Increased remote work : Information security awareness, knowledge and Uncertainty

Wilfrid Azan, Bettina Schneider, Silvester Ivanaj, Marc Gilg

INCREASED REMOTE WORK :

INFORMATION SECURITY AWARENESS, KNOWLEDGE AND UNCERTAINTY”

Research Paper

Abstract— Is risk awareness a factor that influences the risk of IT system usage? What role does cybersecurity training and security awareness play in the context of COVID-19 pandemic restrictions? In this contribution, the authors focus on prospect theory, as it addresses the concept of uncertainty in combination with risk perception in human decision-making. The concept of social engineering and the relevance of cybersecurity awareness are described in the following sections. The data collected in our study strongly confirm the increased dependency of users on their devices and Internet connectivity. The study also strongly confirms the role of the cybersecurity training and security awareness play in the context of COVID-19 pandemic restrictions. A confirmation of cognitive framing in man-machine interaction reduces the risks in social engineering situations. We find the three phases of the choice process (choice rule, framing and evaluation) which appear in Kahneman & Tversky (1986) and the results, are relevant for the decision. We confirm the evaluation phase, the user focuses on the decision, probably with caution and increased concentration and slow thinking. Although not very formal, framing theory focuses on the rules that govern the representation of acts, outcomes, and contingencies (Tversky & Kahneman, 1986). Social engineering offers a rich context of observation of computational social systems.

Keywords— knowledge, social engineering, information system

1. INTRODUCTION

During the COVID-19 pandemic, the number of cyberattacks in developed countries exploded (public hospitals, companies and administration). As a result, many companies turned to remote work models. This radical change in the way companies operate has often been rushed in order to respond to the government’s decision to lockdown employees. The result has been an increase in the use of new technologies, fostering the digitalization of documents and procedures. The Internet has enabled millions of people to access countless pieces of information over the last 25 years. Its development has also generated a new form of delinquency: cybercrime, and among its modus operandi social engineering. Even if the efficiency of security measures to protect sensitive information is increasing, users remain vulnerable to manipulation. Consequently, the human element remains a weak link in systems tending toward maximum security. For decades, uncertainty has been considered in economic theory. Prospect theory, as one major stream, has set theoretical ground to explain the perception of risks and the evaluation of dangerous situations. The interaction of humans and machines is of course included in the scope of this theory. Among these interactions are cyberattacks and social engineering. Early studies of decision-making under uncertainty focused on Bayesian learning (subjective expected utility; Savage, 1954), game theory (von Neumann and Morgenstern, 1944) and cognitive and behavioural science (e.g. prospect theory; Kahneman and Tversky, 1979). Arrow (1951, p. 404) describe this research landscape as comprising “a set of conceivable actions that an individual might take, each leading to certain consequences” — that is, decisions where the option and outcome sets are closed.

Cyberattacks and especially social engineering occur when users of individual or collective information systems are in a state of psychological weakness, fear, anxiety for loved ones, and sometimes distress. An attack targets this weakness by using various manipulation techniques to obtain sensitive information. The field of social engineering is still in its infancy with respect to formal definitions and attack models (Schneider et al., 2020; Disparte and Furlow, 2017; SANS Institute, 2018; Sawyer and Hancock, 2018; Blau, 2017; see the effectiveness of security awareness programs, e.g. Ki-Aries and Faily, 2017). Information security awareness among employees and, in particular, managerial information security awareness (MISA) are regarded as important for the development of an effective information security culture in organizations and for the success of security programs (Wilson and Hash, 2003). Studies revealed that there is a lack of guidance explicitly aimed at senior management (Schneider et al., 2020). As an example, it would be interesting to investigate in factors that specifically build MISA, as the managerial aspect was found to be critical to the overall performance of an organization's information systems security (Haeussinger & Kranz, 2017). In addition, the hierarchical level of the individual in a company would be one field for future research in the context of managers' information security awareness (Jaeger, 2018).

To contribute to the field of MISA, our article explores two research questions in the context of increased remote work models and related social engineering attacks:

- Is risk awareness a factor that influences the risk of IT system usage?
- What role does cybersecurity training and security awareness play in the context of COVID-19 pandemic restrictions?

There is a lack of literature concerning the effect of knowledge transfer on security awareness. In this article, our contributions are to relate social engineering to a theoretical framework (prospect theory). Second, we address the relationship of social engineering to cognitive human functions and especially an awareness of human data processing cognitive functions. Third, we analyse the role of the knowledge in facing risks and uncertainty exposition of the user. Fourth, we delimitate the impact of the COVID-19 crisis on the mechanical correlation between uncertainty and cyberattacks. The remainder of this paper is structured as follows: In the following section, the theoretical background on human behavior under uncertainty is elaborated. In particular, the authors focus on prospect theory, as it addresses the concept of uncertainty in combination with risk perception in human decision-making. The concept of social engineering and the relevance of cybersecurity awareness are described in the following sections, and the research design is detailed. The results are discussed in the final section.

2. THEORETICAL FRAMEWORK

This part links an established theory in economics (prospect theory) with the impact of uncertainty on economic decisions to the cognitive biases exploited by "social engineers".

A. Prospect theory and decision paradigm The prospect theory and decision paradigm omit the important contexts in which the sets are open-ended, such as the COVID pandemic. In management research, attempts to classify and understand uncertainty have typically focused on the locus of uncertainty, i.e. missing information. For example, "behavioral uncertainty" refers to uncertainty about how individuals will act and also on the trust they place in the source Kahneman et al. (2011) referred to Ellsberg (1961). In making choices, our affect sometimes overrides our reason when we rely more on what is familiar to us than on an event with a perceivable exact probability distribution but which is foreign to us. (Heath & Tversky, 1991).

On the cybercriminal side, the choice is made under constraints and utility functions (see further). The important mechanism is that losses are greater than gains (Kahneman and Tversky, 1984; Tversky and Kahneman, 1991). The asymmetry in behaviour between the user and cybercriminal can be explained by revenue maximization effects or by decreased risk aversion. The criminal is a "participant" of social engineering makes decision. The prospect theory describes how individuals assess their loss and gain perspectives in an asymmetric manner.This predatory behaviour results from a lower perceived risk

because the authorities are overwhelmed and from a maximum perceived gain since the market value resulting from the slowing down of the hospital's functioning by blocking computer access to X-rays, scans, and medical examinations has a disastrous collective impact. The pandemic and remote work situation jointly changed the perceptual frameworks in place in the user and the cybercriminal (Azan & Gilg, 2021).

B. Uncertainty categories and risks The uncertainty contained in prospect theory is segmented. A typology of uncertainties exists in the literature. We identified the set of options and the set of outcomes—whether open or closed—as key distinguishing features. We distinguish four general areas. Following conventional terminology as much as possible, we call these domains (1) ambiguous uncertainty, (2) creative uncertainty, (3) procedural uncertainty and (4) substantive uncertainty.

While these approaches describe where uncertainty arises, we describe uncertainty in terms of why something is uncertain, i.e. why the probabilities are indeterminate. Milliken's (1987) well-known distinction between state, effect, and response uncertainty can also be elucidated by our framework to explain how and why some environments are perceived as unpredictable. State uncertainty and effect uncertainty, for example, both correspond to what we call environmental uncertainty, derived from the complex and dynamic nature of the environment, which causes the set of outcomes to be perceived as open-ended.

The uncertainty comes from an ambiguity connected with the answers to be proposed. "Ambiguity is uncertainty about probability, created by missing information that is relevant and could be known" (Snow, 2010; Dequech 2011; Dosi et Egidi 1991; Dequech 2000, see Table 1). The decision criterion cannot rely on probabilistic scenarios. The following criteria of decision that can be used are the Savage's criterion, Wald,'s criterion, Maxmin and Hurwicz criterion. Response uncertainty, or the uncertainty that results from not knowing the responses of competitors to any chosen course of action, is the result of an open set of outcomes derived from a competitor's open set of options. Since one cannot necessarily know how others will act, one cannot predict how those actions will affect a given outcome.

Uncertainty can be procedural. The substantiveprocedural dimension reflects Simon's (1979) distinction between substantive and procedural rationality: whether uncertainty arises from a lack of information (substantive) or a lack of computational ability (procedural). The weak-strong dimension reflects Knight's (1921) distinction between probabilistic (weak) and no probabilistic (strong) scenarios. The ambiguous fundamental dimension distinguishes between stable, finite realities that are simply unknown (ambiguous) and realities that are subject to structural change. This is not predetermined due to the creative capacity of individuals. Because decisions are based on perceived uncertainty, the nature of options and outcome sets, and thus the type of uncertainty, are subjective and often tacit.

Uncertainty can be creative. The dimensions distinguish between stable, finite realities that are simply unknown (ambiguous) and realities that are subject to undetermined structural change due to the creative capacity of individuals. Here, the distinction between actual and perceived uncertainty becomes important. Because decisions are based on perceived uncertainty, the nature of options and outcome sets, and thus the type of uncertainty, are subjective and often tacit.

Users react differently to uncertainty. Some are terrorized by the urgency, the noise emitted by the site or an often-fictitious threat. Social engineering or social engineering attacks aim to obtain confidential information by manipulating the victim remotely, especially by telephone. The objective is to access confidential data, for example, by using and exploiting the human and psychological flaws of the victims. As a cybercrime, social engineering is much less significant than the major cyber espionage cases reported in the press because the decisive element is not technology. It is necessarily combined with the human factor, which is perceived by the criminal as the weak point of the information system. The victim is consenting and does not realize that he/she has been attacked.

Table 1. Types of uncertainty

Uncertai nty	Ambigu ous uncertai nty	Creative uncertainty or fundamental uncertainty	Procedural uncertainty	Substantive uncertai nty
Questions	How does an individu al handle the open set of possible response s of other involved parties to any chosen course of action ? The uncertainty comes from an ambiguit y connected with the answers to propose	What set of conceivable actions can an individual perform, each with certain consequences in the face of uncertainty (problem solving, scenarios) ?	What procedure will circumvent the ambiguity of choices?	How does an individual evaluate the options, and what are the probabili ties associated with the scenario s? What are the outcomes of a complex situation ?
Definition	"ambiguity is uncertai nty about probability, created by missing informat ion that is relevant and could be known' (Snow, 2010)	Fundamental uncertainty, by contrast, is characterized by the possibility of creativity and nonpredeter mined structural change (Dequech, 2011)	"limitations on the computati onal and cognitive capabilities of the agents to pursue unambiguously their objectives, given the available informatio n" (Simon, 1983)	"the lack of all the informat ion which would be necessar y to make decision s with certain outcome s' (Dosi & Egidi, 1991)
Exampl es :	Worst case scenario Savage criterion Wald criterion , Maxmin and Hurwicz criteria of decision, Savage axiom	Improvisation bricolage (Ciborra, 2000)	Intelligenc e modelling Choice process	Real options, game theory

1.3. Security awareness and social engineering

The human factor is a major cause of cybersecurity incidents in organizations, whereas the senior management is a user group particularly exposed to cyber risks. Although managerial information security awareness (MISA) is of high relevance, there is a lack of support in the development of MISA programs from academia. Research Proposal 1: Knowledge about cybersecurity increases security awareness.

Information security awareness of employees and managers, as well as their compliance with security policies needs to be increased in order to reduce the risk of cyber incidents (Bauer et al., 2017). Information security awareness training aims to equip employees with knowledge and competences to be able to recognize threats and be familiar with effective countermeasure and appropriate behavior. Information security awareness is especially important for senior managers and in particular, for CIOs and CISOs, which have the responsibility to manage and oversee the cybersecurity strategy of organizations. The managerial aspects of cybersecurity along with organizational and strategic elements should hence not be neglected (Madnick and Mangelsdorf, 2017; Schneider et al., 2020).

Research Proposal 2a: Increased knowledge about cybersecurity is correlated with perceived procedural uncertainty.

Research Proposal 2b : Increased knowledge about cybersecurity is correlated with perceived creative uncertainty.

Research Proposal 2c : Increased knowledge about cybersecurity is correlated with perceived ambiguous uncertainty.

Research Proposal 2d : Increased knowledge about cybersecurity is correlated with perceived substantive uncertainty.

Hancock prevalence effect, provides a simulation of form of cyberattack in human investigates - automation teathe ming, rare signals are a clerical email work in using an email task. The results demonstratedmediating role of the more difficult to volving messages conta existence and power of prevalence effects in eISA. mail detect, even when ining sensitive personal cybersecurity. Attacks that delivered at a rate of 1% considering their information. were significantly more likely to succeed, and the It is recommended to address MISA as priority and call proportionally low overall pattern of accuracy across managers to become active players in the cybdeclining SP ersecurity occurrence. exhibited logarithmic decay.arena (Choi et al., 2006). Managerial cybersecurity

Staub 1990 This study, based 1211 interviewed Many permit their installations to be either lightly awareness is a prerequisite for employees to have high on the managers protected or wholly unprotected, apparently willing to levels of information security awareness (Haeussinger criminological 1063 managers of the risk major losses from computer abuse. and Kranz, 2017). Straub explored another aspect of theory of general DATA Processing

deterrence, Management cyberattacks (Azan et al., 2019) with a focus on investigated Association computer crime, a concept that falls under the umbrella whether a of offense, crime, and disciplinary misconduct. management Executives must deal with organizations with illicit, decision to invest in abusive or criminal use of computers. Two important IS security results aspects are considered: the theft of data and the in more effective concealment by perpetrators of infractions or control of computer disciplinary breaches. A first study by Straub examined abuse.

Choi et al. 2008 The purpose of this A model is developed, The results of the study provide empirical support that how IS managers deal with these two problems. Data for paper was to and the relationship MATIS is directly the study were collected from 1,063 randomland positively related to MISA. The y selected empirically validate between MISA and paper suggests that intention to act and the risk-cost members of the Data Processing Management the conjectural MATIS. The hypotheses tradeAssociation (DPMA). The originality of the -off of the MATIS are other possible constructs research, relationship of the research model that should be incorporated into future research. The published in 1990, is that it

characterizes illegal acts between are tested emprically conceptual model employed as a theoretical basis also independent of the law (e.g. unauthorized access to managerial sugcertain databases or modification of hardgests that other factors such as the environment in ware) by information, which an organization operates (e.g. industry) also associating them with behavioral patterns. If the law security awareness plays a major role in determining information security presents the offences abstractly, then the research has the (managerial actions MISA) and decisions independently of MISA.merit of characterizing in a more flexible way t he notion toward information of fault, consubstantially with the evolution of security (MATIS). technology. Blau 2017 Research points to DecisionResearch proposal 4-makers must use their judgement to estimate : The COVID-19 crisis stimulated steps that security how much to invest in cybersecurity, but some computer-supported work and cyberattacks. executives and decisionCybercrimina-makers may rely on the wrong models when ls capitalize on the fact that cybersecurity other cybersecurity considering where and how much to invest.is in essence a case of human automa tion, with both the professionals can machine and the human as potentially vulnerable take to circumvent (Schneider et al., 2020; Sawyer and Hancock 2018). CEOs' human Social engineering aims to obtain confidential biases and motivate decision-makers to information by manipulating the victim remotely, invest more in especially by telephone. The objective is to access cyber confidential data, for example, by using and exploiting infrastructure. the human and psychological flaws of the victims. As a Montanez et al. 2020 Expert speculating Openness: the willingness to experience new things, cybercrime, social engineering is much less significant advice conscientiousness: favoursthan the major cyberespionage cases report-norms, exhibiting selfed in the press because the decisive element is not technology. It is necessarily combined with the human factor, which is perceived by the criminal as the weak point of the information system. The victim is consenting and does not realize at the time that she or he has been attacked. Detecting human weaknesses in computer systems is often the result of psychological approaches. The underlying cognitive mechanisms in social engineering are well-known and are largely found in the work of Tversky and Kahneman (1986): on the one hand, actors, criminals who hope to maximize their gain, and on the other hand, users, victims who are concerned with limiting their risks. Kahneman (2011) focused his work on the speed of thought, as mentioned in the introduction. We have a mechanical way of thinking that allows us, for example, to quickly process two hundred emails in our mailbox without paying close attention to them. This thinking makes us vulnerable to attack because it relies on the plausible and does not pay attention to details. An ignorance of attacks based on approximation in a falsely reassuring work environment creates a danger for users and companies. In the application of the work of Kahneman et al. (2011), a user clicking on a message is a decision, which according to the theory depends on a choice, rule and frame. It is the latter perceptual frame that criminals act on in social engineering. When the user fixes his attention on the message, the stimuli linked to the context, coronavirus, pandemic and WHO will interfere and modify the attention mechanisms. The information is a source of difference for the user that can condition his survival. For the criminal, COVID-19 opens the way to maximizing gains. Some decisional determinants are identified by the cybercriminal.

Research Proposal 5: Perceived social engineering attacks are correlated with security awareness.

3. RESEARCH DESIGN AND RESULTS

The guiding theory for our research was prospect theory and its following in the literature.

A. Knowledge and fifteen questions

Fifteen questions were based on knowledge about cybersecurity (example: what is your definition of social engineering?). These questions were asked after a panel session about cybercriminality that aimed to make students more aware of cybersecurity. The 15 questions enable the calculation of a score. The score differentiates all the respondents. The Spearman matrix is determined. In statistics, the Spearman correlation or Spearman rho is a measure of nonparametric statistical dependence between two variables. The Spearman correlation is studied when two statistical variables seem to be correlated without the relationship between the two variables being of affine type. This consists of finding a correlation coefficient not between the values taken by the two variables but between the ranks of these values. It

estimates the extent to which the relationship between two variables can be described by a monotonic function. If there are no repeated data, then a perfect Spearman correlation of +1 or -1 is obtained when one variable is a perfect monotonic function of the other. Covariance is calculated on the rank of the variables at the Pearson difference.

To conduct a first validation of our research, a cohort of 103 students was surveyed. They came from the fields of economics and management (undergraduate), business law (graduate) and network computing (undergraduate). Based on the research proposals derived in the previous section, the items were aggregated into three dimensions: knowledge, uncertainty, and awareness (see details below).

A statistical analysis resulted in the figures listed in the following tables. In the principal component analysis, several dimensions determine the inertia of the scatterplot.

B. Results and dimensions

The most important dimension of the study (the knowledge in the PCA) is linked to the organization of the courses, the perception of their progression (Q33), the structuring of the teachings, and the knowledge delivered in a corpus. The knowledge content, animation and interactivity are correlated in dimension 1 with pedagogical support, feelings of security, and precautions to be taken in the use of the computer. Knowledge is a factor of considering uncertainty and is strongly correlated with security awareness. Through knowledge, we make the user aware of the risks linked to cyberattacks and particularly to social engineering.

Dimension 2 in the PCA shows the nature of uncertainty and its treatment by security awareness. The latter is correlated with the uncertainty of creativity, the uncertainty of ambiguity of the choices and of the situations, in addition to the uncertainty due to COVID19, and the uncertainty linked to the curiosity and the approximate treatment of the situations.

Table 2 - Results of the statistical analysis

Table 4 - Results of the statistical analysis

Constructs	Items	Coefficients factorials	Explained Variance %	Cronbach Alpha
KNOWLEDGE	CONC	0,899	64,712	0,888
	MASTER	0,859		
	ADVI	0,840		
	EXPLOI	0,785		
	ASSET	0,735		
	PROG	0,688		
UNCERTAINTY	AMBI	0,813	55,312	0,724
	SUBUNCE	0,769		
	PROCUNCE	0,707		
	CREAAMBI	0,678		
AWARENESS	SLOW	0,898	60,448	0,829
	EXPLOI	0,854		
	SLOWIT	0,838		
	INVOL	0,693		
	SLOWFISH	0,551		

The third dimension in the PCA shows solutions to perceived risks, perceived interest, empathy in the face of attack situations in case of erroneous instructions, and the calculation of risks in the face of exposure to cyberattacks for which security awareness provides a better representation. The use of a connection is more important if it allows for the transmission of critical information or the management of important parts of the budget. This dimension also associates perceptions of cyberattacks and reveals drivers of action such as empathy and the injustice of erroneous instructions. We can clearly see that the

variables of social interaction (Q22, Q35, 18b) and appropriation of the organization's data are inversely related to the feeling of vulnerability to cyberattacks (Q53), particularly with regard to social engineering (Q53B). We did not indicate it in the matrix above, but a fourth dimension in the PCA could have been mentioned. The fourth dimension reveals the modus operandi of the attacks, social engineering, the role of voice attacks, and the role of urgency in the attacks (for some, more than four attacks during confinement). It is inversely related to training and especially strongly inversely correlated to awareness in the use of the computer in what we call slow-thinking security awareness. It is inversely related to Q15a, i.e. to the results obtained in the scoring. Urgency is an element that facilitates (Q56) attacks and the feeling of vulnerability (Q53).

If we look in detail, as knowledge increases, so does the perceived uncertainty, and the awareness of risk levels increases. If we specify the issues related to attacks by mentioning social engineering, there is a slight correlation between awareness and scoring (test about cybercriminality). There is a very strong correlation between learning-in-progress facilitating the culture of awareness and the score obtained. The score obtained correlates well with the user's feeling after taking the course. The better the latter is, the better the score.

"I feel a sense of control over computer security thanks to the MSI course" correlates well with the score obtained. The course is seen as a way to cope with containment. "The computer security awareness of the Lyon II MSI course (TV5 monde case) will allow me to make the most of my internet connection (computer, smartphone) during lockdown" is a response that shows very good correlation with the scoring. This is corroborated by question 19. Security awareness training (e.g. TD on the TV5 monde case in the MSI course or other teaching) provides tips that help overcome cybersecurity-related difficulties.

Collective mechanisms to fight cyberattacks are relatively effective. "I act to ensure respect for security rules in the organization (L2, MSI, University of Lyon 2)". The TD on security (for example, the TV 5 monde case or the Kaspersky case) increases my knowledge of computer security. I receive feedback (e.g. a message, reward point or good grade) on my progress. Scoring about the cybercriminality correlates negatively with the uncertainty of "during containment, my curiosity is exploited", so this is the weapon to defeat cyberattacks. This is consistent with the work of Schneider et al. (2020). Q16 correlates well with question Q30 on feedback. It reflects the need for guidance of younger users and the need to provide them with feedback in cyberattack experiences.Q18, the empathy variable, is interesting because it is linked to the awareness of the progressiveness of the course. In other words, it is not possible to feel empathy only after mastering the content delivered in the course. The feeling of change in learning methods for students is negatively related to question 25 and the variable with respect to safety rules. Q25 is "I act to ensure that safety rules are respected in the organization" (L2, MSI, University of Lyon 2). This way of functioning is positively correlated with the risks linked to the emergency. Change is positively correlated with the risk that hackers will take advantage of inattention and build on mistakes to increase their reach and attacks.

Uncertainty is perceived in contrasting ways. If the uncertainty linked to the ambiguity of the choices to creativity is obvious, then the "procedural uncertainty" in Q60 is correlated with the scoring, and we know what to do when we obtain a good score. Last one allows us to evaluate the risks in order to make the right decisions. We observe that the dichotomy between the score of question 15, the level of knowledge, is inversely correlated with question 24 with regard to an intuitive experience that is immediate and characterized by rapid thinking. Q24 is "I become little aware of my environment while I am taking a computer security awareness course" (University of Lyon 2, L2, MSI course).

The social engineering proposed here as voice phishing correlates well with the distributed course material and with the feeling of a lack of awareness while using the computer. This feeling is related to question 34 and a sense of safety in using a computer.

4. DISCUSSION

It is possible to limit the risks by transferring knowledge to the actors, and the mechanisms at work are more individual than collective.

1. Security awareness reduces the risks of social engineering thanks to cognitive framing. A confirmation of cognitive framing in man-machine interaction reduces the risks in social engineering situations. We find the three phases of the choice process (choice rule, framing and evaluation) which appear in Kahneman & Tversky (1986) and the results, are relevant for the decision. In the evaluation phase, the user focuses on the decision, probably with caution and increased concentration. Although not very formal, framing theory focuses on the rules that govern the representation of acts, outcomes, and contingencies (Tversky & Kahneman, 1986).

As noted in and to reiterate the work of Kahneman et al. (2011), a user clicking on a message makes a decision which, according to the theory, depends on a choice, rule and frame. When the user fixes her or his attention on the message, the stimuli related to the context (the coronavirus pandemic) will interfere and modify the attention mechanisms. The simulated, feigned urgency forces the user to revise his or her probability calculations. As it appears in our study, this technique of necessary urgency, dictated by the events and the seriousness of the situation, makes it possible to turn to the mechanisms of security awareness. This confirms that slow thinking associated with data processing is a lens. As concluded in Montanez et al. (2020), we have presented a framework for systematizing human cognition through the lens of social-engineering cyberattacks, which exploit weaknesses in human cognition functions.

As Montanez et al. (2020, p. 1) explained, "Adequate defence against social engineering cyberattacks requires a deeper understanding of what aspects of human cognition are exploited by these cyberattacks, why humans are susceptible to these cyberattacks, and how we can minimize or at least mitigate their damage." "A course about social engineering is a factor of mitigation of damages caused by cyberattacks and liberates creative uncertainty, calculus uncertainty ambiguity uncertainty.

It contains persuasion" (Wright, 2014). If it is possible to observe chains of causalities, then remote work leads to an increased use of the computer, increased use of the latter to carry out financial operations, and an increased perceived value. The study shows that a minimum base of knowledge is needed to face these increased risks. The study shows that by paying more attention to explicit risks, we can avoid fishing, identify attacks, and then mobilize collective measures based on mutual aid and the identification of criminogenic situations. Conversely, this absence allows panic to occur and does not allow one to come to the aid of others.

A. Confirmation of categories of uncertainties in efficient programs

In cybersecurity knowledge, the quantitative study confirms the first studies of Schneider et al. (2020). Topics most relevant to the organization's ecosystem must be chosen to limit creative uncertainty. The security culture and the needs of the business should serve as the basis for creating collaterals for security awareness trainings (Schneider et al., 2020; Manke & Winkler, 2013, p. 24).

To limit procedural uncertainty, organizations must develop program content specific to various user groups to enable role-based training. To limit uncertainty, the training material should be relevant to the job duties of the individuals participating in the training (Schneider et al., 2020; Horenbeeck, 2017; Osterman Research Inc., 2018; PCI Security Standards Council, 2014). To limit ambiguous uncertainty, effective messaging tailored to a desired outcome is required with a focus on behavioural change. ISACA (2019) highlighted that security awareness programs are often launched without the definition of a clear objective. Osterman Research, Inc. (2019, p. 13) stated that the ultimate goal, the desired outcome of security awareness programs, is behaviour modification. Security awareness training is about improving the behaviour of employees who have the potential of undermining the security provided by the organization's security infrastructure (Schneider et al., 2020).

Substantive uncertainty is also a major concern for social engineering and cyberattacks. Organizations must deliver trainings sufficiently often to avoid the limited capacity of the human mind. The load of information delivered to employees should be considered. To achieve this goal, the training content should be broken down into 'consumable' units. In addition, a modular structure is a suitable measure to avoid information overload (ISACA (2019).

Awareness materials are multimodal: It is important to deliver awareness materials across multiple channels. To ensure that employees remember the information disseminated during awareness training programs, it is recommended to use multiple channels for communication to ensure that employees are exposed to the same information repeatedly. This will help them to better retain information (PCI Security Standards Council, 2014). It is important to build upon high-quality content, which is simple to understand and presented in a form that is easy to digest, enjoyable and frictionless.

B. Centrality of knowledge

Our study puts forward a knowledge base as it first incorporates the factor of uncertainty and second,as the data collection accounts for the particularities of human perception during COVID-19 restrictions. Sawyer and Hancock focused on a specific effect (the prevalence effect) in email-based attacks. Our study has a different methodological approach: we used a questionnaire and used a broader perspective on social engineering. In addition, we investigated the correlations between risk perception, cybersecurity awareness and education. Contrary to Straub, our study incorporates recent data. While Straub was more dedicated to investigating management investment decisions, our study has its origin in risk perception, which is regarded to be the root cause of further security-related behaviour and decisions. Choi's study suggested that awareness plays a crucial role in managerial actions toward cybersecurity; however, that study concluded that more factors need to be incorporated. With our study, we take this identified gap further and, e.g. incorporate the factor of uncertainty into account. Blau et al. (2017) focused on cybersecurity-related investment decisions of senior management. Our study is not dedicated to capturing factors for investment decisions. However, our study suggests that computersupported work increased in importance and that business-critical tasks have increasingly shifted into cyberspace.

Montanez et al.(2020) proposed a framework of human cognitive functions to accommodate social engineering cyberattacks. Our study proposes an alternative, taking into account the factor of uncertainty, which is explicitly prevalent in times of a pandemic, and tests the correlations with empirical data. Wright investigated the response to social engineering messages, while our study more broadly investigated social-engineering cyberattacks.

4. CONCLUSION

Our data analysis supported the proposal of risk awareness as a positive factor in more secure IT system usage. The study also revealed a correlation between perceived risk in IT system usage and knowledge. An increased level of cybersecurityrelated knowledge arrives with a higher perception of uncertainty. The authors' previous qualitative research with senior managers (Schneider et al., 2020) also revealed this paradox. While the interviewed senior manager regarded his or her own cybersecurity maturity as being very high initially, his or her own perception changed throughout the interview as the senior manager increasingly perceived threats in cyberspace behaviour.

What role does cybersecurity training and security awareness play in the context of COVID-19? The data collected in our study strongly confirm the increased dependency of users on their devices and Internet connectivity. Participants reported conducting multiple critical transactions via online connections within a single business day. Technology plays an essential role in administering both work and private life. The data collected in our study strongly confirm the increased dependency of users on their devices and Internet connectivity. Participants reported conducting multiple critical transactions

via online connections within a single business day. Technology plays an essential role in administering both work and private life. The rising number of cyberattacks in times of the

COVID-19 crisis enforces the importance of cybersecurity training and awareness programs at all levels including business students who might become future managers as well as today's senior management. The study strongly confirm the role of the cybersecurity training and security awareness play in the box.context of COVID-19 pandemic restrictions A confirmation of cognitive framing in man-machine interaction reduces the risks in social engineering situations. We find the three phases of the choice process (choice rule, framing and evaluation) which appear in Kahneman & Tversky (1986) and the results, are relevant for the decision. We confirm the evaluation phase, the user focuses on the decision, probably with caution and increased concentration and slow thinking. Although not very formal, framing theory focuses on the rules that govern the representation of acts, outcomes, and contingencies (Tversky & Kahneman, 1986).

As plans for future research, we intend to overcome two limitations of the current study. First, empirical data were collected from students. Even though the students were based in relevant fields of management and business, we need to validate our findings with a target group of managers in future research. Second, using a questionnaire as a main data source allowed us to collect the reported behavior of the study participants but did not reveal real behavior in cybersecurity-related situations. It is desirable to triangulate the data collection method. As an example, the authors developed a virtual cybersecurity escape room where players need to find relief from a serious successful cybersecurity attacks in a company scenario. This game includes a social engineering attack by phishing. Game executions with (senior) managers could provide enhanced insights into cybersecurity behavior in a time-constrained security challenge. Social engineering offers a rich context of observation of computational social systems.

References

Abraham, S. 2011. "Information security behavior: factors and research directions,"in Proceedings of the American Conference on Information Systems, Detroit, USA.

Bauer, S., Bernroider, E. W. N., and Chudzikowski, K. 2017. "Prevention is better than cure! Designing information security awareness programs to overcome users' noncompliance with information security policies in banks", Computers & Security (68), pp. 145–159.

Blau, A. 2017. "Better Cybersecurity Starts with Fixing Your Employees' Bad Habits," Harvard Business Review (retrieved from https://hbr.org/2017/12/better-cybersecurity-starts-withfixing-your-employees-bad-habits).

Choi, N, Kim, D., Jahyun, G., and Whitmore, A. 2008. "Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action,"Information Management & Computer Security(16:5), pp. 484-501.

Choi, N., Kim, D., and Goo, J. 2006. "Managerial Information Security Awareness' Impact on an Organization's Information Security Performance," in Proceedings of the American Conference on Information Systems, Acapulco, Mexico.

Dequech D. (2011), Uncertainty: A Typology and Refinements of Existing Concepts Author(s): David Dequech Source: Journal of Economic Issues , SEPTEMBER, Vol. 45, No. 3, pp. 621-640

Disparte, D., and Furlow, C. 2017. "The best cybersecurity investment you can make is better training,"Harvard Business

Review, pp. 2-4. FBI 2018. Business E-Mail Compromise. The 12 Billion Dollar Scam(retrieved fromhttps://www.ic3.gov/media/2018/180712.aspx).

Dosi, G., Egidi, M. 1991. Substantive and procedural uncertainty. J Evol Econ 1, 145–168

https://doi.org/10.1007/BF01224917

Ellsberg, D. (1961). "Risk, Ambiguity, and the Savage Axioms," Quarterly Journal of Economics 75, p.643-659 [10] Green, A. Parrish, J., Smith, J.N. and Thatcher J.B. 2018. "SNS Use, Risk, and

Executive Behavior,"in Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, San Francisco, December 13.

Haeussinger, F., and Kranz, J. 2017. "Antecedents of employees' information, Security awareness - review, synthesis, and directions for futureresearch," in Proceedings of the 25th European Conference on Information Systems (ECIS).

Heath, C. And A., Tversky (1991). "Preference And Belief." Ambiguity And Competence In Choice Under Uncertainty," Journal Of Risk And Uncertainty 4, 5-28.

Hevner, A.R., March, S.T., Park, J., and Ram, S. 2004. "Design science in information systems research,"MISQuarterly(28:1), pp. 75-105.

ISACA 2019. Improving security awareness using marketing techniques (retrieved fromhttps://www.isaca.org/bookstore/bookstore-wht_papersdigital/whpisa).

Jaeger, L. 2018. "Information Security Awareness: Literature Review and Integrative Framework," in Proceedings of the 51st Hawaii International Conference on System Sciences, Hawaii International Conference on System Sciences. (https://doi.org/10.24251/hicss.2018.593).

Kahneman, D. (2011), Système 1, Système 2, Les Deux Vitesses De La Pensée, Flamarion, Paris

Kahneman, D. and A., Tversky. (1979). "Prospect Theory: An Analysis Of Decision Under Risk,"Econometrica 47, 263-291.

Kahneman, D. And A., Tversky. (1984). "Choices, Values And Frames," American Psychologist 39, 341-350.

Kahneman, D., Paul, S. , And A. , Tversky (Eds.). (1982). Judgment Under Uncertainty: Heuristics And Biases. New York: Cambridge University Press.

Ki-Aries, D., and Faily, S. 2017. "Persona-Centred Information Security Awareness," Computers & Security(70),Elsevier BV, pp. 663–674. (https://doi.org/10.1016/j.cose.2017.08.001).

Madnick, S., and Mangelsdorf, I.B.M.E. 2017. "What executives get wrong about cybersecurity,"Sloan Management Review, Winter 2017, pp. 22-24.

Manke, S., and Winkler, I. 2013. The Habits of Highly Successful Security Awareness(retrieved from http://www.securementem.com/wpcontent/uploads/2013/07/Habits_white_paper.pdf).Mimecast 2018. State of Email Security 2018(retrieved fromhttps://www.mimecast.com/globalassets/documents/ebook/ stateemailsecurity-2018.pdf).

Miltgen C. & Azan W. (2009), Utilisation d'internet, propension au mensonge dans le comportement des utilisateurs et interrogations sur l'activation de la technologie, Session spéciale Systèmes d'identification électronique : perceptions de confiance et de confidentialité, 11ème colloque de l'International Business Information Management Association, Le Caire, Egypte.

Montanez, R., Golob, E., Xu, S. (2020), Human Cognition Through the Lens of Social Engineering Cyberattacks, Frontiers in Psychology,

Olt, C. M.,Gerlach, J.,Sonnenschein, R., and Buxmann, P. 2019.

"On the Benefits of Senior Executives' Information Security Awareness," in International Conference on Information Systems (ICIS), Munich, Germany, 15.-18.12.2019.

Osterman ResearchInc. 2019. Addressing the Top 10 Security Issues Organizations Face (retrieved fromhttps://www.knowbe4.com/hubfs/Addressing_the_Top_10 _Security_Issues_Organizations_Face_KnowBe4.pdf).

PCI Security Standards Council, 2014. Information Supplement: Best Practices for Implementing a Security Awareness Program (retrieved fromhttps://www.pcisecuritystandards.org/documents/PCI_DSS _V1.0_Best_Practices_for_Implementing_Security_Awareness _Program.pdf).

Rolls, D. 2017. "The hacker-prone C-Suite: Why executives tend to get the short straw when it comes to cyber risk,"CSO Magazine,September 2017 (retrieved from https://www2.cso.com.au/article/627571/hacker-prone-csuite-why-executives-tend-get-short-straw-when-it-comescyber-risk/).

Rothrock, R. A., Kaplan, J., and Van Der Oord, F. 2018. "The board's role in managing cybersecurity risks,"MIT Sloan Management Review(59:2), pp. 12-15.

Safa, N. S., Von Solms, R., and Furnell, S. 2016. "Information security policy compliance model in organizations," Computers & Security(56), pp. 70-82.

SANS Institute 2018. SANS Security Awareness Report 2018: Building Successful Security Awareness Programs(retrieved fromhttps://www.sans.org/sites/default/files/2018-05/2018 SANS Security Awareness Report.pdf).

Saunders, M., Lewis, P., andThornhill, A. 2012. Research Methods for Business Students(6th Edition),Essex: Pearson

Education Limited.Sawyer, B. D., and Hancock, P. A. 2018. "Hacking the Human: The Prevalence Paradox in Cybersecurity,"Human Factors: The Journal of the Human Factors and Ergonomics Society(60:5), pp. 597–609.

Schneider, B., Asprion P.-M., Azan W. (2020), A Practical Guideline For Developing A Security Awareness Program Targeted Towards Senior Managers, Research Paper.

Simon H.A. (1983b), Search and reasoning in problem solving, Artificial Intelligence, 21, p. 7-29.

Simon H.A. (1990), Sciences des systems, sciences de l'artificiel, AFCET Systèmes, 2eme Edition, Dunod, paris

Snow (2010), Ambiguity and the value of information, Journal of Risk and Uncertainty, 40, 133-45, 20

Straub, D. W. 1990. "Effective IS Security: An Empirical Study,"Information Systems Research(1:3), pp. 255-276.

Toussaint, G. W. (2015). Executive security awareness primer(Master Thesis, Utica College) (retrieved fromhttps://search.proquest.com/openview/3f8bface444421e6f7 f1ee2fe550881e/1?pq-origsite=gscholar&cbl=18750&diss=y).

Tversky, A. And D. Kahneman (1986), Rational Choice And The Framing Of Decisions," The Journal Of Business 59(4), Part 2, $251-$278.

Tversky, A. And D., Kahneman (1991), "Loss Aversion In Riskless Choice: A Reference Dependent Model," Quarterly Journal Of Economics 107(4), 1039-1061.

Tversky, A., Paul S., And D. Kahneman. (1990), The Causes Of Preference Reversal, The American Economic Review 80(1), 204-217.

Tversky, A., Shmuel S., And Paul S. . (1988), Contingent Weighting In Judgment And Choice, Psychological Review 95(3), 371-384.

Venkatraman, S., C. M. K.,Cheung, Z. W. Y.,Lee, F. D.,Davis, and Viswanath V. 2018. "The "Darth" Side of Technology Use: An Inductively Derived Typology of Cyberdeviance," Journal of Management Information Systems(35:4), pp. 1060-1091.

Vishwanath, A., Herath, T., Chen, R., Wang, J., and Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decis. Support Syst. 51, 576–586. doi: 10.1016/j.dss.2011.03.002

Von Solms,R., and Van Niekerk, J. 2013. "From information security to cyber security,"Computers & security(38), pp. 97102.

Williams, T. 2018. "C-Level execs and ex-employees pose greatest cybersecurity risk," The Economist(retrieved from https://execed.economist.com/blog/industry-trends/c-levelexecs-and-ex-employees-pose-greatest-cybersecurity-risk).

Wilson, M., and Hash, J. 2003. "Building an information technology security awareness and training program", NIST Special publication(800:50), pp. 1-39.Yin, R.K. 2009. Case study research: Design and methods,Thousand Oaks, CA: Sage.

Wright, R. T., and Marett, K. (2010). The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. J. Manage. Inform. Syst. 27, 273–
303. doi: 10.2753/MIS0742-12222 70111

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., and Marett, K. (2014). Research note-influence techniques in phishing attacks: an examination of vulnerability and resistance. Inform. Syst. Res. 25, 385–400. doi: 10.1287/isre.2014.0522