12-12-2020

Toward Conceptualizing Perplexity in Cybersecurity: An Exploratory Study

Malte Greulich

Sebastian Lins

Daniel Pienta

Jason Bennett Thatcher

Ali Sunyaev

Toward Conceptualizing Perplexity in Cybersecurity: An Exploratory Study

Malte Greulich[1]
Department of Economics and Management, Karlsruhe Institute of Technology,
Karlsruhe, Baden-Württemberg, Germany

Sebastian Lins
Department of Economics and Management, Karlsruhe Institute of Technology,
Karlsruhe, Baden-Württemberg, Germany

Daniel Pienta
Hankamer School of Business, Baylor University,
Waco, Texas, United States

Jason Bennett Thatcher
Fox School of Business, Temple University,
Philadelphia, Pennsylvania, United States

Ali Sunyaev
Department of Economics and Management, Karlsruhe Institute of Technology,
Karlsruhe, Baden-Württemberg, Germany

ABSTRACT

As cybersecurity threats evolve and cybersecurity teams update digital security infrastructures, employees often get perplexed by the threats and corresponding countermeasures. Drawing insight from a literature review and a qualitative exploratory study with 85 participants, this paper defines *cybersecurity perplexity*, a paradoxical psychological state that individuals experience when facing adverse cybersecurity conditions in the workplace (e.g., ambiguous or surprising security policies or awareness of cybersecurity threats). Cybersecurity perplexity has three interrelated dimensions: cybersecurity confusion, cybersecurity pressure, and cybersecurity response uncertainty. Central to cybersecurity perplexity is that individuals are confused and uncertain about how to respond, yet feel pressure to act, to adverse cybersecurity conditions. Our data suggests that perplexity merits researchers' attention because it can arise from myriad cybersecurity conditions that individuals frequently

[1] Corresponding author. greulich@kit.edu +49 721 608 45635

encounter in the workplace. We contribute to the cybersecurity literature by providing a conceptualization of cybersecurity perplexity and initiating a discussion about this novel phenomenon encouraging future research.

Keywords: cybersecurity perplexity, information security, cybersecurity, confusion

INTRODUCTION

> *What perplexed me is that if an e-mail looks legitimate, which phishing e-mails often do, how do you avoid opening it in the first place? You need [to] open it and look at its contents to realize that it's a scam sometimes. I realized I was perplexed because I had questions about how to handle those e-mails the right way.*
> (Study participant after completing a security training)

Cybercrime remains a pressing issue for information technology (IT) managers and employees alike. As cybersecurity threats evolve and organizations' cybersecurity teams update digital security infrastructures, individual employees often get perplexed by the threats and corresponding countermeasures (e.g., anti-malware software, multi-factor authentication, or encryption) (Baskerville et al. 2018). In its general sense, perplexity is a state of confusion in which individuals cannot make sense of or solve situational demands (Merriam-Webster 2020). The study participant's quote above illustrates that organizations' security countermeasures can perplex individuals because they are difficult to understand or apply in day-to-day work. Similarly, an alert of anti-malware software informing a user about a severe malware infection can perplex users because users might be confused about the cause of the infection, the potential consequences, or what they should do to stop the infection.

While cybersecurity's practical complexities and ambiguity provide many opportunities for individuals to get perplexed, cybersecurity research is void of a conceptualization or a definition of perplexity. Studying perplexity in the cybersecurity context offers two important insights for cybersecurity researchers and practitioners. On the one hand, being perplexed can

hold back employees from acting securely, such as complying with an information security policy or responding to emerging cybersecurity threats appropriately, because their minds are occupied and unable to respond to the situation as needed. On the other hand, being perplexed can also lead employees to pause and become more mindful by seeking information to move past a state of perplexity. Better understanding of why perplexity emerges and how to mitigate its adverse outcomes, therefore, offers abundant opportunities for cybersecurity research. Second, and equally important, neither the cybersecurity nor the broader information systems (IS) literature has examined perplexity resulting in a lack of understanding of this important concept.

Hence, we ask: *How can perplexity be conceptualized in cybersecurity?*

In this paper, we develop a conceptual definition of *cybersecurity perplexity*, identify its core dimensions (i.e., confusion, pressure, and response uncertainty), and derive a tentative conceptual model that positions cybersecurity perplexity in relation to potential antecedents (i.e., adverse cybersecurity conditions) and consequences (i.e., individuals' behavioral, cognitive or emotional coping responses). To do so, we triangulate across a cross-disciplinary review of the literature and data drawn from 85 participants who describe 204 perplexing situations. This paper contributes to research by providing a stage for discussing perplexity in the cybersecurity community and providing an initial conceptualization of cybersecurity perplexity necessary to study this novel phenomenon.

LITERATURE REVIEW

The term "perplexity" as used in everyday language, conveys a state in which people are "confused because something is difficult to understand or solve" (Merriam-Webster 2020). Imagine the mental state of a doctor trying to make a time-sensitive diagnosis on a rare and complex medical condition of a patient, or a nuclear power plant operator trying to understand

and resolve an incomprehensible notification of a critical system failure. Perplexed individuals have not yet formed opinions because they make sense of what is happening and cannot decide for a course of action. While perplexed individuals may eventually decide on a course of action, such as the doctor running additional tests, or the operator identifying the appropriate emergency protocol, being perplexed disrupts routines and planned courses of action, typically delaying any action taking place, and potentially leading to adverse consequences, such as the death of a patient or a reactor meltdown, or positive consequences, such as identifying a solution or workaround to a problem.

To understand academic use of the term "perplexity", we conducted a keyword search for "perplexity" in titles, abstracts, and keywords in seven major scientific databases: AIS Electronic Library, ACM Digital Library, EBSCOhost, Emerald Insight, IEEE Xplore Digital Library, ProQuest, and ScienceDirect. This open search yielded 1200 results. We narrowed our search by focusing on articles that use perplexity to denote an individual's mental state, while a vast majority of articles used the term to refer to a statistical metric to evaluate probabilistic models (Jelinek et al. 1977) or used it without going further into the concept. By screening titles, abstracts, and keywords, we identified ten relevant articles. We complemented the results with a search on Google Scholar using a snowballing approach (Wohlin 2014) to broaden our literature base. At this point, we also included articles on confusion, paralysis, bewilderment, or stress, as related terms. Additionally, we conducted individual literature searches on concepts relevant to perplexity, including confusion and stress. This snowballing approach resulted in 59 relevant articles.

Our analysis of the literature revealed much conceptual ambiguity and diverse use of the term "perplexity". In psychology, perplexity is associated with a lack of automatic grasp of

meaning that can be symptomatic for severe mental disorders (e.g., Parnas et al. 2005). In marketing and consumer research, researchers used the term to describe individuals' information processing and decision making, such as green consumers' being perplexed by environmental information (Moisander 2007). We found that perplexity has also been used interchangeably with "confusion" to examine the impairment of decision-making abilities (Walsh and Mitchell 2010). Likewise, communications researchers used the term to illustrate convoluted meanings of risk information (Jardine and Hrudey 1997). Finally, in an education and learning context, we found that the state of perplexity had been studied as a trigger of reflective thinking and learning (e.g., Dewey 1997).

While IS researchers have not directly studied perplexity as a mental state, they have long recognized that feeling overwhelmed or uncertain influences IT users' behavior. For example, IS research finds that information overload has adverse consequences in decision making (Eppler and Mengis 2004), that stress caused by IT use leads to exhaustion and burnout (Tarafdar et al. 2019), or that security-related stress promotes security policy violations (D'Arcy et al. 2014).

To advance understanding of perplexity's implications for cybersecurity, we used our literature review to inform a qualitative exploratory study in order to develop a domain-specific conceptualization of perplexity relevant to cybersecurity. Such a conceptualization is essential because it could help explain why employees become perplexed by, for example, multi-step procedures necessary to configure the multi-factor-authentication on a personal mobile device.

METHOD

Data Collection

Informed by our literature review, we drew on guidelines suggested by MacKenzie and Podsakoff (2011) to develop a contextualized, conceptual, definition of cybersecurity perplexity.

In particular, we used a qualitative online survey in which we recruited participants from Amazon's Mechanical Turk (MTurk), asking them to describe cybersecurity-related situations in which they got perplexed. MTurk is a suitable platform for reaching cyber-savvy employees, which aligns with our survey setting and objective. We restricted potential participants to those with a high reputation (at least 95% approval ratings and at least 5,000 conducted tasks) to ensure high data quality. Also, we restricted participation to the US to reduce cultural biases. Research has demonstrated that survey data collected using MTurk has high reliability and provide high-quality data comparable to student samples or online convenience samples (e.g., Lowry et al. 2016).

To focus attention on perplexity in the cybersecurity context, we provided participants with a short introduction to the survey (i.e., explaining that we are interested in participants' experiences with cybersecurity in a work context), and more importantly, a working definition and related perplexity examples based on insights from the literature review. Subsequently, we asked three questions about situations in which they felt perplexed: 1) *What situation made you feel perplexed about cybersecurity?* 2) *How did you realize that you were perplexed?* and 3) *What were the consequences (e.g., for yourself or others) of you being perplexed?* We asked participants to describe three scenarios using these questions. In total, we obtained 110 complete responses. Excluding 25 invalid responses (e.g., participants who rushed through the survey or provided low-quality answers) yielded a final sample of 85 participants who provided 204 scenario descriptions. On average, each participant reported 2.4 scenarios. More men (31% females) participated in our survey, and participants were, on average, 35 years old. Most participants were employed full-time (5% part-time) and spend on average 70% of a typical working day using the organization's computer systems. They worked on average six years for

their current employer in information technology (18%), sales (16%), banking/finance (16%), academic (15%), health care (8%), manufacturing (7%), or other industries (20%).

Data Analysis

We followed a four-step approach to analyze the scenario descriptions provided by participants and to derive a conceptualization of cybersecurity perplexity. First, open coding was used to process the scenarios and label concepts in the data (Corbin and Strauss 2015). One author analyzed each scenario in detail and derived initial dimensions, antecedents, and outcomes of cybersecurity perplexity. The procedure resulted in 76 open codes. For example, the author labeled the statement, *"I was confused by the software and how it worked"* as *"confused"*, and noted it as a potential core dimension of cybersecurity perplexity.

Second, we aggregated codes, compared the emergence of similar codes across scenarios, and discussed whether these relate to perplexing situations. Particularly, we focused on what notion is at the core of being perplexed. By comparing identified codes across the scenarios, we were able to identify confusion and response uncertainty as candidate dimensions.

Third, we returned to the literature to increase our understanding of the coded concepts. For example, we looked into research on "response uncertainty" to better understand the concept and related the emotion of "feeling helpless" to this dimension. We also noted "surprise" as a potential antecedent of confusion, as argued by prior research (D'Mello and Graesser 2012). Additionally, we compared the scenarios with the literature about perplexity. For example, we identified productive responses, such as "doing more research" to overcome the perplexing situation, which aligns with the educational literature (e.g., Dewey 1997).

Fourth, with our updated understanding of coded concepts, we returned to the scenarios, following the selective coding paradigm (Corbin and Strauss 2015). This step's objective was to

validate the identified concepts and ensure that the concepts still relate to the empirical data. During this final coding step, we observed that genuinely perplexing situations are characterized by individuals being confused and uncertain, yet feeling a pressing need to act. We, therefore, added "pressure" as a core dimension of cybersecurity perplexity. With this new insight, we took a final look at related research to increase our understanding of the concept of pressure. Appendix A illustrates our coding results.

CONCEPTUALIZATION OF CYBERSECURITY PERPLEXITY

Our qualitative coding and data analysis process suggests that *cybersecurity perplexity* relates to three components (Table 1): 1) cybersecurity perplexity reflects an individual's paradoxical *psychological state* with the three interrelated dimensions of *cybersecurity confusion*, *cybersecurity pressure*, and *cybersecurity response uncertainty*, 2), is evoked by *adverse cybersecurity conditions*, and 3), causes an individual's *behavioral*, *cognitive or emotional coping responses* that influence *security-related intentions or behaviors*. Figure 1 depicts a tentative conceptual model. We explain each component in the following paragraphs.

Concept	Definition	Related concepts
Cybersecurity perplexity	The paradoxical psychological state that individuals experience when facing adverse cybersecurity conditions in the workplace.	**This study**
Adverse cybersecurity conditions	An individual's perception of IS characteristics, cybersecurity threats, or organizational cybersecurity countermeasures that can evoke cybersecurity perplexity.	Technology environmental conditions (e.g., Tarafdar et al. 2019)
Cybersecurity confusion	An individual's failure to correctly interpret adverse cybersecurity conditions (adapted from Turnbull et al. 2000).	Consumer confusion (e.g., Turnbull et al. 2000; Walsh and Mitchell 2010)
Cybersecurity pressure	An individual's perceived external or internal pressure to act upon adverse cybersecurity conditions.	Mandatory IT use (e.g., Bhattacherjee et al. 2018; Boss et al. 2009)
Cybersecurity response uncertainty	An individual's lack of knowledge of response options for coping with potentially adverse cybersecurity conditions and/or an inability to predict the likely consequences of a chosen response (adapted from Milliken 1987).	Response uncertainty (e.g., Milliken 1987); uncertainty about information security investments (Shao et al. 2020)

Table 1. Concept Definitions

Definition of Cybersecurity Perplexity

We define *cybersecurity perplexity* as a paradoxical psychological state that individuals experience when facing adverse cybersecurity conditions in the workplace. *Adverse cybersecurity conditions* refer to an individual's perception of IS characteristics, cybersecurity threats, or organizational security countermeasures that can evoke cybersecurity perplexity. Adverse cybersecurity conditions may include the perception of invasive IS practices, ambiguous or surprising information security policies, or awareness of cybersecurity threats. Central to our conceptualization of cybersecurity perplexity is that individuals are confused and uncertain about responding to adverse cybersecurity conditions, yet feel pressure to act or respond. For example, when an individual receives a notification that malware has infected her system, she might be confused about how it happened or what the consequences are. Yet, she feels pressure to deal with the threat in some way. The perception of contradictory demands evoked by cybersecurity conditions reveals paradoxical tensions that individuals cannot resolve quickly.

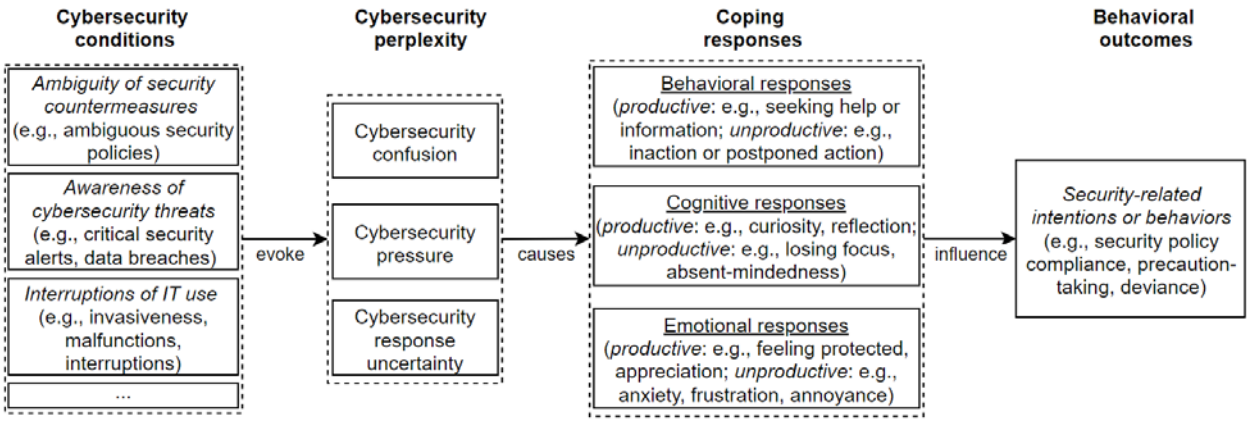

Figure 1. A tentative conceptual model for studying cybersecurity perplexity

Cybersecurity Confusion

Cybersecurity confusion refers to an individual's failure to correctly interpret adverse cybersecurity conditions (Turnbull et al. 2000). Confusion is associated with a momentarily or longer-lasting cognitive impasse (e.g., *"I run up against a wall of not understanding about*

what's happening" (scenario #193), or "*One day the 2FA stopped working for me, and I couldn't figure out why.*" (#246)). Individuals might not understand why they were attacked, how the attack worked, or what the attack means for themselves or others (e.g., "*I did not understand how the virus could spread to the entire network*" (#88)). Likewise, individuals might get confused by inconclusive security practices (e.g., "*I did not understand why a VPN [Virtual Private Network] was important and how it was used to protect [organizational] information.*" (#84)) or weak usability of protective technologies (e.g., "*I couldn't figure out how to work the [antivirus] software.*" (#25)).

Cybersecurity confusion is an essential dimension of cybersecurity perplexity because it captures how individuals do not entirely understand what the requirements imposed by adverse cybersecurity conditions (e.g., ambiguous security policies) mean for themselves or others.

Cybersecurity Pressure

Cybersecurity pressure refers to an individual's perceived external or internal pressure to act upon adverse cybersecurity conditions. Concerning external pressure, the perception of cybersecurity threats (e.g., a malicious file detected by the antivirus software (#182)) can urge individuals to seek support from coworkers or IT staff (e.g., "*I was forced to reach out for help and explain the situation to others.*" (#182)). Besides, security training also calls upon individuals to act securely, such as to avoid clicking on links in e-mails (e.g., "*Being told not to click on any links whatsoever in any e-mails.*" (#193)) or installing software on their own (#329). Correspondingly, research finds that threat perceptions can motivate threat avoidance behaviors (Liang and Xue 2009) and that security appeals can promote secure behaviors when working with IT (Boss et al. 2009; Johnston and Warkentin 2010).

In contrast, internal pressures can also make individuals engage in secure behaviors (e.g., "*I wanted to know more […] I wanted to know about how concerned we should be.*" (#212), or "*[cybersecurity] made me have a greater appreciation for the work that went into it. It also made me want to learn more.*" (#217)). Research supports this view by finding that appeals to intrinsic motivation (Menard et al. 2017), or affective commitment to the organization (Posey et al. 2015) can promote secure behaviors.

Common to all examples is that individuals feel some degree of pressure to respond to cybersecurity conditions that require them to act. However, due to cybersecurity perplexity, taking immediate action is often impossible, which creates strain for the individual.

Cybersecurity Response Uncertainty

Cybersecurity response uncertainty refers to situations in which an individual is unsure how to respond adequately to adverse cybersecurity conditions to avoid risks or harm to themselves or others. Response uncertainty may include a lack of knowledge of response options (e.g., "*I never know what is the best practice [for managing passwords]*" (#23)) and/or the inability to predict the likely consequences of a chosen response (e.g., "*It is clear there is no one right way to remember the hundreds of passwords needed in today's world.*" (#23)) (Milliken 1987). For instance, individuals might be unable to predict a chosen response's actual consequence because of a lack of knowledge or understanding (e.g., that a weak password can be exploited by cybercriminals). Response uncertainty is likely to occur when individuals perceive a need to act (Milliken 1987), such as responding to an imminent cybersecurity threat. Cybersecurity response uncertainty may also reflect an emotional state of helplessness when individuals perceive a low potential to cope with adverse cybersecurity conditions (e.g., "*It seems if a hacker wants to hack you, there's little you can do beyond disconnecting from the*

internet." (#47)) (Lazarus 1991). Overall, our results suggest that, when individuals are perplexed, they seem to lack a clear understanding of suitable options to handle adverse cybersecurity conditions, which may inhibit a mindful response.

Consequences of Cybersecurity Perplexity

Our analysis revealed that participants respond in productive or unproductive ways to cybersecurity perplexity. We distinguish between behavioral, cognitive, and emotional coping responses to cybersecurity perplexity. *Productive behavioral responses* include individuals *seeking information* (e.g., doing research, learning about the perplexing situation (#25)), *seeking help* (e.g., ask others for help with the perplexing situation (#182)), or *behavioral change* (e.g., more cautious future use of sensitive information (#73)). On the contrary, *unproductive behavioral responses* included *inaction or reduced behavior* (e.g., no reaction or postponed action (#107)) as well as *insecure behaviors* (e.g., answering a phishing e-mail (#93), writing down passwords (#253)).

Productive cognitive responses included individuals' getting *curious and thinking deeply* about the perplexing situation (e.g., #34), leading to more clarity and understanding of the situation, or *reflecting on past behaviors* similar to the current situation (e.g., #40). *Unproductive cognitive responses* included *losing focus on the task* interrupted by the perplexing situation or *being busy or absent-minded* about the situation for longer periods (e.g., #270).

Productive emotional responses to the perplexing situation included positive emotions such as feeling protected by cybersecurity countermeasures and appreciation for the cybersecurity teams (#217). *Unproductive emotional responses* included, anxiety, frustration, worry, or annoyance (e.g., #181, #23, #84).

DISCUSSION

Our preliminary, qualitative, study suggests that cybersecurity perplexity merits attention. First, cybersecurity perplexity is a paradoxical state because individuals must cope with adverse cybersecurity conditions that call for action; at the same time, they are confused and feel uncertain about how to respond. As long as individuals cannot resolve this contradiction (e.g., through seeking help from a coworker or the IT department), the paradoxical state persists, resulting in adverse consequences, such as insecure individual behaviors.

Second, not every confusing situation renders each individual perplexed or unable to act. Consider an organization issuing to its employees a mandatory security policy on how to handle phishing e-mails. For many employees, the mandatory security policy may seem confusing due to its unfamiliar and ambiguous terminology. However, they are be able to understand the policy and identify and implement necessary changes to their work routines. Following this example, the mandatory policy may not perplex these employees because they do not feel uncertain about what to do, or experience substantial pressure to take the requested actions. For other employees, the mandatory policy may leave them confused and uncertain about what the policy change means for them while feeling pressured to react upon the mandatory policy. These employees may be momentarily paralyzed by the contradiction between the need for action and their inability to decide on a course of action. Cybersecurity perplexity's uniqueness is the simultaneous occurrence of confusion, pressure, and response uncertainty. In perplexing situations, individuals are, at least momentarily and perhaps longer, unable to resolve the discrepancy between what they can do and what they are expected to do.

Third, while the undertone of "perplexity" is negative, our data suggest that this state can lead to positive and productive outcomes. In particular, cybersecurity perplexity can lead to

positive outcomes because it can stimulate reflective thinking (Dewey 1997). For example, being perplexed by a cybersecurity threat can trigger an appraisal process in which individuals assess the potential risk from the cybersecurity threat, identify a viable strategy to deal with it, and thereby lower the risk.

Theoretical and Practical Implications

Our study makes three contributions to the literature. First, for cybersecurity and IS research, we draw attention to the importance of studying perplexity and its relevance to understanding how individuals respond to threats and corresponding organizational countermeasures. Second, we contribute to the cybersecurity literature by providing an initial conceptualization of cybersecurity perplexity. Third, we provide a domain-specific conceptualization that may prove valuable to study similar phenomena in other contexts (e.g., perplexity related to the use of protective measures in healthcare or perplexity related to artificial intelligence).

Our study offers managers two important takeaways. First, the insights suggest that cybersecurity threats and countermeasures in the workplace can be overwhelming for employees. In particular, our study reveals that many everyday cybersecurity-related situations are perplexing for employees because individuals perceive them as confusing, uncertain, and demanding. While such perceptions can evoke productive ways of coping with perplexing situations, they might also negatively influence security behaviors. Second, the insights suggest that managers can resolve perplexity by providing sufficient guidance or help for situations they recognize to cause employees to become perplexed. For instance, Jensen et al. (2017) find that a mindfulness-based training approach that increases participants' contextual awareness and

attention can help to avoid phishing attacks. Such a mindfulness-based training approach that guides employees in these situations could complement existing security training and policies.

Limitations and Future Research

This paper has limitations that warrant future research. First, while we outlined cybersecurity conditions that can evoke perplexity and identified potential cybersecurity perplexity outcomes, further studies that corroborate this research are necessary. For instance, we still lack an understanding of how individuals respond to perplexing situations and what factors influence this response (e.g., distal personality traits or more proximal situational factors). Similarly, future research should look at ways to counteract negative outcomes of cybersecurity perplexity and to foster positive ones.

Second, while we examined cybersecurity perplexity in a work context, perplexity levels may differ for employees in different settings. For instance, a cybersecurity savvy employee working in an incident response team might be less perplexed by a cyberattack than a sales employee with limited cybersecurity knowledge and experience. Similarly, cybersecurity perplexity might also transcend beyond the work context into a personal context. Therefore, we suggest that future research examine perplexity in different contexts and settings and to analyze how these contexts and settings affect one another (e.g., how does resolving perplexing situations at home affect the way individuals cope with perplexing situations at work?).

Third, research lacks a measurement instrument for cybersecurity perplexity to empirically validate its influence in future studies. Therefore, following the thorough conceptual definition of cybersecurity perplexity, we plan to develop, evaluate, refine, and validate a measurement scale for cybersecurity perplexity (MacKenzie and Podsakoff 2011).

CONCLUSION

This study proposes that cybersecurity perplexity, a novel concept, refers to a paradoxical psychological state that individuals experience when facing adverse cybersecurity conditions in the workplace. Insights from a qualitative exploratory study suggest that cybersecurity perplexity merits attention by the cybersecurity community because cybersecurity perplexity seems to influence positive and negative security-relevant outcomes that demand further research.

REFERENCES

Baskerville, R., Rowe, F., and Wolff, F.-C. 2018. "Integration of Information Systems and Cybersecurity Countermeasures," *ACM SIGMIS Database* (49:1), pp. 33-52.

Bhattacherjee, A., Davis, C. J., Connolly, A. J., and Hikmet, N. 2018. "User response to mandatory IT use: a coping theory perspective," *European Journal of Information Systems* (27:4), pp. 395-414.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security," *European Journal of Information Systems* (18:2), pp. 151-164.

Corbin, J., and Strauss, A. 2015. *Basics of Qualitative Research*: *Techniques and Procedures for Developing Grounded Theory*, Thousand Oaks, CA: Sage Publications.

D'Mello, S., and Graesser, A. 2012. "Dynamics of affective states during complex learning," *Learning and Instruction* (22:2), pp. 145-157.

D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285-318.

Dewey, J. 1997. *How we think*, Mineola, NY: Dover Publications.

Eppler, M. J., and Mengis, J. 2004. "The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, MIS, and Related Disciplines," *The Information Society* (20:5), pp. 325-344.

Jardine, C. G., and Hrudey, S. E. 1997. "Mixed Messages in Risk Communication," *Risk Analysis* (17:4), pp. 489-498.

Jelinek, F., Mercer, R. L., Bahl, L. R., and Baker, J. K. 1977. "Perplexity—a measure of the difficulty of speech recognition tasks," *The Journal of the Acoustical Society of America* (62:1), S63-S63.

Jensen, M. L., Dinger, M., Wright, R. T., and Thatcher, J. B. 2017. "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," *Journal of Management Information Systems* (34:2), pp. 597-626.

Johnston, and Warkentin 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Lazarus, R. S. 1991. *Emotion and adaptation*, Oxford University Press.

Liang, H., and Xue, Y. 2009. "Avoidance of information technology threats: a theoretical perspective," *MIS Quarterly* (33:1), pp. 71-90.

Lowry, P. B., D'Arcy, J., Hammer, B., and Moody, G. D. 2016. ""Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels," *The Journal of Strategic Information Systems* (25:3), pp. 232-240.

MacKenzie, and Podsakoff 2011. "Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques," *MIS Quarterly* (35:2), pp. 293-334.

Menard, P., Bott, G. J., and Crossler, R. E. 2017. "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory," *Journal of Management Information Systems* (34:4), pp. 1203-1230.

Merriam-Webster 2020. *Definition of Perplexed*. https://www.merriam-webster.com/dictionary/perplexed. Accessed 21 February 2020.

Milliken, F. J. 1987. "Three Types of Perceived Uncertainty about the Environment: State, Effect, and Response Uncertainty," *Academy of Management Review* (12:1), pp. 133-143.

Moisander, J. 2007. "Motivational complexity of green consumerism," *International Journal of Consumer Studies* (31:4), pp. 404-409.

Parnas, J., Møller, P., Kircher, T., Thalbitzer, J., Jansson, L., Handest, P., and Zahavi, D. 2005. "EASE: Examination of Anomalous Self-Experience," *Psychopathology* (38:5), pp. 236-258.

Posey, C., Roberts, T. L., and Lowry, P. B. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," *Journal of Management Information Systems* (32:4), pp. 179-214.

Shao, X., Siponen, M., and Liu, F. 2020. "Shall we follow? Impact of reputation concern on information security managers' investment decisions," *Computers & Security* (97).

Tarafdar, M., Cooper, C. L., and Stich, J.-F. 2019. "The technostress trifecta - techno eustress, techno distress and design: Theoretical directions and an agenda for research," *Information Systems Journal* (29:1), pp. 6-42.

Turnbull, P. W., Leek, S., and Ying, G. 2000. "Customer Confusion: The Mobile Phone Market," *Journal of Marketing Management* (16:1-3), pp. 143-163.

Walsh, G., and Mitchell, V.-W. 2010. "The effect of consumer confusion proneness on word of mouth, trust, and customer satisfaction," *European Journal of Marketing* (44:6), pp. 838-859.

Wohlin, C. 2014. "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, London, UK, pp. 1-10.

APPENDIX A – ILLUSTRATIVE QUOTES FOR CYBERSECURITY PERPLEXITY

Dimensions	Illustrative quotes
Cybersecurity confusion	(1) "**I am always perplexed by the complexities of online privacy**. From using incognito browsers to ads for VPN, ad blockers, and best practices for keeping your information safe it just seems impossible to keep up with. Part of me wonders if I am even able to slow it down at all. It is when I am not certain how to proceed. I don't know for sure which settings I want, or which devices/services I want to use." (#22) (2) "**I had gotten some spam, phishing e-mail to my work inbox and I was confused about.** I order supplies for my team at the office, and the e-mail dealt with an invoice number so I thought it might have been legit." (#100) (3) "**I felt perplexed when I did not know what a file was that the antivirus software identified as a threat.** I was concerned if I put it there or how it got there. I realized I did not recognize the name of the file and it was worrisome because I should know what is on the computer and an unrecognized file could be a sign of an intrusion." (#182) (4) "A sudden increase in the amount of information being downloaded/uploaded to/from my computer. I monitor the amount of traffic on my machine closely, but can't determine the sources (because I'm not an expert in this area). **I run up against a wall of not understanding about what's happening.**" (#193)
Cybersecurity pressure	(5) "I work for a research study, and data from MRI scans that we collect gets sent to a separate secure server. **We have to connect to that server from our own machines using a ssh protocol.** I don't have any background in using "ftp" and "ssh" or any of those secure file transfer methods, so when I was initially asked to do so, I was perplexed. I realized I was perplexed because I didn't understand the initial instructions and needed someone to walk me through it step by step in more detail. I had to seek help with getting the task done from our computing support staff." (#49) (6) "I felt really perplexed when my antivirus software alerted me that it caught an attempted intrusion into my computer. However, when I looked into the matter, the program the antivirus software flagged as malware wasn't. It was a piece of software that comes in packaged with Windows 10, at least that is what I learned looking up the software that was flagged. **I read online that this piece of software is essential for Windows to function properly yet my antivirus software was urging me to delete the software from my system immediately.** I lost about an hour of work trying to figure out if it was safe to delete or not delete this program." (#151) (7) "**I had to use a VPN.** I did not know how to set it up or get one! I was not able to log in and had a confusing call with IT." (#230)
Cybersecurity response uncertainty	(8) "**The best way to save, store and remember passwords always perplexes me.** With all of the rules for character counts and types with the frequency of changes I never know what is the best practice. Should I use a password "keeper", the one built into my browser, should I write them down somewhere? I am always frustrated trying to remember little changes in password rules." (#23) (9) "I felt perplexed about information security once when I was using an antivirus software. **I was confused about what I was supposed to be doing and how to use it. I realized I was perplexed because I couldn't figure out how to work the software."** (10) "It seems if a hacker wants to hack you, there's little you can do beyond disconnecting from the internet." (#47) (11) "As part of our annual training, my company has us complete one on privacy and security. The training discussed how to avoid phishing attacks (i.e. not to open e-mails, to report the e-mails). **What perplexed me is that if an e-mail looks legitimate, which phishing e-mails often do, how do you avoid opening it in the first place?** You need open it and look at its contents to realize that it's a scam sometimes. **I realized I was perplexed because I had questions about how to handle those e-mails the right way.**" (#50)
Note: Emphasis added in quotes to illustrate the related perplexity dimension.	