Social Preferences in Decision Making under Cybersecurity Risks and Uncertainties

Mazaher Kianpour, Harald Øverby, Stewart James Kowalski, Christopher Frantz

Norwegian University of Science and Technology, Gjøvik, Norway
{mazaher.kianpour;haraldov;stewart.kowalski;christopher.frantz}
@ntnu.no

Abstract. The most costly cybersecurity incidents for organizations result from the failures of their third parties. This means that organizations should not only invest in their own protection and cybersecurity measures, but also pay attention to that of their business and operational partners. While economic impact and real extent of third parties cybersecurity risks is hard to quantify, decision makers inevitably compare their decisions with other entities in their network. This paper presents a theoretically derived model to analyze the impact of social preferences and other factors on the willingness to cooperate in third party ecosystems. We hypothesize that willingness to cooperate among the organizations in the context of cybersecurity increases following the experience of cybersecurity attacks and increased perceived cybersecurity risks. The effects are mediated by perceived cybersecurity value and moderated by social preferences. These hypotheses are tested using a variance-based structural equation modeling analysis based on feedback from a sample of Norwegian organizations. Our empirical results confirm the strong positive impact of social preferences and cybersecurity attack experience on the willingness to cooperate, and support the reciprocal behavior of cybersecurity decision makers. We further show that more perception of cybersecurity risk and value deter the decision makers to cooperate with other organizations.

Keywords: social preferences, behavioral economics, cybersecurity decision making, structural equation modeling, theory development, perceived cybersecurity risk

1 Introduction

As Peter Bernstein states, “The capacity to manage risk, and with it, the appetite to take risk and make forward-looking choices, are key elements of the energy that drives the economic system forward” [1]. While risk taking is driving the modern economics systems forward, uncertainties in cyberspace like the evolving threat landscape and human error, are threatening to slow it down. Nations, organizations and individuals are unsure what a good driving strategy in cyberspace is. Individual preferences and behavioral heterogeneity can play an important role in explaining strategic considerations at organizational levels. Hence, humans play a vital role in cybersecurity strategic decision

making, and at the same time, they are often considered the weakest links in this ecosystem [2].

The area of cybersecurity in organizations has three essential properties. First, it consists of heterogeneous interacting, and in some cases, competitive and even adversarial, stakeholders and actors that are characterized by distinct local cultures, structure, machines, and methods [3]. Stakeholders act upon the basis of their own local states at any given time. Second, cybersecurity problems stem from dynamic systems and are driven by the interaction among various stakeholders. These interactions affect future local states and, therefore, create systemic complexity. Third, there are strategic decision makers whose decision processes take into account past actions, potential future actions, and outcomes of other actors. They have heterogeneous motivations, preferences, and benefits. Since these properties are based on the organizations' unique sets of objectives, processes, and resources, it is difficult to see how a one-size-fits-all cybersecurity strategy can be optimal.

The trend toward more globalized production has increased inter-organizational dependencies. Particularly, businesses are forming multi-layered supply chains, as illustrated in Figure 1. As an externality, security and insecurity can be distributed disproportionately in a supply chain. The coopetition (i.e. organizations may both compete and cooperate at the same time [4]) and interdependent preferences among the organizations face them with a challenge of understanding and measuring the risks that are propagating from them. Recent cybersecurity incidents highlight that it is no longer enough for organizations to focus solely on their in-house cybersecurity defense mechanisms.

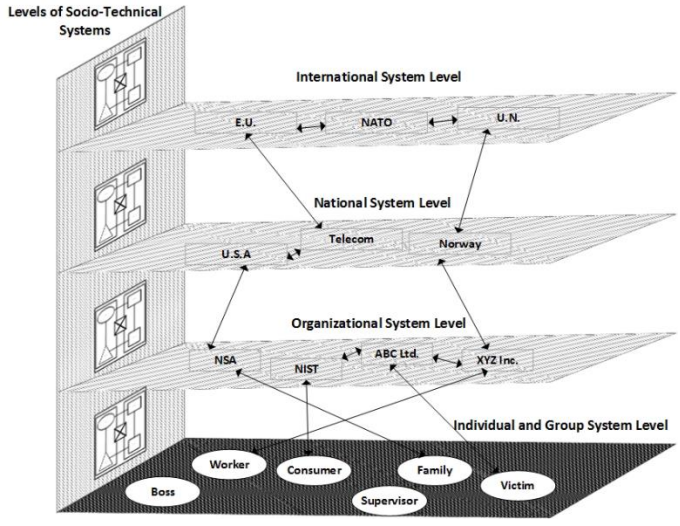

Fig. 1. Interaction among organizations in a socio-technical system is not limited to the organizational level, but also includes different levels of societal actors such as international systems and governments, groups and individuals levels. Each of these actors has their own particular instruments, which can employ different security controls depending on the nature of the system [3].

According to a study from Kaspersky Lab and B2B International, the most costly cybersecurity incidents for businesses result from the failures of their third parties [5]. This means that organizations should not only invest in their own protection and cybersecurity measures, but also pay attention to that of their business partners. To Provide some examples, in December 2018, Managed Health Services (MHS) of Indiana Health Plan announced that a third party data breach potentially exposed up to 31,876 patients' personal data in one of two security incidents the company disclosed [6]. Moreover, attackers expand their reach by targeting third-party services allowing them to steal more data. A new Magecart attack launched through compromised advertising supply chain in November 2018. Attackers loaded their malicious skimming code on 277 e-commerce websites and used their infrastructure of these companies to breach other companies [7].

Different economics models have been employed to address the challenges in the field of cybersecurity in both technical and social aspects [8]–[10]. In these models, agents are rational, selfish, and have complete information about other agents. However, in real-world scenarios, agents might be irrational, reciprocal, and have incomplete information about their environment. In this his paper we outline empirical cybersecurity economics examples on how these standard models fail to model real-world scenarios because they do not properly model the problems when they ignore social preferences.

The key research question is how to model heterogeneous incentives and preferences at the organizational level. The major aim is to better understand under which conditions the social preferences have significant effects on cybersecurity. To achieve this, we aim at developing an understanding of the important determinants of the socially optimal level of cybersecurity to prevent market failures.

Moreover, the paper investigates which type of social preferences (Reciprocal Fairness, Inequity Aversion, Pure Altruism and Spitefulness or Envy [11]) is stronger and quantitatively a core motive in the domain of cybersecurity. We have designed a survey to address these questions. The respondents of this survey are cybersecurity team members (Chief Information Security Officers, Information Security Analysts, Security Consultants, etc.) and decision makers in Norwegian organizations (Chief Executive Officers, Board Members, etc.).

This work is structured as follows. Section 2 provides a background on behavioral economics and proposed models to analyze behavioral determinants in cybersecurity. Section 3 proposes our research model and hypotheses. The methodological approach and data collection process is explained in Section 4. Section 5 presents the empirical results. Theoretical and practical implications are discussed in Section 6. Finally, Section 7 concludes this study.

2 Related Work

Behavioral Economics sits at the intersection of psychology and economics. Standard economic theories assume fully rational, completely selfish and forward-thinking deci-

sion makers. Analytical models based on these assumptions have failed to predict individuals' behavior. However, behavioral economics provides manifold principles considering less rational behavioral choices and other-regarding, interdependent preferences [12].

The application of behavioral economics has become more widespread, most commonly seen in the health domain, and policymakers use it to investigate how predictable deviations from rational behavior can be utilized to steer people to socially desirable directions. This approach is best employed where individuals need to make quick decisions and select the best possible choice.

Thaler and Sunstein [13] and Kahneman [14] popularized the idea that behaviors can be projected into systems and affect the decisions. However, in 1975, Rogers introduced a popular theoretical model of behavior change focusing on the Protection Motivation Theory (PMT) [15]. This model explicitly points out the methods that individuals can assess and counter cyber threats. Dolan et al. [16] proposed a behavior change framework, so-called MINDSPACE, which describes nine behavioral influencers in relation to cybersecurity behavior change paradigm. They discuss that these influencers play important roles in security-related decision making and behavior.

Briggs et al. state that PMT is a useful model in cybersecurity context as it encourages individuals to better protect their cyber assets from cyber threats [17]. They tried to create an effective link between PMT and MINDSPACE to present an integrated framework. This framework can be used to design long term cybersecurity behavioral strategies. It is claimed that the framework can be applied within organizations and provide important insights to managers and practitioners involved in cybersecurity.

There are a variety of psychological models of behavior that address the interplay of attitudes and behaviors. They recognize the importance of psychological traits and attitudes along with the individual's knowledge and experience in decision making. Many of these models are inspired by the Theory of Reasoned Action [18] and Theory of Planned Behavior [19]. The former identifies two factors that determine behavioral intention and assumes that behavior can be completely controlled. The latter, in contrast, differentiates between perceived behavioral control and actual behavioral control.

A survey by Michie et al. [20] shows that there are 80 available models of behavior change in different contexts. The literature review by Sommestad focuses on relevant psychological models for cybersecurity policy compliance [21]. This study identifies 60 different psychological constructs based on established theories including General Deterrence Theory, Neutralization Theory, Social Control Theory, and Theory of Moral Decision-Making. We will focus here on the Theory of Social Preferences, which is studied in behavioral and experimental economics and social psychology. We use this theory in the cybersecurity field to investigate the effects of other-regarding behavior in decision making under cybersecurity risks and uncertainties.

3 Research Model and Hypotheses

This research aims to find the impact of social preferences on the perceived cybersecurity risk, the perceived cybersecurity value, and the willingness to cooperate in third

parties ecosystem to mitigate the probability and impact of future cyber incidents. In the following, we explain our research model, illustrated in Figure 2, and the hypotheses to be tested in the empirical analysis.

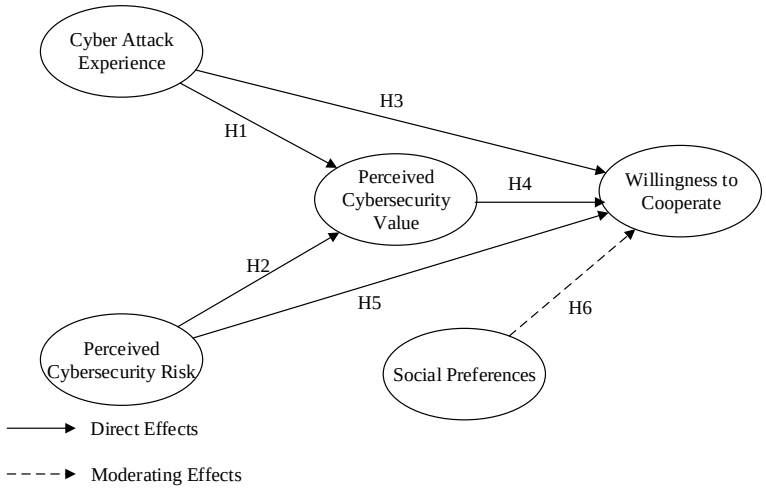

Fig. 2. Research Model in Path Model Notation

As Figure 2 shows, the following hypotheses are proposed to conduct this research:

H1. Cyber attack experience increases the perceived cybersecurity value.
H2. Perceived cybersecurity risk increases the perceived cybersecurity value.
H3. Cyber attack experience increases the likelihood that an organization will cooperate with other organizations to mitigate the probability and impact of future cyber incidents.
H4. Perceived cybersecurity value increases the likelihood that an organization will cooperate with other organizations to mitigate the probability and impact of future cyber incidents.
H5. Perceived cyber risk increases the likelihood that an organization will cooperate with other organizations to mitigate the probability and impact of future cyber incidents.
H6. Social Preferences have moderating effects on the likelihood that an organization will cooperate with other organizations to mitigate the probability and impact of future cyber incidents.

The following latent variables (i.e. research constructs) are used in the proposed model:
Cyber attack Experience: A cyber attack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network [22]. These attacks hit businesses every day and their number is increasing as people are trying to benefit from vulnerable business systems.

According to the third annual report of Ponemon [23], 59% of respondents confirm that their organizations experienced a data breach caused by one of their third parties. 42% of respondents say they had such a data breach in the past 12 months. Additionally, 22% of respondents do not know if they had a third-party data breach in the past 12 months.

Perceived Cybersecurity Risk: Fear of crime consists of two distinct, but highly interrelated, components. First, the rather rational risk perception, which is often stated as the product of the probability of occurrence and the impact of the crime, and second, fear as an emotional feeling of being unsafe [24]. Visser et al. found strong effects of examining prior victimization on perceived risk [25]. Moreover, in a survey by Cisco, 69% of executives indicated that they are not willing to innovate in digital products because of their perceived cybersecurity risks [26]. The finding shows that perceived cybersecurity risk can be a deterrent of cooperation among organizations in digital space.

Perceived Cybersecurity Value: Oscar Wilde said, "A cynic knows the cost of everything and the value of nothing [27]." Cost is a driver for decisions, but not always. Perceived value is what people perceive as the value and worth of a product or service; the higher the perceived value, the more likely it is that they will pay for the product or service.

The reason that we are trying to measure perceived value and understand how it affects the decisions is that they differ from other personal attributes in several ways. Schwartz states that values transcend specific situation and are distinguished from norms, attitudes and specific goals [28]. He also explains that values are observed by subjective importance and they form a unique system of values hierarchies. Values may serve as standards and provide social justifications for behaviors and decisions [29]. Moreover, Sagiv et al. reason that perceived value influences competitive/cooperative behavior and the decisions made [30]. Therefore, to understand and predict the behavior, it is important to consider the perceived cybersecurity value of the agents in the system.

Social Preferences: Game-theoretic predictions are frequently observed in recent experiments on decision making and they have been used to refine behavioral theory. However, explaining decisions outside the laboratory and experimental elicitation of behavior in the context of cybersecurity has not received particular attention in previous studies. We consider that an individual's behavior is affected by three interrelated factors; self-interest, the behavior of others, and the reaction to rewards and punishment.

As a branch of behavioral economics, social preferences describe how economic agents maximize utility considering others' utilities. Differences in social preferences may explain how and why individuals behave in different settings. Social preferences are critical to understand how decision makers scarce resources to themselves and others. These preferences are often dynamic and complex than self-interest.

Willingness to Cooperate: In this study, the willingness to cooperate is defined as the intention of organizations to cooperate with each other to enhance their overall security posture in their third parties ecosystem. These collaborative practices can be performed like creating an incident response team, allocating resources to secure shared critical information, development, and implementation of effective security policies, plans and procedures, etc.

Unlike some studies that only focus on cooperative intentions as the desired behavior, this study also considers the competition among the organizations. The non-selfish motives not only affect cooperation, but also competition incentives. Therefore, we investigate the moderating effects of social preferences on willingness to cooperate in addition to the direct effect of *Cyber Attack Experience*, *Perceived Cybersecurity Risk* and *Perceived Cybersecurity Value*.

4 Research Method

To test the hypotheses outlined in Section 3, we employ Structural Equation Modeling (SEM) [31]. In this section, we describe the reasons behind selecting SEM, data collection and the development of the measurement mode.

4.1 Statistical Method

We live in a complex, multivariate world and studying the impact of one or two variables in isolation would seem relatively artificial and inconsequential [32]. Although modeling always omits some aspect of reality [33], using some approaches (e.g. regression-based approaches) may be too limiting for the analysis of the more complex and realistic situations. Haenlein points out the limitations of the methods such as factor analysis, cluster analysis, and discriminant analysis, which were popular statistical methods in psychology and sociology during the 20th century [34].

To overcome these limitations mentioned above, we apply SEM. This method allows us to model the relationships among multiple independent and dependent constructs, and observable and unobservable variables, simultaneously. There are two approaches to estimate SEM parameters: covariance-based or variance-based. Both approaches are similar, however, the covariance-based approach is more suited for confirmatory theory testing and the variance-based approach rather for theory development [35]. We use the variance-based approach, here and in the following just referred to as Partial Least Squares (PLS), because it is widely used for predictive analysis and is an appropriate technique for theory development as done in this study. This method is furthermore applicable even under conditions of very small sample size. Chin and Newsted indicated that PLS can be performed with a sample size as low as 50 [36]. Moreover, PLS can be used to analyzing models with either reflective, formative or both types of indicators [37].

We use the statistical software SmartPLS 3.0 for parameter estimation as it provides all required features for PLS analysis. First, it supports the PLS Algorithm [38] and bootstrapping, which is considered as the broadly used approach for nonparametric statistics in management, social science, and market research studies. Second, this version supports the consideration of missing values.

4.2 Sample Data

Questback, an affiliated online survey tool with Norwegian University of Science and Technology (NTNU), is used to collect the data. Recall that this study is motivated by a need to understand the effective factors of improving overall cybersecurity in organizations. Therefore, we focused on the individuals who make cybersecurity-related decisions in organizations.

This survey was active for two weeks and the link was inserted in one of the Norwegian Business and Industry Security Council (NSR) news articles[1]. This organization serves the Norwegian business sector in an advisory capacity on matters relating to crime.in different organizations in Norway. Upon clicking the survey link, participants were presented with guidelines and the definition of the terms *Third Parties*, *Retaliatory Actions*, and *Cooperation with third parties*. We provided these definitions in order to prevent ambiguous interpretation of questions. Within the questionnaire, responses to all questions were mandatory, but allowed participants to choose "I have insufficient knowledge to answer this question." if they were unsure about the corresponding question. The survey completion time ranged from 8 to 10 minutes.

As indicated in Section 3, the theoretical constructs identified in our model: *Perceived Cybersecurity Risk*, *Perceived Cybersecurity Value*, *Social Preferences*, and *Cyber Attack Experience* are measured based on different 11 questions in the survey. Answers of 8 questions are reported on 11-point ordinal scales, one question in 5-point frequency scales reporting the update of cybersecurity risk levels in the organization, and 2 questions on the binary scale (Yes, No). These questions are adapted from Ponemon's third annual report [23] and IZA's Preference Survey Module [39].

A total of 66 responses were collected over this period, out of which 62 responses were usable for the study[2]. Table 1 shows the sample demographics of the considered responses.

Communications	**16**
Manager	4
Senior Executive	11
Staff/Technician	1
Defense and Aerospace	**4**
Director	2
Supervisor	2
Entertainment and Media	**1**
Manager	1
Financial services	**11**

1 https://www.nsr-org.no/english/category172.html

2 We employed Mean Value Replacement, when indicators have less than 10% missing values, and Casewise Deletion, when indicators have more than 10% missing values, as missing value treatment approaches. In this study, we considered "I have insufficient knowledge to answer this question." as missing values.

Director	2
Manager	5
Senior Executive	3
Staff/Technician	1
Industrial and Manufacturing	2
Supervisor	2
Public Sector	**10**
Manager	5
Senior Executive	4
Staff/Technician	1
Retail	**1**
Supervisor	1
Technology and Software	**17**
Consultant	6
Director	3
Manager	2
Senior Executive	4
Staff/Technician	2
Total	**62**

Table 1. Demographic profile of respondents

5 Results

To ensure the reliability of the study, we performed the Reliability Analysis to test the internal consistency of related set of questions for each construct. Although Cronbach's alpha is a widely used measurement for internal consistency, it can be easily affected by the number of items in each construct and lead to underestimated results. Hence, we used composite reliability to measure the internal consistency with threshold value of 0.6. Composite reliability is based on factor loadings rather than the correlations observed between the variables.

Convergent validity is another important parameter that refers to the degree which two measures of constructs that theoretically should be related, are in fact related. For convergent validity, the Average Variance Extracted (AVE) of all latent variables should exceed the recommended 0.5 threshold [40].

Table 2 indicates the composite reliability and average variance extracted values of each latent variable. While the values for Perceived Cybersecurity Risk is close to the thresholds, it suggests that the internal consistency and convergent validity of measured variables are acceptable for the study.

After confirming the reliability of the structural model, a complete bootstrapping process was conducted to test the significance of the model at the level of 0.05 confidence interval. We used Bias-Corrected and Accelerated (BCa) bootstrap for estimating nonparametric confidence interval. To ensure the stability of the results, the number of subsamples is 5000. A hypothesis will be accepted only if the test statistics (t-value) is larger than 1.96. Table 3 shows a summary of the hypotheses tests.

Latent Variable	Composite Reliability Value	Average Variance Extracted (AVE)
Cyber Attack Experience	0.85	0.73
Perceived Cybersecurity Risk	0.67	0.51
Perceived Cybersecurity Value	0.94	0.89
Social Preferences	0.79	0.58
Willingness to Cooperate	0.85	0.73

Table 2. Composite reliability and average variance extracted values of each latent variable

Hypothesis	Original Sample (β)	t-Value	Supported?
H1	0.37	2.09	Yes
H2	0.25	1.97	Yes
H3	0.47	4.13	Yes
H4	0.05	0.36	No
H5	0.13	1.59	No
H6	0.30	2.19	Yes

Table 3. Summary of hypothesis tests

As these results show, Cybersecurity Attack Experience (H1) has a significant positive effect on the Perceived Cybersecurity Value. As for H2, Perceived Cybersecurity Risk has a significant positive effect on Perceived Cybersecurity Value. Cybersecurity Attack Experience (H3) also has a significant positive effect on Willingness to Coop-

erate. Regarding H4 and H5, Perceived Cybersecurity Value (H4) and Perceived Cybersecurity Risk (H5) have positive effect on Willingness to Cooperate but not statistically significant which suggests that H4 and H5 are rejected. Finally, hypothesis H6 is supported as the results show Social Preferences have significant effect on Willingness to Cooperate.

Finally, to measure the social preferences of the respondents, we used Social Value Orientation (SVO) framework proposed by Murphy et al [41]. Figure 3 illustrates a graphical representation of the SVO framework.

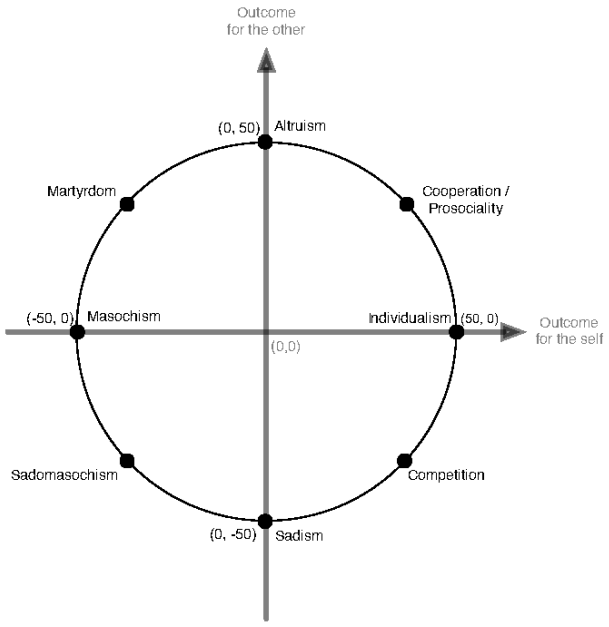

Fig. 3. A graphical representation of Social Value Orientation framework [41].

Figure 4 indicates the ranges within which relevant social preference angles are fallen. These results show that the cooperative behavior among the decision makers in the context of cybersecurity is dominant.

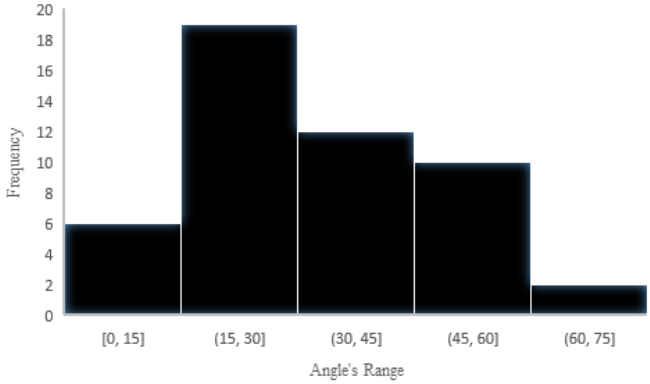

Fig. 4. The ranges of social preference angles

6 Discussion

The significant positive effects of cyber attack experience on willingness to cooperate suggests that organizations that have experienced cyber attacks are more willing to establish or maintain cooperative relationships with other third parties to mitigate the likelihood or impact of future incidents. The consistency between the results of theoretical model and the findings of respondents' social preferences shows that the decision maker's attitude is towards cooperation in the context of cybersecurity.

While the results of this study show that perceived cybersecurity risk and value have positive, but not significant, effects on willingness to cooperate, the related hypotheses are not supported here (hypotheses H4 and H5). A possible explanation is that cybersecurity concerns cause decision makers to delay or ignore cooperation with other organizations. As a result, this lessens their ability to open their network to outside suppliers and third parties.

As for social preferences, the analysis confirms their effective impact on willingness to cooperate. This result suggests that decision makers will reciprocate by adopting positive attitudes to establish or maintain cooperation if other organizations treat them fairly. They even are positive to take retaliatory action against the third parties that cause a cybersecurity incidents or misuse of other organizations' sensitive and confidential information. In this study, a retaliatory action is defined as the discharge, suspension or demotion of a third party, or other adverse business and operational action taken against a third party in the terms and conditions of the contract.

Additionally, the results show that cyber attack experience and perceived cybersecurity risk have significant positive effect on perceived cybersecurity value. However, the mediation analysis of these two variables does not show a significant effect on willingness to cooperate. This outcome can be perfectly explained by the influence of perceived cybersecurity value in opening the door to other third parties.

6.1 Theoretical and Practical Implementation

By testing our research model, this study provides a number of theoretical and practical insights for cybersecurity decision makers to improve their overall cybersecurity posture in their third parties ecosystem. Theoretically, the primary contribution of this study has been to reveal the positive effect of social preferences on the willingness to cooperate among the organizations considering the cybersecurity risks and uncertainties. Previous studies have verified the behavioral models in the context of cybersecurity. This study extends current research and provides evidence that social preferences along with cyber attack experience are essential parts of cooperative willingness.

As the second contribution, this model confirms that perceived cybersecurity risk and value have the strongest impact on the avoidance of cooperation among the organizations. Environmental uncertainties, caused by third parties attacks and weaknesses, and behavioral uncertainty caused by imperfect information or information asymmetry can be two main reasons of this phenomenon. Therefore, our practical implications are mainly directed towards CISOs, but also valuable for other decision makers. To help trusted information sharing, organizations should employ an appropriate, right third party risk management framework based on their structure and business ecosystems. Doing so, they are able to assess the distributed cybersecurity risks in their digital value chain as precise as possible.

7 Conclusions

Cybersecurity decisions are usually not made in a certain, predictable, and isolated environment. Research on the economics of cybersecurity has been largely covered with different perspectives. In this study, we presented a theoretically derived model to explain the impact of social preferences, perceived cybersecurity risk and value, and cyber attack experience on willingness to cooperate in third party ecosystems in the context of cybersecurity. We used variance-based approach of Structural Equation Modeling, so-called Partial Least Square (PLS), to test our research model and analyze the impact of each variable.

The results showed that social preferences and cybersecurity attack experience have significant positive impacts on the willingness to cooperate, and that the dominant preference among the decision makers is towards cooperation and reciprocal behavior. The model also explains that perceived cybersecurity risk and perceived cybersecurity value deter the organizations to cooperate in the context of cybersecurity. The structural equation modeling analysis provides evidence for the small mediating effect of cybersecurity attack experience and perceived cybersecurity risk by perceived cybersecurity value. This highlights the importance of the reduction of victimization and improving the defense controls to enhance the overall cybersecurity posture in the ecosystem.

Our results have some limitations: The composite reliability and average variance extracted values of Perceived Cybersecurity Risk is very close to the thresholds. Future research should overcome this limitation by testing the research model using validated instruments suggested in [42]. The analysis of a single Norwegian organizations sample also limits our results. As Dinev [43] demonstrates the importance of cultural aspects

when studying cybersecurity behavior, a more comprehensive picture should be compared between different countries.

Since the results of this study show cooperative behavior among the organization in the context of cybersecurity, it is crucial to understand the forces shaping this cooperation. Moreover, we will investigate the impact of free-riding incentives and externalities of weak cyberdefenses, as the most important problems in cooperation [44], on the overall cybersecurity posture of the ecosystem. Next step of this study is to use the results of this theory to design and develop serious games that help decision makers to understand the cooperation problems and analyze the conditional cooperation and strategic or non-strategic retaliatory actions. The prototype of these games are an extension of CyberAIMs (Cyber Agents' Interactive Modeling and Simulation) [45], a simulation tool for training System and Adversarial Thinking and strategic decision making.

Acknowledgement

We would like to express our special thanks of gratitude to The Norwegian Business and Industry Security Council (NSR) as well as Mr. Adam Szekeres and Mr. Eivind Kristoffersen Ph.D. Candidates in Information Security, that helped us to design and distribute the survey of this study.

References

[1] P. L. Bernstein and P. L. Bernstein, *Against the gods: The remarkable story of risk*. Wiley New York, 1996.

[2] "Managing Insider Risk Through Training and Culture Report," 2016.

[3] S. Kowalski, "IT insecurity: A multi-disciplinary inquiry.," 1996.

[4] H. Øverby and J. A. Audestad, *Digital Economics*. 2018.

[5] "IT Security: cost-center or strategic investment?," 2017.

[6] HIPAA Journal, "31,876 Managed Health Services of Indiana Health Plan Members Notified of Impermissible Disclosure of PHINo Title," 2019. [Online]. Available: https://www.hipaajournal.com/31876-managed-health-services-indiana-members-data-breaches/.

[7] I. Arghire, "New Magecart Group Targets French Ad Agency," 2019. [Online]. Available: https://www.securityweek.com/new-magecart-group-targets-french-ad-agency. [Accessed: 25-Jan-2019].

[8] R. Anderson and T. Moore, "The Economics of Information Security," *Science (80-.).*, 2006.

[9] C. Vishik, F. Sheldon, and D. Ott, "Economic incentives for cybersecurity: Using economics to design technologies ready for deployment," in *ISSE 2013 Securing Electronic Business Processes*, Springer, 2013, pp. 133–147.

[10] L. A. Gordon and M. P. Loeb, "The Economics of Information Security Investment."

[11] E. Cartwright, *Behavioral economics*. Routledge, 2014.

[12] C. Arney, "Predictably irrational: the hidden forces that shape our decisions," *Math.*

Comput. Educ., vol. 44, no. 1, p. 68, 2010.

[13] R. H. Thaler, "Nudge: Improving decisions about health, wealth, and happiness." Yale University Press New Haven & London, 2008.

[14] D. Kahneman and P. Egan, *Thinking, fast and slow*, vol. 1. Farrar, Straus and Giroux New York, 2011.

[15] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change1," *J. Psychol.*, vol. 91, no. 1, pp. 93–114, 1975.

[16] P. Dolan, M. Hallsworth, D. Halpern, D. King, R. Metcalfe, and I. Vlaev, "Influencing behaviour: The mindspace way," *J. Econ. Psychol.*, vol. 33, no. 1, pp. 264–277, 2012.

[17] P. Briggs, D. Jeske, and L. Coventry, "Behavior change interventions for cybersecurity," in *Behavior Change Research and Theory*, Elsevier, 2017, pp. 115–136.

[18] M. Fishbein and I. Ajzen, "Belief, attitude, intention, and behavior: An introduction to theory and research," 1977.

[19] I. Ajzen, "The theory of planned behavior," *Organ. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, 1991.

[20] S. Michie, R. West, R. Campbell, J. Brown, and H. Gainforth, *ABC of behaviour change theories (ABC of behavior change): An essential resource for researchers, policy makers and practitioners*. Silverback Publishing (Silverback IS), 2014.

[21] T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson, "Variables influencing information security policy compliance: a systematic review of quantitative studies," *Inf. Manag. Comput. Secur.*, vol. 22, no. 1, pp. 42–75, 2014.

[22] Cisco, "What Are the Most Common Cyberattacks?," 2018. [Online]. Available: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html. [Accessed: 25-Nov-2018].

[23] P. Insfitute, "Data risk in the third-party ecosystem," Ponemon Insfitute 2016 Research report. http://www. buckleysandler. com …, 2016.

[24] K. F. Ferraro and R. L. Grange, "The measurement of fear of crime," *Sociol. Inq.*, vol. 57, no. 1, pp. 70–97, 1987.

[25] M. Visser, M. Scholte, and P. Scheepers, "Fear of crime and feelings of unsafety in European countries: Macro and micro explanations in cross-national perspective," *Sociol. Q.*, vol. 54, no. 2, pp. 278–301, 2013.

[26] "Cybersecurity as a Growth Advantage," 2016.

[27] O. Wilde, W. Schmalenbach, and A. Leonhardi, *Lady Windermere's Fan*. Library Editions LLP 4001, 1947.

[28] S. H. Schwartz, "Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries," in *Advances in experimental social psychology*, vol. 25, Elsevier, 1992, pp. 1–65.

[29] L. Sagiv and S. H. Schwartz, "Value priorities and subjective well-being: Direct relations and congruity effects," *Eur. J. Soc. Psychol.*, vol. 30, no. 2, pp. 177–198, 2000.

[30] L. Sagiv, N. Sverdlik, and N. Schwarz, "To compete or to cooperate? Values' impact on perception and action in social dilemma games," *Eur. J. Soc. Psychol.*, vol. 41, no. 1, pp. 64–77, 2011.

[31] R. B. Kline, *Principles and practice of structural equation modeling*. Guilford publications, 2015.

[32] J. Jacoby, "Consumer research: A state of the art review," *J. Mark.*, pp. 87–96, 1978.

[33] S. M. Shugan, “Marketing science, models, monopoly models, and why we need them.” INFORMS, 2002.

[34] M. Haenlein and A. M. Kaplan, “A beginner’s guide to partial least squares analysis,” *Underst. Stat.*, vol. 3, no. 4, pp. 283–297, 2004.

[35] J. Henseler, C. M. Ringle, and R. R. Sinkovics, “The use of partial least squares path modeling in international marketing,” in *New challenges to international marketing*, Emerald Group Publishing Limited, 2009, pp. 277–319.

[36] W. W. Chin and P. R. Newsted, “Structural equation modeling analysis with small samples using partial least squares,” *Stat. Strateg. small sample Res.*, vol. 1, no. 1, pp. 307–341, 1999.

[37] C. Fornell and F. L. Bookstein, “Two structural equation models: LISREL and PLS applied to consumer exit-voice theory,” *J. Mark. Res.*, pp. 440–452, 1982.

[38] J.-M. Becker and I. R. Ismail, “Accounting for sampling weights in PLS path modeling: Simulations and empirical examples,” *Eur. Manag. J.*, vol. 34, no. 6, pp. 606–617, 2016.

[39] A. Falk, A. Becker, T. Dohmen, D. Huffman, and U. Sunde, “The preference survey module: A validated instrument for measuring risk, time, and social preferences,” 2016.

[40] C. Fornell and D. F. Larcker, “Evaluating structural equation models with unobservable variables and measurement error,” *J. Mark. Res.*, pp. 39–50, 1981.

[41] R. O. Murphy, K. A. Ackermann, and M. Handgraaf, “Measuring social value orientation,” 2011.

[42] M. S. Featherman and P. A. Pavlou, “Predicting e-services adoption: a perceived risk facets perspective,” *Int. J. Hum. Comput. Stud.*, vol. 59, no. 4, pp. 451–474, 2003.

[43] T. Dinev, J. Goo, Q. Hu, and K. Nam, “User behaviour towards protective information technologies: the role of national cultural differences,” *Inf. Syst. J.*, vol. 19, no. 4, pp. 391–412, 2009.

[44] J. M. Bauer and M. J. G. Van Eeten, “Cybersecurity: Stakeholder incentives, externalities, and policy options,” *Telecomm. Policy*, vol. 33, no. 10–11, pp. 706–719, 2009.

[45] E. Zoto, S. Kowalski, E. A. Lopez-Rojas, and M. Kianpour, “Using a socio-technical systems approach to design and support systems thinking in cyber security education.”