JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2022, 1–11
https://doi.org/10.1093/cybsec/tyab026
Research paper

Research paper

The impact of a cause–effect elaboration procedure on information security risk perceptions: a construal fit perspective

Zhang Hao Goh [1,*], Minzheng Hou [2] and Hichang Cho [3]

[1]Wee Kim Wee School of Communication and Information, Nanyang Technological University, 31 Nanyang Link, 637718 Singapore, [2]Department of Psychology, Faculty of Arts and Social Sciences, National University of Singapore, 9 Arts Link, Block AS4, Level 2, 117570 Singapore and [3]Department of Communications and New Media, Faculty of Arts & Social Sciences, National University of Singapore, Blk AS6, #03-41, 11 Computing Drive, 117416 Singapore

*Correspondence address. Nanyang Technological University, 31 Nanyang Link, #02-40, Singapore 637718, Singapore. Tel: +65-6904-1240; E-mail: zhanghao.goh@ntu.edu.sg

Author's note: Findings in this paper are part of the first author's doctoral dissertation.

Received 21 April 2021; revised 1 December 2021; accepted 8 December 2021

Abstract

Cybersecurity breaches are on the rise. Extant literature in the development of strategies to enhance IT users' online protective behaviours has neglected users' cognitive processing of cybersecurity risk information. This study demonstrates a cause–effect elaboration procedure based on the concept of construal fit to influence online users' cybersecurity risk perceptions. Using online experiments ($N = 534$), the construal fit between elaboration of causes vs effects of cybersecurity risks and perceived temporal distance (distant vs near) was manipulated. The results revealed that a construal fit between the elaboration of 'effects' (vs 'causes') and temporally 'near' (vs 'distant') cybersecurity risks enhanced users' risk perceptions, which in turn predicted protective behavioural intentions. Ensuring construal fit is a novel, cognition-based approach to safeguard IT users against online threats. Our findings enrich existing staged theories used to investigate cybersecurity risk perceptions and suggest to practitioners that heightened cyber risk perception can effectively be induced by simultaneously enhancing the concreteness of IT users' construal of cybersecurity incidents and emphasizing on its negative consequences (vs causes).

Key words: construal, risk perceptions, cybersecurity, causes vs effects, threat appraisals

Introduction

Cybersecurity breaches have compromised >4 billion records in just the first six months of 2019 [1]. Many criminalistic cyberattacks (such as phishing, malware, password hack, ransomware, scams, and social engineering techniques) are designed to target the weakest link—i.e. humans—identified as the most vulnerable within any digital system [2]. Paradoxically, while the mass public generally express concerns over such cyberthreats, they tend to undermine them and do little to ensure their security online [3]. One reason is diminished risk perception (i.e. low sensitivity) towards cyberthreats [4–7]. Diminished risk perception at the microlevel inadvertently leads to an inadequate engagement in protective online behaviours (e.g. regular updating of anti-virus software) [8], and ultimately, the attenuation of the support for national policies targeting at securing the cyberspace at the macro level [3, 4].

With the expanding threat of cybersecurity breaches [9], the exigency of enhancing IT users' risk perceptions and engagement in protective behaviours is more pronounced than before. Past efforts have largely focused on awareness-based approaches, through campaigns [10] or game-play [11], fear-based approaches [12], cybersecurity-related education and training [13], and more recently, the situational

exposure to cybersecurity incidents (i.e. news stories) to enhance IT users' cybersecurity risk perceptions [3].

Existing cybersecurity studies have acknowledged that the cognitive processes of IT users can influence the way they evaluate and act towards cyberthreats [14], i.e. the mental processes of human beings that involve thinking, assessing/evaluating, imagining, and perceiving [15]. These cognitive processes can sometimes explain why people behave in certain (irrational) ways that they cannot justify (e.g. opening links from a dubious email message) [16]. Indeed, IT users' cognitive processing tendencies, such as optimism bias[1] [17] or cognitive disfluency in perceptions[2] [20], and, more recently, perceived personal relevance biases towards cybersecurity stimuli [3] have been found to influence their evaluation of cyberthreats and to enhance their associated protective behavioural intentions.

The present research introduces a novel approach to enhance IT users' risk perception of cybersecurity incidents by focusing on their construals (i.e. concrete vs abstract construals) about future criminalistic cybersecurity incidents. Human construal process is associated with personal 'experience' of future events vis-à-vis one's present moment [21]. From a construal perspective, personal relevance of the cybersecurity incident to oneself [3] is associated with individuals' concrete construal process [22].

Therefore, by focusing on IT users' construal processes, the present research advances recent developments in cybersecurity literature by demonstrating how construals (i.e. cognitive representations) of cybersecurity incidents can augment IT users' risk perceptions [3]. Situated in construal-level theory (CLT) [23], we develop an elaboration procedure about abstract vs concrete construal (i.e. causes vs effects) of risky cybersecurity incidents to alter individuals' cybersecurity risk perceptions and thereby their intentions to engage in cybersecurity behaviours. Specifically, through experimental methods, we first demonstrated that the elaboration of causes vs effects of cybersecurity incidents evokes abstract vs concrete construals, respectively. With these findings, we showed that verbal elaboration of the effects (vs causes) of cybersecurity incidents effectively heightens IT users' risk perception when they are perceived as temporally proximal (vs distal).

Literature Review

Theoretical framework

Basics of CLT

CLT posits that humans have the capability of experiencing events that are not available in their present moment through their construals [24]. In cognitively representing these events, CLT posits that an individual can form abstract construals or concrete construals [21]. The formation of high-level, schematic, decontextualized mental representations of events constitutes abstract-level construal. In other words, abstract construal contains the gist of information (i.e. superordinate features) of the event. The formation of low-level, incidental, contextualized mental representations of events constitute concrete construal, emphasizing on the subordinate features of the event [23, 24].

Indeed, the utilization of the construal process to augment IT users' evaluative responses towards cyberthreats is not entirely new. There have been some studies that investigate how IT users' risk perception and their cybersecurity behaviours can be enhanced, e.g. through fear appeals in verbal cybersecurity messages [25] or by targeting their construal processes towards safe cyber practices, such as online password use [26].

Predicting and explaining behaviour using CLT

CLT has been applied to wide-ranging contexts and has been demonstrated to be a reliable and viable theoretical framework to explain individuals' behavioural intentions. These studies found that individuals' construal level (either abstract or concrete) plays a role in influencing behavioural intentions or actual behaviours. In other words, thinking concretely or abstractly about a subject matter has different implications on one's behavioural intention or actual behaviour.

For example, in the context of cybersecurity, Kaleta *et al.* [26] found that people who were induced with abstract construal created or intend to choose a stronger password relative to those who were induced to think concretely. This is because abstract construal focuses on the desirability features of the password or the 'why' aspect of having strong password (i.e. prolonged online security benefits), compared with concrete construal that focuses on the 'how' (feasibility) aspect of password management—the latter is associated with using a weak, easy-to-remember, or convenient password. In the context of health promotion, Chiou *et al.* [27] demonstrated that individuals who were primed with abstract construals smoked fewer cigarettes compared with those primed with concrete construals. Abstract construal boosts one's self-control to smoke in the short term by highlighting the central goals of quitting smoking (e.g. overall health benefits, better quality of life) and thereby enhancing one's motivation or behavioural act to stop smoking. On the contrary, concrete construal focuses on the short term's means and resources needed to quit smoking (e.g. immediate lifestyle changes or avoiding smoking in specific places or time of the day) and hence lend a weaker support to one's self-regulation on their smoking behaviour. Duan *et al.* [28] found that construal level (measured as the level of abstraction of climate change imagery) moderates the relationship between one's self-transcendent values (relating to pro-environmentalism) and his/her behavioural intention to engage in mitigation acts targeting climate change. Specifically, participants who were primed to construe concretely about climate change, their self-transcendent values have a greater impact on their concerns towards climate change and their mitigating actions compared with those primed to construe the same issue abstractly.

The present study applies CLT to explain and predict IT users' cybersecurity responses by altering their risk perceptions towards risky cybersecurity incidents. To do that, it is essential to first understand how the constituents of IT users' domain knowledge (i.e. causes and effects) of cybersecurity incidents may correspond with the level of abstraction when they construe them.

High- and low-level properties of 'causes' and 'effects'

Information about 'causes' and 'effects' are fundamental to one's acquisition of knowledge or learning about (cybersecurity) events [29].

1 Optimism bias is a form of cognitive bias that describes how people tend to perceive themselves as unlikely to experience an event with negative consequences.

2 Cognitive fluency refers to the level of ease in processing information in stimuli (e.g. email messages, news reports, advertisements, etc). Research studies have shown that people tend to seek fluency in processing stimuli in various contexts. Cognitive disfluency increases the difficulty in mental information processing; this may dampen people's ability to generalize from concrete scenarios. While disfluency effects have been demonstrated to induce positive cognitive outcomes (such as increased confidence in learning or improvements in memory), it has not always been successful [18, 19]. Given the plethora of manipulation techniques (e.g. using difficult typefaces or visual noises) as well as the wide-ranging outcome measures in various contexts, it may be difficult to ascertain that the disfluency effect is effective in inducing specific and desirable cognitive outcomes in the cybersecurity context.

'Causes' may be perceived as having a more central, superordinate, and essential role compared with 'effects', which plays a peripheral and unstable role in an event [30]. In other words, causes determine the type of effects that one may expect to observe [21, 31]. Research in causality [32] has implicitly linked causes vs effects with abstract and concrete construal, respectively. The cause features of an event (e.g. why did something happen) reflect higher order properties and therefore abstract construal, while the effect features of the event (e.g. what is the consequence of this incident) pertain to lower order properties and therefore represent a concrete construal. Along the same vein, we propose that:

H1: The elaboration of causes and effects of risky cybersecurity events prompts abstract and concrete construals, respectively.

Construing future cyberthreats

Future cyberthreats are not experienced in the present moment (i.e. in the here and now). Construals about these future events therefore embody a form of 'psychological distance' from oneself. In this section, we look deeper into how one's construal of psychologically distant cyberthreats can have an impact on their perceived risks and, consequently, their cybersecurity behaviours. First, we address the general concept of psychological distance in CLT. Second, focusing on one of its dimensions (temporal distance), we discuss how temporal distance relates to abstract and concrete construals. Third, we explore the concept of 'construal fit', explaining how the interaction between the level of construal and temporal distance is hypothesized to influence IT users' risk perception and their cybersecurity behaviour.

Psychological distance

CLT posits that the construal process is egocentric [33]. The psychological distance between the ego (i.e. oneself) and the construed risky event defines the level of abstractness of the mental representation of an event. As a multidimensional construct, psychological distance comprises temporal, social, spatial distances as well as hypotheticality [23].

Temporal distance refers to whether the future cybersecurity incident is perceived as temporally distant or near to oneself. IT users' appraisal of cyberthreats are often shaped by perceived temporal distance to the occurrence of the incident [34]. The perceived temporal distance of cybersecurity incidents (i.e. distal vs proximal) has a direct effect on IT users' cyberthreat sensitivity in the context of cybersecurity [4]. The salience of the cyberthreat increases as they become temporally proximal [35, 36] because, from the CLT perspective, one is able to form more concrete (e.g. vivid) construals that are close to their direct experiences [37]. Moreover, temporal distance is particularly relevant in perceptions about cybersecurity risks[3]. Indeed, the probability of cyberattack is shifting from a mere possibility to becoming inevitable for IT users and organizations dependent on digital technologies [41]. In other words, cybersecurity threats are not a matter of if, but when [42].

Temporal distance and construal level of future events

When construing about temporally distant events, abstract construals 'travel well' [24] and are better than concrete construals. This is because abstract construals involve the essence of the construed event that is largely constant and stable across various contexts compared with concrete construals [33]. Therefore, temporally distant or near events influences the extent to which individuals focus on abstract vs concrete construals [24].

CLT posits that an individual is more likely to focus on causes (vs effects) when the future event is perceived as temporally distant (vs near). Specifically, individuals adopt abstract construal, which focuses on the essential aspects of the informational features on temporally distant events. On the contrary, individuals adopt concrete construal when focusing on peripheral and contextualized information about temporally near events. Low-level features (e.g. effects: details on *how* it may affect oneself) are constitutive to the higher order features (i.e. causes: details on *why* an event occur). For instance, one is more likely to think about the causes (than effects) of a sunburn (e.g. not applying sunblock) when imagining getting a sunburn 1 year later, but more likely to think about the effects (than causes) of the sunburn (e.g. one's appearance) when imagining getting it the next day. To further examine the relationship between cause–effect information and temporal distance, we draw upon the theoretical concept of construal fit.

Construal fit

Construal fit refers to the congruence (or the match) between individuals' level of construal and perceived temporal distance towards the future event. Specifically, it refers to the fit between proximate (vs distal) temporal distance and concrete (vs abstract) construal [43]. Because of their natural correspondence, research has shown that the congruence, or fit, between temporal distance and construals has important implications for cognitive processing and desirable behaviour.

In the context of green appeal in advertising, Chang, Zhang and Xie [44] showed that a congruent match between loss- (vs gain-) message frame and the consequences in the near (vs distant) future in advertising messages leads to more desirable outcomes, more positive attitudes and a higher level of purchase intentions towards environment-friendly products. In the marketing context, Hernandez, Wright, and Ferminiano Rodrigues [45] demonstrated that marketing messages have more persuasive appeals when they focus on the benefit (vs attribute) of the product for purchase in the temporally distant (vs near) future, leading to a more positive evaluation of the product.

There have been a few empirical attempts to explain why the above-mentioned congruity can induce desirable behavioural responses [46]. One of the explanations for the effect of congruence is 'processing fluency'. Processing fluency refers to the ease or difficulty in cognitive processing [47]. In the context of CLT, fluency can be defined as parallelism between abstract vs concrete information features of the event and abstract vs concrete construal, which facilitates cognitive processing. Specifically, when IT users process cybersecurity risk information at abstract (vs concrete) construal, it is cognitively more fluent to process abstract (vs concrete) aspects of the IT threat. The matching provides fluency/cognitive ease in processing which leads to the accentuation of associated behavioural responses.

Construal fit can result in an increased processing fluency where individuals assess the event as 'feeling right' [48] and hence more im-

3 Other dimensions of psychological distances may be relevant to the context of cybersecurity in terms of IT users' cognitive appraisal of cyberthreats. However, existing research studies did not fully address how these dimensions are associated with both the construal tendency of IT users and the temporal uncertainty nature of cybersecurity incidents. The spatial dimension is associated with the fundamental problem that the occurrences of cyberattack traverse spatial (geographical) distance [38]. The application of the social dimension in cybersecurity focuses on interpersonal similarity/closeness on risk perception and the effect of the sharing and exchange of cyber doom rhetoric among peers and with the wider public in online-mediated environments [39]. On the same note, the hypothetical dimension is associated with construing the narrated cyberthreat scenarios as fictitious or apocalyptic [40].

portant, as compared with a 'non-fit state' [49]. In other words, when the appropriate temporal distance (i.e. distant or near) is matched with abstract (vs concrete) construal of an event, the event is perceived as more significant, and individuals will be more motivated to engage in the event-related behaviour [50].

Impact on perceived risks and cybersecurity behaviours

In the context of this study, we expect that when IT users focus on the effect information of a cybersecurity incident, the impact of a temporally near cybersecurity incident on their risk perception should be greater than that of a temporally distal one. Specifically, we posit that because causes represent abstract construal, elaborating on the causes of a cybersecurity incident should lead to the greater perceived severity of the risk when it is imagined to occur in the distant future. Conversely, because effects represent a concrete construal, elaborating on the effects of cybersecurity risks should result in greater perceived severity when they are thought to happen in the near future. Therefore, this study posits that the influence of cause–effect elaboration of cybersecurity risks should be moderated by the temporal distance of which the risks may affect them in the future:

H2a: The effect of the elaboration of cause–effect of risky cybersecurity events on IT users' perceived severity will be moderated by the temporal distance leading to the occurrence of that risk.

Furthermore, the perceived severity of cybersecurity risks should have an impact on protective behavioural intentions as a response to these risks. For example, protection motivation theory (PMT) posits that human's protective behavioural intention is a direct effect of their cognitive appraisal systems, which comprises of threat (i.e. perceived severity and susceptibility) and coping appraisal [51]. Similarly, technology threat avoidance theory (TTAT) maintains that IT users have the behavioural intention to maintain the distance between their desired (safe) online state and the undesired (unsafe) state through their cognitive assessment of the cyberthreat (i.e. whether it is severe and/or probable) as well as their ability to cope with them [52]. As such, we expect that IT users' perceived severity (as a function of the interaction between cause–effect elaboration and temporal distance) should exert downstream implications on IT users' behavioural intentions to protect themselves against cybersecurity risks. Specifically, we hypothesize that:

H2b: Perceived severity mediates the interactive effect of causes vs effects and temporal distance on IT users' protective behavioural intentions (H2b).

Figure 1 provides a summary of our hypotheses. Based on the CLT framework, we hypothesize (in H2a) that the interaction effects between CE (i.e. the elaboration of 'cause' vs 'effect') and perceived temporal occurrence (i.e. distal vs proximal) of cybersecurity threats should heighten IT users' perceived severity about them. Drawing upon existing staged theories (e.g. the PMT and TTAT), we further hypothesize (in H2b) that IT users' perceived severity should mediate the relationship between CE and one's cybersecurity behavioural intention.

Study 1

Study 1 ascertains that the elaboration of causes vs effects of cybersecurity risks indeed prompts abstract vs concrete construal, respectively. The hypothesis for Study 1 is that IT users' elaboration of causes vs effects of cybersecurity risks predicts the adoption of abstract vs concrete mindset, respectively (H1).

Methods

Participants

A priori power analysis was conducted to ensure that we recruited sufficient sample sizes to detect our hypothesized effects reliably. Power analysis using G*Power 3.1 (*t*-tests, Means: Difference between two independent means) [53] suggested a sample size of ~200 to detect a small-to-medium effect size (Cohen's $d = 0.39$) with 80% power.

A total of 212 participants were recruited for Study 1 for an online experiment. Forty-four cases were dropped from the analysis in a validity check, leaving us with 168 participants (106 female). One reason for such a high number of invalid cases could be the open-ended nature of the questions (i.e. elaboration of causes vs effects) requiring relatively more time and mental effort than close-ended ones [54], resulting in participants not responding in good faith. Moreover, open-ended questions, in web questionnaires, has been known for their drawback in terms of collecting large percentage of invalid responses [55]. The average age of the participants was 38.5 years old (SD = 12.5). About 43.3% of participants rated their level of knowledge towards cyberthreats as 'average', and 63.7% of participants spent 21–40 h per week as well as above 40 h per week using the Internet. Full details of the measurement items and their scale can be found in Table S1.

Procedures and measures

The experimental study was conducted on Qualtrics, a commercial survey platform, and was made voluntary. CloudResearch's MTurk Toolkit, which was specifically designed to launch studies on Amazon Mechanical Turk, was used to deploy the online experiment. Eligibility for the study was limited to participants (MTurk workers) who have an approval rating of >98%, located in the United States, and not having attempted any pre-tests pertaining to this study. Approval from a department ethics review committee was obtained prior to the commencement of the experiments in this study.

Upon giving their consent to take part in the study, participants were randomly assigned to either the cause or effect condition ($n = 84$ for both conditions). In both conditions, participants were shown a list of six risky cybersecurity incidents that could potentially occur to them (see Table 1), instructions as adapted from Rim, Hansen and Trope [30], to engage in elaboration. In the cause condition, participants were shown the effects of the six events in sequential order and asked to elaborate (by writing down) their potential causes; in the effect condition, participants were shown the causes of the events and asked to elaborate on their potential effects.

The events were derived from a pilot study targeted at developing a list of risky cybersecurity events drawing from an exclusively criminalistic angle: cyberthreat actors or criminals who are motivated to undertake malicious online activities for financial gain. The events were sourced from various websites explaining the common types of criminalistic cybersecurity breaches that can happen to daily IT users. They also differ in the level of 'obviousness' in terms of the pair matches between causes and effects of the risky cybersecurity incidents. This is because, in reality, IT users may sometimes find a 'cause' of a cyberthreat that obviously matches an 'effect' (or vice versa) and sometimes they do not. The variation in the level of 'obviousness' depends on IT users' a priori experiences of the cybersecurity incidents in their daily lives. Therefore, the list of six risky cybersecurity events (from an original list of 10) was developed with a variation of the level of obviousness among them to consider such real-world nuances.

After the cause or effect elaboration procedure, participants completed the behavioural identification form (BIF) Vallacher and Weg-

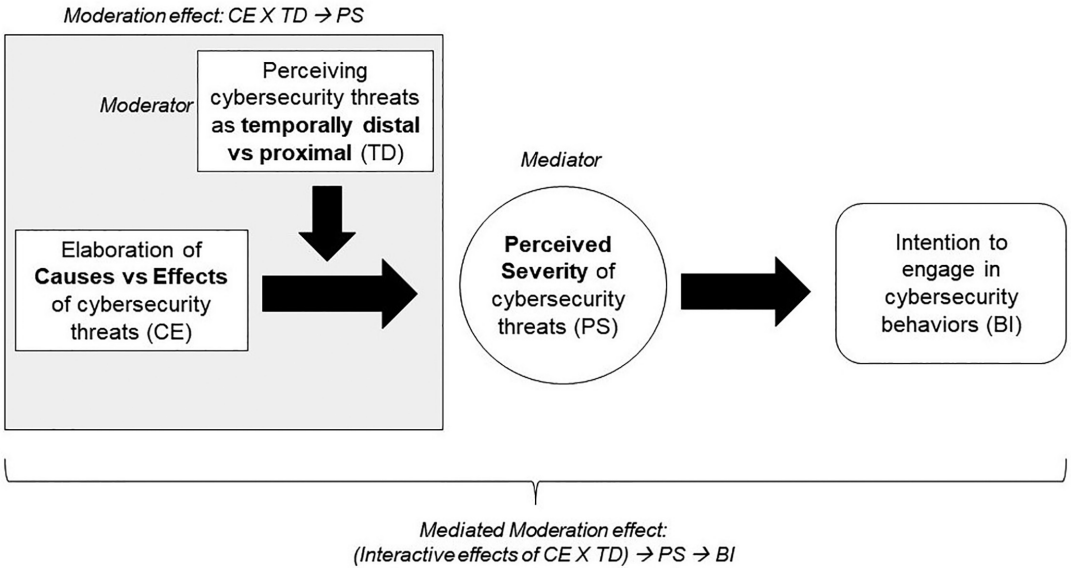


Figure 1: An overview of key relationships in the present study.

Table 1: Cause and effect manipulation in online experiment

Event number	Cause information	Effect information
1	Procrastinating security patches update to your computer	Computer has been affected by a never-before-seen virus
2	Opening an email attachment in an email from an untrusted source	Getting malware and advert pop-ups despite anti-virus says it can block them
3	Not getting the latest internet security suite/update in the market	Programs crash more than usual during execution and computer slowed down substantially
4	Using public Wi-Fi to perform confidential transactions/activities	Someone knows what you have said in your private chats and emails
5	Oversharing of photos and personal details on social media (e.g. Instagram/Facebook)	Getting lots of friend/follower requests from strangers in social media accounts
6	Downloaded and installed software from an untrusted source	Installed software keeps prompting to update personal particulars to receive free upgrades

ner [56], a 25-item questionnaire widely used to measure the state of one's construal level (see Table S2). In the BIF, participants are shown a list of different actions for which one may define either in abstract or concrete terms. For example, 'toothbrushing' can be defined as (i) moving a brush around one's mouth (concrete) or (ii) preventing tooth decay (abstract). A construal level score was summed based on the number of abstract responses selected. Selecting abstract (i.e. high-level) statement will earn them a score of one and zero if a concrete (i.e. low-level) statement is selected. Finally, participants answered demographic questions.

Participants' elaborations of the causes or effects of the risky cybersecurity events were independently and manually assessed for coherence after the experiment and prior to analysis. Responses that were deemed incomprehensible and indicative of a lack of attention were dropped from the analysis [36].

Results

Manipulation check

An independent coder, who had no knowledge about this study, was engaged in checking for cause–effect manipulation by analysing the content generated by the respondents for each condition manually. To determine the sample size for manipulation check, a priori power analysis was performed using G*Power. Results revealed that a sample size of 240 cases would allow us to detect a small to medium effect size, Cohen's $d = 0.39$, with 85% power. Hence, responses from 40 participants (240 cases: 6 events × 40 participants [20 from each cause and effect condition]) were randomly selected. Results of the content analysis showed that, in the cause condition, 78% of the participants' thoughts were coded as causes. While in the effect condition, 92% of the participants' thoughts were coded as effects.

Main analysis

H1 posits that the elaboration of causes and effects of risky cybersecurity events prompts abstract and concrete construals, respectively. The responses from Study 1 were subjected to an independent sample *t*-test. Supporting H1, participants in the cause condition (Mean; $M = 16.0$, standard deviation; SD = 5.71) scored higher in their construal levels than those in the effect condition ($M = 14.2$, SD = 6.09); $t\ (166) = 2.01$, $P = 0.046$). Table 2 summarizes the mean construal scores in both the 'cause' and 'effect' conditions.

Table 2: Construal scores in the 'cause' and 'effect' conditions

Condition	Mean construal score	Standard deviation (SD)
Cause elaboration	16.0	5.71
Effect elaboration	14.2	6.09

Note. Mean construal score in the cause elaboration condition is significantly higher than the mean score in the effect elaboration condition based on an independent samples *t*-test; $t\ (166) = 2.01$, $P = 0.046$.

The effect size ($d = 0.31$)[4] was found to be within Cohen's (1988) convention of small to medium effect sizes (i.e. $d = 0.20$ to 0.50). This indicates that our cause vs effect elaboration procedure was effective in evoking a more abstract vs concrete mindset, respectively.

Study 2

According to CLT, individuals have the cognitive tendency to give attention to abstract (vs low) level construal when they think about (cybersecurity) events in the distant (vs near) future. Drawing upon the results in Study 1, we examined how the construal fit between cause (abstract construal) vs effects (concrete construal) and the manipulated temporal distance of the occurrence of cybersecurity risks (i.e. distant vs near future) can affect their perceived severity of these risks. Ultimately, Study 2 aims to find out how this effect may impact IT users' behavioural intention to protect themselves against the cybersecurity risks.

Method

Participants

To determine the sample size for Study 2, a priori power analysis was once again conducted using G*Power 3.1. Based on the results of this analysis (*F*-tests: ANOVA, fixed effects, special, main effects, and interactions), a sample size of ~400 was required to detect a small-to-medium effect size (Cohen's $f = 0.14$)[5], with 80% power.

A total of 424 participants for this online experiment were recruited from a crowdsourcing data acquisition platform, Amazon Mechanical Turk. Eligibility criteria were the same as in Study 1. Participants who previously attempted or completed Study 1 were not eligible to participate in Study 2. Fifty-eight participants were excluded from analysis for failing the validity checks, leaving 366 participants (225 female) for analysis. The average age of the participants was 37.5 years old (SD = 12.0). About 42.6% of participants rated their level of knowledge towards IT threats as 'average' and spend 21–40 h per week as well as above 40 h per week using the internet (65.1%). Each participant was compensated with US$0.40 for completing the experiment.

Procedures and measures

The study adopted a 2 (Elaboration: Cause vs Effect) × 2 (Temporal distance: Distant vs Near) factorial design: 'cause distant' ($N = 94$), 'cause near' ($N = 93$), 'effect distant' ($N = 92$), and 'effect near' ($N = 87$). Participants were randomly assigned to these four conditions and shown a list of six risky cybersecurity events (see Table 1). To manipulate temporal distance, participants were asked to imagine that each event will happen to them either in the distant future (next year) or near future (tomorrow). Next, participants were asked to elaborate on the causes or effects of the event in sequential order, depending on the condition they were in. While acknowledging that participants may react differently to each of these events, no attempts, however, were made to capture their cognitive reactions immediately after they complete the elaboration task for the respective events.

Upon completing the elaboration task, participants answered a manipulation check question to measure the efficacy of temporal distance manipulation ('The occurrence of the IT events take place in the: (1) Near future … (7) Distant future'). Participants then answered the key dependent variables: perceived severity and protective behavioural intention, each measured on a 7-point Likert scale (1 = strongly disagree, 7 = strongly agree). Perceived severity was measured with three items adapted from Witte [57] (e.g. 'I believe these IT threats are severe', Cronbach alpha: $\alpha = 0.92$). Protective behavioural intention was measured with six items adapted from [58] (e.g. 'I would make plans to avoid these IT threats', $\alpha = 0.90$). Although behavioural intention and actual behaviour may be inconsistent with one another [59], we have drawn upon relevant cognitive theories [60] to assume that the former is a fair representation of the latter. After answering these key measures, participants answered demographic questions before submitting their responses. Arguably, the afore-mentioned key measures are subjective in nature (i.e. self-reported) and hence may be limited in representing actual responses. Nevertheless, such self-reported measures have proven to be fairly accurate and useful for reflecting actual responses in various scholarly works [61, 62]. Full details of the measurement items can be viewed in Table S1.

Results

Manipulation check

Participants in the distant condition ($M = 3.79$, SD = 1.62) perceived that the cybersecurity risks will occur later in the future compared with those in the near condition ($M = 2.16$, SD = 1.43); $t\ (364) = 10.2$, $P < 0.001$, indicating that the temporal distance manipulation was effective. The effect size ($d = 1.07$) was greater than Cohen's convention for a large effect ($d = 0.80$) [63]. The check for cause–effect manipulation was similar to Study 1. The coder rated that 80.8 (85.0) % of the observations in the cause (effect) condition were indeed referring to causes (effects).

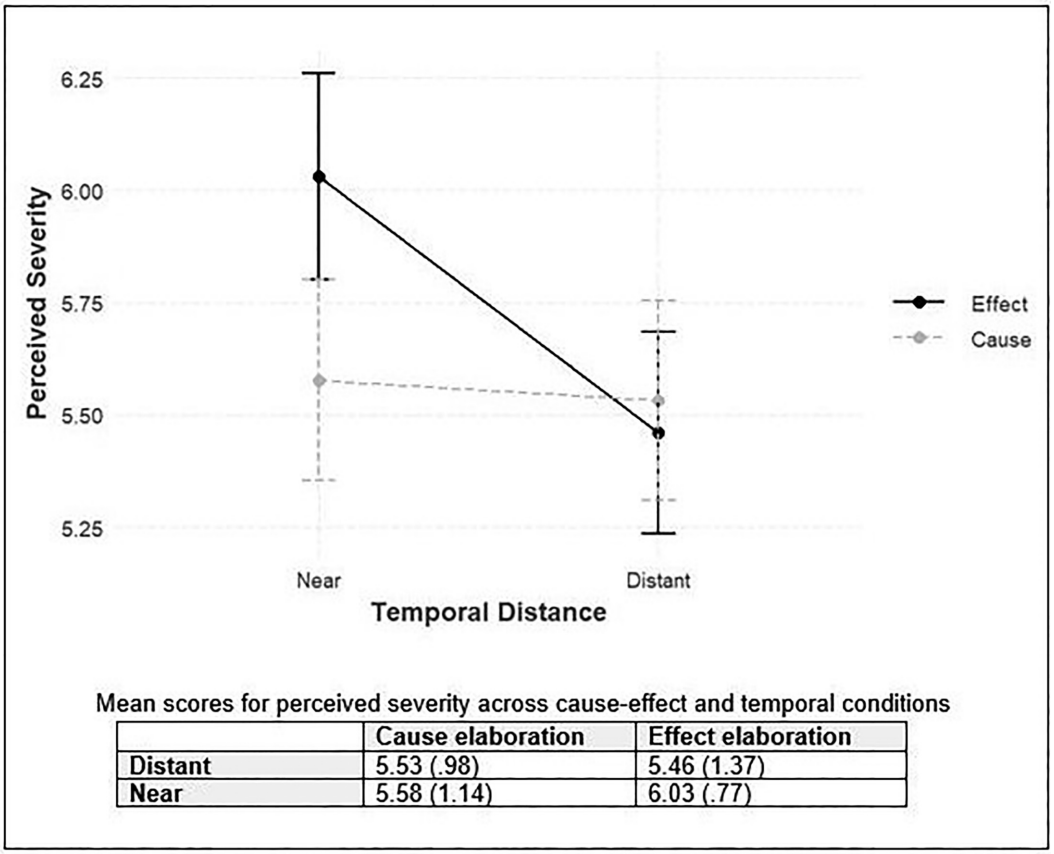
Interaction effect

H2a posits that the effect of the elaboration of causes and effects of risky cybersecurity events on IT users' perceived severity is moderated by their perceived temporal distance leading to the occurrence of that risk, demonstrating a construal fit.

To test this construal fit hypothesis (H2a), participants' risk perceptions were submitted to a 2 (cause vs effect) × 2 (distant vs near) between-subjects ANOVA. There was a significant main effect of temporal distance, $F\ (1, 362) = 7.23$, $P = 0.008$, but not for cause–effect elaboration, $F\ (1, 362) = 2.78$, $P = 0.096$. More importantly, as observed in Fig. 2, there was a significant interaction between elaboration and temporal distance, $F\ (1, 362) = 5.26$, $P = 0.022$, $\eta_p^2 = 0.014$, supporting H2a. Simple effects analysis revealed that elaboration of effects ($M = 6.03$, SD = 0.77) significantly led to higher levels of perceived severity as compared with elaboration of causes ($M = 5.58$, SD = 1.14) when cybersecurity risks were expected to occur in the near future, $F\ (1, 362) = 7.72$, $P = 0.006$. Conversely, elaboration of causes ($M = 5.53$, SD = 0.98) induced higher levels of perceived severity as compared with elaboration of effects ($M = 5.46$,

4 Cohen's *d* is a statistical index of effect size indicating the standardized difference when comparing between two means (in an independent sample *t*-test or analysis of variance test).

5 Cohen's *f* is a statistical index of effect size indicating the standardized average effect across all the levels in an independent variable.



Mean scores for perceived severity across cause-effect and temporal conditions

	Cause elaboration	Effect elaboration
Distant	5.53 (.98)	5.46 (1.37)
Near	5.58 (1.14)	6.03 (.77)

Note. This figure consists of standard error bars. Standard deviation in parentheses.

Figure 2: The interactive effects of cause–effect elaboration and perceived temporal proximity on perceived severity of cybersecurity threats.

SD = 1.37) when cybersecurity risks were expected to occur in the distant future, although this difference was not significant, $F(362) = 0.20$, $P = 0.66$.

Mediated moderation

Building upon H2a, H2b further posits that IT users' perceived severity of the risky cybersecurity events mediates the interactive effects of causes and effects on their online protection behavioural intention. To examine the effects of construal fit on protective behavioural intentions (H2b), we tested a mediated moderation model (see Fig. 2) with SPSS PROCESS, version 3.2 [64]. This model involves a moderated effect that is mediated. To illustrate, *X*'s effect on *Y* is mediated by *M*, with the indirect effect of *X* being moderated by *W*. Specifically, the effect of *X* on *M* is moderated by *W*.

According to Hayes and Rockwood [65], the 'moderation of mediation manifests itself statistically in the form of an indirect effect that depends on a moderator, meaning that it is a function of a moderator'. Such model has been adopted widely across various disciplines despite various controversies regarding its computation methods such as its gravitation towards overall indirect effect [64, 66] and biases caused by measurement error [66].

Using 10 000 bootstrapped samples, the index denoting the mediated moderation (MM) effect was significant: $\beta_{MM} = 0.16$, SE (standard error) = 0.073, 95% CI [0.03, 0.31]. Therefore, H2b is supported. The indirect effect of cause–effect elaboration on protective behavioural intention through perceived severity is not significant at all values of the moderator (temporal distance). Specifically, this indirect effect is significant when IT users perceived the cybersecurity incidents as proximal; $\beta_{proximal} = -0.14$, SE = 0.05, 95% CI [−0.26, −0.05] but not when IT users perceive them as distal; $\beta_{distal} = 0.02$, SE = 0.06, 95% CI [−0.09, 0.13]. Concurrently, we also noted that this indirect effect is significantly moderated: the product (interaction) of cause–effect elaboration and temporal distance has a significant effect on perceived severity; $\beta_{interaction} = 0.53$, SE = 0.23, 95% CI [0.08, 0.98]. Results of the above-mentioned indirect effects are summarized in Table 3.

Figure 3 illustrates the unstandardized path coefficients denoted by *a* (the effect of cause–effect elaboration on perceived severity), *b* (the effect of perceived severity on protective behavioural intention), and *c* (the direct effect of cause–effect elaboration on protective behavioural intention). Cause–effect elaboration has no significant direct impact on IT users' protective behavioural intention; $c = -0.12$, SE = 0.08, 95% CI [−0.28, 0.04]. The elaboration of cause (coded as 1) and effects (coded as 0) has a significant influence on IT users' perceived severity; $a = -0.45$, SE = 0.16, 95% CI [−0.77, −0.13], which in turn has a significant influence on their protective behavioural intention towards cybersecurity risks; $b = 0.31$, SE = 0.04, 95% CI [0.24, 0.39].

Table 3: Summary of direct and indirect effects of the mediated moderation model predicting IT users' online protective behaviour

Indirect effects			
Relationship	Coefficient	SE	95% CI
(CE∗TD) → PS	$\beta_{interaction} = 0.53$	0.23	[0.08, 0.98]
CE →PS →PBI	$\beta_{proximal} = -0.14$	0.05	[−0.26, −0.05]
	$\beta_{distal} = 0.02$	0.06	[−0.09, 0.13]
Direct effects			
CE → PS	$a = -0.45$	0.16	[−0.77, −0.13]
PS → PBI	$b = 0.31$	0.04	[0.24, 0.39]
CE → PBI	$c = -0.12$	0.08	[−0.28, 0.04]
Index of mediated moderation (MM)			
	$\beta_{MM} = 0.16$	0.07	[0.03, 0.31]

Note. β = beta coefficient. CE = cause (coded as '1') vs effect (coded as '0') elaboration; TD = temporal distance: proximal (coded as '0') vs distal (coded as '1'); CE∗TD = interaction term; PS = perceived severity; PBI = protective behavioural intention; SE = standard error.

Discussion

The present research diverges from past approaches that focus on awareness- or fear-based methods to enhance IT users' evaluation of information security risks and their protective behavioural intentions. For the first time, by drawing associations between elaborations of causes vs effects of risky cybersecurity events and level of construal (H1), this study demonstrated the role of construal fit in influencing IT users' cognitive processing of risky cybersecurity events (H2a) and their downstream protective behavioural intentions (H2b). Notably, as hypothesized in H2a, IT users' risk perceptions were the highest when attention was channelled to the elaboration of consequences of temporally near threats. On the other hand, risk perceptions were largely attenuated when attention was directed at the causes of temporally near threats or when users considered temporally distant threats. Our research thus further validates the generalizability of construal fit beyond existing contexts [44].

Notwithstanding, our results supporting H2a also revealed that construal fit might not have as significant an impact on influencing risk perceptions when the elaboration of these cybersecurity events are perceived as distant as compared with near. There can be different explanations for this phenomenon.

First, temporal discounting research has demonstrated that individuals tend to downplay risks when they are temporally distant (vs near) [67]. The corresponding abstract construal of risks may act as a psychological buffer that desensitize IT users to the perceived severity of these risky cybersecurity events. Second, although personal sensitivity towards cyberthreats can be situationally induced by negative information about cybersecurity incidents, such as the 'cyber doom' rhetoric [40], IT users' embeddedness in modern technology plays an important role in influencing such sensitivity [4]. In other words, high dependence on modern digital technology can desensitize one's response to negative reporting of risky cybersecurity events [4]. Our participants were online workers with a high dependence on modern internet technology to generate revenue. They may have a unique level of trust in modern technology, given their high dependency. Thus, there is a possibility of threat normalization among our participants, which makes them less sensitive towards distant cyberthreats. Our findings support the idea that under conditions where cyberthreats are normalized, IT users' cognitive and behavioural responses towards them may still be enhanced through construal fit. Unless when the risks are perceived as temporally near and construed in concrete terms, as demonstrated in our findings (see H2a), we may infer that by 'living with (online) risks', our participants in cyberspace have engaged in a 'normalization of threat' where they perceive (cybersecurity) risks as usual everyday events [68].

The concept of construal fit enriches various staged theories, such as the TTAT and PMT, used by cybersecurity researchers to investigate how IT users' risk perceptions can influence their associated protective behaviours. Research studies adopting these theories have theorized that risk perception is an effective antecedent of IT users' protective behavioural intentions [69]. In our research, we have shown that construal fit is an important antecedent of risk perception, which in turn influences their cybersecurity behavioural intentions. This causal–chain relationship reflects the importance of considering IT users' cognitive processes as antecedents in risk perceptions.

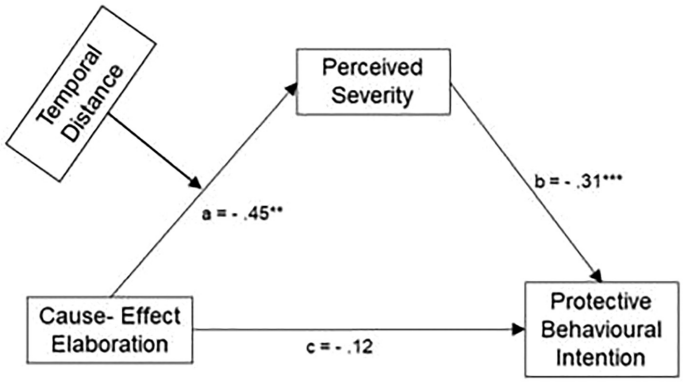
Overall, the findings from this study suggest that it is important for cybersecurity researchers to give due attention to IT users' cognitive tendencies or biases affecting their behavioural intention towards safe cybersecurity practices. Specifically, other than the existing cognitive biases uncovered by current cybersecurity studies to influence IT users' responses towards them [17, 20], the present research highlighted the importance of IT users' construal tendency. Specifically, the situational priming of IT users' construal processes can result in a heightened level of risk perception towards cybersecurity risks.

Our elaboration procedure has practical value for the common use of cause–effect information in the communication of potential cybersecurity risks (or threats in general). The verbal communication of threats typically involves a direct or indirect explication of their causes and effects, constituting one's understanding of that event [66]. IT users typically perceive cybersecurity risks as uncertain and distant (temporally and psychologically) [70]. Our research findings is useful when communicators want to induce a heightened perception of risks from the IT users. To achieve this through a construal fit, communicators can enhance the concreteness of IT users' construal by simultaneously reducing the temporal proximity (imminence) of the threat and emphasizing its negative consequences [71].

The findings in this study shall benefit industry practitioners (e.g. information security champions) advocating for awareness or protection behaviour against potential cybersecurity risks within organizations. The cognitive approach towards enhancing IT users' perception of cybersecurity risks leverages human cognitive tendency (i.e. construal processes) rather than depending on costly software and instructor-led training requiring a dedicated amount of manpower and time.

Henceforth, the core of our CLT-inspired cybersecurity training should focus on IT users' elaboration of negative consequences of possible near future cybersecurity incidents to heighten their risk perception. Specifically, such training requires and emphasizes, active construal (and verbal elaboration) of the negative consequences of temporally near cybersecurity incidents. For example, to elicit such cognitive responses in a meaningful, stimulating, and engaging manner, practitioners can consider gamification [72]. To illustrate, IT users may play a first-person superhero character warning other characters in the game about potential negative consequences of cyberthreats they might face upon observing their risky cyber behaviours given the time left before a cyberattack hits them.

Cybersecurity practitioners should be mindful that the design of a CLT-inspired cybersecurity training is different from that of a standard one. One key difference is that, in a CLT-inspired training, the verbal elaboration of negative consequences of cybersecurity incidents is self-motivated and self-generated by IT users who construe them, rather than spoon-feeding them with possible consequences in



Note. Unstandardized coefficients (a, b, and c) computed using 10,000 bootstrapped samples at 95% confidence interval.

$^{**}p < .01$, $^{***}p < .001$

Figure 3: Mediated moderation model featuring the indirect effects of the cause–effect elaboration of cybersecurity risks on IT users' protective behavioural intention.

standard training packages. Another key difference is the focus on the temporal proximity of the cybersecurity incidents. On the one hand, standard cybersecurity training packages often did not give due attention to the temporal occurrence of cybersecurity incidents as they are narrated to IT users. While on the other, a CLT-inspired one focuses on making IT users aware of the temporal proximity of the cybersecurity incidents in their construal. Nevertheless, like many other interventive cybersecurity training, the success of this approach can be measured by investigating the cybersecurity behavioural change of IT users in the post-training stages [73].

Limitations and Future Directions

Consistent with existing CLT studies demonstrating construal fit [74], this research argued theoretically that the construal fit between cause–effect and temporal distance was due to processing fluency (or 'feeling right'). Future research may include the empirical testing of processing fluency to ascertain this argument. In addition, affective reactions (e.g. fear) are also fundamental to how IT users may evaluate cybersecurity risks. However, these elements were excluded from this research. Future studies may therefore consider how the current construal fit approach may influence affective reactions of IT users.

Like all other key variables in this study, both the measures of participants' construal level and perceived risks were subjective (i.e. self-reported). The issue with the subjective measure is that it may not be an accurate reflection of their cognitive processes towards the stimuli. This is because people rarely have introspective access to their own cognitive processes [75]. Rather, there is a possibility that their self-reports about their perceptions may be guided by their a priori experiences or implicit causal links relating to particular cybersecurity incidents.

Past experiences can influence one's perception of risks as they drive changes to their schemas about staying protected in one's (cyber) environment [76]. However, participants' prior exposures to cybersecurity incidents were not captured in this study. Therefore, prior experiences of cybersecurity incidents may affect their behavioural intention to engage in present cybersecurity behaviours [77]. Future studies should consider participants' past experiences in cybersecurity incidents. Moreover, participants' cognitive responses were not immediately captured after they elaborated on the cause (or effect) for each of the cybersecurity incidents. Such responses may be insightful for future researchers who wish to understand the relative effects of the nature of specific cybersecurity incidents on IT users' risk perceptions while investigating their construal fit.

People's domain knowledge about cyberspace and cybersecurity can affect the way they practise safe cybersecurity behaviours [2, 78]. Domain knowledge in cybersecurity not only facilitates one's mental processing and integration of cues in malicious events in cyberspace but also enhances their awareness of potential cyberattacks, and thereby positively shaping their cybersecurity behaviour [79]. This study focuses on IT users (the mass public) who possess an 'average' level of cybersecurity knowledge. However, other groups of people such as the political elites [80], who have different sets of knowledge, power, and strategies to shape cyberspace securitization [81], were not considered. More research work is needed to investigate whether construal fit may also take place between IT users who are the domain experts (i.e. having a high level of cybersecurity knowledge) and the political elites.

Apart from cybersecurity knowledge, there exist many factors that can influence IT users' adherence to cybersecurity behaviours, e.g. the lowering of economic barriers to safe cyber practices or increasing touchpoints between cybersecurity experts and users [82], or the implementation of mandatory security functions (e.g. two-factor authentication, VPN access). Therefore, future studies should also investigate these factors when predicting IT users' risk perceptions and cybersecurity behaviours and how they construe future cyberthreats. Furthermore, this study assumed consistency between IT users' behavioural intentions and actual behaviour. While such consistency may not always hold (e.g. due to differences in behavioural control) [60], it would be useful for future studies to examine IT users' actual behavioural changes with respect to the construal fit approach.

Lastly, our main findings laid the groundwork for future studies to develop a cybersecurity training package. However, more specific recommendations and their applicability in the filed should be developed and evaluated in the future studies. For example, future studies can investigate the effectiveness of a CLT-driven cybersecurity train-

ing package (as described earlier) against a standard one using a field study.

Conclusion

Although cybersecurity breaches may not happen to IT users every time, their construal about them, however, can take place virtually any time when prompted. Such capability of IT users should not be left unexploited by practitioners advocating for cybersecurity. Indeed, many daily cybersecurity-related activities and decisions (e.g. reporting and deleting emails with dubious or unknown links and attachments, performing installation of anti-malware software, or setting strong account passwords) may have been enacted through construal of some cybersecurity risks that may manifest in near or distant future. Undertaking a construal-level approach towards the advocacy for cybersecurity in today's digital world could be the key to unlocking new strategies to enhance cybersecurity risk perception and their related protective behaviours.

Supplementary Data

Supplementary data available at *Cybersecurity Journal* online.

Conflict of Interest

The authors reported no potential conflict of interest.

References

1. Winder D. *Data breaches expose 4.8 billion records in first six months of 2019*. https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#589246616bd54 (2019, November 09).
2. Wiederhold BK. The role of psychology in enhancing cybersecurity. In: *Cyberpsychology, Behavior, and Social Networking*, Vol. 3. Larchmont, NY: Mary Ann Liebert, Inc., 2014, 131–2.
3. Kostyuk N, Wayne C. The microfoundations of state cybersecurity: cyber risk perceptions and the mass public. *J Glob Secur Stud* 2021;**6**:1–25.
4. Gomez MA, Whyte C. Breaking the myth of cyber doom: securitization and normalization of novel threats. *Int Stud Q* 2021;**65**:1137–50.
5. Lowry DT, Nio TCJ, Leitner DW. Setting the public fear agenda: a longitudinal analysis of network TV crime reporting, public perceptions of crime, and FBI crime statistics. *J Commun* 2003;**53**:61–73.
6. McAlaney J, Benson V. Cybersecurity as a social phenomenon. In: *Cyber Influence and Cognitive Threats*. Cambridge, MA: Academic Press, 2020, 1–8.
7. Slovic P. *The Perception of Risk*. New York, NY: Routledge, 2016.
8. Johnston AC, Warkentin M, Siponen M. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Q* 2015;**39**:113–34.
9. Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. *J Comput Syst Sci* 2014;**80**:973–93.
10. Albrechtsen E. A qualitative study of users' view on information security. *Comput Secur* 2007;**26**:276–89.
11. Monk T, Van Niekerk J, von Solms R. Sweetening the medicine: educating users about information security by means of game play. *SAICSIT '10: 2010 Annual Conference of the South African Institute of Computer Scientists and Information Technologists*. Bela-Bela, South Africa: Association for Computing Machinery, 2010, 193–200.
12. Vance A, Eargle D, Ouimet K. *et al*. Enhancing password security through interactive fear appeals: a web-based field experiment. *46th Hawaii International Conference on System Sciences*. Wailea, Maui, USA, 2013, 2988–97.
13. Grassegger T, Nedbal D. The role of employees' information security awareness on the intention to resist social engineering. *Procedia Comput Sci*. 2021;**181**:59–66.
14. Andrade RO, Yoo SG. Cognitive security: a comprehensive study of cognitive science in cybersecurity. *J Inf Secur Appl* 2019;**48**:1–13.
15. Cherry K. *What is cognition?*. https://www.verywellmind.com/what-is-cognition-2794982 (2021, August 25).
16. Tsohou A, Karyda M, Kokolakis S. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Comput Secur* 2015;**52**:128–41.
17. Schaupp LC, Carter L. The impact of trust, risk and optimism bias on e-file adoption. *Inf Syst Front* 2010;**12**:299–309.
18. Kühl T, Eitel A. Effects of disfluency on cognitive and metacognitive processes and outcomes. *Metacogn Learn* 2016;**11**:1–13.
19. Yue CL, Castel AD, Bjork RA. When disfluency is—and is not—a desirable difficulty: the influence of typeface clarity on metacognitive judgments and memory. *Mem Cognit* 2013;**41**:229–41.
20. Park YW, Herr PM, Kim BC. The effect of disfluency on consumer perceptions of information security. *Mark Lett* 2015;**27**:525–35.
21. Shapira O, Liberman N, Trope N. *et al*. Levels of mental construal. In: Fiske ST, CNs Macrae (eds). *Sage Handbook of Social Cognition*. Thousand Oaks, CA: Sage, 2012, 229–50.
22. Breves P, Schramm H. Bridging psychological distance: the impact of immersive media on distant and proximal environmental issues. *Comput Hum Behav* 2021;**115**:1–9.
23. Trope Y, Liberman N. Construal-level theory of psychological distance. *Psychol Rev* 2010;**117**:440–63.
24. Trope Y, Liberman N. Temporal construal. *Psychol Rev* 2007;**110**:403–21.
25. Schuetz SW, Benjamin Lowry P, Pienta DA. *et al*. The effectiveness of abstract versus concrete fear appeals in information security. *Manag Inf Syst* 2020;**37**:723–57.
26. Kaleta JP, Lee JS, Yoo S. Nudging with construal level theory to improve online password use and intended password choice: a security-usability tradeoff perspective. *Inf Technol People* 2019;**32**:993–1020.
27. Chiou WB, Wu WH, Chang MH. Think abstractly, smoke less: a brief construal-level intervention can promote self-control, leading to reduced cigarette consumption among current smokers. *Addiction* 2013;**108**:985–92.
28. Duan R, Takahashi B, Zwickle A. How effective are concrete and abstract climate change images? The moderating role of construal level in climate change visual communication. *Sci Commun* 2021;**43**:358–87.
29. Waldmann MR. Knowledge-based causal induction. In: Shanks DR, Medin DL, Holyoak K, (eds). *The Psychology of Learning and Motivation*. Cambridge, MA: Academic Press, 1996, 47–88.
30. Rim S, Hansen J, Trope Y. What happens why? Psychological distance and focusing on causes versus consequences of events. *J Pers Soc Psychol* 2013;**104**:457–72.
31. Rehder B. A causal-model theory of conceptual representation and categorization. *Exp Psychol Learn Mem Cogn* 2003;**29**:1141–59.
32. Ahn W, Kim NS. The causal status effect in categorization: an overview. *Psychol Learn Motiv* 2000;**40**:23–65.
33. Liberman N, Trope Y. Traversing psychological distance. *Trends Cogn Sci* 2014;**18**:364–9.
34. Shen C-C, Chiou J-S. The impact of perceived ease of use on Internet service adoption: the moderating effects of temporal distance and perceived risk. *Comput Hum Behav* 2010;**26**:42–50.
35. Bhatia J, Breaux TD. Empirical measurement of perceived privacy risk. *ACM Trans Comput Hum Interact* 2018;**25**:1–47.
36. Rozin P, Royzman EB. Negativity bias, negativity dominance, and contagion. *Pers Soc Psychol Rev* 2001;**5**:296–320.
37. Rosoff H, Cui J, John R. Behavioral experiments exploring victims' response to cyber-based financial fraud and identity theft scenario simulations. *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, 2014, 175–86.

38. Halouzka K, Burita L, Kozak P. *Overview of cyber threats in central European countries*. *Communication and Information Technologies (KIT)*. IEEE, 2021, 1–6.
39. Lawson ST, Yeo SK, Yu H. *et al.* The cyber-doom effect: the impact of fear appeals in the US cyber security debate. *2016 8th International Conference on Cyber Conflict (CyCon)*: IEEE, 2016, 65–80.
40. Lawson S. Beyond cyber-doom: assessing the limits of hypothetical scenarios in the framing of cyber-threats. *J Inf Technol Politics* 2013;**10**: 86–103.
41. Pearlson K, Thorson B, Madnick S. *et al. Cyberattacks are inevitable. Is your company prepared?* https://hbr.org/2021/03/cyberattacks-are-inevitable-is-your-company-prepared (2021, August 25).
42. Thompson EC, McDermott. Not if, but when. *Building a HIPAA-Compliant Cybersecurity Program*. Springer, 2017, 3–14.
43. Fessel F. Increasing level of aspiration by matching construal level and temporal distance. *Soc Psychol Pers Sci* 2011;**2**:103–11.
44. Chang H, Zhang L, Xie GX. Message framing in green advertising: the effect of construal level and consumer environmental concern. *Int J Advert* 2015;**34**:158–76.
45. Hernandez JMDC, Wright SA, Ferminiano Rodrigues F. Attributes versus benefits: the role of construal levels and appeal type on the persuasiveness of marketing messages. *J Advert* 2015;**44**:243–53.
46. Zhang L. How effective are your CSR messages? The moderating role of processing fluency and construal level. *Int J Hosp Manag* 2014;**41**:56–62.
47. Alter AL, Oppenheimer DM. Effects of fluency on psychological distance and mental construal (or why New York is a large city, but "New York" is a civilized jungle). *Psychol Sci* 2008;**19**:161–7.
48. Steinhart Y, Mazursky D, Kamins MA. The "temporal-processing-fit effect": the interplay between regulatory state, temporal distance, and construal levels. *Soc Cogn* 2013;**31**:315–34.
49. White K, MacDonnell R, Dahl DW. It's the mind-set that matters: the role of construal level and message framing in influencing consumer efficacy and conservation behaviors. *J Mark Res* 2015;**48**:472–85.
50. Lee AY, Keller PA, Sternthal B. Value from regulatory construal fit: the persuasive impact of fit between consumer goals and message concreteness. *J Mark Res* 2010;**36**:735–47.
51. Rogers RW. A protection motivation theory of fear appeals and attitude change. *J Psychol* 1975;**91**:93–114.
52. Liang H, Xue Y. Understanding security behaviors in personal computer usage: a threat avoidance perspective. *J Assoc Inf Syst* 2010;**11**:394–413.
53. Faul F, Erdfelder E, Buchner A. *et al.* Statistical power analyses using G*Power 3.1: tests for correlation and regression analyses. *Behav Res Methods* 2009;**41**:1149–60.
54. Payne SL. Are open-ended questions worth the effort? *J Mark Res* 1965;**2**:417–8.
55. Reja U, Manfreda KL, Hlebec V. *et al.* Open-ended vs. close-ended questions in web questionnaires. *Dev Appl Stat* 2003;**19**:159–77.
56. Vallacher RR, Wegner DM. Levels of personal agency: individual variation in action identification. *J Pers Soc Psychol* 1989;**57**:660–71.
57. Witte K. Predicting risk behaviors: development and validation of a diagnostic scale. *J Health Commun* 1996;**1**:317–42.
58. Lwin MO, Stanaland AJS, Chan D. Using protection motivation theory to predict condom usage and assess HIV health communication efficacy in Singapore. *Health Commun* 2010;**25**:69–79.
59. Capar M, Ittersum Kv. Intention-behavior consistency: the effect of time perspective. In: McGill AL, Shavitt S (eds). *NA – Advances in Consumer Research*. Duluth, MN: Association for Consumer Research, 2009, 721.
60. Ajzen I. The theory of planned behavior. *Organ Behav Hum Decis Process* 1991;**50**:179–211.
61. Johns G, Miraglia M. The reliability, validity, and accuracy of self-reported absenteeism from work: a meta-analysis. *J Occup Health Psychol* 2015;**20**:1–14.
62. McKenna H, Treanor C, O'Reilly D. *et al.* Evaluation of the psychometric properties of self-reported measures of alcohol consumption: a COSMIN systematic review. *Subst Abuse Treat Prev Policy* 2018;**13**:1–19.
63. Cohen J. *Statistical Power Analysis for the Behavioral Sciences*. Mahwah, NJ: Lawrence Earlbam Associates, 1988.
64. Hayes AF. *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*. New York, NY: Guilford Press, 2017.
65. Hayes AF, Rockwood NJ. Conditional process analysis: concepts, computation, and advances in the modeling of the contingencies of mechanisms. *Am Behav Sci* 2020;**64**:19–54.
66. Holland SJ, Shore DB, Cortina JM. Review and recommendations for integrating mediation and moderation. *Organ Res Methods* 2017;**20**:686–720.
67. Zwickle A, Wilson RS. Construing risk: implications for risk communication. In: Arvai J, Rivers Ls (eds). *Effective Risk Communication*. London: Routledge, 2013, 216–29.
68. Van Voorst R, Wisner B, Hellman J. *et al.* Introduction to the "risky everyday". *Disaster Prev Manag* 2015;**24**.
69. Tsai HYS, Jiang M, Alhabash S. *et al.* Understanding online safety behaviors: a protection motivation theory perspective. *Comput Secur* 2016;**59**:138–50.
70. Hallam C, Zanella G. Online self-disclosure: the privacy paradox explained as a temporally discounted balance between concerns and rewards. *Comput Hum Behav* 2017;**68**:217–27.
71. Chandran S, Menon G. When a day means more than a year: effects of temporal framing on judgments of health risk. *J Consum Res* 2004;**31**:375–89.
72. Quayyum F. Cyber security education for children through gamification: challenges and research perspectives. *International Conference in Methodologies and Intelligent Systems for Technology Enhanced Learning*, Springer, 2020, 258–63.
73. Abraham S, Chengalur-Smith I. Evaluating the effectiveness of learner controlled information security training. *Comput Secur* 2019;**87**:1–12.
74. Tsai CI, McGill AL. No Pain, no gain? How fluency and construal level affect consumer confidence. *J Consum Res* 2011;**37**:807–21.
75. Nisbett RE, Wilson TD. Telling more than we can know: verbal reports on mental processes. *Psychol Rev* 1977;**84**:231.
76. Blum SC, Silver RC, Poulin MJ. Perceiving risk in a dangerous world: associations between life experiences and risk perceptions. *Soc Cogn* 2014;**32**:297–314.
77. Addae JH, Brown M, Sun X. *et al.* Measuring attitude towards personal data for adaptive cybersecurity. *Inf Comput Secur* 2017;**25**:560–79.
78. Proctor RW, Chen J. The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. *Hum Factors* 2015;**57**:721–7.
79. Ben-Asher N, Gonzalez C. Effects of cyber security knowledge on attack detection. *Comput Hum Behav* 2015;**48**:51–61.
80. Kertzer JD. Re-assessing elite-public gaps in political behavior. *Am J Pol Sci* 2020:1–15.
81. Pigman L. Russia's vision of cyberspace: a danger to regime security, public safety, and societal norms and cohesion. *J Cyber Policy* 2019;**4**:22–34.
82. Neiman AB, Ruppar T, Michael H. *et al. CDC grand rounds: improving medication adherence for chronic disease management—innovations and opportunities*. https://www.cdc.gov/mmwr/volumes/66/wr/mm6645a2.htm (2021, August 25).