraisal is the *optimism bias*, where we tend to overestimate personal positive outcomes at the cost of underestimating personal negative outcomes, affecting forecasting of risk (Pfleeger & Caputo, 2012; Warkentin et al., 2013). Whilst employees can be made aware of risk, they more often than not underestimate it in relation to themselves and their organisation (Warkentin et al., 2013). Optimism bias may be evolutionary response to ease anxiety for things outside of our control (Sharot, 2011; Weinstein & Klein, 1995). However, even a small decline in domain specific optimism can support increases in the availability bias, resulting in more realistic threat appraisals (Arkes, 1991; Chen et al., 2022; Weinstein, 1980).

Unrealistic optimism has been linked to poor threat appraisals in the context of technology risk assessments, e-waste, and perception of risk towards a pandemic (Bottemanne et al., 2020; Chen et al., 2021; Loske et al., 2013; Warkentin et al., 2013; Shalev et al., 2014).

However, reducing the optimism bias is difficult: it is so robust that even increasing knowledge about it can still result in people heuristically believing they are less susceptible (Croskerry et al., 2013; Jolls & Sunstein, 2006). There are interventions(Cutello et al., 2021; White et al., 2011): clarifying the underlying factor (unambiguous definition); reducing optimism estimates in future activities (insight); and being informed that evaluation of actions are taking place (accountability); and. These are not without downsides though. For example, increased accountability can reduce self-efficacy. Taken together, the evidence suggests that threat appraisal is important to behavior change and thus it will be included within the measurement tool.

A coping appraisal(s) is formed based on the perceived success of deploying a response and mechanisms involved including *self-efficacy, response efficacy and response costs*. Self-efficacy is an judgement or expectancy of skills and capabilities a person believes are needed to influence a course of action, and whether they feel able to execute a response or not (Maddux & Gosselin, 2012). It is believed to be biological and triggered by an emotional need to master a task, including perceptions of task value (Maddux & Gosselin, 2012). For cybersecurity, definitions of self-efficacy types have been proposed from computers, information security, the internet, privacy, coping, and perceived behavioral control (Conetta, 2019; Raineri & Resig, 2020; Safa et al., 2015). Somewhat alarmingly, it is assumed that tools to measure cybersecurity self-efficacy are measuring the same construct, but this is not always the case. Self-efficacy differs from ability and competency due to its task specific focus, without consideration of e.g. cost and/or effort (Agha et al., 2019; van den Broeck et al., 2010). However, experiential factors are important including commendation by peers, witnessing others performing effectively, and practice and achievement (Maddux & Gosselin, 2012). Ultimately, when self-efficacy perceptions change, behavior change should follow.

Self efficacy effects on behavior are arguably linked with *response efficacy*; perception of the likelihood that a response will achieve a desired goal (Cismaru et al., 2009) and is impacted by other factors including social and cultural norms. Bandura (1982) discussed how both must be aligned to achieve response success. A behavior will most likely not be committed to unless necessary environmental conditions are in place. Like self-efficacy, response efficacy is impacted by perceptions of threat severity and thus is also likely important in terms of human cybersecurity vulnerabilities.

Response efficacy is related in more than one way to *response costs*, including finance, effort and time required to invest for a response to be a success (Cismaru et al., 2009). For example, even if reliable firewall software is available and can easily be installed, financial and/or time costs can be reasons why it is not acquired and installed. Response efficacy and costs are at opposite ends of a continuum with response efficacy decreasing the more costs are required to prepare for and execute a behavior (Cismaru et al., 2009). Response efficacy and costs are not as well researched as threat appraisal and self-efficacy, but are prominent within behavior change models, and relate to other factors. As such, both will be included within the measurement tool.

2.2. The Health Belief Model and Avoidance Theory

Other theories and models share similarities to PMT and are useful to consider. The *Health Belief Model* (HMB) focuses on the expectancy-value principle, where perceived expectation of risk and cost of not taking action influence motivation to act (Anwar, 2017; Rosenstock, 1974, 1990). PMT and the HBM share similarities including threat appraisal and self-efficacy factors (Prentice-Dunn & Rogers, 1986). However, the HBM offers a more hierarchical approach to behavior change whereas PMT is more focussed on behavioral continuums. *Avoidance Theory* (AT), and more recently *Technology Threat Avoidance Theory* (TTAT) also present similar features such as fear of threat as a motivational driver to avoid a task, in connection with perceived effectiveness of an alternative coping behavior (Carpenter et al., 2019; Herrnstein, 1969; Liang & Xue, 2009; Mowrer, 1939; Rachman, 1976).

Whilst the HBM and TTAT have been utilised within cybersecurity behavior research, this is less so than the PMT. However, we must consider all important key constructs that have been shown to evoke behavior change. Therefore, susceptibility and severity (linked to threat appraisal), benefits of action (linked to response efficacy), benefits to action (linked to response costs) and self-efficacy will be included within the measurement tool. At least some of the aspects reviewed thus far appear related to behavior that is planned. Next, we review the leading Theory of Planned Behavior (Ajzen, 1991) to speak to other aspects that may underpin cybersecurity behavior(s).

2.3. The Theory of Planned Behavior

Aspects of the *Theory of Planned Behavior* (Ajzen, 1991) can also be predictive of why humans sometimes display cyber risky behaviors. According to PMT, we consider actions based on: (i) an overall evaluation of the behavior (*attitude*); (ii) access to relevant internal and external resources to perform that behavior (*perceived behavioral control* – not unlike self-efficacy), and (iii) whether significant others believe they should perform it (*subjective norms*: e.g. Burns & Roberts, 2013; Safa et al., 2015). the TPB and PMT are somewhat complimentary with e.g. scholars such as Sulaimen et al. (2022) recently supporting integration to better understand cybersecurity behavior.

Attitudes (especially those that have been held for some time) influence behavior(s). Attitude is defined as a general evaluation of an object or event that influences behavior (Azjen, 1991; Conner & Armitage, 1998) and can be covert (feelings, thoughts) or overt - expressed via behavior (Pickens, 2005); and created due to e.g., personality traits, motivations, and values (Pickens, 2005). Within Fishbein and Ajzen's (1975) Expectancy-Value Model, attitudes are formed for people, things, places and events. The Elaboration Likelihood Model (Petty & Cacioppo, 1986) describes how enduring positive or negative attitudes result from how high a degree of thought (*elaboration*) is placed on a human or non-human thing. They can depend on social contagion mirroring those in their social group, even subconsciously (Scherer & Cho, 2003) to reduce cognitive dissonance. People can try to reduce conflict through changing a behavior (which can be notoriously difficult especially if it is something engaged in regularly and over a long time-period) or rationalising it (e.g. believing that nicotine based vapes are not as bad a cigarettes containing nicotine and therefore vaping (sometimes excessively) instead of smoking cigarettes). The potential influence of attitudes are considered in even more depth in theoretical frameworks such as the Knowledge, Attitude and Behavior Model (KAB, e.g. Scholl et al., 2018)

2.4. The Knowledge, Attitude and Behavior Model (KAB)

The KAB (Scholl et al., 2018) highlights the relationship between attitude and behavior, and the need to separate attitude from knowledge alone. A more negative attitude towards cybersecurity can result in more cyber-risky acts and vice versa (Haddlington, 2018, 2017). Employees may have the knowledge to protect themselves and their organisation from being 'successfully' cyber-attacked, but without a positive attitude toward required behavior, they are far less likely to adopt it putting their organization at risk.

Subjective norms are important. These are an individual's perception of the likelihood that a significant other(s) will perform a behavior and the extent to which they will do the same thing (Conner & Armitage, 1998; McGill & Thompson, 2017), and includes cultural and social norms. We tend to learn to behave like others who are frequently around us, using intuitive heuristics (Raafat et al., 2009; Scherer & Cho, 2003; van Bavel et al., 2019). Some argue that any relationship can be allayed by increasing self-efficacy (Ajzen, 1991; McGill & Thompson, 2017). The higher the individual self-efficacy, the less likely people will look to others to guide their behavior choice (Wang et al., 2015) – for example – having a srong negative attitude towards smoking and vaping and not engaging in either even if significant others around us are.

2.5. The Technology Acceptance Model (TAM: David, 1985, 1989) and Unified Theory of Acceptance and Use of Technology model (UTAUT; Venkatesh et al., 2003)

Models of technology attitudes, behavior, usage and acceptance are also important and relevant. For example, the TAM (David, 1985, 1989) focuses on two main factors: *performance expectancy* – i.e. usefulness, and *effort expectancy* – i.e. ease of use. The UTAUT (Venkatesh et al., 2003), based on the TAM, assesses technology acceptance through intention of use and includes: *social influence* – potential peer impact (like social norms), and, *facilitating conditions* – knowledge and resources needed for technology to be successful, and the presence of intentions that suggest continued use into the future. UTAUT2 (Venkatesh et al. 2012), developed for the acceptance of commercial products, includes additional constructs: *hedonic motivation* – i.e., does the technology afford experiential benefits; *price value* – i.e., its value for money; and *habits* – what routines does it invoke. *Trust* has also been included, and more recently: artificial intelligence (AI) acceptance, including system transparency (Kessler & Martin, 2017; Venkatesh, 2022; Wanner et al., 2022). UTAUT has high reliability (α = .7-.9) across many domains e.g., internet services and mobile banking, (Oh & Yoon, 2013; Zhou et al., 2010). The original four factors (performance expectancy, effort expectancy, facilitating conditions and social influence) with the addition trust will be included within the new measurement tool.

2.6 Theoretical Summary

Taken together, threat appraisal, response efficacy, self-efficacy, response costs, attitude, subjective norms, and technology acceptance and use seem to be crucial to achieving behavior change in general with applicability across multiple application domains including technology and cybersecurity. Four of the six theories /models reviewed (PMT, HBM, AT/TTAT, and TPB) contain a self-efficacy element, with three containing a factor on how we appraise threat. It is important that factors linked are included within the cybersecurity behavior tool. Based on TAM and TATT, performance expectancy, effort expectancy, facilitating conditions and social influence with the addition trust will also be incorporated.

In addition to these theoretical and modelled constructs, other factors can influence our attitudes and behaviors, including individual differences in a more general sense (e.g. age, gender, risk taking propensity, and impulsivity) as well as those that are more relate to how we (may) perceive and interact with technology (including training and awareness), and more specific organisational factors (e.g. psychological ownership). It is crucial that these are considered together with (and not in isolation of) theoretical aspects discussed so far for the development of a powerful tool that can capture as much variance as possible accounting for human cybersecurity vulnerabilities. Noting some of these factors are at least in some respects also rooted in some of the theoretical foundations discussed thus far. It is to these literatures we turn to next.

3. Individual Differences Factors

3.1. Demographics

Demographic factors are also of importance with age and gender notably examined as predictors of cybersecurity behavior. Parrish, Bailey and Courtney (2009) identified significant relationships between susceptibility to phishing techniques for 18-25-year olds compared to older age groups. Findings from Sheng et al. (2010) also indicated higher susceptibility amongst women. Gratian et al. (2018) employed the Security Behavior Intentions Scale (SeBIS) to examine both age and gebder. SeBIS includes four security behaviors: password generation, device securement, , proactive awareness, and updating. They found that age did not have a unique effect, although 18-25-year-olds created weaker passwords. They also found that females were more risky across all measures. Gender differences are perhaps attributable to males, in general, perceiving themselves as having higher technology-related self–efficacy and general resilience than females (Anwar et al., 2017; Branley-Bell et al., 2022; Gratian et al, 2018). There is also still a concerning under-representation of women in information technology (IT) and science, technology, engineering and mathematics (STEM) areas (Kshetri & Chhetri., 2022). Though, some mixed findings have been reported. A study by Fatokun et al. (2019) within the banking domain - found that men were more susceptible to phishing despite there being an evident gender divide in relation to other aspects of their study.

In a recent study, age was a significant negative predictor of information and communication technology cybersecurity behavior, with older users again found to create stronger and more secure passwords (Branley-Bell et al., 2022). Though others have found older adults feel neither motivated or capable in relation to cybersecurity (Morrison et al. 2021; Whitty et al. 2015). Overall, and despite some contrasting findings, it seems that in general – being younger, and female – can be predictors of cybersecurity risk. Thus, age and gender questions will be included within the measurement tool to not only examine their possible relationships but also relationship strength in relation to other included factors.

3.2. Risk-taking, Decision-making Strategy and Impulsivity

Risk-taking attitude, decision-making strategy and impulsivity have also received attention within the cybersecurity research literature. Egelman and Peer (2015) found less desirable cybersecurity behaviors in more impulsive participants and those more likely to take health/safety risks and procrastinate, or rely on others when making decisions. The negative relationship between impulsivity and cybersecurity behavior has perhaps unsurprisingly been found in several studies (e.g. Hadlington 2017), perhaps due to impaired processing of contextual cues for detecting cyber threat when reacting rapidly (Jeske et al., 2014). As such, impulsivity measures will be included within the tool.

Gratian et al. (2018) built on Egelman and Peer's (2015) findings, investigating risk-taking attitude and decision-making style in an educational setting, and specifically asked if and how gender and personality relate to cybersecurity behaviors. A spontaneous less rational decision-making style was linked to negative cybersecurity behaviors (and vice versa). This differs from Egelman and Peer (2015) where they found that only avoidant decision-making related to behavior. Gratian et al. (2018) also found that risk-taking attitude was predictive: those who take higher health/safety risks generated weaker passwords than those who take greater financial risks.

Taken together, demographic factors including age and gender, and individual differences such as decision-making style, impulsivity and risk taking propensity seem predictive of risky cybersecurity behaviors. Questions and scales on these will be included within the tool.

3.3. Technology Acceptance, Usage, and Cybersecurity Preparedness

Next, we consider individual differences in technology acceptance and usage. Research within fields such as Human-Computer Interaction (HCI) has focussed on how acceptance and adoption of technology influences intentions to behave in certain ways (Sun et al., 2013). Though, more is required to better understand how these impact cybersecurity behavior change framework (Chenoweth, 2007; Fei et al., 2022). Integrated behavior change and technology acceptance models have been applied to the health domain, exploring behavior towards use of electronic patient records, mobile health services and medical wearables (Hsieh et al., 2017; Mamra et al., 2017; Rahi et al., 2021). It seems crucial that these models are considered in the context of human cybersecurity behavior and behavior change.

Other factors linked to cybersecurity include antecedents to dimensions within the Theory of Planned Behavior (TPB) reviewed earlier: cybersecurity awareness, involvement and experience n cybersecurity, organisational commitment, value in cybersecurity policy, attachment to (or psychological ownership of) an organisation’s technology, and maladaptive rewards. Their importance for a tool and framework for measuring human cybersecurity risks and behavior is discussed across the next two subsections.

Safa et al. (2015) present three antecedents to cybersecurity attitude, cybersecurity self-efficacy and subjective norms. First, *information (or cyber) security awareness (ISA)* is the need to maintain updated accurate knowledge of cybersecurity risk and effective coping behavior (with this being an antecedent to attitude). Second, *cybersecurity experience and involvement (ISEI)* involves time and energy needed to increase experience and improve behavior (an antecedent to perceived behavioral control or self-efficacy). Third, *information security organizational policies and procedures (ISOP)* involve the perception of employee organisational guidance and its effectiveness (an antecedent of subjective norms).

It is critical that employees maintain a state of awareness in cybersecurity where their implicit and explicit knowledge of cyber-threats is current, as are behaviors required to minimise a potential breach situation. According to Safa et al (2015) and Zwilling et al (2022), there are three key aspects to maintaining employee awareness (): *awareness and training programmes completed* (and consistency of completion); *motivation for* collaboration, and a *knowledge sharing culture*; . Implicit knowledge exists in the mind, and explicit knowledge is outwardly communicated (Nickols, 2000). Tacit knowledge is learned through experience and not always easily explained (e.g. how to ride a bicycle). Knowledge can be declarative or procedural (like tacit knowledge and related to experience of doing), whereas tacit and procedural knowledge are arguably processed unconsciously. Together, they are of importance to cybersecurity behavior in that they build habits and can impact risk in a positive or negative manner.

Knowledge sharing can be encouraged through collaborative meetings and fostered unintentionally through herding – including: social contagion, group think, the bandwagon effect, and social priming (Raafat, Chater & Frith, 2009). Herding supports decisions on believed shared view(s) and behavior(s) (Hodas & Lerman, 2014) resulting in distribution of desirable and undesirable knowledge. Group think is used with the intention of maintaining group harmony and inhibiting conflicting opinions. It can be more powerful with face-to-face interaction, in that it promotes impartial leadership and increased self-efficacy, encouraging social risk-taking. The bandwagon effect, where herding behaviors are based on belief popularity, can also promote positive messaging (Lee et al., 2020; Waddell & Sundar, 2020). Also, Behavioral Threshold Analysis can be used - as a ‘tipping point’ tool - to determine the number of people needed to adopt a behavior for herding to occur in the first place (Snyman & Kruger, 2021).

Level of experience and involvement in cybersecurity (e.g. policies and procedures) may also be linked to behavior change. Information security experience and involvement (ISEI), an antecedent to cybersecurity self-efficacy, is the time and energy exerted to an object/event, with involvement increasing experience and improved behavioral intention and cybersecurity capabilities (Safa et al., 2015). The experiential journey from novice to expert allows individuals to recognise features and patterns in an object/event that can help formulate central principles from which more controlled future decisions follow (Bion, 2021). Through systematic adaptation, tacit knowledge can be incrementally built through learned experiences, providing capabilities that can be actioned but not easily communicated.

Involvement and engagement in cybersecurity develops with experience and increases motivation through empowerment (Amah & Ahiauzu, 2013; Osborne & Hammoud, 2017). Affording employees control over some decisions and goals has been shown to improve innovation, self-esteem, company trust, workplace relations, and creative problem-solving (Freeman et al., 2000; Naqshbandi et al., 2019; Obiekwe et al., 2019). Involvement must be active (Cox et al., 2006; Markey & Townsend, 2013). Increased participation in development of policies and strategies can also improve psychological ownership (Hedstrom et al., 2011; Lin & Wittmer, 2017). The IKEA effect is also linked where higher value is placed on objects, outcomes or even ideas that have had personal input (Franke et al. 2010), through increased feelings of competence (Norton et al., 2012). Like psychological ownership, investing more time in an artefact increases its perceived value and loss aversion (Baxter et al., 2015; Lee & Chen, 2011) – for example if a system and / or device is breached in the event of a cyber-attack.

Information security operation policy (ISOP) considers perceptions of policies and processes created to inform employees of behaviors required to protect against cyber-attacks. However, the importance of employee perceptions of cybersecurity policy is not always considered, with the focus mainly on compliance (i.e. tick-box data). As such, employees can fail to follow company cybersecurity policies, resulting in unintentional insider threat (Gheyas & Abdallah, 2016). Patterson (2017) explored the relationship between employees and policy within small businesses, highlighting a lack of employee involvement in its creation, resulting in ill-fit. The outcome can often be a “them-versus-us” culture, rather than agreed policy designed with and to be used by employees (Ashenden & Sasse, 2013; Hedstrom et al., 2011).

Taken together, the evidence suggests that higher employee experience of and interest in technology, data and policy will result in reduced cybersecurity vulnerabilities. As such, these factors will be included within the tool.

3.4. (Other) Organisational Factors

There are other individual differences, specifically linked with organisational factors, that are also predictive of cybersecurity vulnerabilities or indeed strengths. For example, organisational commitment - an employee’s ability to identify with their organisation and align with its goals (Karim & Noor, 2017) – has been found to be linked to cybersecurity behavior. The higher the sense of attachment towards a workplace, the higher the productivity and lower an employee’s potential risk (Reeve et al., 2020). These can underpin key reasons why an employee remains within and/or loyal to an organisation (Meyer & Allen, 1991: i.e. *they want to* (emotional attachment), *they have to* (e.g. financially) and/or *they feel they ought to* (obliged). Employee organisational commitment based on emotional attachment seems to result in the highest performance and greater adherence to policies (Karim & Noor, 2017; Scholl & Scholl, 2018) and thus must be considered within an employee cyber security measurement tool.

In addition to connections between organisational commitment and ISOP, this factor has also been found to be related to threat appraisal, with higher organisational commitment resulting in higher perceptions of severity of attack should one occur (Posey, Roberts & Lowry, 2015). Organisational commitment has also been linked to improved employee engagement as within the ISEI (Cox et al., 2006; Osborne & Hammoud, 2017).

Psychological ownership is the feeling of mental claim or possession of an object driving the need to control (and perhaps then protect) it (Baxter et al., 2015). It can be an internal motivator of cybersecurity behavioral intention, with those more attached to the organisation more likely to try and protect devices (Raddatz et al., 2020). It is associated with self-efficacy, where any impact on behavior is more powerful the higher the perceptions of psychological attachment are to a device (Verkijika, 2020). It has also been linked to the adoption of digital technologies, such as increased physical attachment via touchscreens, and social media usage increased through co-creation of avatars within apps (Brasel and Gips 2014; Kirk & Swain 2018; Zhao et al. 2016).

Psychological ownership is centred around the *endowment effect* decision-making heuristic, where higher value is often placed on possessions that are owned (Pfleeger & Caputo, 2012). With foundations in loss aversion, psychological ownership can result in unwillingness to swap an endowed item even for one of similar or higher value. With an object psychologically owned (such as a personal mobile telephone), it is viewed more favourably and becomes an extension of the self (Dyne & Pierce, 2004). Renaud et al. (2019) found it can also be present for cybersecurity tasks with participants being attached to their password routines, over-valuing these personal strategies, and being less willing to change. Feelings of attachment will occur towards the object increasing its perceived value, and therefore a need to better guard it to avoid loss (Baxter et al., 2015).

A number of antecedent factors are important for psychological ownership, including: time and effort invested, increasing control, , and getting to know it intimately (Baxter, Aurisicchio & Childs, 2015; Peck et al., 2021). The more control a user has over technology for personal comfort, the more they will try and protect it (Lee & Chen, 2011). Baxter et al. (2015) discuss ways in which an item can be controlled and these include: spatially (e.g. having it in an accessible position), based on configuration (e.g. personalising images and sounds), temporally (being able to access the item when desired), via rate control (it being constantly available) and with transformational control (e.g. having more personalized desktop icons). Together, these can increase recognition of technology just by viewing or switching it on. Control therefore centres around freedom to personalise hardware, software and settings, and can encourage safer cybersecurity behaviors.

Self-investment is another poetically important psychological ownership factor, where increasing time, energy and effort exerted results in perceiving an object as an extension of the self (Baxter et al., 2015). Self-investing in work technology can occur: through creation, repair and maintenance; using it as a repository; using emblems; and preference recall (Baxter et al., 2015). Whilst most employees are not involved in the creation of technology, personalising settings and options regarding e.g., protective casing, screen savers, photographs, and some software options can help increase psychological ownership.

Another antecedent of psychological ownership is intimate knowledge, where over time, an item becomes more special than similar items (Baxter et al., 2015; Lee & Chen, 2011). This has six contributing variables including: ageing, disclosure, periodic signalling, enabling, proximity, and simplification. Maturing alongside technology will result in employee ability to even better identify it through ‘bumps and scratches’ over time. Therefore, the longer the technology remains with the employee, the more attached they will tend to become to it and arguably then, the more motivated to protect it from physical and other damage.

Finally, we consider maladaptive rewards. These are intrinsic and extrinsic rewards a person may experience by not actively trying to protect themselves or their organisation from a cyber-attack. Intrinsic maladaptive rewards relate to internal benefits such as getting gratification for not protecting an organisation. Extrinsic rewards are motivated by not protecting an organisation, e.g. for financial gain. Should maladaptive benefits outweigh threat perception, an employee may opt for such internal and external benefits (Hassandoust & Techatassanasoontorn, 2020). Such rewards can also result in unintentional behaviors, through neglect or lack of attention resulting in security 'slip-ups', or be intentional such as providing system access to a threat actor due to low organisational commitment (Gheyas & Abdallah, 2016). Both types of risky behaviors are major problems for organisations and thus seem crucial to consider within a measurement tool

Some have built on behavior change models including intrinsic and extrinsic maladaptive threat behaviors (Hassandoust & Techatassanasoontorn., 2020; Safa et al., 2015). However, there is a dearth of research, perhaps due to ethical concerns (Liang et al., 2016). Though there is a literature on insider threat, a partially similar concept - defined as a current or former employee who exceeds, misuses or grants access to others in order to negatively impact an organisation's security (Greitzer et al., 2016). Similar to maladaptive rewards, insider threat can be deliberate or unintentional due to lack of care (Khan, Houghton, & Sharples, 2022), motivated by e.g. frustration, financial difficulties and/or reduced company loyalty. A number of psychological concerns have been identified as predisposing someone to be an insider threat, such as an anti-social personality (Kahn et al. 2022). More research is required to better understand how internal and external rewards impact employee security behaviors. As such, intrinsic and extrinsic maladaptive reward are considered within the current studies.

Overall, higher levels of organisational commitment and in particular – psychological ownership – seem to relate strongly to higher perceptions of value loss avoidance. Both factors appear to be key predictors of cybersecurity vulnerabilities and potential strengths. As such, scales and measures relating to both will be included within the tool created for the currents study.

4. The Current Studies

Three quantitative questionnaire-based studies are presented. Multiple existing questionnaires were employed and combined based upon factors deemed important to relating to risky cybersecurity behaviors within the previous sections. These are all highly valid and reliable measures employed by multiple researchers across many published studies although have never been combined in the way they are in this paper. The main aim of each study is to evaluate the numerous theoretical and empirically based factors identified and discussed that together may predict human – and in particular employee – cybersecurity vulnerabilities and behavior. By streamlining these factors – scales and questionnaires – into a tool and developing a framework based on findings, more effective interventions can be created to reduce human cybersecurity risk. Study 1[2] was designed to collectively explore constructs from a number of psychological theories (e.g. PMT, TPB, AT, TTAT), models (e.g. KAB, HBM), individual differences (e.g. age, gender, risk taking propensity), technology acceptance and adoption factors (e.g. cybersecurity awareness, involvement, experience and value in cybersecurity), and organisational factors (e.g. organisational commitment, psychological ownership of an organisation's technology, maladaptive rewards). that have been noted as influential to risky and/or cybersecurity behavior. The key novelty here is that they have never been brought together in a single tool. Study 2 – with a sample from a large multinational organisation (rather than university staff and students as in Study 1) – examines the underlying structure of the predictive constructs in Study 1 and their potential relationships, to identify latent factors. Study 3 strengthens the validity of the tool and framework by investigating how the latent factors determined in Study 2 relate to

[2] Note that Study 1 within the current paper is based on Bishop, L. M., Morgan, P. L., Asquith, P. M., Raywood-Burke, G., Wedgbury, A., & Jones, K (2020). Examining human individual differences in cyber security and possible implications for human-machine interface design. Presented at: *22nd International Conference on Human-Computer Interaction (HCII 2020),* Virtual, 19-24 July 2020. HCI for Cybersecurity, Privacy and Trust, vol.12210 Springer, Cham, pp. 51-66. The full study including comprehensive findings are presented within the current paper.

cybersecurity behaviors amongst employees of multiple organisations to further strengthen the ecological validity of the novel tool.

5. General Method

5.1. Design

A within participant correlational design was employed across all studies. They were designed to examine relationships between cybersecurity behavior and socio-psychological factors, perceptual abilities, a habitual factor, and socio-economic factors. Cybersecurity behaviors included: IT skill level, level of cybersecurity training, importance of role in cybersecurity, personality, risk-taking preferences, decision-making styles, impulsivity, and acceptance of the internet. Perceptual attributes included: threat appraisal, attitude, self-efficacy, subjective norms, perceived behavioral control, response efficacy, response costs, awareness, and organisation policy. The habitual factor was experience and involvement. Finally, the socio-emotional factors were intrinsic and extrinsic maladaptive rewards, organisational commitment, and psychological ownership.

5.2. Materials and Procedure

Studies were developed using *Qualtrics*© and completed online. Participants (including students in Study 1) had to be in active employment. Following instructions and consent, participants provided age, gender and education information (General Certificates of Education – GCSEs, Advanced-Levels – A-Levels, undergraduate degree, Master degree, Doctorate, other). They then rated importance in cybersecurity, from 1 (extremely important) to 5 (not at all important), level of IT skill, from 1 (poor) to 5 (excellent) and cybersecurity training level, from 1 (none) to 5 (expert). All other questionnaires were randomised to eliminate potential order effects. A full debrief was provided at the end of each study.

International Personality Item Pool (IPIP) personality traits (Goldberg et al., 2006): Fifty statements (10 per subscale): openness to experience, extroversion, neuroticism, conscientiousness, and agreeableness. Participants rated the extent each statement applied to them from 1 (very inaccurate) to 5 (very accurate).

Domain Specific Risk Taking (DOSPERT) scale (Blais & Weber, 2006): Thirty questions (six per subscale): social, recreational, financial, health/safety, and ethical. Participants rated how likely they were to engage in each from 1 (extremely unlikely) to 7 (extremely likely).

General Decision-making Styles (GDMS: Scott & Bruce, 1995) Twenty-five statements with five overarching decision-making styles (intuitive, dependent, avoidant, rational, spontaneous) with ratings ranging from 1 (strongly disagree) to 5 (strongly agree).

Barratt Impulsiveness Scale (BIS-11: Patton et al, 1995): Thirty statements with participants rating how regularly they had experienced each ranging from 1 (rarely/never) to 5 (always).

The IPIP, DOSPERT, GDMS and BIS-11 questionnaires were also utilised (as in Egelman & Peer, 2015; Gratian et al., 2018).

User Acceptance of Information Technology (UTAUT) scale (Venkatesh et al., 2003): Thirty statements with nine subscales (performance expectancy, effort expectancy, social influence, trust, facilitating conditions, hedonic motivation, price value, habit and behavioral intention) rated from 1 (strongly disagree) to 7 (strongly agree).

Combined Theory of Planner Behavior (TPB) and Protection Motivation Theory (PMT) (Safa et al., 2015): Forty-two statements (e.g. *'I am aware of potential security threat'*) from nine sub-scales (e.g. threat appraisal) rated from 1 (strongly disagree) to 7 (strongly agree). Thirty-three questions from McGill & Thompson (2017) and Posey et al. (2015) were included on e.g., intrinsic and extrinsic maladaptive rewards (e.g. *'I feel a high degree of ownership for* *my work computer and its contents'*) across four sub-scales (e.g. organisational commitment) rated from 1 (strongly disagree) to 7 (strongly agree).

Cybersecurity behavior was measured by the *behavior construct within the PMT and TPB questionnaire*, rated from 1 (strongly disagree) to 7 (strongly agree) with five statements such as *'I consider security experts recommendations in my information security manner'*.

Reliability of Measures and Data Preparation

Cronbach's alpha tests revealed good to excellent reliability for the BIS-11(α = .87), GDMS (α = .78 - .90), DOSPERT (α = .64 - .86), IPIP (α = .75 - .91), combined TPB and PMT subscales (α = .77 - .89), and additional constructs from PMT subscales (α = .69 - .88). For UTAUT subscales, acceptable to excellent reliability was achieved (α = .69 - .95). The cybersecurity awareness construct also had excellent reliability (~ α =.90). Missing data were replaced with grand means and outliers windsorized to the next available non-extreme value.

6. Study 1

Study 1 was exploratory with a number of hypotheses. First, that reported cybersecurity behavior would significantly differ across demographics (age, gender, education). Based on the weighting of the literature reviewed, that younger participants and females would report more risky cybersecurity behaviors than older participants and males. Significant relationships were also predicted between reported cybersecurity behavior and individual differences: personality, impulsivity, risk-taking preferences, and decision-making styles. Again, based on the literature reviewed that those higher in impulsivity and risk-taking preferences, and with more spontaneous irrational decision making styes will report more risky cybersecurity behaviors. Significant relationships were also predicted between reported cybersecurity behaviors and key constructs from behavior change theories and models: threat appraisal, response efficacy, self-efficacy, response costs, attitude, and subjective norms.

Additionally, significant correlations were predicted between reported cybersecurity behavior and: information security organization policy, information security awareness, information security experience and involvement, psychological ownership, organisational commitment, and intrinsic and extrinsic maladaptive rewards. For example, that those with higher information security awareness and experience and involvement as well as those with stronger psychological ownership of devices and higher organisational commitment would report less risky cybersecurity behaviors.

6.1. Participants

Seventy participants were recruited from the Cardiff University staff, PhD and undergraduate student pools (48% of sample) and *Prolific* (52%). All were in full- or part-time employment. The sample consisted of 31% male, 68% female and 1% of a different identity, with an average age of 34.92 years (*SD* 10.67). Some students received course credits and others were paid £8.00. The majority of undergraduate students received course credits (a requirement of their research methods training). Cybersecurity behaviors did not differ between students and non-students/staff (*ps* > .05) noting this includes those who were paid and not paid (received credits). Samples were matched by age and education level. Whilst 50% of participants within the student sample were female, 84% of *Prolific* participants identified as female.

6.2. Results

Reliability of measures was examined first. Initially, a test of internal consistency was applied to all measures. Cronbach's Alpha tests revealed good to excellent reliability for the Barratt Impulsivity questionnaire (α = .87), GDMS decision-making style questionnaire subscales (α = .78 - .90), DOSPERT risk-taking preferences questionnaire subscales (α = .64 - .86), IPIP Personality Traits questionnaire subscales (α = .75 - .91), the combined TPB and PMT questionnaire subscales (α = .77 - .89), and additional constructs included from the protection motivation questionnaire subscales (α = .69 - .88). The same tests established that for UTAUT subscales, reliability was acceptable to excellent (α = .69 - .95). The key assumptions for parametric analysis were not met due to the use of ordinal data. Therefore, non-parametric tests were applied. Assumptions for all statistical tests were analysed and met. Any missing observations within the dataset were replaced with the grand mean for each question and any outliers, determined as three interquartile range (IQR) points from the mean were windsorized to the next available value not considered extreme (with the same procedure applied within subsequent studies).

Cybersecurity Behavior

The sample median score was 6 (IQR = 1). This indicates that, on average, participants moderately agreed that their cybersecurity behavior is conscious and favourable.

Participant Demographics

Differences in reported cyber security behavior were predicted based on age; gender, and level of education. Kruskal-Wallis analyses revealed no significant differences: age (H = 11.56, p = .99); gender (H = 2.17, p = .34); and education (H = 4.03, p = .40).

Individual Differences

Spearman's Rho correlations were applied. There were non-significant relationships for reported cyber behavior and ratings of IT skill (*Mdn* = 4, IQR = 1, suggesting moderate-high skill), *r* = .07, n = 71, *p* = .58; level of cybersecurity education (*Mdn* = 2, IQR = 1, suggesting beginners), *r* = .20, n = 71, *p* = .09; or perceived importance of role in protection their organisation (*Mdn* = 4, IQR = 1, suggesting role is very important), *r* = .17, n = 71, *p* = .17.

Next, relationships between cybersecurity behavior and socio-psychological factors were explored. Starting with personality, those more conscientious (*Mdn* = 4, IQR = 1) reported significantly more conscious cybersecurity behavior (*r* = .34, *n* = 71, *p* = .004) with a medium effect size (Table 1). There were non-significant relationships for levels of extraversion (*Mdn* = 3.5, IQR = 1; *r* = .20, *n* = 71, *p* = .10), agreeableness (*Mdn* = 4, IQR = .5; *r* = .01, *n* = 71, *p* = .92), neuroticism (*Mdn* = 2.5, IQR = 1.5; *r* = -.18, *n* = 71, *p* = .13) and openness to experience (*Mdn* = 4, IQR = 1; *r* = .20, *n* = 71, *p* = .10).

For impulsivity (*Mdn* = 2, IQR = .5), and as predicted, a significant negative relationship was found (*r* = -.30, *n* = 71, *p* = .01), with a medium effect size (Table 1).

As predicted, a significant positive relationship was found between social risk-taking (*Mdn* = 5.5, IQR = 1) and reported cybersecurity behavior (*r* = .33, *n* = 71, *p* = .004**)** with a medium effect size (Table 1). There were no significant relationships for recreational risk-taking (*Mdn* = 2.5, IQR = 3; *r* = .13, *n* = 71, *p* = .28), financial risk-taking (*Mdn* = 2, IQR = 1.5; *r* = .16, *n* = 71, *p* = .19), health/safety risk-taking (*Mdn* = 2, IQR = 3; *r* = .06, *n* = 71, *p* = .59) or ethical risk-taking (*Mdn* = 5.5, IQR = 1.5; *r* = -.01, *n* = 71, *p* = .93).

There were no significant relationships for any decision-making style: intuitive (*Mdn* = 3, IQR = 1: *r* = .04, *n* = 71, *p* = .77), dependent (*Mdn* = 4, IQR = 1: *r* = .01, *n* = 71, *p* = .99), rational (*Mdn* = 4, IQR = 0: *r* = -18, *n* = 71, *p* = .13), avoidant (*Mdn* = 2, IQR = 2: *r* = -.13, *n* = 71, *p* = .29), or spontaneous (*Mdn* = 2, IQR = 1: *r* = -.17, *n* = 71, *p* = .15).

Acceptance of cybersecurity measures were considered. For perceived effort expectancy, participants moderately-strongly agreed that cybersecurity tasks are easy to undertake (*Mdn* = 6.5, IQR = 1). This significantly related to cybersecurity behavior (*Mdn* = 6.5, IQR = 1: *r* = .30, *n* = 71, *p* = .01), with a low-medium effect (Table 1). There were no significant relationships for performance expectancy (*Mdn* = 6, IQR = 1.5: *r* = -.21, *n* = 71, *p* = .07), social influence (*Mdn* = 5, IQR = 2: *r* = .10, n = 71, *p* = .43), facilitating conditions (*Mdn* = 6, IQR = 1.5: *r* = .19, *n* = 71, *p* = .12), or trust (*Mdn* = 3, IQR = 3; *r* = -.14, *n* = 71, *p* = .23).

The following perceptual factors from behavior change theories significantly and positively related to cybersecurity behavior (Table 1): threat appraisal (*Mdn* = 6, IQR = 1): with a medium effect size (*r* = .36, *n* = 71, *p* = .002), security self-efficacy (*Mdn* = 5.5, IQR = 1) with a large effect size (*r* = .66, *n* = 71, *p* < .001) and information security attitude (*Mdn* = 6, IQR = 1) with a medium effect size (*r* = .43, *n* = 71, *p* < .001). This was not the case for response efficacy (*Mdn* 5, IQR = 1; *r* = .17, *n* = 71, *p* = .16), response costs (*Mdn* = 4, IQR = 2; *r* = -.205, *n* = 71, *p* = .09) or subjective norms (*Mdn* = 5, IQR = 2; *r* = .12, *n* = 71, *p* = .33).

Three antecedents of the TPB were examined: information security experience and involvement (*Mdn* = 5, IQR = 2), information security awareness (*Mdn* = 5, IQR = 2) and information security organisation policy (*Mdn* = 5.5, IQR = 1.5). Performance expectancy of cybersecurity tasks was high (*Mdn* = 6, IQR = 1.5) with moderate agreeance that cybersecurity measures are easy to undertake. All significantly positively correlated with cyber security behavior Table 1), with large effects (*r* = .64, *n* = 71, *p* = < .001; *r* = .63, *n* = 71, *p* = < .001; *r* = .54, *n* = 71, *p* = < .001, respectfully).

Four perceptual and socio-emotional factors were analysed: organisational commitment (*Mdn* = 5, IQR = 3), psychological ownership (*Mdn* = 5, IQR = 2) intrinsic maladaptive rewards (*Mdn* = 1, IQR = .5) and extrinsic maladaptive rewards (*Mdn* = 1, IQR = 2). Participants reported being very unlikely to wish to gain from loss to their organisations, suggesting low levels of insider threat. Psychological ownership significantly related to reported cyber security behavior with a small effect size (r = .27, n = 71, p = .02, Table 1), yet organisational commitment (r = .19, n = 71, p = .11), intrinsic maladaptive rewards (r = -.22, n = 71, p = .07) and extrinsic maladaptive rewards (r = .06, n = 71, p = .63) did not.

Table 1.

Factors significantly relating to cybersecurity behaviors (with effect sizes)

Construct	Correlation
Large Effect Size (>.50)	
Security self-efficacy	r = .66, n = 71, p < .001
Information security experience and involvement	r = .64, n = 71, p < .001
Information security awareness	r = .63, n = 71, p < .001
Information security organisational policy	r = .54, n = 71, p < .001
Medium Effect Size (>.30, <.49)	
Information security attitude	r = .43, n = 71, p < .001
Threat appraisal	r = .36, n = 71, p = .002
Conscientiousness	r = .34, n = 71, p = .004
Social risk-taking	r = .33, n = 71, p = .004
Impulsivity	r = -.30, n = 71, p = .011
Effort expectancy	r = .30, n = 71, p = .012
Small Effect Size (>.10, <.29)	
Psychological ownership	r = .27, n = 71, p = .021

3.3. Study 1 Discussion

The main aim of Study 1 was to develop a first iteration of a holistic human cybersecurity behavior measurement tool. It involved exploratory investigation into how several previously reported factors – brought together within the same tool – significantly relate to reported cybersecurity behavior.

No significant differences were found between age and gender types and reported cybersecurity behavior. Prior research has tended to focus on very specific cybersecurity tasks e.g., device securement and password management, rather than the more global perception of cybersecurity behavior within the current study. Educational level was not significant either, although no specific prediction was made based on it.

We predicted more secure behavior would be found amongst those with higher in extroversion and conscientiousness. Only conscientiousness was significant. Those higher in conscientiousness are generally more self-controlled, orderly, thorough and diligent and seem to be more risk-aware in their cyber decisions. The lack of relationship for extroversion could again be due to the more general cybersecurity behaviors probed.

Previous research highlighted health and safety, ethical and financial risk-taking as related to cybersecurity behavior (Egelman & Peer, 2015; Gratian et al., 2018). In contrast, we found that security behaviors were related to social risk-taking only. Perhaps those more comfortable in disagreeing with others will act against shadow security workarounds that are often taken within workplaces (Kirlappos, 2016; Kirlappos et al., 2014, 2015).

The role of impulsivity was supported as in previous studies (e.g., Egelman & Peer 2015). It is key that interventions are focussed on slowing down decision-making processes, allowing more logically processing of information. Of the UTAUT constructs originating from TAM, performance expectancy did not significantly relate, although effort expectancy did with those finding cybersecurity tasks easier to explicate more likely to report positive cybersecurity behavior. This supports previous findings, with effort expectancy influencing positive and secure behavior in mobile commerce (Alrawi et al., 2020), payments (Ariffin et al., 2020), and banking (Ivanova & Kim, 2022). There were no significant relationships between additional UTAUT factors: facilitating conditions, social influence and trust.

These findings suggest that secure behavior is more likely in those that take more time to consider behavior, are comfortable disagreeing with others and feel that cybersecurity behaviors are worth effort. Interventions could involve e.g. decision-making ‘speed bumps’, to decrease consequences of unconscious decision-making. However, these may impact perceptions of effort expectancy and more effort to find shadow workarounds. Another option is a feedback tool making it easier for employees to speak or act against the ‘risky’ shadow security behaviors witnessed. This might discourage social risk-taking, and provide a forum to discuss views on interventions that are impacting effort expectancy.

Threat appraisal, cyber-security attitude, subjective norms, response efficacy, self-efficacy, response costs, psychological ownership, cybersecurity awareness, and cybersecurity organisation policy were examined. Security self-efficacy had the strongest relationship: supporting research within the health domain (e.g. Floyd et al., 2000) and in other cybersecurity studies (e.g. van Bavel et al., 2019). There are at least four ways to increase self-efficacy: experience, witnessing success of others, social encouragement, and reducing physiological senses of stress. It is important that employees are supported to increase their cybersecurity abilities, with a culture of witnessing success of others and experiencing social encouragement around security. This will also likely support knowledge transfer (Elliot et al., 2011; Elliot & McGregor, 2001; Nicholls, 1984).

Information security attitude, the perception of securing information, also significantly related with cybersecurity behavior (as in Safa et al., 2015). This reinforces aspects of the TPB (Azjen’s, 1991) where attitudes repeatedly influence intentions and behaviors. Ajzen and Fishbein (1975) posit *attitude* as a construct relating to the expectancy-value theory, where behavior execution rests on the expected chance of achieving the task alongside value placed upon it. Improving attitude towards cybersecurity may hinge on increasing evaluation of the safety of an organisation’s systems, as well as self-internal perception of ability.

Threat appraisal also significantly correlated with cybersecurity behavior, further reinforcing behavior change theory recommendations: specifically that choice to act / not to act relates to a perception of the potential likelihood and severity of risk. Many employees may feel they have little to lose at work and utilise what they believe are secure systems (Jones et al., 2021). Thus, increasing threat appraisal may hinge on informing employees of system weaknesses and improving knowledge of potential loss should a security breach occur. From a behavior change theory perspective, it is key that people view cybersecurity as achievable, a breach as highly possible, and protecting company systems as valuable.

Significant relationships were found between reported cybersecurity behavior and the three antecedents of influencing factors in the TPB (Safa et al. 2015). IS awareness (antecedent for IS attitude), IS experience and involvement (antecedent of IS self-efficacy) and IS operation policy (antecedent of subjective norms) positively related. Those with higher awareness of how to remain up-to-date about security were more likely to report positive security behavior. IS operation policy positively related to behavior despite subjective norms, a potential successor, not reaching significance. Those recognising value in security policy may report behaviors that have company risk in mind. Overall, increasing employee perception of involvement in cybersecurity tasks, regularly updating their knowledge of current risks and protective behaviors, and supporting them to see value in organisation policy will likely lead to improved cybersecurity behavior.

Psychological ownership also positively correlated with cybersecurity behavior. Higher psychological ownership has been found to be related to greater levels of attachment to and perceived responsibility of an object (McGill & Thompson, 2017; Peck et al., 2021). This can be achieved by investing more time and having more control, and improving cognitive and affective evaluations. Thus, self-investment seems crucial (Lee & Chen, 2011).

In terms of IS experience and involvement (ISEI), those more experienced and enmeshed in the cybersecurity chain, reported more positive cybersecurity behavior. However, high levels of cybersecurity involvement can be particularly difficult in large organisations with separate IT and cybersecurity teams. All too often, employees receive infrequent training cybersecurity training sessions making it difficult for them to feel part of the solution. Including them in as many aspects of cybersecurity as possible and giving feedback when their behavior has had a positive influence (e.g. successfully reporting phishing) will not only increase perceptions of involvement, but in turn improve level of experience.

Some other predictions were not supported. Of three key factors (self-efficacy, response efficacy, response costs) previously found to be important in appraisal of a response, only self-efficacy was significant. This is perhaps no surprise, as despite prominence in behavior change models, a lack of clarification around the importance of other factors to cybersecurity behavior is evident. Also, literature suggests that social norms only become important if self-efficacy is low (Ajzen, 1991; McGill & Thompson, 2017).

In relation to socio-emotional factors, neither intrinsic nor extrinsic maladaptive rewards related to reported behavior. Participants reported being unlikely to wish to gain from their organisation experiencing loss (low insider threat). However, and for some (perhaps), there may have been anxiety due to repercussion worry or social desirability effects.

Organisational commitment did not reach significance; in contrast to previous findings (Ertan et al., 2020; Karim & Noor, 2017). However, Reeve et al. (2020) found that whilst it can influence cybersecurity behavior in relation to mobile phones, this was not the case with malware or phishing attacks. As noted earlier, this non-significant finding in Study 1 could be due to more global measures of cybersecurity behaviors included.

Overall, Study 1 has confirmed the efficacy of a first iteration tool effectively to measure relationships between multiple factors linked to risky cybersecurity behaviors. From this, tentative recommendations for organisations motivated to improve employee cybersecurity behaviors have been developed; outlined within Table 2.

Table 2.

Recommendations for organisations to alleviate employee cybersecurity risks

Metric	Recommendation
IS Awareness	Provide a culture where employees stay up to date on current risk and coping strategies.
IS Organisation Policy	Include employees in the optimisation of cybersecurity policy to increase perception of its value and increase its use.
IS Experience and Involvement	Utilise feedback around employee sentiment towards cybersecurity training that supports not just education but skill proficiency.
IS Self-efficacy	Ensure employees can proficiently conduct required cybersecurity skills and perceive themselves as having the ability to do so.
Threat Appraisal	Regularly update employees on cyber incidents in- and out-side of the organisation.
IS Attitude	Help employees consider benefits of cybersecurity behaviors by increasing risk perception and simplifying counter actions.

7. Study 2

Study 2 set out to confirm and extend correlational findings from Study 1 with participants from a large global organisation. A number of hypotheses were set, largely based on Study 1 findings. First, that individual differences (conscientiousness, impulsivity, social risk-taking) would significantly relate to reported behavior. For example, that higher cybersecurity risky behaviors reported would positively correlate with being higher in impulsivity and social risk taking although being negatively correlated with higher conscientiousness. Second, that reported behavior would correlate with factors in models of behavior change: information security attitude, threat appraisal, and self-efficacy with the same predictions as in Study 1. Third, that additional constructs found to previously relate, both in the literature and Study 1 (psychological ownership, IS awareness, IS organisation policy, effort expectancy, and IS experience and involvement) would correlate here in the same way as in Study 1. Study 2 further builds upon Study 1 by including an exploratory factor analysis for item reduction and regression analyses to investigate how related constructs may better fit into a predictive model.

7.1. Methodological Differences to Study 1

One-hundred-and-fifty-six participants, 84% male and 16% female, were recruited within a multinational organisation, via their internal UK Intranet with a mean age of 40.64 (*SD* 9.81). They were not rewarded for taking part. Questions on intrinsic and extrinsic maladaptive rewards and organisational commitment were removed as there were no significant relationships with reported behavior in Study 1. Social desirability questions were removed given the voluntary participation in a Study developed to increase employee awareness of human cybersecurity risks and not to potentially e.g. identify insider treat type behavior.

7.2. Results

Reliability of measures was examined first. Cronbach's Alpha tests of internal consistency were applied to all measures as in Study 1. Good reliability was found for the Barratt Impulsivity questionnaire ($\alpha = .73$) and acceptable to good reliability was calculated for all subscales of the DOSPERT risk-taking preferences questionnaire ($\alpha = .60 - .82$). The IPIP personality subscales reached acceptable to good reliability ($\alpha = .61 - .82$) except for conscientiousness which had poor reliability ($\alpha = .54$). Effort expectancy ($\alpha = .83$) from the UTAUT showed good reliability. Finally for the combined TPB and PMT questionnaire all subscales displayed good reliability ($\alpha = .74 - .89$) as did the set of statements used to measure psychological ownership ($\alpha = .88$). The key assumptions for parametric testing were not met due to the use of ordinal data, and therefore non-parametric statistical tests were utilised. Assumptions for all statistical tests used were analysed and met. Any missing observations within the dataset were replaced with the grand mean for each question and any outliers determined were windsorized to the next available value not considered extreme. There was no significant skewness or kurtosis.

Cybersecurity Behavior

Cybersecurity behavior was similar to Study 1 (Study 2 *Mdn* = 6, IQR = 2). The sample moderately agreed that their cybersecurity behavior is conscious and favourable.

Demographic Factors

There were no significant differences for gender ($H = 2.090$ $p = .15$) or education level ($H = .63$, $p = .99$). However, and unlike Study 1, a significant difference was found for age and reported cybersecurity behavior ($H = 12.803$, $p = 0.03$). Those aged 45-54-years reported significantly more conscious cybersecurity behaviors than the 25-34 ($p = .01$) and 35-44 ($p =$

.03) age groups. Also, the 55-64-year group were more likely to report cybersecurity behaviors than the 25-34 ($p = .006$) and 35- 44 ($p = .013$) groups.

Individual Differences

Spearman’s Rho tests were applied to explore relationships between reported cybersecurity behavior and socio-psychological factors (personality, impulsivity, risk-taking preferences). For personality sub-types, associations were analysed for reported cybersecurity behaviors and extraversion (*Mdn* = 3, IQR = 1.5), conscientiousness (*Mdn* = 4, IQR = 1), agreeableness (*Mdn* = 4, IQR = .5) neuroticism (*Mdn* = 2.5, IQR = 1) and openness to experience (Mdn = 4, IQR = .5). Unlike Study 1, no significant relationships were found between behavior and conscientiousness ($r = .06$, $n = 153$, $p = .44$, Table 3), nor: extraversion ($r = .08$, $n = 153$, $p = .33$), agreeableness ($r = .09$, $n = 153$, $p = .08$), neuroticism ($r = -.02$, $n = 153$, $p = .80$), or openness to experience ($r = .130$, $n = 153$, $p = .10$).

As predicted, social risk-taking propensity (*Mdn* = 5, IQR = 2) significantly correlated with reported behavior ($r = .23$, n = 155, $p = .004$), with a small effect size (Table 3). Those less likely to take ethical risks (*Mdn* = 1, IQR = 1) were more likely to report positive behavior, with a small effect size ($r = .21$, $n = 155$, $p = .009$, Table 3). However, as with Study 1, no significant relationships were found for recreational risk-taking (*Mdn* = 3.5, IQR = 3.5; $r = .05$, $n = 155$, $p = .54$), financial risk-taking (*Mdn* = 1, IQR = 1; $r = .14$, $n = 155$, $p = .09$) or health/safety risk-taking (*Mdn* = 2, IQR = 1.5; $r =- .05$, $n = 155$, $p = .55$).

Participants reported occasionally behaving impulsively, with a large dispersion (*Mdn* = 2, IQR = .5). Despite a significant relationship in Study 1, this was not the case in Study 2 ($r = .14$; $n = 155$, $p = .09$). Attitude towards cybersecurity (*Mdn* = 5, IQR = 2) significantly related, with a large effect size ($r = .68$, $n = 155$, $p < .001$, Table 2). As in Study 1, there was a significant relationship between behavior and psychological ownership (*Mdn* = 4, IQR = 2), with a medium effect (r = .30, n = 155, p < .001, Table 3).

Perceptual factors were examined. For threat appraisal, participants reported a potentially high probability and severity if cautionary action is not taken (*Mdn* = 7, IQR = 2); and this significantly correlated with cybersecurity behavior (r = .70, n = 155, p > .001), with a large effect size (Table 3). For security self-efficacy, participants rated high on skills required to protect themselves and their organisation from a cyber-attack (*Mdn* = 6, IQR = 1.5) also with a significant relationship (r = .54, n = 155, p < .001), and large effect (Table 3). Unlike Study 1, subjective norms (*Mdn* = 5, IQR = 2) significantly related to reported behavior, with a small effect size (r = .28, n = 155, p > .001, Table 3). For effort expectancy, participants moderately agreed that cybersecurity tasks are easy to undertake (*Mdn* = 6, IQR = 1) and as with Study 1, it significantly related to reported behavior, with a small effect size (r = .18, n = 155, p = .03, Table 3). Antecedents of factors from the TPB were also analysed. ISA (*Mdn* = 6.5, IQR = 1) significantly related to reported behavior with a large effect (r = .68, n = 155, p < .001) as did information security experience and involvement (*Mdn* = 7, IQR = 1; r = .64, n = 155, p < .001), see Table 3.

The habitual factor, ISOP was analysed (*Mdn* = 7, IQR = 1). As in Study 1, there was a significant correlation (r = .64, n = 155, p < .001), with a large effect size (Table 3).

Table 3.

Factors significantly relating to cybersecurity behaviors (with effect sizes). *Note.* Compared with Study 1.

Construct	***Study 1***	***Study 2***
Large Effect Sizes in Study 2 (>.5)		
Threat appraisal	r = .36, n = 71, p = .002	r = .70, n = 155, p < .001
Information security awareness	r = .63, n = 71, p < .001	r = .68, n = 155, p < .001
Information security attitude	r = .43, n = 71, p < .001	r = .68, n = 155, p < .001

IS experience and involvement	*r* = .64, *n* = 71, *p* < .001	*r* = .64, *n* = 155, *p* < .001
IS organisation policy	*r* = .54, *n* = 71, *p* < .001	*r* = .57, *n* = 155, *p* < .001
Information security self-efficacy	*r* = .66, *n* = 71, *p* < .001	*r* = .54, *n* = 155, *p* < .001
Medium Effect Sizes in Study 2 (>.3, <.49)		
Psychological ownership	*r* = .27, *n* = 71, *p* = .021	*r* = .30, *n* = 155, *p* < .001
Small Effect Sizes in Study 2 (>.1, <.29)		
Subjective Norms	Did not correlate	*r* = .28, *n* = 155, *p* > .001
Social risk-taking	*r* = .33, n = 71, *p* = .004	*r* = .23, *n* = 155, *p* = .004
Ethical risk-taking	Did not correlate	*r* = .21, *n* = 155, *p* = .009
Effort expectancy	*r* = .30, *n* = 71, *p* = .012	*r* = .18, *n* = 155, *p* = .029
Conscientiousness	*r* = .34, *n* = 71, *p* = .004	Did not correlate
Impulsivity	*r* = -.30, *n* = 71, *p* = .011	Did not correlate

Exploratory Factor Analysis (EFA)

First, a principal axis factoring extraction method was used with no rotation initially applied to generate a scree plot and determine latent variables. Two factors were identified before the elbow and three found to account for 36.34% of variance. A varimax rotation was then applied. A number of factors cross-loaded, thus a promax rotation was utilised. Two factors still cross-loaded and were excluded: ‘I understand the risk of information security incidents’ (from ISA); and, ‘I have suitable capability in order to manage information security risk due to my experience’ (from ISEI). Variance reduced to 35.22% (Table 4).

As the third factor identified (ethical risk-taking) only had one item (‘Passing off somebody else’s work as your own’) loading onto the latent variable, it was excluded from the model resulting in two unobserved variables considered (Figure 1). Variable 1 is labelled ‘Cybersecurity Awareness’, due to underlying items such as the original awareness construct, and also general attitude towards cybersecurity, how threat is appraised, experience and involvement in cybersecurity, self-efficacy in the use of secure measures, and views on cybersecurity operation policy. Together, the items generate an unobserved variable that appears to capture a holistic experience of the human within cybersecurity. The second latent variable includes six of the seven items within the psychological ownership measure and maintained the label ‘Psychological Ownership’ (Figure 1).

Regression Analyses

A stepwise regression was run with the two factors identified by the EFA, as well as age. Iteration halted at model 1 (F (1, 151) = 189.77, $p < .001$) where 55% of variance in reported behavior was explained by *Cybersecurity Awareness* (adjusted $R^2 = .55$), the latent variable generated as part of the EFA. Psychological ownership and age were extracted from the model as neither significantly explained additional variance.

Table 4.

Factor loadings for the exploratory factor analysis in Study 2

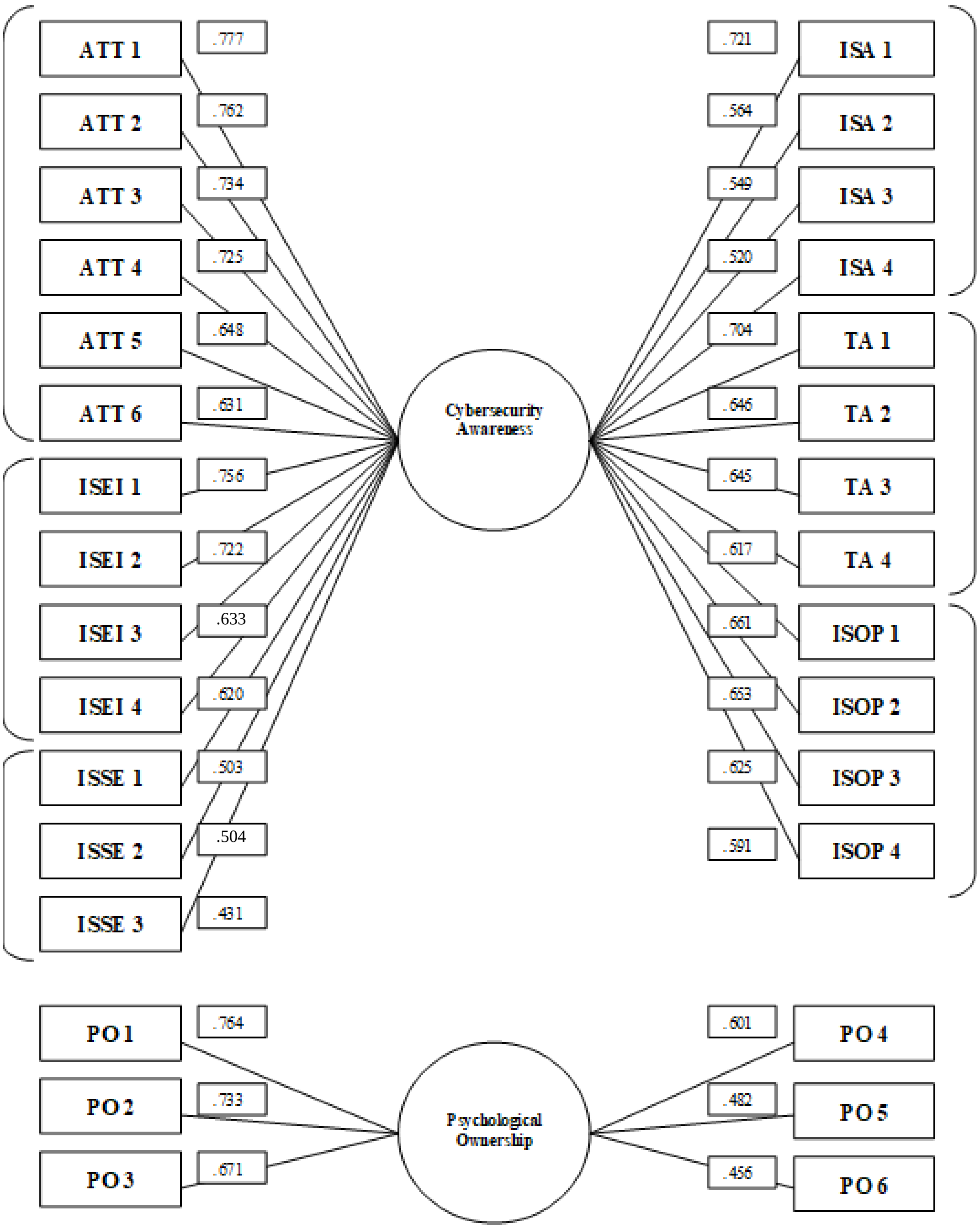
No.	Factor	Item	Loading	Eigenvalue	Variance
1	Cybersecurity Awareness	Careful information security behavior is necessary (ATT1)	.78	25.400	24.27%
		My attitude towards careful information security behavior is favourable (ATT2)	.76		
		My experience helps me to recognise and assess information security threat (ISEI1)	.76		
		I believe that careful information security behavior is valuable in an organisation (ATT3)	.73		
		Practising careful information security behavior is useful (ATT 4)	.73		
		My experience increases my ability to have a safe behavior in terms of information security (ISEI2)	.72		
		I keep myself updated in terms of information security knowledge to increase my awareness (ISA1)	.72		
		Hackers attack with different methods and I should be careful in this dynamic environment (TA1)	.70		
		Information security policies and procedures affect my behavior (ISOP1)	.66		
		Behavior in line with organisational information security policies and procedures is of value in my organisation (ISOP2)	.65		
		I have a positive view about changing users' information security behavior to be more considered (ATT5)	.65		
		I know the probability of security breach increases if I do not consider information security policies (TA2)	.65		
		I could fall victim to different kinds of attack if I do not follow information security policies (TA3)	.65		
		Careful Information security behavior is beneficial (ATT6)	.63		

		I can sense the level of information security threat due to my experience in this domain (ISEI3)	.63		
		Information security policies and procedures have attracted my attention (ISOP3)	.63		
		I am involved with information security and I care about my behavior in my job (ISEI4)	.62		
		The security of my data will be weak if I do not consider information security policies (TA4)	.62		
		Information security policies and procedures are important in my organisation (ISOP4)	.59		
		I share information security knowledge to increase my awareness (ISA2)	.56		
		I have sufficient knowledge about the cost of information security breaches (ISA3)	.55		
		I am aware of potential security threat (ISA4)	.52		
		I have the skills to protect my business and private data (ISSE1)	.50		
		I think the protection of my data is in my control in terms of information security violations (ISSE2)	.50		
		I have the ability to prevent information security violations (ISSE-3)	.43		
2	Psychological Ownership	When I think about it, I see an extension of my life in my work computer (PO1)	.76	8.11	6.95%
		I personally invested a lot in my work computer, e.g. time, effort, money (PO2)	.73		
		I personally invested a lot in the software/applications on my work computer, e.g. time, effort, money (PO3)	.67		
		I see my work computer as an extension of myself (PO4)	.60		
		I feel a high degree of ownership for my work computer and its contents (PO5)	.48		
		The information stored on my work computer is very important to me (PO6)	.46		
3	Ethical Risk-Taking	Passing off somebody else’s work as your own (ERT1)	.41	5.53	4.00%

Only factor loadings > .04 are presented (see e.g., Matsunaga, 2010; Watkins, 2021)

Figure 1.

EFA model. *Note.* Att – Information Security Attitude, ISEI – Information Security Experience and Involvement, ISSE – Information Security Self-efficacy, ISA – Information Security Awareness, TA – Threat Appraisal, ISOP – Information Security Operation Policy, PO – Psychological Ownership.



7.3. Study 2 Discussion

One aim of Study 2 was to further examine factors within Study 1 that significantly related to reported cybersecurity, with a larger sample of UK employees working for the same global organisation. Another aim was to use exploratory factor analysis (EFA) to potentially refine the large number of factors contained within our emerging framework. Regression analyses were conducted utilising the refined EFA model, to better understand which of the latent variables would explain the largest portion of variance in reported cybersecurity behavior.

Previous research has found age to be a significant predictor of cybersecurity behavior (e.g. Gratian et al., 2015; Sheng et al., 2010) and this was (unlike Study 1) also the case in Study 2 - with those in the 45–54 and 55–64 groups reporting significantly greater conscious cybersecurity behaviors. However, age was not a significant predictor within the regression model (see also Gratian et al. 2018). As with Study 1, there was no effect of gender.

Study 2 revealed that the same eleven factors (conscientiousness, impulsivity, social risk-taking, psychological ownership, threat appraisal, self-efficacy, attitude, awareness, organisation policy, effort expectancy, experience and involvement) significantly correlated with reported behavior; as in Study 1. However, and due to the large number of related factors (and inter-correlations between them) an EFA was conducted to determine whether items informing these metrics load in a way that uncovers a more succinct set of unobserved variables. Two latent variables emerged: one that solely represents Psychological Ownership, and another - Cybersecurity Awareness - informed by twenty-five items across six different observed constructs (TA, ISSE, IS attitude, ISA, ISEI, ISOP). However, Psychological Ownership did not explain additional variance within the regression model that followed.

The number of observed constructs and determining measurement items loading onto the Cybersecurity Awareness latent variable indicate that a global construct has been identified that in Study 2 could account for 55% of the variance in cybersecurity behavior within the regression model. Encapsulating the need for an awareness of threat probability, protection ability, experiences, attitudes, policies and more, suggesting awareness of cybersecurity generally is required to positively inform behavior. Cybersecurity awareness is a term regularly used within the field to describe how end-users experience cybersecurity, in relation to understanding of threat risk *and* perceptions of efficacy to exhibit behaviors that will help prevent risk. There have however been long-standing differences concerning how awareness is best defined (Chaudhary et al., 2023; Zwilling et al., 2022). It must be noted that programmes used within many organisations to provide employees with updates and education around risk, are often also termed ‘cybersecurity awareness’. However, this is simply describing the mode used to improve levels of awareness, and not awareness itself.

Awareness as a concept is still debated making it even more difficult to determine how cybersecurity awareness should be defined. It includes factors such as situational awareness, assessments of competence, perceptions and psychological aspects, policy, behavior, task specific knowledge, and interventions for improvement (Chaudhary, 2023). Gafoor (2012) suggest three forms of awareness: *about* something (knowledge on a topic), *of* something (subjective perceptions of a topic), and *ability* (having conscious ability to do something). It has also been conceptualised as a lower form of surface level knowledge. However, Travethan (2017) suggests awareness is related to the attention or mindfulness of a subject, in particular its dangers. For example, how mindful people are of certain risks and the need to avoid them, with knowledge at its root (Khader et al, 2021; Zwilling et al., 2022). This definition appears useful in cybersecurity awareness, due to its distinct focus on risk.

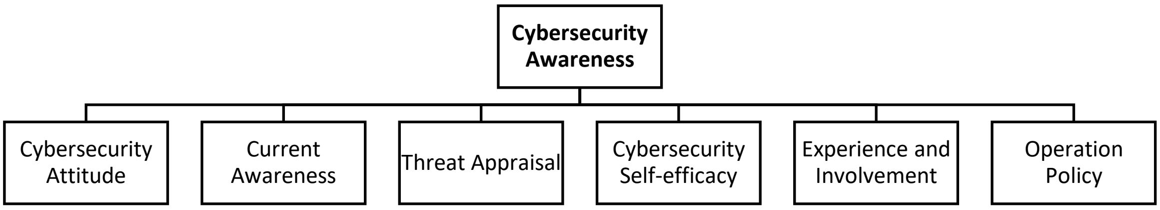
Awareness was often conceptualised as a state of mind where only a small amount of information is activated at any given time, replaced by different forms of information as soon as something falls out of use (Carr, 1979). However, awareness is believed to influence behavior, even when not at the forefront of thought (Merikle, 1984). Humans can be ‘aware’ of many things: who they are, what they do, what they are currently doing.

Awareness can appear synonymously with ‘consciousness’ - *collective experiences within a single individual about a person, situation, item or object* (Marton, 2000). The complexity of awareness detailed by this classification may also beneficial within cybersecurity, in reference to of past and present experiences, perceptions, tasks and roles. Humans are capable of holding multiple experiences within awareness, and in relation to the same thing. It is not as simple as being either ‘aware’ or unaware’ of something. Some experiences of awareness may be directly related to an object in question; and others to the way it is situated within the physical world; spatially or temporally (Marton, 2000). For example, a cyber-attack can be related to the physical being of a human hacker, or more generally the online environment where it exists. A financially motivated cyber-attack may feel spatially close to a person, as would a physical robbery. Or indeed, more distant due to the nature of cyberspace. Experiences surrounding awareness will differ between individuals, situations, and prior exposure and in relation to the past, present, and beliefs about the future (Marton, 2000).

Psychological ownership, whilst significantly related to reported behavior within both Studies 1 and 2, and a latent variable in the EFA, did not add to the predictive power of the regression model. It could be that as a factor, it is important due to a moderating effect only, much in the same way as self-efficacy (Verkijika, 2020). It is important that future research continues to explore how psychological ownership fits with employee intentions and how interventions to increase it may impact cybersecurity perceptions and in turn behavior.

Taken together, the findings suggest that safer cybersecurity behavior is more likely to occur if cybersecurity awareness is high. To achieve this, organisations should strive to: ensure positive past experiences exist to develop a sense of involvement in and a good attitude towards cybersecurity; that security awareness is current; that employees perceive policy to be usable, and, that perceptions around future risk are realistic, with employees that feel able to counter those risks as and when required. Together, these factors form a new *Employee Cybersecurity Awareness Framework* (ECAF) – illustrated within Figure 2

Figure 2.
The Employee Cybersecurity Awareness Framework (ECAF)



Organisational interventions should target the six key themes within the ECAF. For example, threat appraisal could potentially be increased by providing employees with regular updates on cyber-attacks experienced within an organisation and outside of it, to ensure they have a realistic understanding of the likely probability and severity of a successful attack. Study 3 will widen the participant sample further. A key aim is to verify findings of the regression model in Study 2 and provide additional support for the ECAF. A fuller description of the ECAF is detailed in the General Discussion based on the findings from all three studies.

8. Study 3

The main aim of Study 3 was to provide further support for our proposed ECAF amongst a larger and more general employed population. It was predicted that the regression analysis findings of Study 2 would be replicated in full. Also, that the latent Cybersecurity Awareness factor identified in Study 2 would also significantly predict reported cybersecurity behavior. In the interest of brevity, these are the main findings considered.

8.1. Method

Three-hundred and twenty-six employed participants were recruited via *Prolific* from multiple organisations. Forty-four percent were male, 55% female, and 0.5% of a different identity with 0.5% declining to answer. Average age was 34.72 (*SD* 11.16) and all were well educated (71% with an undergraduate degree / higher qualification). All other aspects of the method were the same as in Study 2.

8.2. Results

For reliability, a test of internal consistency was applied to the human-centric cybersecurity framework identified within Study 2, with Cronbach's Alpha reaching excellent within the 'cybersecurity awareness' construct ($\alpha = .91$). The key assumptions for parametric testing were not met due to the use of ordinal data, and therefore non-parametric statistical tests were utilised. Assumptions for all statistical tests used were analysed and met. As in Study 1 and 2, any missing observations were replaced with the grand mean for each question and outliers determined by 3 IQR points from the mean were windsorized to the next available value not considered extreme.

Cybersecurity Behavior

Cybersecurity behavior had a median score across participants of six (IQR = 2). Thus, the sample moderately agreed that their cybersecurity behavior is conscious and favourable.

Regression Analyses

Whilst a stepwise approach was used in Study 2 as no precedent was available to determine how factors should be entered, an enter mode was used in Study 3 as cybersecurity awareness

(Mdn = 6, IQR = 1) was the only factor under investigation. The Study 2 model was verified within Study 3 (F (1, 324) = 489.29, $p < .001$), explaining 60% of the variance ($R^2 = .60$).

8.3. Study 3 Discussion

The main aim of Study 3 was to further validate Study 1 and 2 findings, by investigating factors both related to, and predictive of reported cyber-security behavior, across a larger working sample than in these previous studies. It was key to assess and confirm that those individual differences highlighted as predictive of cybersecurity behavior in Studies 1 and 2 are those most likely to be useful in measuring employee risk within organisations. Also key was to validate the Employee Cybersecurity Awareness Framework (ECAF) such that that organisations can better measure and manage human vulnerabilities in cybersecurity, and develop interventions tailored to these vulnerabilities. By providing organisations with an insight into how employees across a range of organisations are experiencing cybersecurity, time and budget can be more optimally allocated with the goal of improving behavior.

It was predicted that the cybersecurity awareness latent factor, identified via EFA and confirmed by a regression analysis within Study 2, would significantly predict reported cybersecurity behavior in Study 3. This was confirmed, with cybersecurity awareness significantly predicting 60% of behavior. This gives us more confidence in our novel overarching framework. The observed factors include threat appraisal, information security experience and involvement, information security self-efficacy, information security attitude, information security awareness and information security organisation policy (Figure 2).

Jeong et al. (2019) analysed twenty-seven papers that had identified factors, models or frameworks of particular importance for an improved understanding of human factors in cyber security. Of these, only three focussed on information security awareness (two with data collection). Metalidou et al. (2014) considered facilitating (or indeed inhibiting) factors such as motivation, beliefs and use of technology. McCormac et al. (2017), rather than specifically measuring cybersecurity awareness, explored personality traits and risk propensity in cybersecurity knowledge, attitude and behavior. In describing awareness, both emphasise the importance of factors such as knowledge of policy, attitudes towards cybersecurity, and behavior motivation. Whilst the ECAF considers similar constructs such as policy and motivation in terms of threat appraisal and attitude: it goes further in highlighting other key factors such as employee security self-efficacy and experience.

Whilst others have proposed cybersecurity awareness frameworks (e.g. Khader et al., 2021; Wang et al., 2018), they tend to focus on the generation of a process for deployment of a cybersecurity awareness tool, rather than a predictive model. Hijji and Alam (2022) developed the Cybersecurity Awareness and Training framework (CAT) for raising awareness via a specific training schedule across a number of different cybersecurity topics (e.g. cybersecurity basics, social engineering). Another framework developed by Bada et al. (2019) assesses the capabilities and maturity of a cybersecurity awareness programme. Both refer to cybersecurity awareness as a form of training intervention rather than an employee state of mind. The ECAF is novel in that it can be used to measure employee perceptions of their experience in cybersecurity and how this influences cybersecurity awareness. It pulls together aspects of behavior change theory that can indicate how to help move employees towards a more enlightened level of awareness and therefore more secure behaviors.

To summarize, Study 3 confirmed the regression findings from Study 2 – in particular cybersecurity awareness as a latent factor significantly influencing how employees choose to act in the context of cybersecurity behavior. Cybersecurity awareness is a construct that encapsulates how employees perceive threat and their ability to protect themselves and their organisation, as well as attitude towards cybersecurity. It is based on previous experience of and involvement in cybersecurity matters, knowledge of how to remain up-to-date and perceptions of cybersecurity policy usability. The finding of a principal cybersecurity awareness factor, explaining 60% of reported behavior, will be invaluable for organisations. The ECAF and measurement tool can be used by them to better understand how employees are experiencing cybersecurity, associated vulnerabilities, and where to focus intervention.

9. General Discussion

Three studies were conducted to investigate individual differences that best explain employee vulnerability to engaging in risky cybersecurity behaviors. The motivation was to develop a tool and framework for organisations to use in the measurement, management and mitigation of employee susceptibility to cybersecurity risk. Study 1 involved exploration of previously reported end-user demographics and individual differences that have been found (not always consistently) to relate to risky cybersecurity behavior. This is the first time these constructs have been investigated collectively, in one study. Study 2 involved a more refined version of the tool used in Study 1, focussing on significant correlating factors and with larger sample of employees from the same organisation. Regressions were conducted based on a refined EFA model – that uncovered one of two latent factors: *Cybersecurity Awareness* - accounting for 55% of the variance in reported behavior. (Psychological Ownership was a latent factor but did not improve the regression model). Study 3 offered further validation with an even larger sample of employees from multiple organisations, confirming the Cybersecurity Awareness latent variable to be predictive of behavior, accounting for 60% of the variance.

The key outcome is the Employee Cybersecurity Assessment Framework (ECAF) that can be used by organisations to better measure employee risky cybersecurity behaviors and inform intervention. Six observed factors underpin the ECAF: threat appraisal, information security self-efficacy, information security awareness, information security attitude, information security operation policy, and information security experience and involvement.

Threat appraisal refers to how an employee perceives probability and potential severity of a cyber-attack, with higher probability and severity resulting in more conscious behavior (McGill and Thompson, 2017). It is an important factor in most behavior change theories, with regular attempts to manipulate through e.g. fear appeals. It is informed by the availability bias, and can assist quick calculations of risk probability based on the number of instances of an event held in memory resulting in how probability is calculated and therefore motivation to act (Taylor-Gooby & Zinn, 2006; Tversky & Kahneman, 1973). Should an organisation identify threat appraisal as low amongst employees (e.g. via the ECAF), they can improve it through regular and salient updates on recent cyber-incidents.

There are however concerns with threat appraisal persuasion. Giving employees additional details of security incidents will add cognitive strain and may induce anxiety. Employees may try and avoid information relating to negative events. It is perhaps more practical and ethical to use subtle primes, such as vibrations via a smart device. Smart nudges delivered through biotechnology can be useful for cybersecurity awareness generally, by providing reminders, updates and more - in real-time; promoting quick behavior adaptation (Mele, 2021).

Information Security Self-efficacy refers to skills and capabilities a person believes are required to bring about a course of action, and whether they perceive themselves as capable in deploying them (Maddux & Gosselin, 2012). We ordinarily judge ability in two ways: by improvements in self-ability (self-referenced), and, in relation to the ability of others (other referenced), with the latter believed to be the most useful (Nicholls 1984). Higher self-efficacy can be achieved through e.g. self-mastery of a skill, praising achievement of the skill by peers, and affective physical feedback (Maddux & Gosselin, 2012; Ryan & Deci, 2020).

Self-efficacy, amongst other factors within the ECAF (e.g. information security experience and involvement) can be improved through gamification e.g. with application of points and awards to encourage engagement and increase self-efficacy (e.g. van Steen & Deeleman, 2021). Serious games (e.g. games for education) allow employees to practice identifying cyber threats until the desired behaviors become automatic (e.g. Troja, 2023).

Information security awareness denotes employees perceptions on their ability to remain informed on current risks and how to provide protection. High information security awareness can occur through a knowledge sharing culture and cross-company collaboration (Safa et al., 2015; Zwilling et al., 2022). Deployment of a collaborative virtual community could assist with constructing, comparing and sharing knowledge (De Laat, 2023), and can successful due to the power of social dynamics. Carley (2020) discusses the importance of applying the same processes to benefit cybersecurity. Online communities can also be used to increase threat appraisal, improve perceptions of involvement, and help better shape policy. However, issues include policing content in relation to negative (including mis-) information (Altman et al., 2019; Kretschmer et al., 2022; Nickerson et al., 2017).

Information security experience and involvement acknowledges the importance of perceptions of interactions with cybersecurity in the past, and how such experiences influence how employees choose to interact with cybersecurity (Safa et al., 2015). If they do not feel they have previously been involved in cybersecurity or that involvement was negative, they are unlikely to see value in future interactions. By involving employees in the creation and adaptation of cybersecurity policy, the IKEA effect can occur with them placing higher value on things they have spent time helping to shape (Franke et al., 2010; Norton et al., 2012).

Information security attitude is the way in which an employee has evaluated cybersecurity, based on feelings, beliefs and emotions towards it. Attitudes help guide behavior and simplify reasoning on how to act (Maio & Haddock, 2007). It is crucial that employees have a positive attitude towards cybersecurity and why it is needed. Attitudes can be implicit or explicit and are difficult to change due to humans constantly searching for confirmatory information and feeling uncomfortable when considering a belief that differs from one they hold (Bohner & Dickel, 2011). Persuasion can encourage attitude change, either negatively as found within many phishing email studies or more positively with debiasing (Bada et al., 2019). It is perhaps again a social aspect that will support the largest change in cybersecurity attitude, with people feeling more connected to others when they hold the same view towards a behavior (Albarracin & Shavitt, 2018). A supportive community that fosters positive discourse in relation to cybersecurity could have a large impact on cybersecurity attitude.

Information Security Operation Policy relates to perceptions of policies that organisations create to inform employees about behaviors required to protect information from cyber-attacks. Though policy can result in a ‘them versus us’ attitude, with employees adapting them to fit their own agendas (Ashenden and Sasse, 2013; Hedstrom et al., 2011; Lin and Wittmer, 2017). By including employees in the generation and tailoring of company policy, feelings of empowerment will develop leading to higher value in their content. Collaborative virtual communities can be useful in collating employee feedback on the usability of policy, for example, helping to understand where security workarounds are occurring. Sentiment analysis, the use of natural language processing to identify affective states on a topic, can be used to highlight quickly from the collaborative text and inform positive intervention.

These six factors and underlying heuristics can help provide guidance around where employee cybersecurity awareness may need support. By measuring cybersecurity awareness utilising the ECAF, organisations can improve understanding around employee vulnerability to cyber-attacks. This can inform interventions to improve behavior by reducing risks.

9.1. Limitations and Future Directions

The early studies took place during the covid-19 pandemic. Online testing with self-report measures were used given the circumstances, and can be prone to subjective interpretation and response. Despite 55-60% of the variance in reported cybersecurity behavior explained, future studies should couple these measures with objective tests where possible. Linked to this limitation was the relatively small sample size in Study 1, largely due to participants having to work differently and having less opportunity to take part in research studies. The data was collected from participants within the UK only and we must be cautious about over-generalising findings to other countries and cultures (see also e.g. Marcinkiewicz, Wallbridge, Zhang, & Morgan, 2022). In terms of measure specific limitations, Alhalafi and Veeraraghavan (2023) have begun to conceptualise a cybersecurity UTAUT based model to include the concepts of safety, resiliency, availability, confidentiality and integrity, with positive results. This should be considered in future studies.

10. Conclusion

With people continually regarded as the weakest link in cyber security, falling victim to progressively refined cyber-attack methods, it is paramount that we better understand vulnerability factors that lead to risky cyber security behaviors. Only then can we optimize interventions, including those developed to equip employees to less susceptible to exhibiting such behaviors. Findings from three studies involving a battery of established questionnaires and other measures tested amongst students and university staff (Study 1), and then further refined and tested on employees of a large multinational organization (Study 2) and after exploratory factor analysis again with employees of a multiple organizations (Study 3) led to the development a new tool – the Employee Cybersecurity Awareness Framework (ECAF). The ECAF can account for 60% of the variance in data with cybersecurity awareness at its core and six underlying factors: threat appraisal, information security self-efficacy, information security awareness, information security attitude, information security operation policy and cybersecurity experience and involvement. The ECAF is a powerful predictive tool that can be utilized organisations to optimally measure employee cybersecurity risk factors and determine interventions tailored to risk profiles.

References

Agha, S., Tollefson, D., Paul, S., Green, D., & Babigumira, J. B. (2019). Use of the Fogg behavior model to assess the impact of a social marketing campaign on condom use in Pakistan. *Journal of Health Communication, 24(3),* 284-292.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organızational Behavior And Human Decision Processes, 50,* 179-211.

Ajzen, I., & Fishbein, M. (1975). A Bayesian analysis of attribution processes. *Psychological Bulletin*, *82*(2), 261.

Alhalafi, N., & Veeraraghavan, P. (2023). Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. *Smart Cities*, *6*(3), 1523-1544.

Alrawi, M. A. S., Samy, G. N., Yusoff, R. C. M., Shanmugam, B., Lakshmiganthan, R., Maarop, N., & Kamaruddin, N. (2020). Examining factors that effect on the acceptance of mobile commerce in Malaysia based on revised UTAUT. *Indonesian Journal of Electrical Engineering and Computer Science*, *20*(3), 1173-1184.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations. *Proceedings of the 51st Hawaii International Conference on System Sciences*.

Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S. B. (2019). Toward sustainable behavior change: an approach for cyber security education training and awareness. *European Conference on Information Systems.*

Altman, E. J., Nagle, F., & Tushman, M. (2021). The Translucent Hand of Managed Ecosystems: Engaging Communities for Value Creation and Capture. *Harvard Business School Strategy Unit Working Paper,* (19-096), 19-096.

Amah, E., & Ahiauzu, A. (2013). Employee involvement and organizational effectiveness. *Journal of Management Development*, *32*(7), 661-674.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437-443.

Ariffin, N. H. M., Ahmad, F., & Haneef, U. M. (2020). Acceptance of mobile payments by retailers using UTAUT model. *Indonesian Journal of Electrical Engineering and Computer Science*, *19*(1), 149-155.

Arkes, H. R. (1991). Costs and benefits of judgment errors: Implications for debiasing. *Psychological Bulletin*, *110*(3), 486.

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy?. *Computers & Security*, *39*, 396-405.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, *37*(2), 122.

Baxter, W. L., Aurisicchio, M., & Childs, P. R. (2015). A psychological ownership approach to designing object attachment. *Journal of Engineering Design*, *26*(4-6), 140-156.

Bion, W. R. (2021). *Learning from experience*. Routledge.

Bishop, L. M. (2024). *The Employee Experience in Cybersecurity and How to Mitigate Risk*. Unpublished Doctoral Thesis. Cardiff University, UK.

Blais, A. R., & Weber, E. U. (2006). A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision making*, *1*(1), 33-47.

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotton, S. (2015). Determinants of online safety behavior: Towards an intervention strategy for college students. *Behavior Information Technology, 34(10)*, 1022-1035.

Bohner, G., & Dickel, N. (2011). Attitudes and attitude change. *Annual Review of Psychology*, *62*, 391-417.

Bottemanne, H., Morlaàs, O., Fossati, P., & Schmidt, L. (2020). Does the coronavirus epidemic take advantage of human optimism bias?. *Frontiers in Psychology*, *11*.

Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring Age and Gender Differences in ICT Cybersecurity Behavior. *Human Behavior and Emerging Technologies*, *2022*.

Brasel, S. A., & Gips, J. (2014). Tablets, touchscreens, and touchpads: How varying touch interfaces trigger psychological ownership and endowment. *Journal of Consumer Psychology, 24(2)*, 226-233.

Briggs, P., Jeske, D., & Coventry, L. (2017). Behavior change interventions for cybersecurity. In *Behavior Change Research and Theory* (pp. 115-136). Academic Press.

Brock, T. C. (1968). Implications of commodity theory for value change. In *Psychological Foundations of Attitudes* (pp. 243-275). Academic Press.

Burn, S. M. (2017). Appeal to bystander interventions: A normative approach to health and risk messaging. In *Oxford Research Encyclopedia of Communication*.

Burns, S., & Roberts, L. (2013). Applying the theory of planned behavior to predicting online safety behavior. *Crime Prevention and Community Safety*, *15*, 48-64.

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *arXiv preprint arXiv:1606.00887*.

Carley, K. M. (2020). Social cybersecurity: an emerging science. *Computational and Mathematical Organization Theory, 26(4),* 365-381.

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, *44*.

Carr, D. (1979). The logic of knowing how and ability. *Mind*, *88(351)*, 394-409.

Carroll, J. S. (1978). The effect of imagining an event on expectations for the event: An interpretation in terms of the availability heuristic. *Journal of Experimental Social Psychology*, *14*(1), 88-96.

Cavanagh, G. F., Moberg, D. J., & Velasquez, M. (1981). The ethics of organizational politics. *Academy of Management Review*, *6(3)*, 363-374.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review*, *50*, 100592.

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International Journal of Security and its Applications*, *10*(1), 247-256.

Chen, H., Turel, O., & Yuan, Y. (2022). E-waste information security protection motivation: the role of optimism bias. *Information Technology & People, 35*(2), 600-620.

Chenoweth, T., Minch, R., & Tabor, S. (2007). Expanding views of technology acceptance: seeking factors explaining security control adoption. *AMCIS 2007 Proceedings*, 321.

Cismaru, M., Nagpal, A., & Krishnamurthy, P. (2009). The role of cost and response-efficacy in persuasiveness of health recommendations. *Journal of Health Psychology*, *14*(1), 135-141.

Conetta, C. (2019). Individual differences in cyber security. *McNair Research Journal SJSU*, *15(1)*, Article 4.

Conner, M., & Armitage, C. J. (1998). Extending the theory of planned behavior: A review and avenues for further research. *Journal of Applied Social Psychology*, *28*(15), 1429-1464.

Corradini, I. (2020). *Building a Cybersecurity Culture in Organizations* (Vol. 284). Berlin/Heidelberg, Germany: Springer International Publishing.

Cox, A., Zagelmeyer, S., & Marchington, M. (2006). Embedding employee involvement and participation at work. *Human Resource Management Journal*, *16*(3), 250-267.

Croskerry, P., Singhal, G., & Mamede, S. (2013). Cognitive debiasing 1: origins of bias and theory of debiasing. *BMJ Quality & Safety*, *22*(Suppl 2), ii58-ii64.

Cutello, C. A., Walsh, C., Hanoch, Y., & Hellier, E. (2021). Reducing optimism bias in the driver's seat: Comparing two interventions. *Transportation Research Part F: Traffic Psychology and Behaviour*, *78*, 207-217.

Davis, F. D. (1985). A technology acceptance model for empirically testing new end-user information systems: theory and results. *Unpublished Doctoral Thesis*. Cambridge, MA.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-340.

De Laat, M. (2023). Network and content analysis in an online community discourse. *In Computer Support for Collaborative Learning* (pp. 625-626). Routledge.

Dupuis, M., & Renaud, K. (2021). Scoping the ethical principles of cybersecurity fear appeals. *Ethics and Information Technology, 23*(3), 265-284.

Dwivedi, Y. K., Rana, N. P., Chen, H., & Williams, M. D. (2011). A Meta-analysis of the Unified Theory of Acceptance and Use of Technology (UTAUT). In *Governance and Sustainability in Information Systems. Managing the Transfer and Diffusion of IT: IFIP WG 8.6 International Working Conference, Hamburg, Germany, September 22-24, 2011. Proceedings* (pp. 155-170). Springer Berlin Heidelberg.

Egelman, S., & Peer, E. (2015, April). Scaling the security wall: Developing a security behavior intentions scale (SEBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2873-2882).

Elliot, A. J., & McGregor, H. A. (2001). A 2× 2 achievement goal framework. *Journal of Personality and Social Psychology, 80*(3), 501.

Elliot, A. J., Murayama, K., & Pekrun, R. (2011). A 3× 2 achievement goal model. *Journal of Educational Psychology, 103*(3), 632.

Ertan, A., Crossland, G., Heath, C., Denny, D., & Jensen, R. (2020). Cyber security behavior in organisations. *arXiv preprint arXiv:2004.*11768.

Fei, Z., Kassim, N. M., & Mohamad, W. N. (2022). Factors influencing the adoption of IoT based mobile health services in China: A conceptual framework. *Global Business and Management Research, 14(3s),* 1094-1104.

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.

Fogg, B. J. (2009). A behavior model for persuasive design. In *Proceedings of the 4th international Conference on Persuasive Technology* (pp. 1-7).

Franke, N., & Schreier, M. (2010). Why customers value self-designed products: The importance of process effort and enjoyment. *Journal of Product Innovation Management*, *27*(7), 1020-1031.

Friedman, B., Khan Jr, P. H., & Howe, D. C. (2000). Trust online. *Communications of the ACM*, *43*(12), 34-40.

Furnell, S. M., Alotaibi, F., & Esmael, R. (2019). Aligning security practice with policy: Guiding and nudging towards better behavior. Retrieved from: https://pearl.plymouth.ac.uk/bitstream/handle/10026.1/12764/Paper%202452%20-%20Final.pdf?sequence=1

Gafoor, K. A. (2012). Considerations in the Measurement of Awareness. *National Seminar on Emerging trends in education, Department of Education, University of Calicut.*

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Analytics*, *1*(1), 1-29.

Goldberg, L. R., Johnson, J. A., Eber, H. W., Hogan, R., Ashton, M. C., Cloninger, C. R., & Gough, H. G. (2006). The international personality item pool and the future of public-domain personality measures. *Journal of Research in Personality*, *40*(1), 84-96.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345-358.

Greitzer, F. L., Imran, M., Purl, J., Axelrad, E. T., Leong, Y. M., Becker, D. E., ... & Sticha, P. J. (2016). Developing an Ontology for Individual and Organizational Sociotechnical Indicators of Insider Threat Risk. *In STIDS* (pp. 19-27).

Gupta, M. (2015). A study on employees perception towards employee engagement. *Globsyn Management Journal*, *9*(1/2), 45-51.

Hadlington, L. (2017). Human factors in cybersecurity: examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon, 3(7),* e00346.

Hadlington, L. J. (2018). Employees attitudes towards cyber security and risky online behaviors: an empirical assessment in the United Kingdom. *International Journal of Cyber Criminology*, *12(1)*, 269-281.

Hassandoust, F., & Techatassanasoontorn, A. A. (2020). Understanding users' information security awareness and intentions: A full nomology of protection motivation theory. In *Cyber influence and cognitive threats* (pp. 129-143). Academic Press.

Heckhausen, J. E., & Heckhausen, H. E. (2008). *Motivation and action*. Cambridge University Press.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, *20*(4), 373-384.

Herrnstein, R. J. (1969). Method and theory in the study of avoidance. *Psychological Review, 76*(1), 49–69.

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) framework for remote working employees. *Sensors*, *22*, 8663.

Hodas, N. O., & Lerman, K. (2014). The simple rules of social contagion. *Scientific Reports*, *4*(1), 4343.

Hsieh, H. L., Kuo, Y. M., Wang, S. R., Chuang, B. K., & Tsai, C. H. (2017). A study of personal health record user's behavioral model based on the PMT and UTAUT integrative perspective. *International Journal of Environmental Research and Public Health, 14(1),* 8.

Hudson, J. M., & Bruckman, A. S. (2004). The bystander effect: A lens for understanding patterns of participation. *The Journal of the Learning Sciences*, *13*(2), 165-195.

Ivanova, A., & Kim, J. Y. (2022). Acceptance and use of mobile banking in Central Asia: Evidence from modified UTAUT model. *The Journal of Asian Finance, Economics and Business*, *9*(2), 217-227.

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)* (pp. 338-345). IEEE.

Jeske, D., Coventry, L., Briggs, P., & van Moorsel, A. (2014). Nudging whom how: Nudging whom how: IT proficiency, impulse control and secure behavior. *In: Personalizing Behavior Change Technologies.* CHI Workshop, 27 April.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly,* 549-566.

Jolls, C., & Sunstein, C. R. (2006). Debiasing through law. *The Journal of Legal Studies*, *35*(1), 199-242.

Jones, K. S., Lodinger, N. R., Widlus, B. P., Namin, A. S., & Hewett, R. (2021). Do warning message design recommendations address why non-experts do not protect themselves from cybersecurity threats? a review. *International Journal of Human–Computer Interaction*, *37*(18), 1709-1719.

Khan, N., J. Houghton, R. & Sharples, S. (2022). Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks. *Cognition, Technology & Work, 24,* 393–421.

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

Kahneman, D. (2003). A perspective on judgment and choice: mapping bounded rationality. *American Psychologist*, *58*(9), 697.

Kahneman, D. (2011). *Thinking, Fast and Slow*. Macmillan.

Karim, N. H. A., & Noor, M. N. H. N. M. (2013). Investigating the correlate and predictors of affective and continuance organisational commitment among Malaysian academic librarians. *Malaysian Journal of Library & Information Science, 13(2).*

Keller, C., Siegrist, M., & Gutscher, H. (2006). The role of the affect and availability heuristics in risk communication. *Risk Analysis*, *26*(3), 631-639.

Keller, P. A. (2006). Regulatory focus and efficacy of health messages. *Journal of Consumer Research, 33*(1), 109-114.

Kessler, S. K., & Martin, M. (2017). How do potential users perceive the adoption of new technologies within the field of AI and Internet-of-Things? A revision of the UTAUT 2 model using voice assistants. *Unpublished Masters Thesis.* Lund University.

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information, 12(10),* 417.

Kirk, C. P., & Swain, S. D. (2018). Consumer psychological ownership of digital technology. *Psychological Ownership and Consumer Behavior*, 69-90.

Kirlappos, I. (2016). Learning from shadow security: understanding non-compliant behaviors to improve information security management. *Unpublished PhD Thesis.* UCL.

Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). Shadow security as a tool for the learning organization. *Acm Sigcas Computers and Society*, *45*(1), 29-37.

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from Shadow Security: Why understanding non-compliance provides the basis for effective security. *In. Proceedings of the Workshop on Usable Security.*

Kolb, D. A. (2014). *Experiential Learning: Experience as the Source of Learning and Development*. FT Press.

Kretschmer, M., Furgal, U., & Schlesinger, P. (2022). The emergence of platform regulation in the UK: an empirical-legal study. *Weizenbaum Journal of the Digital Society–special issue: Democracy in Flux–Order, Dynamics and Voices in Digital Public Spheres.*

Krupić, D., Žuro, B., & Corr, P. J. (2021). Anxiety and threat magnification in subjective and physiological responses of fear of heights induced by virtual reality. *Personality and Individual Differences, 169,* 109720.

Kshetri, N., & Chhetri, M. (2022). Gender asymmetry in cybersecurity: socioeconomic causes and consequences. *Computer*, *55*(2), 72-77.

Kuraku, S. (2022). Kuraku, S. (2022). Curiosity Clicks: The Need for Security Awareness (Doctoral dissertation, University of the Cumberlands).

Lee, S., Atkinson, L., & Sung, Y. H. (2022). Online bandwagon effects: Quantitative versus qualitative cues in online comments sections. *New Media & Society*, *24*(3), 580-599.

Lee, Y., & Chen, A. N. (2011). Usability design and psychological ownership of a virtual world. *Journal of Management Information Systems*, *28*(3), 269-308.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 71-90.

Liang, N.P., Biros, D.P., & Luse, A. (2016). Taxonomy of Malicious Insiders: A Proof of Concept Study. *Americas Conference on Information Systems.*

Loewenstein, G., & Lerner, J. S. (2002). The role of affect in decision making. In Richard J Davidson, Klaus R Scherer, and H Hill Goldsmith (eds), *Handbook of Affective Sciences*. NY: Oxford Academic.

Loske, A., Widjaja, T., & Buxmann, P. (2013). Cloud computing providers' unrealistic optimism regarding IT security risks: A threat to users?. *Thirty Fourth International Conference on Information Systems, Milan 2013*.

Lowry, P. B., Moody, G. D., Parameswaran, S., & Brown, N. (2023). Examining the differential effectiveness of fear appeals in information security management using two-stage meta-analysis. *Journal of Management Information Systems.*

Maddux, J. E., & Gosselin, J. T. (2012). *Self-efficacy*. The Guilford Press.

Maio, G. R., & Haddock, G. (2007). Attitude change. *Social Psychology: Handbook of Basic Principles*, 565-586. London: Sage.

Mamra, A., Sibghatullah, A. S., Ananta, G. P., Alazzam, M. B., Ahmed, Y. H., & Doheir, M. (2017). A proposed framework to investigate the user acceptance of personal health records in Malaysia using UTAUT2 and PMT. *International Journal of Advanced Computer Science and Applications, 8(3).*

Maranguníć, N., & Granić, A. (2015). Technology acceptance model: a literature review from 1986 to 2013. *Universal Access in the Information Society*, *14*, 81-95.

Marcinkiewicz, V., Wallbridge, C. D., Zhang, Q., & Morgan, P. L. (2022). Integrating humanoid robots into simulation software generated animations to explore judgments on self-driving car Accidents. *Presented at: IEEE Ro-Man 2022 Conference – Trust, Acceptance and Social Cues in Human-Robot Interaction (SCRITA)*, Naples, Italy, 29 August - 2 September 2022.

Markey, R., & Townsend, K. (2013). Contemporary trends in employee involvement and participation. *Journal of Industrial Relations*, *55*(4), 475-487.

Marton, F. (2000). The structure of awareness. *Phenomenography*, *10216*, 102-116.

Matsunaga, M. (2010). How to factor-analyze your data right: do's, don'ts, and how-to's. *International Journal of Psychological Research, 3(1),* 97-110.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156.

McGill, T., & Thompson, N. (2017). Old risks, new challenges: exploring differences in security between home computer and mobile device use. *Behavior & Information Technology*, *36*(11), 1111-1124.

Mele, C., Spena, T. R., Kaartemo, V., & Marzullo, M. L. (2021). Smart nudging: How cognitive technologies enable choice architectures for value co-creation. *Journal of Business Research*, *129*, 949-960.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences, 147,* 424-428.

Meyer, J. P., & Allen, N. J. (1991). A three-component conceptualization of organizational commitment. *Human Resource Management Review*, *1*(1), 61-89.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106-143.

Morrison, B., Coventry, L., & Briggs, P. (2021). How do older adults feel about engaging with cyber-security?. *Human Behavior and Emerging Technologies*, *3*(5), 1033-1049.

Moschovitis, C. (2019). Why do cyber security programmes fail?. *Cyber Security: A Peer-Reviewed Journal*, *2*(4), 303-309.

Mowrer, O. H. (1939). A stimulus-response analysis of anxiety and its role as a reinforcing agent. *Psychological Review*, *46*(6), 553-565.

Naqshbandi, M. M., Tabche, I., & Choudhary, N. (2019). Managing open innovation: The roles of empowering leadership and employee involvement climate. *Management Decision*, *57*(3), 703-723.

Nicholls, J. G. (1984). Achievement motivation: conceptions of ability, subjective experience, task choice, and performance. *Psychological Review*, *91*(3), 328.

Nichols, T. W., & Erakovich, R. (2013). Authentic leadership and implicit theory: a normative form of leadership?. *Leadership & Organization Development Journal*.

Nickerson, J. A., Wuebker, R., & Zenger, T. (2017). Problems, theories, and governing the crowd. *Strategic Organization*, *15(2),* 275–288

Nickols, F. (2000). The knowledge in knowledge management. *The Knowledge Management Yearbook, 2000–2001*, 12, 21.

Nisbet, E., & Weiss, R. (2010). Top-down versus bottom-up. *Science*, *328(5983)*, 1241-1243.

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A Human Factors problem. *HOLISTICA–Journal of Business and Public Administration*, *13*(1), 49-72.

Norton, M. I., Mochon, D., & Ariely, D. (2012). The IKEA effect: When labor leads to love. *Journal of Consumer Psychology*, *22*(3), 453-460.

Obiekwe, O., Zeb-Obipi, I., & Ejo-Orusa, H. (2019). Employee involvement in organizations: benefits, challenges and implications. *Management and Human Resource Research Journal*, *8*, 1-11.

Oh, J. C., & Yoon, S. J. (2014). Predicting the use of online information services based on a modified UTAUT model. *Behavior & Information Technology*, *33*(7), 716-729.

Osborne, S., & Hammoud, M. S. (2017). Effective employee engagement in the workplace. *International Journal of Applied Management and Technology*, *16*(1), 4.

Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). A personality based model for determining susceptibility to phishing attacks. *Little Rock: Uni of Arkansas*, 285-296.

Patterson, J. (2017). Cyber-security policy decisions in small businesses. *Unpublished Doctoral Thesis*. Walden University.

Peck, J., Kirk, C. P., Luangrath, A. W., & Shu, S. B. (2021). Caring for the commons: Using psychological ownership to enhance stewardship behavior for public goods. *Journal of Marketing*, *85*(2), 33-49.

Petty, R. E., Cacioppo, J. T., Petty, R. E., & Cacioppo, J. T. (1986). *The elaboration likelihood model of persuasion* (pp. 1-24). Springer New York.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597-611.

Pickens, J. (2005). Attitudes and perceptions. *Organizational Behavior in Healthcare*, *4*(7), 43-76.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214.

Proctor, R. W., & Chen, J. (2015). The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. *Human Factors*, *57*(5), 721-727.

Raafat, R. M., Chater, N., & Frith, C. (2009). Herding in humans. *Trends in Cognitive Sciences*, *13*(10), 420-428.

Raddatz, N. I., Coyne, J. G., & Trinkle, B. S. (2020). Internal motivators for the protection of organizational data. *Journal of Information Systems, 34(3),* 199-211.

Rahi, S., Khan, M. M., & Alghizzawi, M. (2021). Factors influencing the adoption of telemedicine health services during COVID-19 pandemic crisis: an integrative research model. *Enterprise Information Systems, 15(6)*, 769-793.

Raineri, E. M., & Resig, J. (2020). Evaluating self-efficacy pertaining to cybersecurity for small businesses. *Journal of Applied Business & Economics, 22(12).*

Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. In *29th European Safety and Reliability Conference.* 4036-4043.

Renaud, K., Otondo, R., & Warkentin, M. (2019). “This is the way ‘I’ create my passwords”... does the endowment effect deter people from changing the way they create their passwords? *Computers & Security*, *82*, 241-260.

Renaud, K., Searle, R., & Dupuis, M. (2021, October). Shame in cyber security: effective behavior modification tool or counterproductive foil? In *New Security Paradigms Workshop* (pp. 70-87).

Roberts, B. W., Lejuez, C., Krueger, R. F., Richards, J. M., & Hill, P. L. (2014). What is conscientiousness and how can it be assessed?. *Developmental Psychology*, *50*(5), 1315.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93-114.

Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health Education Monographs*, *2*(4), 328-335.

Rosenstock. (1990). The health belief model: Explaining health behavior through experiences. *Health Behavior & Health Education: Theory, Research and Practice*, 39-63.

Ryan, R. M., & Deci, E. L. (2000). Intrinsic and extrinsic motivations: Classic definitions and new directions. *Contemporary Educational Psychology*, *25*(1), 54-67.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behavior formation in organizations. *Computers & Security*, *53*, 65-78.

Salazar, M., Gaviria, J., Laorden, C., & Bringas, P. G. (2013, March). Enhancing cybersecurity learning through an augmented reality-based serious game. In *2013 IEEE global engineering education conference (EDUCON)* (pp. 602-607). IEEE.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology Journal*, *19*(3), 122-131.

Schenk, D. H. (2011). Exploiting the salience bias in designing taxes. *Yale J. on Reg.*, *28*, 253.

Scherer, C. W., & Cho, H. (2003). A social network contagion theory of risk perception. *Risk Analysis: An International Journal*, *23*(2), 261-267.

Scholl, M. C., Fuhrmann, F., & Scholl, L. R. (2018). Scientific knowledge of the human side of information security as a basis for sustainable trainings in organizational practices. *Proceedings of the 51st Hawaii International Conference on System Sciences.*

Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, *37*(3), 723-757.

Scott, S. G., & Bruce, R. A. (1995). Decision-making style: The development and assessment of a new measure. *Educational and Psychological Measurement*, *55*(5), 818-831.

Shaari, R., Rahman, S. A. A., & Rajab, A. (2014). Self-efficacy as a determined factor for knowledge sharing awareness. *International Journal of Trade, Economics and Finance*, *5*(1), 39.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, 102974.

Shalev, E., Keil, M., Lee, J. S., & Ganzach, Y. (2014). Optimism bias in managing it project risks: a construal level theory perspective. *ECIS 2014 Proceedings.*

Sharot, T. (2011). The optimism bias. *Current Biology*, *21*(23), 941-945.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373-382).

Shillair, R., & Dutton, W. H. (2016). Supporting a cybersecurity mindset: getting internet users into the cat and mouse game. *Available at SSRN 2756736*.

Skinner, T., Taylor, J., Dale, J., & McAlaney, J. (2018, April). The development of intervention e-learning materials and implementation techniques for cyber-security behavior change. *ACM SIG CHI.*

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2007). The affect heuristic. *European Journal of Operational Research*, *177*(3), 1333-1352.

Snyman, D., & Kruger, H. (2021). Group Behavior in Cybersecurity. *Encyclopedia of Cryptography, Security and Privacy*.

Sun, Y., Wang, N., Guo, X., & Peng, Z. (2013). Understanding the acceptance of mobile health services: a comparison and integration of alternative models. *Journal of Electronic Commerce Research, 14(2),* 183.

Taillard, M. O. (2000). Persuasive communication: the case of marketing. *Working Papers in Linguistics, 12,* 145-174.

Tannenbaum, M. B., Hepler, J., Zimmerman, R. S., Saul, L., Jacobs, S., Wilson, K., & Albarracín, D. (2015). Appealing to fear: A meta-analysis of fear appeal effectiveness and theories. *Psychological Bulletin, 141(6),* 1178.

Troja, E., DeBello, J. E., & Truong, L. M. (2023, March). Teaching effective and gamified cybersecurity using the Metaverse: Challenges and opportunities. In *2023 IEEE World Engineering Education Conference (EDUNINE)* (pp. 1-6). IEEE.

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.

Van den Broeck, A., Vansteenkiste, M., De Witte, H., Soenens, B., & Lens, W. (2010). Capturing autonomy, competence, and relatedness at work: Construction and initial validation of the Work-related Basic Need Satisfaction scale. *Journal of Occupational and Organizational Psychology*, *83*(4), 981-1002.

Steen, T. van, & Deeleman, J. R. A. (2021). Successful gamification of cybersecurity training. *Cyberpsychology, Behavior, And Social Networking, 24(9),* 593-598.

Venema, T. A., Kroese, F. M., & De Ridder, D. T. (2018). I’m still standing: A longitudinal study on the effect of a default nudge. *Psychology & Health*, *33*(5), 669-681.

Venkatesh, V. (2022). Adoption and use of AI tools: a research agenda grounded in UTAUT. *Annals of Operations Research*, 1-12.

Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2), 273-315.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425-478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 157-178.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 157-178.

Verizon (2022). 2022 Data Breach Investigations Report. Retrieved from: https://www.verizon.com/business/resources/reports/dbir/

Verizon (2024). 2022 Data Breach Investigations Report. Retrieved from: https://www.verizon.com/business/resources/T19f/reports/2024-dbir-data-breach-investigations-report.pdf

Verkijika, S. F. (2020). Employees' Cybersecurity Behavior in the Mobile Context: The Role of Self-Efficacy and Psychological Ownership. *In. 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC*), 1-5.

Waddell, T. F., & Sundar, S. S. (2020). Bandwagon effects in social television: How audience metrics related to size and opinion affect the enjoyment of digital media. *Computers in Human Behavior, 107,* 106270.

Wang, J. L., Jackson, L. A., Wang, H. Z., & Gaskin, J. (2015). Predicting social networking site (SNS) use: Personality, attitudes, motivation and internet self-efficacy. *Personality and Individual Differences*, *80*, 119-124.

Wang, Y., Qi, B., Zou, H. X., & Li, J. X. (2018). Framework of raising cyber security awareness. *In 2018 IEEE 18th International Conference on Communication Technology (ICCT),* 865-869.

Wanner, J., Herm, L. V., Heinrich, K., & Janiesch, C. (2022). The effect of transparency and trust on intelligent system acceptance: Evidence from a user-based study. *Electronic Markets*, *32*(4), 2079-2102.

Warkentin, M., Xu, Z., & Mutchler, L. A. (2013). *I'm safer than you: the role of optimism bias in personal IT risk assessments*. *In Proceedings of the 2013 Dewald Roode Workshop on Information Systems Security Research,* Niagara Falls, NY.

Watkins, M. W. (2021). *A step-by-step guide to exploratory factor analysis with SPSS.* Routledge.

Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology, 39*(5), 806.

Weinstein, N. D., & Klein, W. M. (1995). Resistance of personal risk perceptions to debiasing interventions. *Health Psychology, 14*(2), 132.

White, M. J., Cunningham, L. C., & Titchener, K. (2011). Young drivers' optimism bias for accident risk and driving skill: Accountability and insight experience manipulations. *Accident Analysis & Prevention, 43*(4), 1309-1315.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 3-7.

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring Susceptibility to Phishing in the Workplace. *International Journal of Human-Computer Studies, 120*, 1-13.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior, 27*(5), 591-615.

Yeoh, W., Huang, H., Lee, W. S., Al Jafari, F., & Mansson, R. (2022). Simulated phishing attack and embedded training campaign. *Journal of Computer Information Systems, 62*(4), 802-821.

Zhao, Q., Chen, C. D., & Wang, J. L. (2016). The effects of psychological ownership and TAM on social media loyalty: An integrated model. *Telematics and Informatics, 33(4),* 959-972.

Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. *Computers in Human Behavior*, *26*(4), 760-767.

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