Navigating the Shadows: Analyzing Negotiation Strategies in Ransomware Incidents and their Impact on Outcome

Frank Westerveld

Faculty of Behavioural, Management and Social Sciences
Departments of Business Administration and Communication Science
University of Twente

Thesis
MSc Business Administration
MSc Communication Science

First supervisor: Dr. H. Kizgin
Second Supervisor: Dr. A.A.C.G. van der Graaf
Third Supervisor: Dr. G.M.A. Lodder

7th of April, 2024

Abstract

Purpose - This study investigates the impact of various negotiation strategies on ransomware negotiation outcomes from the victim's perspective. It offers a comprehensive theoretical framework on ransomware negotiation concepts and processes, as well as a framework outlining potentially useful crisis negotiation strategies. The foundational premise suggests that victims emphasizing empathy, dignity preservation, and emotional reassurance may achieve more favorable results. Consequently, it was hypothesized that negotiation strategies such as being kind, being equal, emotional appeal, legitimizing, and rational persuasion, would positively influence ransomware negotiation outcomes.

Design/methodology/approach - Drawing upon 16 authentic ransomware negotiations, provided by Northwave Cyber Security, this study utilized coded transcripts as its primary data. The hypotheses were tested using linear regression analysis, employing the discount factor (defined as the variance between the initial ransom amount and the final negotiated ransom amount) as the dependent variable and conceptualization of ransomware negotiation outcome.

Findings - The study could not reject the null hypotheses that employing the aforementioned strategies significantly improve ransomware negotiation outcomes.

Research limitations/implications - The regression analysis was hindered by a small sample size, which compromised the assumptions necessary for regression analysis. This highlights the imperative for future research on larger datasets to ensure robust statistical analyses.

Practical implications - With the theoretical framework outlined in this study, cybersecurity organizations and ransomware victims can gain profound insights into the intricacies of ransomware negotiations, along with potentially valuable crisis negotiation strategies they can utilize in their negotiations with cybercriminals.

Originality/value – To the author’s knowledge, the impact of traditional crisis negotiation strategies on ransomware negotiations has not been academically explored. Hence, this study offers a fresh perspective on ransomware negotiations and presents an exploratory framework for future research.

Acknowledgements

Acknowledging the profound guidance, patience, and feedback provided by Dr. Hatice Kizgin, my esteemed first supervisor, feels like an understatement. Dr. Shenja van der Graaf, my second supervisor, equally deserves heartfelt appreciation for generously sharing her knowledge and expertise. Additionally, I am deeply thankful to Dr. Gerine Lodder, my third supervisor, whose extensive academic insights and practical experience in ransomware negotiations were indispensable throughout this endeavor. Their invaluable guidance made this journey possible.

Special recognition goes to Michalis Georgiou, PhD Candidate at the University of Twente, specializing in ransomware negotiations, whose informal guidance and collaborative coding sessions greatly enriched my research experience. I am also indebted to Prof. Dr. Ellen Giebels, whose illuminating teachings during the University of Twente's Honours programme 'Great Negotiators', specifically on her Table of Ten, ignited my passion for researching this topic.

I am profoundly grateful to Northwave Cyber Security for granting me the opportunity to pursue my graduate research. The supportive environment fostered by every member of the Northwave team, during my internship, significantly contributed to my growth and development. Thank you very much.

Acknowledgment is also due to my family, particularly my grandparents, parents, and partner, whose unwavering belief in me served as a constant source of motivation and encouragement. Finally, and of utmost personal significance to me, I want to honor my late grandfather, Lambert Johan Velthuis, for his unwavering support and guidance throughout my life. I owe my presence here today to his unwavering support and guidance: *Bedankt voor alles opa, deze is voor jou.*

Table of Content

1. Introduction

In recent years, cyber-attacks have surged to become one of the most pressing risks faced by both public and private sectors. This trend, which began gaining momentum in 2020, shows no signs of abating. Projections indicate that by 2025, cyber-attacks targeting Internet of Things (IoT) devices are set to double (McLean, 2024). The COVID-19 pandemic exacerbated the situation, with cybercrime soaring by an alarming 600% (PurpleSec, 2023). Ransomware attacks, in particular, have emerged as a source of concern. Already during the initial six months of 2022, approximately 236.1 million ransomware attacks were documented worldwide (Griffiths, 2024). Ransomware involves the use of malicious software to encrypt computer systems or data, holding them hostage until the victim pays a ransom demanded by the perpetrators. Since its inception, this insidious form of cyber-attack has undergone significant changes and advancements, transforming from a rudimentary attack to a complex and formidable menace in the cyber landscape. The initial attacks like GPCode and Archievus targeted a larger number of victims with relatively smaller ransoms. However, as the technology evolved, so did the ransomware's capabilities and scale of impact. Menacing variants such as CryptoLocker, WannaCry, and Maze ransomware surfaced, inflicting considerable damage on both individuals and organizations. The attacks became more sophisticated, utilizing double extortion tactics and employing anti-analysis techniques to evade detection (Razaulla et al., 2023). Although extortion-based threats seemed to decline in 2018 due to the rise of cryptocurrency mining malware, this period marked a turning point for ransomware, leading to the emergence of "Big Game Hunting." This phenomenon aimed at generating higher revenue through targeted attacks with lower attack volumes (Keshavarzi & Ghaffary, 2023).

Within Big Game Hunting, cyber criminals (often referred to as threat actors) invest substantial effort into breaching these defenses and meticulously calculate the highest ransom they believe their victims will be willing to pay (Faivre, 2022). As the stakes soar, negotiations for the ransom demand become a pivotal and critical element in this sinister game. Researchers, such as Ryan et al. (2022), have shed light on how these threat actors are more open to negotiations, seeking to ensure the payment of higher ransoms. However, despite the growing prevalence and severity of ransomware incidents, there remains a significant knowledge gap regarding the effectiveness of various negotiation approaches in securing favorable outcomes. Wade (2022) highlights the potential of applying crisis and hostage negotiation theories to the cyber domain. While the academic field of crisis and hostage negotiation is extensively researched, its

applicability in the cyber domain remains largely unexplored. Giebels (2002) presents ten specific influence strategies, divided into relational and content strategies. In high-stakes hostage situations, relational strategies emphasizing relationship-building, softer approaches, and emotional elements tend to outperform those focused solely on substantive content, confrontational approaches, or cognitive strategies. These strategies aim to proactively mitigate negative outcomes, particularly during the volatile and uncertain initial phases of such situations, as emphasized by Giebels (2002). Taylor's (2002) comprehensive model on crisis negotiation communication behavior underscores the significance of integrative (relationship-building) interactions over distributive (content-focused) tactics, highlighting the effectiveness of gentler negotiation approaches. However, research exploring the effectiveness of these softer influence strategies within the cyber domain and specifically in ransomware negotiations is lacking. This study aims to address this gap in the literature. To fill this gap, the following research questions have been developed:

Table 1

Research Questions (own elaboration)

Research Question	Emperical Approach	
	Literature review	Data Analysis
What concepts and processes encompass ransomware negotiations?	Yes	No
What could be effective strategies for negotiating with ransomware attackers?	Yes	No
What is the impact of different negotiation strategies on ransomware negotiation outcomes from the perspective of the victim?	Yes	Yes

The study is structured as follows: Initially, it provides a theoretical background followed by the formulation of hypotheses, which suggest the effectiveness of certain negotiation strategies in influencing ransomware negotiation outcomes. Subsequently, chapters three and four delve into the research methodology employed and present the obtained results. Finally, chapter five is dedicated to discussing the results alongside their limitations, while also identifying potential avenues for future research.

2. Theoretical Framework

This theoretical framework will delve into the concepts and processes inherent in ransomware negotiations, utilizing the theoretical insights provided by Bazerman et al. (2000). It will explore the influence of mental models, ethics, communication mediums, the involvement of multiple negotiation parties, and cross-cultural dynamics on ransomware negotiations. Additionally, traditional crisis negotiation theories will be outlined in the second part of this framework, establishing the connection with ransomware negotiations, and proposing five hypotheses. Finally, the dependent variable will be delineated in the last part of this theoretical framework.

2.1. Defining Ransomware Negotiations

According to Thompson et al. (2010), negotiation, a cornerstone of interpersonal decision-making, is especially critical when individuals seek to achieve goals that cannot be attained unilaterally. They delineate two primary outcomes of negotiation: integrative, where agreements optimally satisfy all parties without potential for further benefit without detriment to others, and distributive, characterized by a zero-sum allocation of finite resources, reminiscent of the dynamics in the ultimatum game. According to Bazerman et al. (2000), the process and outcome of negotiations cannot be fully understood without a clearer understanding of various factors, namely negotiators' mental models, ethical considerations, the number of parties within a negotiation, the choice of communication medium, and cross-cultural concepts.

Mental model

Bazerman et al. (2000) define a mental model as a cognitive representation of the expected negotiation, a representation that encompasses understanding of the self, negotiator relationships, attributions about the other, and perceptions and knowledge of the bargaining structure and process. According to Hernandez-Castro et al. (2017), the primary goal of threat actors is presumably to maximize profits derived from infected computers. Within the context of crisis negotiations (further elaboration on this concept will be provided in subsequent paragraphs), this behavior can be interpreted as instrumental, marked by rational decision-making, goal-oriented actions, and substantive demands (Vecchi et al., 2005). Hernandez-Castro et al. (2017) state that the criminal's profit from their ransomware operations can be expressed as a summation over all targeted victims, where each victim's ransom amount is subtracted by the cost of handling ransom money. Additionally, a fixed cost of operating the malware is accounted for in the profit calculation. Hack and Wu (2021) augment this profit

equation by introducing additional variables, providing a comprehensive structural overview of the factors influencing the modus operandi of threat actors. They define P as cybercriminals total profit from N victims. In their equation, Hack and Wu (2021) describe variables such as the ransom demand per victim (in their equation noted as r_i), the percentage of ransom after converting to untraceable currency (in their equation noted as l_i), and the percentage left after paying 'Ransomware-as-a-Service' (additional elucidation on this concept will follow in subsequent paragraphs) fees (in their equation noted as m_i), where they note fees range from 10% to 30%, but can be zero.

$$\mathrm{P} = \Sigma_{i=1}^{\mathrm{N}}(r_i * m_i * l_i) * f(i) - c_i$$

Hack and Wu (2021) assume that cybercriminals also make investments to conduct ransomware attacks (in the equation noted as c_i). These costs include risk costs, which refers to the expenses incurred to avoid being held accountable for the attack (i.e., setting up proxies to hide the attacker's identity, covering up any evidence of human involvement, and even bribing local authorities to avoid detection and legal consequences) and penetration costs: expenses associated with gaining access to the target's network (i.e., hiring skilled hackers, purchasing access to malware, exploits, or distribution services, and any other illicit means of obtaining unauthorized access to the target's network) (Hack & Wu, 2021).

In the above equation (included because of its structured depiction of the instrumental nature of threat actors' operations), the binary function $f(i)$ resembles the binary decision of the victim to pay the ransom or not. They state that key determinants in this 'Willingness to Pay' (WTP) decision-making process include ethics (i.e., firm policies of non-cooperation with criminals), ransom amount (with higher demands potentially deterring payment), remediation costs (crucial for victims; manageable costs compared to the ransom amount may favor recovery over payment), and regulation costs (entailing expenses related to data breach fines, especially under regulations like GDPR) (Hack & Wu, 2021). Further expansion on the concept of ethics will be offered in the following paragraphs. Another variable that directly impacts WTP, not accounted for by Hack and Wu (2021), is the probability of file recovery. The conventional notion suggests that to maximize profit, threat actors should always return files upon payment. However, in the context of ransomware 2.0 (Li & Liao, 2020), an alternative business model emerges, challenging this assumption by introducing the possibility of selling stolen data. Li and Liao

(2020) employ game theory to analyze the dilemma faced by threat actors in deciding whether to sell the data and the corresponding WTP of victims. Within their computational framework, they introduce variables representing the victim's decision to pay the ransom (ρ), the attacker's decision to return the data (r), and the decision to sell the data (s). The profitability anticipated by the attacker from a victim (π) takes into account various factors such as the cost of returning files (C_r), data transaction cost (C_d), and the market value of stolen data (D_i). The utility or payoff for the victim (μ) incorporates elements such as the ransom paid (R), the value of locked files to the victim ($V_{r,i}$), and the potential loss if data is sold ($L_{d,i}$). Game theory analysis reveals multiple outcomes in ransomware negotiations, emphasizing the significance of the threat actor's reputation in influencing WTP. In scenarios where reputation is irrelevant, the decision to sell stolen data becomes more profitable than traditional ransomware tactics. However, cooperation and trust between both parties can lead to mutual benefit, particularly when the value of files exceeds the cost of returning them. This underscores the importance of reputation for ransomware as a sustainable model, highlighting the potential for cooperation within certain ransom ranges.

Table 2

The payoffs to different outcomes in the data-selling ransomware game (Li & Liao, 2020)

Outcome			Attacker (π)	Victim (μ)
$\rho = 0$	$r = 0$	$s = 0$	0	$-V_{r,i}$
$\rho = 0$	$r = 0$	$s = 1$	$D_i - C_d$	$-V_{r,i} - L_{d,i}$
$\rho = 0$	$r = 1$	$s = 0$	$-C_r$	0
$\rho = 0$	$r = 1$	$s = 1$	$D_i - C_d - C_r$	$-L_{d,i}$
$\rho = 1$	$r = 0$	$s = 0$	R	$-R - V_{r,i}$
$\rho = 1$	$r = 0$	$s = 1$	$R+D_i - C_d$	$-R - V_{r,i} - L_{d,i}$
$\rho = 1$	$r = 1$	$s = 0$	$R - C_r$	$-R$
$\rho = 1$	$r = 1$	$s = 1$	$R+D_i - C_d - C_r$	$-R - L_{d,i}$

Ransomware 2.0 represents a significant advancement for threat actors, posing challenges to traditional defense measures. Li and Liao (2020) suggest that while file backups, as advocated by Hernandez-Castro et al. (2017), have been effective against ransomware 1.0, they may not suffice against ransomware 2.0 due to its extortion aspect. Li and Liao (2020) propose the never-pay-ransom strategy as effective against traditional ransomware, where profitability relies on victim compliance. However, this strategy proves less effective against data-selling ransomware, as attackers can profit from selling stolen data irrespective of ransom payment.

Concurrently, the models proposed by Hernandez-Castro et al. (2017), Hack and Wu (2021), and Li and Liao (2020) overlook the financial impact of business disruption on WTP. While they touch on various factors such as victim valuation of files and remediation costs, they fail to address the significant impact of system downtime on business processes. This oversight is critical given the reliance of businesses on enterprise information systems (EIS) for core functions (Zimba & Chishimba, 2019) and the resulting utility costs and WTP implications. Addressing these issues promptly is emphasized as essential by Faivre (2022) to mitigate accumulating costs from disruptions.

Having analyzed the incentives driving both threat actors and victims in ransomware negotiations, thereby hinting at the inherent imbalance in this dynamic, the following paragraph will delve deeper into the ransomware negotiation process. This elaboration aims to expand the mental model by exploring the intricacies of negotiation dynamics.

Li and Liao (2020) outline a four-stage game theory model. In Stage 1, the attacker successfully launches a ransomware attack on N victims, resulting in lost access to files and stolen confidential data. The attacker then demands a ransom payment R. In Stage 2, upon observing R, the victims decide whether to pay the ransom. This stage represents the victims' decision-making regarding ransom payment. Following the victims' decision on ransom payment in Stage 3, the attacker decides whether to return the files. Stage 4 involves the attacker determining the fate of the stolen data—whether to sell it or take no action. Stages 3 and 4 encompass the attacker's follow-up decision-making. However, this game theory model lacks an actual bargaining process. Moreover, it initiates with the attack, neglecting the fact that threat actors often research their victims and consciously employ price discrimination strategies. Limited research has focused on understanding how threat actors determine the initial ransom amount in ransomware attacks. Hack and Wu's (2021) research outlines the evolution of ransomware tactics, with Warikoo (2023) identifying three distinct periods: pre-2014, 2015-2017, and post-2017. During these phases, threat actors adapted their strategies, leading to the emergence of personalized pricing models and the targeting of large organizations through tactics like big game hunting (BGH). Hack and Wu (2021) identify three primary price discrimination strategies employed by threat actors, while Faivre (2022) observes a trend towards a more calculated approach. Analyst1 emphasizes the thorough research conducted by threat actors before negotiations, including gathering information on victims' financial status. An illustrative excerpt comes from a LockBit 3.0 affiliate, who asserts “So why do you start

with lies. We know exactly what kind of company you are. How much money you make, how many employees you have, computers, and so on. The ransom price is always fair. $4,000,000" (Sentsova & DiMaggio, 2023). Additionally, Sentsova and Dimaggio (2023) state that the presence of cyber insurance influences ransom amounts, with threat actors aiming to maximize payouts from insured amounts. With these calculated pricing strategies in mind, Faivre (2022) sheds light on the negotiation process (see Appendix A), indicating that cybercriminals present a ransom demand (R) and await the victim's response. The victim, influenced by their WTP, may choose to accept, reject, or propose a counteroffer. Threat actors, in turn, may accept, raise the counteroffer, or reject it, opting for alternative actions such as selling the data. Despite seeming contrary to rationality, this behavior aligns with cybercriminals' positions, which often start at or below zero due to initial investments in the ransomware attack. Hack and Wu (2021) previously introduced these initial investments as the cost of carrying out the ransomware attack (c_i), encompassing "Risk cost" and "Penetration costs."

Ethics

In addition to mental models, Bazerman et al. (2000) highlight the significance of ethical considerations in negotiation. Ethics establish general standards for acceptable conduct and guide negotiators in determining permissible strategies. The preceding paragraph shows that Hack and Wu (2021) have already incorporated ethics as a factor influencing WTP. Hofmann (2020) expands upon victim's ethics, stating that many organizational leaders initially refrain from negotiation or payment in ransomware situations due to ethical concerns and the fear of funding criminal activities. However, when critical assets like personal data or life-saving medical devices are at risk, organizations may have no alternative but to pay. Despite being a last resort, paying the ransom ensures a safer strategy, with 95% of organizations regaining access to their data or systems after payment. Furthermore, ransomware attacks now commonly involve threats to leak data if the ransom remains unpaid (Hack & Wu, 2021; Hofmann, 2020; Li & Liao, 2020). This trend is a response to stringent global data protection regulations like the General Data Protection Regulation (GDPR), which impose significant financial penalties on organizations experiencing breaches, thereby increasing the likelihood of ransom payment to prevent breaches entirely. According to Hofmann (2020) the decision to pay a ransom revolves around two primary factors: ethical considerations, particularly when sensitive personal data, critical infrastructure, or lives are at risk, and financial implications, where the cost of downtime may outweigh the ransom amount. Should an organization opt to proceed with ransom payment, Hoffman (2020) claims that several crucial steps must be taken to ensure

a professional and secure process. Firstly, conventional incident response procedures should be initiated, involving forensic analysis to assess data and system recovery possibilities from backups. Simultaneously, organizations should open communication channels with the attacker, potentially negotiating for a reduced ransom and confirming decryption capabilities through a decrypted key. Next to that, is advisable to engage a negotiation specialist with expertise in specific ransomware strains and threat actor behavior, providing valuable intelligence for informed decision-making and negotiation tactics. Critical components of the negotiation process include requesting a 'proof of life' demonstration from the hackers by decrypting a portion of the hostage files. Additionally, organizations must strategically plan ransom payment, prioritizing the restoration of essential operations and swiftly backing up restored systems to fortify against future attacks (Hofmann, 2020).

Faivre (2022) discusses the predatory nature of cybercriminals in targeted ransomware attacks, likening the negotiation dynamic to kidnapping scenarios. Cybercriminals meticulously choose targets through research and cost-benefit analysis, causing significant operational disruptions and exploiting victims' vulnerabilities. This power imbalance is exacerbated by victims' lack of information about the cybercriminals, hindering their ability to improve their negotiating position. Contrary to the perception of cybercriminals solely driven by financial motives, Hofmann (2020) highlights ethical considerations within the threat landscape. The Hollywood Presbyterian Medical Center attack, for instance, faced criticism from Eastern European cybercriminals for its recklessness and unacceptability despite targeting Westerners. While some underground community members supported the attack, a majority condemned the perpetrators, revealing an ethical divide. Financial incentives have gradually overshadowed ethical concerns since 2016, as evidenced by the shift towards profit-making motives. LockBit 3.0 syndicate, as illustrated by Analyst1 (Sentsova & DiMaggio, 2023), exemplifies this shift with the introduction of stringent negotiation guidelines aimed at maximizing ransom payouts. These rules recommend ransom amounts as a percentage of victim companies' revenue, with specific ranges based on revenue brackets, and enforce restrictions on discount offers to increase the likelihood of payment.

Number of Negotiation Parties

The LockBit 3.0 rules of conduct, as highlighted by Sentsova and DiMaggio (2023), offer initial insights into the intricate nature of the threat landscape and the diverse stakeholders involved in ransomware negotiations. Meland et al. (2020) discuss the emergence of Ransomware-as-a-Service (RaaS) on darknet markets, presenting it as a franchise-like model enabling individuals lacking programming expertise to engage in ransomware attacks and profit from the illicit economy. This phenomenon democratizes criminal activity, providing entry opportunities for ordinary individuals and smaller actors, while simultaneously mitigating the risk of detection and exposure for those orchestrating the operations at the apex of the criminal hierarchy. According to Keijzer (n.d.), ransomware attacks typically unfold in three phases: the IN phase for initial access, the THROUGH phase for control acquisition, and the OUT phase for leverage. Keijzer (n.d.) delineates seven distinct roles involved in these attacks, with the initial access broker obtaining entry to victim networks, ransomware affiliates executing lateral movement and deploying ransomware, and data managers handling exfiltration tasks. Furthermore, ransomware operators oversee the ransomware business model (e.g., developing ransomware or hosting infrastructure), negotiators engage in ransom discussions with victims, chasers apply pressure for payment, and accountants launder ransom proceeds. Notably, these roles operate independently and exhibit specialized functions, indicating a complex and orchestrated value chain within ransomware operations. Recent arrests targeting money laundering activities associated with ransomware underscore the involvement of distinct actors in different facets of the criminal enterprise. According to Bazerman et al. (2000), as the number of parties in a negotiation grows, the complexity of the dispute escalates rapidly. Negotiators often simplify the negotiation process by relying on group norms, forming coalitions, or implementing decision-making procedures (as illustrated in the LockBit 3.0 code of conduct outlined by Sentsoca and DiMaggio, 2023).

Choice of Communication Medium

According to Bazerman et al. (2000), the method of communication plays a crucial role in negotiation outcomes. Face-to-face interaction fosters trust and honesty, while written or digital communication can breed suspicion and impede progress. Griessmair et al. (2015) further explain that the choice between synchronous and asynchronous digital channels affects real-time interaction and the ability to review exchanges. Faivre (2022) adds that in ransomware negotiations, trust-building is challenging due to the transactional nature of the interaction, lacking a focus on long-term relationships. Additionally, cybercriminals assert their dominance

through verbal communication, often employing dictatorial tones and issuing threats to limit victims' alternatives. They exploit human vulnerabilities through social engineering tactics, manipulating emotions to induce irrational behavior. For instance, during the WannaCry attack, cybercriminals used dynamic visuals and timers to evoke a sense of urgency and danger among victims (Faivre, 2022).

Cross Cultural Differences

According to Bazerman et al. (2000), cross-cultural differences in negotiation can be analyzed across four key dimensions: collectivism-individualism, power distance, communication context, and perceptions of time. While much research has focused on collectivism-individualism, exploring behavioral and cognitive aspects, relying solely on cultural value dimensions has limitations in predicting outcomes. Integrating mental models with cultural factors may offer more promising insights. However, the practical viability of such changes for typical negotiators remains unconfirmed by research.

Understanding cybercriminal characteristics presents challenges due to limited access to offenders and reliance on self-reported data (Stoddart, 2022). Stoddart (2022) highlights Russia and China as the primary cyber threats to the West, with North Korea and Iran posing lesser threats. Organized crime groups, particularly from Eastern Europe with ties to Russia, are heavily involved in cyberattacks, often operating in gray zones with some degree of state protection, effectively becoming state-protected 'privateers.' This relationship varies from delegation to orchestration and sanctioning, with states like Russia benefiting from plausible deniability. The complexity of cyber threats extends beyond state actors, involving industrial competitors, foreign intelligence services, hackers, and hacktivists, sometimes leading to misattributions and false flags.

Despite sparse academic literature, numerous reports and blog posts offer valuable insights. Cyberclan.com (*Demographics and Motivation of Cyber Attacks by Nation State Actors: New Kids on the Block*, 2023) reports a 20% increase in nation-state cyber-attacks on critical infrastructure in 2023, largely attributed to Russia's actions against Ukraine (These attacks may not necessarily involve ransomware but could manifest as other forms of intrusion as well). Private organizations also face targeting, with 86% claiming victimization. Stoddart (2022) suggests many organized crime networks, especially those tied to Russia, are rooted in Eastern Europe, often with tacit approval from the Russian state as long as they serve national interests.

These networks may adopt negotiation tactics influenced by Russian cultural norms characterized by high-context communication (Adair et al., 2004; Kamphuis et al., 2006). Other significant players in nation-sponsored cyber-attacks include Iran, China, North Korea, and Iraq. The EU CERT (*Threat Landscape Report 2023*, n.d.) acknowledges the complexity of attributing threat actors to specific countries. In 2023, Russia-linked cyber activity targeted Ukrainian organizations and those associated with the war on Ukraine. China-focused actors targeted specific sectors, employing shared tools and infrastructure, posing challenges for differentiation. Increased Iran-linked activity coincided with events like the Israel-Hamas conflict. The complexity of the threat landscape and the involvement of various cultures in ransomware negotiations are evident. When considering the threat actor value chain outlined by Keijzer (n.d.), it becomes apparent that negotiators may not necessarily operate from the countries one would expect. This makes pinpointing cross-cultural dynamics in ransomware negotiations extremely challenging.

Definition

Ransomware negotiations present formidable challenges rooted in the need to comprehend the decision-making processes of both threat actors and victims. This necessitates a thorough understanding of the profitability of ransomware operations for attackers, as well as the WTP for victims, all while navigating complex ethical considerations. Ethical dilemmas loom large, as organizations confront the moral quandary of whether to submit to ransom demands, while simultaneously grappling with the potential ramifications of data breaches and financial losses. The involvement of multiple stakeholders, including the threat actor value chain, victims, and intermediary negotiators, amplifies the complexity of these negotiations. Communication channels between threat actors and victims further complicate matters, particularly in digital environments where trust-building is hindered by the absence of face-to-face communication and cybercriminals' exploitation of human vulnerabilities. Additionally, ransomware negotiations often traverse cultural boundaries, demanding a nuanced understanding of diverse communication norms and practices. Successfully integrating these cultural nuances into negotiation strategies requires meticulous attention. Moreover, negotiation dynamics are heavily influenced by financial considerations, including the economic impact of business disruptions caused by ransomware attacks. Furthermore, the ever-evolving landscape of ransomware tactics, exemplified by the advent of ransomware 2.0 and the adoption of protocols such as Lockbit 3.0's code of conduct, underscores the ongoing challenges faced by defenders.

Thus, adapting to these dynamic tactics is imperative for achieving successful outcomes in ransomware negotiations within an increasingly sophisticated threat landscape.

Based on the above elaboration, this study defines ransomware negotiations as the intricate and multifaceted interactions between threat actors and victims, encompassing the process of navigating complex decision-making dynamics amidst ethical dilemmas, financial considerations, and cultural nuances. These negotiations entail assessing the profitability of ransomware operations for attackers, evaluating the willingness of victims to comply with demands, and managing the involvement of multiple stakeholders, including intermediaries like negotiation specialists. Communication channels between threat actors and victims, often conducted digitally, present challenges in trust-building and understanding due to cybercriminals' exploitation of human vulnerabilities. Successful ransomware negotiations require a holistic approach that integrates ethical, financial, and cultural factors while adapting to the evolving tactics employed by threat actors in an ever-changing threat landscape.

2.2. Crisis negotiation strategies

Now that the concept of ransomware negotiations is clearly defined, this study delves into the concept of crisis negotiations, as Wade (2022) highlights the potential of applying crisis and hostage negotiation theories to the cyber domain. Distinct from conventional negotiation paradigms, crisis negotiation emerges in high-stakes environments, marked not by collaborative intent but by a coercive, often manipulative atmosphere where the assumption of good faith is absent. Central to crisis negotiation are scenarios involving direct threats to life or safety, such as hostage-taking for instrumental gains (e.g., ransom) or expressive purposes (e.g., power assertion), necessitating specialized intervention strategies (Rogan & Hammer, 1995; Vecchi et al., 2005). This domain finds contemporary relevance in ransomware attacks, where cybercriminals, akin to traditional hostage-takers, leverage data encryption or exfiltration to extort, employing strategies that mirror the instrumental objectives of classic hostage scenarios. This analogy thus underscores the potential of applying crisis and hostage negotiation theories to the cyber domain, suggesting a methodological crossover for addressing and mitigating the impacts of ransomware incidents (Wade, 2022). Through this lens, the academic discourse around negotiation can be expanded to include digital extortion, bridging traditional concepts with modern cybersecurity challenges.

Grubb (2010) provides an overview of crisis negotiation in the 21st century, by reviewing literature on hostage negotiation historically, the dynamics of crisis situations typically encountered by hostage negotiators the models existing to conceptualize crisis negotiation, and the strategies utilized by negotiators to successfully resolve crisis negotiations.

Fisher and Ury (1981, as cited in Grubb, 2010) introduced principled negotiation, emphasizing an "interest-based" approach to conflict resolution. Their model advocates four key principles: separating the person from the problem, focusing on mutual interests rather than individual positions, generating options for mutual gain, and insisting on objective criteria to judge agreements' effectiveness. By dissociating individuals from the issue, parties can avoid perceiving responses as personal attacks. Prioritizing interests over positions allows for solutions satisfying both parties. Generating options fosters successful conflict resolution by seeking mutual benefits. Objective criteria, such as scientific findings or legal precedent, are crucial for evaluating agreements, especially in conflicting interest scenarios. While influential, this model has been critiqued for its limited applicability in crisis situations involving individuals in irrational cognitive states, such as severe mental illness or emotional conflict, hindering their ability to engage in rational negotiation processes. Ury (1991, as cited in Grubb, 2010) expanded upon his earlier work, devising a five-step model for challenging negotiations, including hostage situations. The first step, 'Don't React—Go to the Balcony', advises negotiators to observe rather than engage emotionally, akin to a third-party observer on a balcony watching a play. The second step, 'Stepping to Their Side', involves portraying the hostage taker as an ally, fostering collaboration through active listening techniques. 'Change the Game', the third step, entails reframing demands to explore solutions and alternatives. 'Build a Golden Bridge', the fourth stage, aims to facilitate agreement by involving the subject in decision-making, fostering collaboration and avoiding resistance. Encouraging the hostage taker to say yes not only aids negotiation but also preserves their dignity, facilitating resolution. This model concludes with the stage titled 'Make it Hard to Say No', which builds upon the fourth stage by not only increasing the subject's inclination to say yes, but also making it challenging for them to refuse, thereby enhancing the likelihood of successful resolution. While this model offers a toolkit of techniques for crisis situations, it relies on some degree of cognitive rational processing from both parties, a feature often absents in the mindset of hostage takers. Given the common involvement of emotionally disturbed or mentally disordered individuals in crisis incidents, it's likely that a different negotiation approach, less systematic or hierarchical and more crisis-intervention based, will be necessary. Once cognitive processes

and rationalization have been somewhat restored, more cognitively based problem-solving techniques, such as those discussed above, can be employed (Grubb, 2010). Donohue et al. (1991, as mentioned in Grubb, 2010) present a model distinguishing between crisis (distributive) and normative (integrative) bargaining strategies employed by hostage negotiators. They emphasize the negotiation's focus on relationship (expressive) and substantive (material) issues, with initial stages addressing relational aspects like power dynamics and trust, shifting towards material concerns once relational issues are resolved. The aim is to move hostage takers away from crisis bargaining towards normative bargaining for crisis resolution. Hammer and Rogan (1997, as cited in Grubb, 2010) echo this, urging negotiators to transition from relational and identity-focused crisis bargaining to normative bargaining centered on instrumental needs, facilitating successful crisis resolution. This approach prioritizes adapting negotiation styles to meet the perpetrator's needs, whether crisis or normative bargaining, rather than focusing on specific techniques (Grubb, 2010). The S.A.F.E. model, developed by Hammer and Rogan (1997, as citred in Grubb, 2010), offers a structured approach to crisis negotiation, drawing from behavioral science research and input from experienced negotiators. It identifies four key triggers—Substantive Demands, Attunement, Face, and Emotion—that influence subject behavior during crises. Each trigger represents a communicative frame guiding the interaction between negotiator and subject. Substantive Demands focus on problem-solving for peaceful surrender, Attunement on building relational trust, Face on validating the subject's self-image, and Emotion on addressing emotional distress. Negotiators aim to identify the subject's dominant frame and tailor their communication style accordingly to facilitate de-escalation and resolution. The Behavioral Influence Stairway Model (BISM), developed by Vecchi (2007, as cited in Grubb, 2010), is a crisis negotiation model based on active listening principles, adapted from the Federal Bureau of Investigation Crisis Negotiation Unit (FBI CNU). It emphasizes relationship-building between negotiator and subject to achieve a peaceful resolution. Drawing parallels with Motivational Interviewing, the BISM focuses on skills like empathy, rapport, and active listening to facilitate behavior change. It comprises four elements: active listening skills, empathy, rapport, and behavioral influence. Progression through the stages involves utilizing these skills, with active listening as a foundational aspect. Effective use of these skills increases the likelihood of positive behavior change and crisis resolution, as evidenced by research (Vecchi et al., 2005, as cited in Grubb, 2010).

The Cylindrical Model of Crisis Negotiation, developed by Taylor (2002, as cited in Grubb, 2010), emphasizes the complexity of negotiation by focusing on levels of interaction, motivational emphases, and behavior intensity. Based on qualitative data from nine resolved hostage negotiation cases, the model identifies three levels of interaction: avoidance, distributive, and integrative. Negotiators aim to progress subjects through these levels to achieve cooperation and reconciliation of divergent interests. Additionally, the model identifies three motivational emphases: Instrumental, Relational, and Identity themes, reflecting subjects' needs, relationships, and concerns for self-preservation. Lastly, the model considers the intensity of negotiation behavior, noting that intense behaviors can hinder negotiation success. Taylor's model offers a dynamic view of negotiation behavior, facilitating a comprehensive understanding of communication patterns throughout the negotiation process. Lastly, the Structured Tactical Engagement Process (STEPS) model, developed by Kellin and McMurtry (2007, as cited in Grubb, 2010), draws from the domain of change management to provide a framework for managing crisis situations. The model identifies four stages: Precontemplation, Contemplation, Preparation, and Action, each representing the subject's progression toward behavioral change and peaceful resolution. Negotiators utilize various skills and techniques to guide subjects through these stages. Initially, subjects may be uncooperative and unrealistic (Precontemplation), requiring negotiators to build rapport to encourage contemplation of change. As subjects move into contemplation, negotiators affirm the need for resolution while increasing confidence. In the Preparation stage, subjects commit to change and negotiators become more proactive in problem-solving to develop an exit strategy. Finally, in the Action stage, subjects implement the agreed-upon plan, with negotiators providing support and direction until resolution is achieved. The STEPS model integrates concepts from the transtheoretical model of change and motivational interviewing to facilitate behavior change in crisis situations, emphasizing the importance of establishing rapport and positive relationships.

These various theories and models of crisis negotiation discussed share common principles aimed at facilitating peaceful resolutions in challenging situations. Central to these approaches is the emphasis on building rapport and trust between negotiators and subjects, recognizing the critical role of positive relationships in achieving successful outcomes. Moreover, the problem-solving orientation emphasized in many models underscores the importance of generating options for mutual gain and exploring alternatives during negotiations. Adaptability is another key theme, with negotiators encouraged to tailor their strategies based on the evolving dynamics of the situation and the stage of negotiation. Additionally, several models incorporate the

concept of stages of change, acknowledging that subjects may progress through different phases of readiness for behavior change during the negotiation process. While some theories assume rational cognitive processing, others acknowledge the presence of emotionally distressed individuals, highlighting the need for flexible and adapted approaches in such cases. Together, these common elements highlight the multifaceted nature of crisis negotiation and the diverse skills and strategies required to navigate and resolve complex crisis incidents effectively. As Wade (2022) mentioned, there is a potential of applying crisis and hostage negotiation theories to the cyber domain. He introduces the "Wade and Seek" methodology, advocating for building rapport with hackers by recognizing their expertise and showing willingness to cooperate. His theory, in combination with traditional crisis negotiation discourse, highlight the importance of addressing the relational dimensions within ransomware negotiations, suggesting that an effective negotiation strategy should involve not only determining the ransom amount but also skillfully managing the interpersonal dynamics with the adversarial parties. Thus, establishing rapport emerges as a potentially advantageous strategy. The concept of rapport-building sheds light on various techniques such as effective verbal and non-verbal communication, finding common ground, and offering support and understanding, all aimed at fostering productive dialogue (Vallano & Compo, 2015). Vallano and Compo (2015) conceive rapport in a broader sense as a productive working relationship that yields actionable intelligence, proposing that such a relationship, while not always positive, should facilitate the achievement of investigative objectives.

While Vallano and Compo's (2015) exploration provides valuable insights into rapport-building techniques, it does not delve deeply into the broader domain of relationship-building. Giebels (2002), however, does so and conceptualizes relationship-building as the nuanced skill of influencing others through effective communication with the goal of changing their attitudes, beliefs, or behaviors. This influence is inherently tied to social interactions and is a cornerstone of most relational dynamics. Given that negotiations, especially those involving conflicting interests that require collaborative efforts toward mutual goals, are fundamentally influenced by interpersonal relationships, the strategic cultivation of such relationships becomes paramount. Building on Cialdini's (2001, as cited in Giebels 2002) work on behavior change, Giebels (2002) identifies six psychological mechanisms driving change: liking, authority, social proof, scarcity, reciprocity, and cognitive dissonance. She extends this framework by exploring managerial influence styles, leading to her 'Table of Ten' that categorizes ten negotiation

strategies into relational (e.g., "Being kind," "Being equal," and "Being credible") and content strategies. For a comprehensive overview of these strategies, see Table 3.

Table 3

The Table of Ten (Giebels, 2002, p. 149)

Tactic	Brief description
1. Being kind	Friendly, empathic and helpful behavior
2. Being equal	Statements aimed at good cooperation. Corresponding experiences or common enemy.
3. Being credible	Conduct that shows expertise or knowledge of the business or lets you know you are trustworthy
4. Emotional appeal	Statements aimed at releasing feelings in the other person toward significant others or oneself (self-image)
5. Intimidation	Directly or indirectly threatening punishment, attacking or accusing the other person personally.
6. Imposing restriction	Procrastinating or making something available on a limited basis
7. Direct pressure	Put pressure on the other person in a neutral way by being firm.
8. Legitimizing	Refer to what has been agreed upon in society or with others.
9. Trading	Praise or offer, give and take.
10. Rational persuasion	The use of persuasive arguments and logic

Giebels (2002) underscores the pivotal role of communication in influencing negotiations, particularly in crisis negotiation scenarios. In such situations, the primary objective is to shift from confrontational approaches to cooperative problem-solving. Strategies like empathy, dignity preservation, and emotional reassurance, as mentioned in Rogan and Hammer (1995), play a crucial role in achieving this shift. Another significant concept to consider is face threat sensitivity, which implies that negotiators are less likely to reach agreements when their sense of face, or dignity, is threatened. This concept indirectly supports the idea that maintaining a kind and respectful approach, which preserves the other party's face, may enhance negotiation outcomes, as suggested by White et al. (2004). With empathy, dignity preservation through addressing face threat sensitivity, and emotional assurance in mind, this research will concentrate on strategies that encompass these perspectives, namely "Being kind," "Being equal," "Emotional appeal," "Legitimizing," and "Rational persuasion."

See Appendix B for an overview of the theories utilized in this theoretical framework.

2.3. Hypotheses

The theoretical framework highlighted above (an overview can be found in Appendix B) provides the basis for the hypotheses of this study. The foundation of these hypotheses is that, through employing influence strategies that focus on empathy, dignity preservation (through addressing face threat sensitivity), and emotional assurance, negotiation outcomes can be enhanced (Rogan & Hammer, 1995; White et al., 2004).

Giebels (2002) conceptualizes "Being Equal," a relational strategy, as the articulation of similar personal experiences and the emphasis on mutual interdependence. Kamphuis et al. (2006) categorizes crisis negotiations into three distinct phases and observe that, during the initial phase, the application of the "Being Equal" strategy correlates with higher effectiveness in negotiations than its absence, underscoring the pivotal role of this strategy in pacifying the aggressor. This strategy's efficacy extends into the problem-solving phase, suggesting the necessity of co-creating solutions with the perpetrator and establishing a strong rapport, which they argue might be essential for exerting further influence (Kamphuis et al., 2006). This perspective aligns with Vallano and Compo's (2015) findings, who advocate for the establishment of common ground as a means to cultivate rapport and encourage cooperative dialogue. This approach also resonates with the "Wade and Seek" method (Wade, 2021) which seeks to engender rapport with hackers, in part by demonstrating a willingness to cooperate. Considering these sources and informed by Faivre's (2022) examination, which highlights the mutual advantages of effective resolutions for both adversaries and victims, the first hypothesis is proposed:

H1: Being Equal significantly improves ransomware negotiation outcomes.

The Being Kind" strategy involves friendly and helpful behavior. As previously mentioned, strategies that prioritize building relationships tend to be more effective than those centered on tough or cognitive approaches (2002). While Kamphuis et al. (2006) did not find support for the hypothesized effectiveness of this strategy, they state that that may very well be due to the fact that "Being Kind" is a commonly used approach. Nevertheless, Wade (2021) recommends negotiators to display warmth and a cooperative attitude. This phenomenon may be attributed to the concept of face threat sensitivity, which suggests that negotiators are less inclined to reach agreements when their sense of face is at risk. This observation indirectly reinforces the notion that adopting a considerate and respectful approach, one that preserves the dignity and

face of the other party, could enhance the outcomes of negotiations (White et al., 2004). In consideration of these findings, the second hypothesis is proposed:

H2: Being Kind significantly improves ransomware negotiation outcomes.

Building on the previous discussion, strategies that focus on relationships, softness, and emotional connections are generally seen as more effective than those that are purely content-driven, rigid, and analytical. The "Emotional Appeal" strategy, despite being categorized as a content strategy, embodies a soft and emotive approach, closely aligning with the "Being Equal" and "Being Kind" principles (Kamphuis et al., 2006). Kopelman et al. (2006) suggest that displaying positive emotions can lead to more cooperative outcomes. Their research suggests that, in a dispute situation, even if you feel angry, there could be benefits to displaying positive emotion, hinting at the potential effectiveness of Emotional Appeal. Shirako et al. (2015) found that negotiators who appeal to the sympathy of their counterparts achieve improved outcomes, both in terms of value claiming and value creation. This suggests that Emotional Appeal, by eliciting sympathy, could positively impact negotiation outcomes. Wade (2021) effectively utilizes this strategy by acknowledging threat actors' skills. Based on this understanding, the third hypothesis is proposed:

H3: Utilizing Emotional Appeal significantly improves ransomware negotiation outcomes.

Rational persuasion, a strategy involving the use of logical arguments to influence behavior through attitude shifts (Giebels, 2002), can play a pivotal role in negotiation outcomes. Grobe (2010) highlights that in negotiations, persuasive arguments posit the ability to primarily alter participants' beliefs about a situation, rather than their underlying preferences. This indicates that successful negotiations often depend on the ability to shift the other party's perspective, making them more receptive to new solutions. For instance, in ransomware negotiations, Hack and Wu (2021) recommend effectively communicating financial constraints as a strategy for obtaining lower ransoms. Communicating financial limitations might initially appear as an example of the "Imposing Restriction" strategy, but incorporating logical reasoning transforms it into "Rational Persuasion." Perreault and Kida (2011) found that rational persuasion tactics, like informing clients about precedents set by other companies, can significantly influence client concessions in auditor-client negotiations. These tactics not only lead to greater concessions but also foster positive relations between negotiators, underscoring the

effectiveness of rational persuasion in achieving favorable outcomes and enhancing satisfaction in negotiations. In light of the above, the fourth hypothesis is proposed:

H4: Rational Persuasion significantly improves ransomware negotiation outcomes.

Cultural backgrounds significantly shape preferences for specific influencing tactics, suggesting that congruence with an individual's cultural norms enhances the efficacy of such approaches (Bazerman et al., 2000; Giebels, 2002). For example, rational persuasion may be more effective in individualistic cultures than in collectivist ones. Despite the growing research on cybercriminal traits, challenges such as accessing offenders and reliance on self-reported data limit these studies. Yet, recent theory teaches us that many organized crime networks, particularly those with ties to Russia, operate from Eastern Europe, with a noted relationship between these syndicates and the Russian state that allows for their activities as long as they serve national interests and target foreign entities (Stoddart, 2022). Russian culture, known for its high-context communication, favors indirect and nuanced negotiation strategies, aligning with the broader high-context cultural norms that value implicit communication and situational cues (Adair et al., 2004; Kamphuis et al., 2006). In light of these considerations, we propose that the use of legitimizing strategies, which appeal to societal norms or prior agreements, will positively influence ransomware negotiation outcomes.

H5: Legitimizing significantly improves ransomware negotiation outcomes.

2.4. Discount

In the hypotheses, references to the concept of "ransomware negotiation outcomes" are made, yet determining the success of such outcomes presents a complex challenge, given the multifaceted nature of these negotiations, as analyzed through the lens of Bazerman et al. (2000)'s theory. Negotiation effectiveness can be gauged through various factors. For instance, negotiation effectiveness has been assessed based on gain, the fairness of the outcome, consensus regarding the outcome, and the relational dynamics between both parties (Scanzoni & Godwin, 1990). Considering that threat actors are primarily driven by financial gain and often employ price discrimination strategies, such as offering discounts to victims as part of their negotiation tactics (Faivre, 2022; Hack & Wu, 2021; Hernandez-Castro et al., 2017), and conversely, victims seek to minimize the financial impact of the ransom demand while swiftly restoring their business operations (Faivre, 2022; Hofmann, 2020), this study measures the

effectiveness of ransomware negotiation outcomes, from the perspective of the victim, through the discount percentage. This factor encapsulates the difference in percentages between the initial ransom demand and the final negotiated ransom amount. According to Babbie (2020), ratio measurements, such as percentages, offer several advantages: they enable comparisons between ratio variables to ascertain their differences, establish which one is greater, quantify their discrepancy, and determine their relative proportions. Therefore, in the scope of this study, this measurement approach offers several advantages. Firstly, due to the contrasting goals highlighted by Faivre (2022), Hack and Wu (2021), and Hernandez-Castro et al. (2017), a higher discount factor signifies a more favorable outcome for the victim, indicating successful negotiation efforts in reducing the financial burden imposed by the threat actor. Furthermore, by focusing on the difference between the initial and final ransom amounts, this metric inherently accounts for the dynamic nature of ransomware negotiations. It acknowledges the fluidity of the negotiation process, where concessions and counteroffers may be made iteratively until a mutually agreeable resolution is reached (Faivre, 2022). It's crucial to note that in this study, this metric considers the negotiation process's success irrespective of whether the ransom is ultimately paid or not. Combining the hypotheses and the discount factor as the dependent variable leads to the following research model:

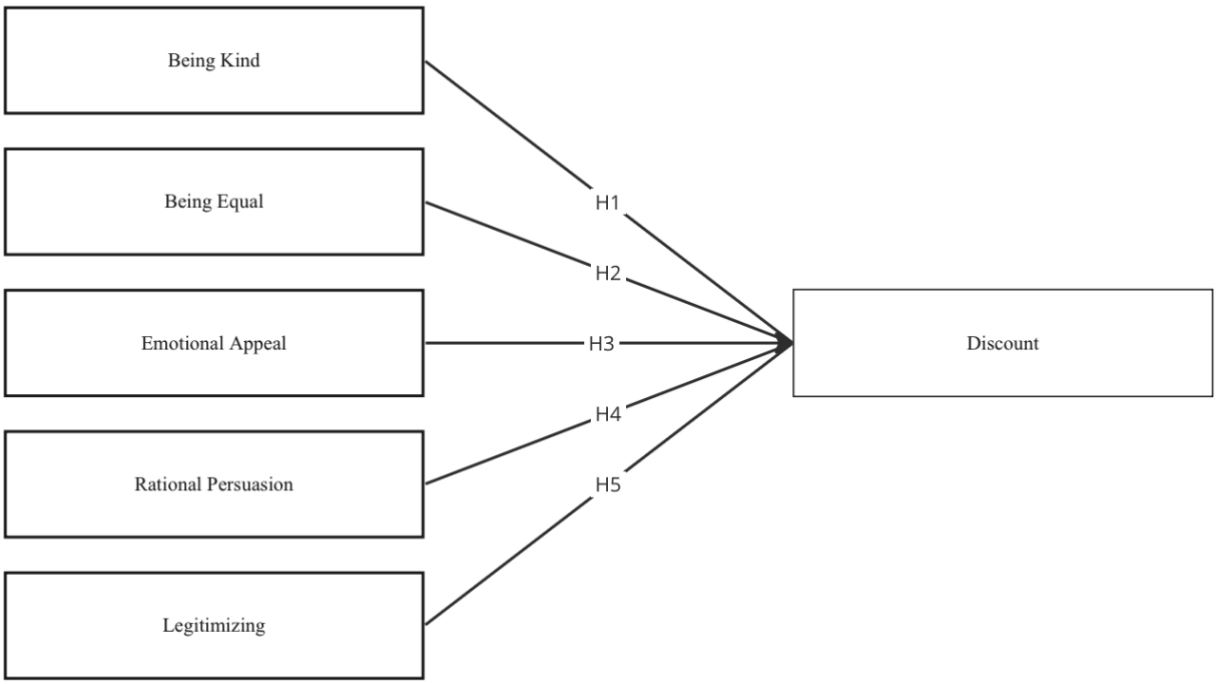


Figure 3: *Theoretical model*

3. Methodology

This section outlines the data gathering process, coding methodology, and analysis approach employed in the study, providing insight into its methodology and approach.

3.1. Data

In this study, the dataset analyzed comprised logs sourced from 16 ransomware negotiations, which were provided by Northwave Cyber Security (hereafter: Northwave), a prominent entity within the cybersecurity domain. Northwave operates primarily within Europe, with its headquarters located in the Netherlands. Notably, the organization maintains a global presence, spanning across 50+ countries. Employing a substantial workforce of over 250 security experts, Northwave responds to hundreds of cyber threats, including ransomware incidents, on an annual basis. Before gaining access to their data, a non-disclosure agreement (NDA) was (required to be) signed, stipulating that no information utilized in this study would pertain to any of Northwave's customers or contain sensitive details about Northwave's operations.

The logs provided by Northwave varied in length, ranging from 252 messages to 33, with an average of 76 messages and a median of 64 messages. Within these negotiations, involvement from nine distinct threat actors was identified: Conti, Karakurt, Babuk, LockBit2.0, Alphav/Blackcat, Darkside, Doppelpaymer, Blackbasta, and Egregor. Conti was involved in eight instances, Lockbit 2.0 in two instances, and each of the other threat actors was signaled once. It's worth noting that the ransomware negotiations included in the analysis adhered to a specific criterion: they had to reach a clear resolution, indicating whether the victim ultimately paid the ransom amount or not. This ensured that the entire negotiation process could be effectively analyzed.

3.2. Coding process

The logs where coded using a comprehensive coding scheme adapted from Euwema and Giebels (forthcoming; see Appendix C), aimed to capture the major influence tactics utilized during crisis negotiations. As can be read in the theoretical framework of this study, three of the codes ("being kind," "being equal," and "being credible") focused on the sender's relationship with the other party. For instance, "being equal" was used to identify utterances highlighting common ground between the parties (e.g., "Let's try to resolve this today"). The remaining eight codes ("Emotional Appeal", "Intimidation", "Imposing Restriction", "Direct Pressure", "Legitimizing", "Exchanging" and "Rational Persuasion) primarily pertained to the

content of the message and the conveyed information. For example, "Emotional Appeal" captured instances where negotiators appealed to the other party's emotions (e.g., "We kindly ask you not to call our employees anymore and request you not to publish our data or DDOS us"). It's worth noting that "information sharing" differed from other codes as it didn't necessarily involve an attempt to influence but rather encompassed behaviors such as discussing priorities, comparing positions, or acknowledging the other party's message. In this study, each speaking turn underwent coding by the author and a second coder, Michalis Georgiou, PhD candidate of the University of Twente, specializing in the field of Ransomware Negotiations. Prior to coding the negotiation transcripts, both coders underwent an extensive 20-hour training process. This training involved collaborative coding and discussion of practice transcripts, utilizing the Table of Ten and its associated categories. The aim of this training was to achieve a satisfactory level of interrater reliability, measured at 0.80 using Cohen's kappa coefficient, through continuous practice and discussion. After reaching this level of interrater reliability, each negotiation transcript from the Northwave database was independently coded by both coders. Interrater reliability scores ranged from 0.75 to 0.86 Cohen's kappa, averaging at 0.81. In instances of coding disagreement, both coders engaged in discussion to reach consensus. The agreed-upon code was then used in the final coding process, conducted sequentially according to the order of utterances in the negotiation transcripts. It's important to note that the analysis in this study focuses solely on utterances from the perspective of the victim, excluding those from the perspective of the threat actor. This deliberate choice allows for a concentrated exploration of the strategies employed by victims (or negotiators acting on behalf of the victim) and their relationship with negotiation outcomes.

3.3. Data analysis

In this study regression analysis was conducted to test the five hypotheses. By examining how these influence strategies relate to the discount factor, insights were gained into the dynamics of negotiation tactics and their impact on decision-making processes. Utilizing linear regression allowed for the quantification of the relationship between influence strategies and the discount factor. This method facilitated the identification of any significant associations between the variables, providing a quantitative understanding of their interplay. Furthermore, linear regression enabled the estimation of the strength and direction of these relationships, thereby enhancing the interpretability of the findings. However, it's important to acknowledge certain limitations and considerations associated with linear regression in this context. Firstly, while linear regression assumes a linear relationship between the predictor variables (influence

strategies) and the outcome variable (discount factor), this assumption may not always hold true in practice. Non-linear relationships may exist, which could lead to biased estimates and inaccurate conclusions. Additionally, linear regression may not capture the full complexity of the relationship between influence strategies and the discount factor, as it assumes a simple additive model without accounting for potential interactions or non-linear effects. Furthermore, the reliance on observational data in regression analysis presents challenges in establishing causality. While regression can identify associations between variables, it cannot establish causal relationships definitively. Confounding variables or reverse causality may confound the results, highlighting the need for cautious interpretation. Despite these limitations, linear regression offers valuable insights into the relationship between influence strategies and the discount factor, providing a quantitative framework for understanding the dynamics of negotiation processes.

4. Results

In this results section, descriptive statistics of both the dependent and independent variables are provided, alongside the results of the hypothesis tests via the outcomes of linear regression analysis.

4.1. Descriptive statistics

The dataset's descriptive statistics reveal a landscape rich in financial diversity. Annual revenues span from €5 million to €22.8 billion, reflecting substantial heterogeneity among entities. The mean annual revenue of €4.92 billion, coupled with a pronounced standard deviation of €6.94 billion and positive skewness of 2.213, suggests a distribution where most entities earn less than the mean, with a few outliers earning significantly higher revenues. Initial ransom demands, ranging from €34,400 to €3.79 million, show similar variability, with an average demand of €5.97 million and a high skewness of 2.949, indicating a right-skewed distribution, according to Hair et al. (2009). Final ransom figures, ranging from €12,900 to €5.69 million, display a contraction in range compared to initial demands, with a mean of €1.64 million and a lower, but according to Hair et al. (2009) still high, skewness of 1.196. The application of discounts, ranging from 0% to 98%, with a mean of approximately 51.87%, showcases a narrower dispersion around the mean, with skewness close to zero, indicating a fairly symmetrical distribution according to Hair et al. (2009). The binary variable denoting payment status, with a mean of 0.5 and a standard deviation of 0.516, highlights an equal distribution of ransom payments being made or not made, underscoring the varied responses among entities to ransom demands and the complex financial impacts of such incidents.

Table 5

Descriptive statistics Financial Variables

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness
Annual Revenue	10	5000000.00	2280000000.00	491924653.8000	693609269.03959	2.213
Initial Ransom	16	34400.00	37936729.00	5971469.5625	9399030.43511	2.949
Final Ransom	16	12900.00	5690509.00	1640604.5625	1735663.32025	1.196
Discount	16	.00	98.00	51.8738	25.90042	.068
Paid	16	0	1	.50	.516	.000

Heir et al. (2009) state that boxplots provide a visual summary of the distribution of a dataset. Boxplots consists of a box, which represents the interquartile range (IQR) containing the middle

50% of the data, with the median depicted by a solid line within the box. The length of the box indicates the spread of the observations, with a larger box suggesting greater variability. The whiskers extend from the box to the smallest and largest observations within one quartile range from the box. Any data points beyond this range are considered outliers or extreme values and are represented by symbols outside the whiskers. The position of the median within the box can indicate skewness in the data: if the median is closer to one end of the box, it suggests skewness in the opposite direction. In examining the box plot of annual revenue (see Appendix E), a pronounced right-skewed distribution can be observed. The data's median is notably lower than the upper quartile, implying a substantial asymmetry in the revenue figures. This asymmetry is further accentuated by the presence of an outlier, represented by a point just below the 25-billion-mark, indicative of an entity whose annual revenue markedly exceeds that of its counterparts. The interquartile range, extending from the lowest revenue value close to zero to a third quartile under the 2 billion mark, underscores the concentration of the majority of entities within a more modest revenue bracket. The absence of a lower whisker indicates that the lower quartile is positioned at the minimum revenue value, further substantiating the clustering of entities at the lower end of the revenue spectrum. These observations are particularly interesting as they reveal not only the variability and distribution of revenues among the entities but also highlight the impact of extreme values on the overall financial landscape portrayed by the dataset.

The distribution of discounts applied (see Appendix E), exhibits a symmetric pattern with a median value at approximately 50 percent. The interquartile range, encompassing the middle 50 percent of the data, extends from about 25 to 75, indicating a moderately consistent range of discounts across the observations. Notably, the discounts range from a minimum of 0 to a maximum of 98 (as also can be seen in Table 5), with no outliers detected, suggesting a uniform discounting approach among the cases. The whiskers reach these extreme values, confirming the absence of anomalies in discount practices. This uniformity is further underscored by the symmetry of the box plot, with the median line centrally positioned within the box, indicative of a balanced distribution with no significant skew. The consistency in discount percentages points to a standardized negotiation pattern where, on average, discounts tend to hover around the halfway mark, reflecting a commonality in the reduction of initial ransom demands.

The descriptive statistical analysis of the eleven influence strategies employed by victims in ransomware negotiations (see Table 6) reveals a nuanced landscape of negotiation tactics.

While certain strategies such as "Being Kind" demonstrate moderate and consistent usage, others like "Being Equal" and "Being Credible" exhibit more variability in deployment. The presence of skewed distributions, as indicated by values outside the -1 to +1 range, which Hair et al. (2009) suggest, signify substantial skewness, is particularly notable in tactics such as "Intimidation." This observation implies that there are occasional spikes in usage of these tactics, rather than a consistent and uniform application. Additionally, the variable utilization of strategies such as "Imposing Restriction" indicates adaptability in response to negotiation dynamics. Despite these fluctuations, "Exchanging" emerges as a commonly employed tactic, underscoring its significance in ransomware negotiation scenarios.

Table 6

Descriptive Statistics Influence Strategies in percentages

Variable	Minimum	Maximum	Mean	Std. Deviation	Skewness
1. Being Kind	5.56	31.03	15.7031	6.93156	.330
2. Being Equal	.00	4.00	.9116	1.51881	1.280
3. Being Credible	.00	9.38	1.0831	2.61960	2.731
4. Emotional Appeal	.00	8.33	1.5483	2.80130	1.705
5. Intimidation	.00	1.39	.0868	.34722	4.000
6. Imposing Restriction	.00	29.41	12.7127	8.50491	.421
7. Direct Pressure	.00	16.67	2.3347	4.43956	2.575
8. Legitimizing	.00	5.88	1.4322	2.16335	1.166
9. Exchanging	5.71	44.00	22.1790	12.14083	.350
10. Rational Persuasion	.00	29.03	10.9057	7.63666	.740
11. Information Exchange	12.90	57.69	31.1027	15.08918	.485

The correlation analysis presented in Table 7 unveils the intricate relationships between various influence strategies and information exchange within ransomware negotiations. Notably, while some strategies exhibit positive correlations, such as "Being Kind" and "Being Equal," others display negative associations, like "Being Kind" and "Emotional Appeal." These findings underscore the nuanced interplay among different approaches to influence, suggesting complex patterns of interaction. Moreover, the statistically significant negative correlation between "Information Exchange" and "Legitimizing" (-.561, $p<.05$) highlights a substantial relationship, indicating that increased information sharing is associated with decreased attempts to legitimize actions. The lack of statistical significance in many other correlations emphasizes the need for cautious interpretation, suggesting that observed relationships may not necessarily imply causation.

Table 7

Correlation Analysis Influence Strategies

Variable	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.
1. Being Kind	--										
2. Being Equal	.222	--									
3. Being Credible	.033	-.183	--								
4. Emotional Appeal	-.447	.186	-.180	--							
5. Intimidation	.251	.328	.031	-.015	--						
6. Imposing Restriction	.161	-.394	-.245	-.268	-.312	--					
7. Direct Pressure	.158	-.125	.351	-.108	-.057	.047	--				
8. Legitimizing	-.305	-.144	-.280	.456	-.177	.268	-.322	--			
9. Exchanging	-.223	.357	.052	.097	-.304	-.084	-.193	.182	--		
10. Rational Persuasion	.072	.147	.024	-.120	-.090	-.346	.092	-.057	-.235	--	
11. Information Exchange	-.361	-.295	-.117	.133	.334	-.308	-.265	-.194	-.561*	-.169	--

*. Correlation is significant at the 0.05 level (2-tailed).

The scatterplot analysis of this correlation, which can be seen in Appendix D, reveals a discernible negative linear relationship between the influence strategy "Exchanging" and "Information Exchange," as evidenced by the regression equation $y=36.22-0.45x$. The negative slope of the regression line signifies that an increase in the percentage of "Information Exchange" is associated with a concomitant decrease in the percentage of "Exchanging," at a rate of 0.45 units per percentage increase. However, the coefficient of determination, $R2$, is 0.315, indicating that only 31.5% of the variance in "Exchanging" can be accounted for by its linear relationship with "Information Exchange." This suggests that additional factors, not represented in this bivariate analysis, likely influence the "Exchanging" strategy. The scatter of data points around the fitted regression line and the expanding confidence intervals at higher levels of "Information Exchange" suggest variability that is not captured fully by the model, indicative of potential heteroscedasticity. The absence of pronounced outliers implies that the negative relationship is not unduly influenced by anomalous data points. Nonetheless, the moderate $R2$ value necessitates a cautious interpretation of these results, particularly considering the small sample size and potential violations of the assumptions of normality and independence. This analytical caveat underscores the preliminary nature of the findings and highlights the need for further investigation into the dynamics between these influence strategies.

4.2. Regression analysis

The regression analysis conducted to evaluate the hypotheses (see Table 7) produced largely inconclusive findings and encountered several challenges concerning the regression assumptions essential for a valid linear model.

Table 7

Regression analysis Independent Variables on Discount

Coefficients[a]

		B	Std. Error	Beta	t	Sig.
1	(Constant)	51.158	15.369		3.329	.008
	Being Kind	-2.641	2.497	-.400	-1.058	.315
	Being Equal	4.806	15.762	.115	.305	.767
	Emotional Appeal	8.100	6.487	.450	1.249	.240
	Legitimizing	-21.475	14.192	-.522	-1.513	.161
	Rational Persuasion	4.910	3.084	.452	1.592	.143

a. Dependent Variable: Discount

Being Equal

The first hypothesis (H1: Being Equal significantly improves ransomware negotiation outcomes) could not find support in this study, as the null hypothesis could not be rejected ($B = 4.806$, $t = 0.305$, $p = 0.767$). The Shapiro-Wilk test ($W(16) = 0.500$, $p < 0.001$) raised concerns regarding the normality assumption in residuals, which is crucial in linear regression analysis. Despite indications of homoscedasticity in the scatterplot, uncertainties persisted due to the limited sample size and the potential presence of outliers. Additionally, a Durbin-Watson statistic of 2.192 indicated positive autocorrelation among residuals, impacting their independence and consequently casting doubt on the reliability of hypothesis tests conducted using the model. These findings underscore the complexities and limitations inherent in evaluating the impact of Being Equal on ransomware negotiation outcomes within the scope of this study.

Being Kind

Also, the second hypothesis (H2: Being Kind significantly improves ransomware negotiation outcomes) could not be supported by this study, as the null hypothesis could not be rejected ($B = -2.641$, $t = -1.058$, $p = .315$). This indicates that there is no significant (positive) linear relationship between Being Kind and Discount. Moreover, a Shapiro-Wilk test ($W(16) = 0.458$,

$p < .001$) challenged the assumption of normality in the residual distribution, which is essential in linear regression analysis. Although the scatterplot of standardized residuals against predicted values (see Appendix D) tentatively suggested homoscedasticity, indicating consistent spread, uncertainties emerged due to the small sample size and the possibility of outliers. Additionally, a Durbin-Watson statistic of 1.896 revealed positive autocorrelation among residuals, compromising their independence and, consequently, the reliability of hypothesis tests conducted using the model. These discoveries emphasize the intricacies and constraints involved in assessing the influence of Being Kind on ransomware negotiation outcomes within the confines of this study.

Emotional Appeal

The third hypothesis (H3: Emotional Appeal significantly improves ransomware negotiation outcomes) could not gather support from this study, as the null hypothesis could not be rejected ($B = 8.100$, $t = 1.249$, $p = 0.240$). This indicates an absence of a significant (positive) linear relationship between Emotional Appeal and ransomware negotiation outcomes (measured through Discount). Moreover, the lack of definitive linearity, along with the presence of an outlier, raised concerns about the assumption of linearity. Additionally, the Shapiro-Wilk test ($W(16) = 0.485$, $p < 0.001$) challenged the normality assumption in residuals, which is crucial in linear regression analysis. Despite indications of homoscedasticity in the scatterplot (see Appendix D), uncertainties persisted due to the small sample size and potential outliers. Furthermore, a Durbin-Watson statistic of 1.850 suggested positive autocorrelation among residuals, compromising their independence and, consequently, the reliability of hypothesis tests conducted using the model. These findings highlight the complexities and limitations inherent in evaluating the impact of Emotional Appeal on ransomware negotiation outcomes within the parameters of this study.

Legitimizing

The fourth hypothesis (H4: Legitimizing significantly improves ransomware negotiation outcomes) also failed to find support in this study, as the null hypothesis could not be rejected ($B = -21.475$, $t = -1.513$, $p = 0.161$). Notably, despite the lack of statistical significance, the outcomes even suggest a negative relationship. Concerning “Legitimizing,” the non-random distribution of residuals, as confirmed by the Shapiro-Wilk test ($W(16) = 0.791$, $p = 0.002$), challenged the crucial assumption of normality required in linear regression. Moreover, a Durbin-Watson statistic of 1.751 indicated positive autocorrelation among residuals,

compromising their independence and, consequently, casting doubt on the reliability of hypothesis tests conducted using the model. These findings highlight the challenges and limitations in evaluating the impact of Legitimizing on ransomware negotiation outcomes within the context of this study.

Rational Persuassion

Also, the fifth and final hypothesis (H5: Rational Persuasion significantly improves ransomware negotiation outcomes) did not find support in this study, as the null hypothesis could not be rejected ($B = 4.910$, $t = 1.592$, $p = 0.143$). Furthermore, when analyzing "Rational Persuasion," the Shapiro-Wilk test ($W(16) = 0.433$, $p < 0.001$) contested the normality assumption in residual distribution, which is crucial in linear regression. Despite indications of potential non-randomness in the scatterplot (see Appendix D), uncertainties persisted due to the small sample size and the presence of outliers. Additionally, a Durbin-Watson statistic of 1.826 indicated positive autocorrelation among residuals, compromising their independence and, consequently, the reliability of hypothesis tests. These findings underscore the complexities and limitations involved in examining the impact of Rational Persuasion on ransomware negotiation outcomes within the scope of this study.

The hypotheses tested in the study aimed to investigate the impact of different influence strategies on ransomware negotiation outcomes. However, none of the hypotheses received support as the null hypotheses could not be rejected, indicating a lack of significant linear relationships between the influence strategies and negotiation outcomes. Several challenges were encountered, including violations of assumptions such as normality in residual distribution, potential outliers, and positive autocorrelation among residuals, which cast doubts on the reliability of the regression models. These findings highlight the complexities and limitations inherent in examining the effectiveness of influence strategies in ransomware negotiations within the framework of this study.

Table 8

Hypothesis table

Hypothesis	Null hypothesis
H1: Being Equal significantly improves Ransomware Negotiation Outcomes.	Not rejected
H2: Being Kind significantly improves Ransomware Negotiation Outcomes.	Not rejected
H3: Emotional Appeal significantly improves Ransomware Negotiation Outcomes.	Not rejected
H4: Rational Persuasion significantly improves Ransomware Negotiation Outcomes.	Not rejected
H5: Legitimizing significantly improves Ransomware Negotiation Outcomes.	Not rejected

5. Discussion

The following section offers an interpretation of the study's findings, shedding light on the complexities of ransomware negotiations, while also addressing limitations, proposing future research avenues, and highlighting the study's contributions.

5.1. Interpretation of the results

This study attempted to answer the question, "What is the impact of different negotiation strategies on ransomware negotiation outcomes from the victim's perspective?" To address this central question effectively, it explored the concepts and processes that encompass ransomware negotiations and the potential strategies for negotiating with threat actors. It concluded that ransomware negotiations usually take place in high-stakes environments with the primary goal of securing the release of compromised data or systems, often in exchange for a monetary payment. Similar to crisis negotiation scenarios that involve direct threats to life or safety, ransomware negotiations require specialized intervention strategies aimed at resolving the situation and minimizing potential harm. Wade (2022) suggested the applicability of traditional crisis negotiation strategies in ransomware negotiation contexts. The foundational premise of this investigation was that ransomware negotiations, similar to traditional crisis situations, could benefit from approaches centered on empathy, dignity preservation, and emotional reassurance (Rogan & Hammer, 1995). It was assumed that these approaches improve negotiators' effectiveness by reducing confrontational stances and fostering a more collaborative environment. However, the study could not reject the null hypothesis that employing Being Kind, Being Equal, Emotional Appeal, Rational Persuasion, and Legitimizing strategies significantly improve ransomware negotiation outcomes.

Before delving into the individual hypotheses, it's important to consider several overarching factors that might have influenced the study's ability to detect significant effects across all hypotheses. Firstly, the size and representativeness of the sample may not have been sufficient, potentially limiting the power to observe a meaningful impact. Additionally, the presence of confounding variables, which were not accounted for in the analysis, could have influenced both the application of the strategy and its effectiveness in negotiations (this aspect is expanded upon in the section discussing the study's limitations). Furthermore, the relationship between the variables involved might not be straightforward; potential non-linear dynamics and interactions could have been overlooked, thereby affecting the analysis's accuracy. Another critical aspect to consider is whether the assumptions required for regression analysis were fully

met, as any violations could undermine the validity of the findings. Lastly, the specific context of each ransomware attack, including the unique motivations and objectives of the perpetrators, could have significantly influenced the negotiation outcomes. Understanding these contextual nuances is crucial for interpreting the results accurately and for formulating strategies that are responsive to the varied and complex nature of ransomware incidents.

In the subsequent paragraphs, this study delves deeper into the various hypotheses proposed earlier.

Being Equal

Based on the premise that emphasizing cooperation, co-creation of solutions, and the establishment of rapport are crucial elements for effective negotiation (Kamphuis et al., 2006; Vallano & Compo, 2015; Wade, 2021), it was hypothesized that employing the "Being Equal" strategy would enhance ransomware negotiation outcomes. However, despite this expectation, the hypothesis could not be supported, with several factors potentially contributing to this outcome. The inability to reject the null hypothesis in our study could stem from a variety of factors. Bazerman et al. (2000) presents a theoretical framework identifying five key elements that impact the negotiation process and outcomes: mental models, cultural dynamics, communication methods, ethical considerations, and the number of parties involved in negotiations. A significant factor to consider is the mental model of the threat actor, which might lean towards a more distributive negotiation style than anticipated. This distributive mindset, focusing on dividing a fixed set of resources (the "fixed-pie" principle), suggests that the threat actors may not view mutual goals or dependencies as advantageous, contradicting Faivre's (2022) assumption that a swift resolution of ransomware incidents benefits both parties. Cultural influences also play a crucial role, according to Bazerman et al. (2000). The sample of negotiators in this study might come from backgrounds less receptive to collaborative strategies. Stoddart (2022) indicates that many threat actors targeting Western countries have ties to Russia or its government. Although Russia has historically been viewed as collectivistic, research by Mamontov et al. (2014) reveals a shift towards individualism in modern Russian business practices, driven by market economy influences and a departure from Soviet-era collectivism. As Stoddart (2022) previously mentioned, it’s hard to say for certain where specific threat actors come from. Nevertheless, it could very well be that negotiators from more individualistic cultures might be less open to influence strategies that emphasize collaborative problem-solving. It's also possible that negotiators of this particular type constituted a

significant portion of the study's sample. Communication medium is another critical factor. According to Bazerman et al. (2000), face-to-face interactions tend to foster trust and honesty, whereas written or digital communications can create suspicion and hinder negotiation progress. The digital nature of these negotiations could have caused the threat actors to perceive the "Being Equal" influence strategies as insincere, thereby increasing suspicion. From an ethical standpoint, Faivre (2022) draws parallels between the dynamics of threat actor negotiations in ransomware attacks and kidnapping scenarios, highlighting the threat actors' predatory nature. They often select their targets through meticulous research and cost-benefit analysis, exploiting vulnerabilities to cause operational disruptions. This deliberate emphasis on power imbalances by threat actors, deviating from an integrative negotiation stance, exploits the victims' weakened negotiating position due to their limited information about the attackers. Lastly, the complexity introduced by the number of negotiating parties could have influenced the outcomes. Research by Keijzer (n.d.) and Sentsova and DiMaggio (2023) suggests that threat actors often adhere to their own value chains and engagement rules to maximize their profits. These established rules might limit negotiations to specific targets and objectives, encouraging a more instrumental approach from the threat actor and making them less responsive to general influence strategies.

Being Kind

Drawing on the premise that strategies emphasizing relationship-building tend to yield greater effectiveness compared to approaches rooted in toughness or cognitive tactics, and aligning with the advocacy for a warm and cooperative demeanor that upholds the dignity and face of all parties involved (Wade, 2021; White et al., 2004), it was hypothesized that employing the "Being Kind" strategy would enhance ransomware negotiation outcomes. However, despite these expectations, the hypothesis could not be substantiated, suggesting a need for further examination and consideration of potential contributing factors. One potential explanation for this outcome could be the prevalence of the "Being Kind" approach, as also noted by Kamphuis et al. (2006). The "Being Kind" strategy, alongside the "Exchanging" tactic, emerges as the most frequently employed method on average within this study, with no instances where "Being Kind" was entirely absent. Delving into Bazerman et al.'s (2000) theoretical framework provides several plausible reasons for this observation, particularly through the lens of mental models. Studies by Faivre (2022), Hack and Wu (2021), Hernandez-Castro et al. (2017), and Li and Liao (2020) highlight the primary motivation of threat actors: financial gain. This objective suggests that threat actors might adopt a more instrumental approach, potentially diminishing

their receptiveness to softer influence strategies that prioritize relational aspects. Li and Liao (2020) underscore the importance of reputation in their business model: upholding a ‘tough’ image might be part of the modus operandi of a certain threat actor. This necessity might render them less open to kindness, perceiving it as a weakness or an insincere tactic. However, "Being Kind" could lay the groundwork for implementing other influence strategies, though such connections were beyond the scope of this study due to its limitations and the absence of contrasting negotiations (i.e., cases without "Being Kind") in the database. The impact of the number of negotiating parties, as discussed by Keijzer (n.d.) and Sentsova and DiMaggio (2023), could also have played a role in the observed outcomes. Their research suggests that threat actors construct their own value chains and rules of engagement to maximize profits, which may restrict negotiations to specific targets and strategies, fostering a more transactional rather than relational approach. Additionally, the communication medium remains a critical factor. Similar to the "Being Equal" strategy, the digital nature of these negotiations might lead threat actors to question the sincerity of "Being Kind" strategies, potentially heightening skepticism and undermining their effectiveness.

Emotional Appeal

Emotional appeal, traditionally viewed as a tactic within content strategies, deeply resonates with the principles of fostering equality and kindness in relationships. Studies by Kopelman et al. (2006) and Shirako et al. (2015) highlight that the strategic expression of positive emotions and empathy can significantly enhance the outcomes of negotiations by fostering a cooperative environment. This suggests a potential for emotional appeal to positively influence negotiation results. However, the anticipated support for this hypothesis encounters challenges. For instance, Wade (2021) adeptly employs emotional appeal by recognizing the competencies of adversaries, suggesting the nuanced effectiveness of such strategies. The failure to confirm the hypothesis in certain instances might be attributed to the negotiators' inability to convincingly convey emotional appeal, possibly due to perceived insincerity (i.e., due to the digital nature of these negotiations). This is akin to the principles of equality and kindness, where the effectiveness may be hindered by the adversary's mental model, which may favor a more competitive and transactional negotiation approach, thus being less responsive to commendation. The efficacy of emotional appeal might also depend on how it is executed. Hofmann (2020) demonstrates that some adversaries maintain ethical standards. Therefore, aligning Emotional Appeal with these ethical values could potentially enhance negotiation outcomes. Additionally, cultural factors could influence receptivity to emotional appeal. For

example, the remasculinization of Russia under Putin, as discussed by Riabov and Riabova (2014), has bolstered its popularity by fostering a robust national masculinity. This cultural backdrop might imply that negotiators from such masculine cultures may exhibit lower sensitivity to emotional appeals. While pinpointing the exact cultural origins of threat actors poses a challenge, it's plausible to consider that negotiators hailing from predominantly masculine cultures might be inherently less receptive to emotional appeals. This insight prompts a reevaluation of the nuanced dynamics at play in the effectiveness of emotional appeal strategies in negotiations, highlighting the intricate interplay of sincerity, cultural context, and strategic execution.

Legitimizing

Bazerman et al. (2000) and Giebels (2002) have both underscored the profound influence of cultural backgrounds on the selection of persuasive tactics, pointing out that strategies resonating with cultural norms tend to be more effective. This insight is particularly relevant in the context of ransomware negotiations, which are characterized by complex interplays of cultural and individual differences. It was theorized that Legitimizing, within the framework of Russian cultural norms, could lead to improved outcomes, drawing on research by Adair et al. (2004), Kamphuis et al. (2006), and Stoddart (2022). However, this theory encountered challenges in garnering empirical support. One critical consideration is the assumption that the cultural norms of threat actors are reflective of broader societal norms in Russia, which may not necessarily be accurate (I.e., the negotiator doesn’t originate from Russia). Bazerman et al. (2000) highlights that cultural background and an individual's mental model both play crucial roles in influencing behaviors. Furthermore, Faivre (2022) discusses the existence of a power imbalance in these situations. When negotiators attempt to legitimize their positions by referencing external norms and rules, it could trigger a defensive reaction from threat actors, who may perceive their power position as being challenged and, consequently, become resistant to these external influences. Additionally, individuals engaged in unethical behaviors, such as cybercriminals, might inherently display a disregard for general rules and norms, given that ethical considerations are pivotal in shaping negotiation processes and outcomes, as noted by Bazerman (2020). Keijzer (n.d.) and Sentsova and DiMaggio (2023) provide insights into how threat actors create their own value systems and rules of engagement, suggesting the development of a distinct subculture among them. This emergent culture could diminish their openness to external norms and influences. Therefore, it's essential to reevaluate the effectiveness of legitimizing strategies in ransomware negotiations, considering the unique

cultural constructs and mental models of cybercriminals, which may diverge significantly from societal norms and resist conventional influence tactics.

Rational Persuasion

Grobe (2010) points out that persuasive arguments aim to shift beliefs about a given situation, a strategy pivotal for changing viewpoints. In the realm of ransomware negotiations, Hack and Wu (2021) recommend the strategic disclosure of financial limitations to reduce ransom demands, leveraging constraints as a form of rational persuasion. This approach is supported by Perreault and Kida (2011), who observed that rational persuasion tactics can significantly impact negotiation outcomes, leading to greater concessions and fostering positive relationships. However, it's worth noting that Perreault and Kida (2011) did not specifically explore crisis negotiation contexts, casting some doubt on the direct applicability of their findings to high-stakes ransomware negotiations. Drawing on these insights, the proposition was made that Rational Persuasion could markedly enhance the outcomes of ransomware negotiations. Unfortunately, empirical evidence did not back this hypothesis. The lack of significant impact from rational persuasion invites two plausible interpretations: either the threat actor, while rational, is motivated by objectives that rational persuasion fails to address, or the rationality of the threat actor has been overestimated. Li and Liao (2020) emphasize the critical role of a threat actor's reputation, while Faivre (2022), Hack and Wu (2021), and Hernandez-Castro et al. (2017) highlight the primary motivation for threat actors to maximize profit. This suggests that a threat actor might be committed to maintaining a tough reputation by making minimal concessions. If the rationality of the threat actor is indeed overestimated, one might expect traditional crisis negotiation techniques, which focus on building rapport and steering the conversation from emotional reactions toward more reasoned decision-making (as outlined by Grubbs, 2010), to be effective. This assumption, however, appears to be contradicted by the observed ineffectiveness of rational persuasion in this context. This discrepancy underscores the complexity of ransomware negotiations and suggests that a deeper understanding of threat actors' motivations and decision-making processes is essential for developing effective negotiation strategies. It also points to the need for adaptive negotiation tactics that can navigate the nuanced and often unpredictable nature of these high-stakes interactions.

5.2. Limitations and Future Research

The primary constraint of this study stems from its limited sample size, a consequence of the unique and confidential nature of the data, which significantly restricts the scope for a more extensive dataset, thereby affecting the reliability and generalizability of our findings. As such, the results must be approached with caution and regarded as exploratory due to the diminished statistical power that hampers the identification of significant effects. Furthermore, the methodology employed for coding, which assigns a single code to each utterance, may not fully capture the complexity of multiple influence strategies potentially co-occurring within a single spoken term, thus neglecting the nuanced interplay and cumulative impact of various strategies. This issue is compounded by the data's limited scope, sourced exclusively from a solitary cybersecurity firm, which might not provide a comprehensive view of the diverse influence strategies and negotiation styles prevalent in the field. The geographical concentration of the data, primarily from the Benelux region, further narrows the study's applicability, as the findings may not extend to other regions with distinct legal, cultural, and economic contexts influencing cybersecurity negotiations. Additionally, the subjective nature of the data collection methodology, despite efforts to ensure high interrater reliability, could lead to different interpretations by other researchers, thereby introducing a potential variability in the coding of influence strategies.

In the preceding paragraphs, the potential influence of unaccounted-for confounding variables on the analysis was highlighted. Bazerman et al. (2000) provided valuable insights into understanding the dynamics of ransomware negotiations, including mental models, ethics, communication mediums, multiple negotiation parties, and cross-cultural dynamics. However, this study employed a relatively simple theoretical model, overlooking ethical considerations of the victim, the impact of communication mediums on influence strategy effectiveness, the role of the threat actor value chain on negotiation outcomes, and cross-cultural dynamics. These aspects present avenues for future research to explore their impact on ransomware negotiations. Additionally, future studies could investigate how threat actors assess the value of compromised data, incorporate upfront costs such as those associated with system infiltration or Ransomware as a Service (RaaS) into their negotiation strategies, and evaluate the importance of time in negotiations (Faivre, 2022; Hack & Wu, 2021; Hernandez-Castro et al.; 2017; Li & Liao, 2020).

Furthermore, Hernandez-Castro et al. (2017) and Hack and Wu (2021) highlighted that cybercriminals' earnings are bolstered by victimizing multiple entities. Sharmeen et al. (2020)

noted that RaaS significantly lowers the entry barrier to ransomware distribution, thereby amplifying the frequency and diversity of ransomware incidents. This study operated under the assumption that each negotiation was an isolated event. However, it is possible that threat actors, or RaaS affiliates, do not adhere to a policy of treating each negotiation as an isolated event. Instead, they might be engaging with broader monetary targets, thus challenging the notion of isolated negotiations and independent ransomware negotiation outcomes.

The large standard errors relative to the coefficient values, along with the challenged assumptions for regression, suggest potential volatility in the data or, more likely, an undersized sample. This could be diminishing the ability to accurately capture the true effects of these variables. It implies that further research with larger sample sizes or additional variables might be crucial for a more precise understanding of the underlying dynamics. However, what if there is genuinely no effect between the proposed influence strategies and the ransomware negotiation outcome? The shift from traditional high-stakes crisis negotiation strategies to those suitable for cyber extortion demands careful reconsideration based on these findings. The nature of cybercrime, marked by its impersonality and the goal-oriented behavior of cybercriminals, introduces distinct challenges. Kroneberg et al. (2010) argue that individuals involved in deliberate criminal acts often demonstrate a type of instrumental rationality, potentially making them less amenable to the conventional influence strategies that hinge on moral or ethical considerations. Furthermore, the aspect of anonymity is significant; research into the link between anonymity and antisocial behavior in isolated settings reveals that non-identifiability and lack of accountability amplify antisocial tendencies, implying that anonymity facilitates deviation from norms (Tatsuya Nogami & Jiro Takai, 2008). The role of anonymity is complex and two-fold, as other studies show that individuals are prone to act more selfishly and unethically towards those who are anonymous compared to those who are not. This is further underscored by findings that anticipated guilt is a crucial mediator in these interactions, indicating that anonymous individuals are more susceptible to unethical treatment, shedding light on the prevalence of unethical actions in these contexts (Yam & Reynolds, 2016). The combination of impersonality, the two-way nature of anonymity, and a focus on objectives may present substantial challenges, potentially making threat actors resistant to more subtle forms of persuasion or influence altogether.

An intriguing avenue for further investigation lies in the ‘Exchanging’ strategy detailed in Giebels’ Table of Ten (2002). This strategy, rooted in Cialdini’s concept of ‘reciprocity’, posits

that individuals are inclined to assist those who have helped them and oppose those who have harmed their interests, as outlined by Perugini et al. (2003). According to Giebels (2002), the exchange strategy involves soliciting a return favor, reducing one's offer, or proposing a trade. In the framework of reciprocity, Paese and Gilin (2000) discovered that in distributive bargaining, when one party unequivocally engages in a cooperative action, it can foster increased cooperation from the other side, manifesting in less stringent offers and greater willingness to settle for lower profits. One exemplary manifestation of such behavior is when negotiators disclose their alternatives (or BATNA: Best Alternative To Negotiated Agreement). This disclosure holds the potential to influence the eventual negotiated price and the employment of unilateral bargaining strategies by the opposing side, often resulting in inflated prices when buyers reveal their alternatives to sellers (Bolkan & Goodboy, 2021). The underlying rationale is that revealing one's BATNA (in the context of Ransomware negotiations, often referring to 'Recovery' options) may enable an individual to exert influence by stipulating that, for a deal to be made, the proposed agreement must surpass (or be at least equivalent to) their subsequent best alternative. However, this action could inadvertently provide the adversary with a tactical advantage, as it may restrict negotiators' ability to demand beyond this alternative once it is exposed.

Furthermore, 'Exchanging' involves reducing one's offer. Williams et al. (2011) assert that a critical aspect of effective negotiation is the selection of a concession strategy. Bartos (1964) found that concession-making tends to be a less effective strategy, with negotiators making fewer concessions typically receiving higher payoffs. The role of structural concession-making in ransomware negotiation outcomes could indeed offer a compelling area of study, aligning with research by Donohue and Roberto (1996). They advocate for a blend of integrative and distributive negotiating techniques, underlining negotiation as a complex system capable of taking numerous unpredictable turns.

5.3. Contributions

Although the results did not reach statistical significance, primarily due to limitations in sample size, this study still offers a notable contribution to the emerging realm of ransomware negotiations. The study not only elucidates the intricate dynamics inherent in negotiating with threat actors, but also underscores the challenges posed by contextual factors, including cultural nuances, anonymity, and the evolving landscape of cybercrime. Grounded in Bazerman et al. (2000) this study provides a theoretical lens through which to understand the concepts and

processes involved in ransomware negotiations, including mental models, ethical considerations, communication mediums, the involvement of multiple negotiation parties, and cross-cultural dynamics. By incorporating this framework, future research can adopt a more holistic approach to analyzing ransomware negotiations, taking into account not only the strategies employed by negotiators but also the broader contextual factors that shape the negotiation process.

Moreover, the study's exploration of the potential impact of various negotiation strategies, such as Being Equal, Being Kind, Emotional Appeal, Rational Persuasion, and Legitimizing, provides a nuanced understanding of the effectiveness of these approaches in the context of ransomware negotiations. While the study did not find significant support for the hypothesized effects of these strategies, the identification of unexplored avenues for future research offers valuable directions for inquiry. Overall, by addressing these gaps and incorporating insights from Bazerman et al. (2000) and other relevant literature, future studies can contribute to a more comprehensive understanding of ransomware negotiations. By adopting a multidimensional approach that accounts for both the strategies employed by negotiators and the contextual factors that shape the negotiation process, researchers can inform the development of more effective intervention strategies to mitigate the impact of ransomware attacks.

REFERENCES

Adair, W. L., Brett, J. M., Lempereur, A., Okumura, T., Shikhirev, P., Tinsley, C. H., & Lytle, A. L. (2004). Culture and negotiation strategy. *Negotiation Journal*, *20*(1), 87–111. https://doi.org/10.1111/j.1571-9979.2004.00008.x

Allred, K. G., Mallozzi, J. S., Matsui, F., & Raia, C. P. (1997). The influence of anger and compassion on negotiation performance. *Organizational Behavior and Human Decision Processes*, *70*(3), 175–187. https://doi.org/10.1006/obhd.1997.2705

Babbie, E. R. (2020). *The practice of social research* (15th ed.). Cengage AU.

Bazerman, M. H., Curhan, J. R., Moore, D. A., & Valley, K. L. (2000). Negotiation. *Annual Review of Psychology*, *51*(1), 279–314. https://doi.org/10.1146/annurev.psych.51.1.279

Bolkan, S., & Goodboy, A. K. (2021). Negotiating in distributive bargaining scenarios: the effect of sharing one's alternative. *Communication Studies*, *72*(4), 720–733. https://doi.org/10.1080/10510974.2021.1953101

Connolly, L. Y., & Borrion, H. (2022). Reducing ransomware Crime: Analysis of victims' payment decisions. *Computers & Security*, *119*, 102760. https://doi.org/10.1016/j.cose.2022.102760

Demographics and Motivation of Cyber attacks by Nation State Actors: New Kids on the Block. (2023, February 27). Cyberclan.com. Retrieved March 25, 2024, from https://cyberclan.com/us/knowledge/demographics-and-motivation-of-cyber-attacks-by-nation-state-actors-new-kids-on-the-block-2/

Donohue, W. A., Kaufmann, G., Smith, R., & Ramesh, C. (1991). Crisis bargaining: A framework for understanding intense conflict. *International Journal of Group Tensions*, *21*(2), 133-154.

Donohue, W. A., & Roberto, A. J. (1996). AN EMPIRICAL EXAMINATION OF THREE MODELS OF INTEGRATIVE AND DISTRIBUTIVE BARGAINING. *International Journal of Conflict Management*, *7*(3), 209–229. https://doi.org/10.1108/eb022782

Edwards, M. S., Williams, E., Peersman, C., & Rashid, A. (2022). Characterising Cybercriminals: A review. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2202.07419

Faivre, J. (2023). Negotiations in Tech : An analysis of Asymmetric ransomware negotiations. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4530094

Fisher, R., & Ury, W. R. (1981). *Getting to Yes*. Houghton-Mifflin.

Fu, P., Kennedy, J. C., Tata, J., Yukl, G., Bond, M. H., Peng, T. K., Srinivas, E. S., Howell, J. P., Prieto, L., Koopman, P., Boonstra, J., Pasa, S. F., Lacassagne, M., Higashide, H., & Cheosakul, A. (2004). The impact of societal cultural values and individual social beliefs on the perceived effectiveness of managerial influence strategies: a meso approach. *Journal of International Business Studies*, *35*(4), 284–305. https://doi.org/10.1057/palgrave.jibs.8400090

Giebels, E. (2002). Beïnvloeding in gijzelingsonderhandelingen: de tafel van tien. *Nederlands Tijdschrift Voor De Psychologie En Haar Grensgebieden*, *57*, 145–154. https://research.rug.nl/en/publications/be%C3%AFnvloeding-in-gijzelingsonderhandelingen-de-tafel-van-tien

Giordano, G. A., Stoner, J., Brouer, R. L., & George, J. F. (2008). Computer mediated negotiations and deception. In *IGI Global eBooks* (pp. 220–229). https://doi.org/10.4018/978-1-59904-863-5.ch017

Griessmair, M., Hippmann, P., & Gettinger, J. (2015). Emotions in e-Negotiations. In *Springer eBooks* (pp. 101–135). https://doi.org/10.1007/978-94-017-9963-8_5

Griffiths, C. (2024, March 1). The Latest Cyber Crime Statistics (updated March 2024) | AAG IT Support. *AAG IT Services*. Retrieved March 20, 2024, from https://aag-it.com/the-latest-cyber-crime-statistics/

Grubb, A. (2010). Modern day hostage (crisis) negotiation: The evolution of an art form within the policing arena. *Aggression and Violent Behavior*, *15*(5), 341–348. https://doi.org/10.1016/j.avb.2010.06.002

Hack, P., & Wu, Z. (2021, November 12). *"We wait, because we know you." Inside the ransomware negotiation economics.*Research.nccgroup.com. Retrieved July 27, 2023, from https://research.nccgroup.com/2021/11/12/we-wait-because-we-know-you-inside-the-ransomware-negotiation-economics/

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. (2009). *Multivariate data analysis* (7th ed.). Pearson.

Hammer, M. R., & Rogan, R. G. (1997). Negotiation models in crisis situations: The value of a communication-based approach. *Dynamic processes of crisis negotiation: Theory, research and practice*, 9-23.

Hernandez-Castro, J., Cartwright, E., & Stepanova, A. (2017). Economic analysis of ransomware. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1703.06660

Hofmann, T. (2020). How organisations can ethically negotiate ransomware

payments. *Network Security*, *2020*(10), 13–17. https://doi.org/10.1016/s1353-4858(20)30118-5

Ireland, C. A., & Vecchi, G. M. (2009). The Behavioral Influence Stairway Model (BISM): a framework for managing terrorist crisis situations? *Behavioral Sciences of Terrorism and Political Aggression*, *1*(3), 203–218. https://doi.org/10.1080/19434470903017722

Kamphuis, W., Giebels, E., & Noelanders, S. (2006). Effectieve beïnvloeding in crisisonderhandelingen: De rol van soort incident en fase van de onderhandeling. In *Netherlands Journal of Psychology* (Vol. 61, Issue 2).

Keijzer, N. (n.d.). Inside the world of ransomware part 2/3: Different roles within a ransomware attack. *Inside The World Of Ransomware Part 2/3: Different Roles Within A Ransomware Attack*. Retrieved March 24, 2024, from https://northwave-cybersecurity.com/threat-intel-research/inside-the-world-of-ransomware-part-2-3-different-roles-within-a-ransomware-attack

Kellin, B. R. C., & McMurtry, C. M. (2007). STEPS–Structured Tactical Engagement Process. *Journal of Police Crisis Negotiations*, *7*(2), 29–51. https://doi.org/10.1300/j173v07n02_03

Keshavarzi, M., & Ghaffary, H. R. (2023). An ontology-driven framework for knowledge representation of digital extortion attacks. *Computers in Human Behavior*, *139*, 107520. https://doi.org/10.1016/j.chb.2022.107520

Kopelman, S., Rosette, A. S., & Thompson, L. (2006). The three faces of Eve: Strategic displays of positive, negative, and neutral emotions in negotiations. *Organizational Behavior and Human Decision Processes*, *99*(1), 81–101. https://doi.org/10.1016/j.obhdp.2005.08.003

Kroneberg, C., Heintze, I., & Mehlkop, G. (2010). THE INTERPLAY OF MORAL NORMS AND INSTRUMENTAL INCENTIVES IN CRIME CAUSATION*. *Criminology*, *48*(1), 259–294. https://doi.org/10.1111/j.1745-9125.2010.00187.x

Li, Z., & Liao, Q. (2020). Ransomware 2.0. *ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3407023.3409196

Mamontov, V. D., Кожевникова, T. M., & Radyukova, Y. (2014). Collectivism and individualism in modern Russia. *Asian Social Science*, *10*(23). https://doi.org/10.5539/ass.v10n23p199

McLean, M. (2024, January 4). *2024 Must-Know Cyber Attack statistics and Trends |*

Embroker. Embroker. Retrieved March 20, 2024, from https://www.embroker.com/blog/cyber-attack-statistics/

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security*, *92*, 101762. https://doi.org/10.1016/j.cose.2020.101762

Morris, M. W., Larrick, R. P., & Su, S. K. (1999). Misperceiving negotiation counterparts: When situationally determined bargaining behaviors are attributed to personality traits. *Journal of Personality and Social Psychology*, *77*(1), 52–67. https://doi.org/10.1037/0022-3514.77.1.52

Nogami, T. (2009). Reexamination of the association between anonymity and Self-Interested Unethical Behavior in adults. *The Psychological Record*, *59*(2), 259–272. https://doi.org/10.1007/bf03395662

Nogami, T., & Takai, J. (2008). Effects of anonymity on antisocial behavior committed by individuals. *Psychological Reports*, *102*(1), 119–130. https://doi.org/10.2466/pr0.102.1.119-130

Northwave Cyber Security - your safe digital journey - home. (n.d.). Retrieved March 26, 2024, from https://northwave-cybersecurity.com/

Ohtsubo, Y., & Kameda, T. (1998). The function of equality heuristic in distributive bargaining: negotiated allocation of costs and benefits in a demand revelation context. *Journal of Experimental Social Psychology*, *34*(1), 90–108. https://doi.org/10.1006/jesp.1997.1340

Paese, P. W., & Gilin, D. (2000). When an Adversary is Caught Telling the Truth: Reciprocal Cooperation Versus Self-Interest in Distributive Bargaining. *Personality and Social Psychology Bulletin*, *26*(1), 79–90. https://doi.org/10.1177/0146167200261008

Perreault, S., & Kida, T. (2011). The relative effectiveness of persuasion tactics in auditor–client negotiations. *Accounting, Organizations and Society*, *36*(8), 534–547. https://doi.org/10.1016/j.aos.2011.09.001

Perugini, M., Gallucci, M., Presaghi, F., & Ercolani, A. P. (2003). The personal norm of reciprocity. *European Journal of Personality*, *17*(4), 251–283. https://doi.org/10.1002/per.474

PurpleSec. (2023, February 22). *2023 Cyber Security Statistics: The ultimate list of stats, data & trends | PurpleSec*. Retrieved March 20, 2024, from https://purplesec.us/resources/cyber-security-statistics/#Cybercrime

Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B. C. M., &

Assi, C. (2023). The Age of Ransomware: A survey on the evolution, taxonomy, and research directions. *IEEE Access*, *11*, 40698–40723. https://doi.org/10.1109/access.2023.3268535

Riabov, O., & Riabova, T. (2014). The remasculinization of Russia? *Problems of Post-communism*, *61*(2), 23–35. https://doi.org/10.2753/ppc1075-8216610202

Rogan, R. G., & Hammer, M. R. (1995). Assessing Message Affect in Crisis Negotiations An Exploratory Study. *Human Communication Research*, *21*(4), 553–574. https://doi.org/10.1111/j.1468-2958.1995.tb00358.x

Ryan, P., Fokker, J., Healy, S., & Amann, A. (2022). Dynamics of Targeted Ransomware Negotiation. *IEEE Access*, *10*, 32836–32844. https://doi.org/10.1109/access.2022.3160748

Scanzoni, J., & Godwin, D. D. (1990). Negotiation effectiveness and acceptable outcomes. *Social Psychology Quarterly*, *53*(3), 239. https://doi.org/10.2307/2786962

Sentsova, A., & DiMaggio, J. (2023). *Negotiating with LockBit: Uncovering the Evolution of Operations and Newly Established Rules*. Analyst1. Retrieved March 20, 2024, from https://analyst1.com/blog-negotiating-with-lockbit-uncovering-the-evolution-of-operations-and-newly-established-rules/

Sharmeen, S., Ahmed, Y. A., Huda, S., Koçer, B. Ş., & Hassan, M. M. (2020). Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. *IEEE Access*, *8*, 24522–24534. https://doi.org/10.1109/access.2020.2970466

Shirako, A., Kilduff, G. J., & Kray, L. J. (2015). Is there a place for sympathy in negotiation? Finding strength in weakness. *Organizational Behavior and Human Decision Processes*, *131*, 95–109. https://doi.org/10.1016/j.obhdp.2015.09.004

Stoddart, K. (2022). Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. In *Springer eBooks* (pp. 351–399). https://doi.org/10.1007/978-3-030-97299-8_6

Taylor, P. J. (2002). A cylindrical model of communication behavior in crisis negotiations. *Human Communication Research*, *28*(1), 7–48. https://doi.org/10.1111/j.1468-2958.2002.tb00797.x

Thompson, L., Wang, J., & Gunia, B. C. (2010). Negotiation. *Annual Review of Psychology*, *61*(1), 491–515. https://doi.org/10.1146/annurev.psych.093008.100458

Threat Landscape Report 2023. (n.d.). cert.europe.eu. Retrieved March 25, 2024, from https://cert.europa.eu/publications/threat-intelligence/tlr2023/

Ury, W. (1991). *Getting past No: Negotiating with Difficult People*. Bantam.

Vallano, J. P., & Compo, N. S. (2015). Rapport-building with cooperative witnesses and criminal suspects: A theoretical and empirical review. *Psychology, Public Policy and Law*, *21*(1), 85–99. https://doi.org/10.1037/law0000035

Van Kleef, G. A., De Dreu, C. K. W., & Manstead, A. S. R. (2004). The interpersonal Effects of Emotions in Negotiations: A motivated information processing approach. *Journal of Personality and Social Psychology*, *87*(4), 510–528. https://doi.org/10.1037/0022-3514.87.4.510

Vecchi, G. (2007). Crisis communication: Skills building in an online environment. *Unpublished manuscript. Quantico, VA: Behavioral Science Unit, FBI Academy*.

Vecchi, G. M., Van Hasselt, V. B., & Romano, S. J. (2005). Crisis (hostage) negotiation: current strategies and issues in high-risk conflict resolution. *Aggression and Violent Behavior*, *10*(5), 533–551. https://doi.org/10.1016/j.avb.2004.10.001

Wade, M. (2021). Digital hostages: Leveraging ransomware attacks in cyberspace. *Business Horizons*. https://doi.org/10.1016/j.bushor.2021.07.014

Wall, J. A. (1977). Operantly conditioning a negotiator's concession making. *Journal of Experimental Social Psychology*, *13*(5), 431–440. https://doi.org/10.1016/0022-1031(77)90028-2

Warikoo, A. (2023). Perspective Chapter: Ransomware. In *IntechOpen eBooks*. https://doi.org/10.5772/intechopen.108433

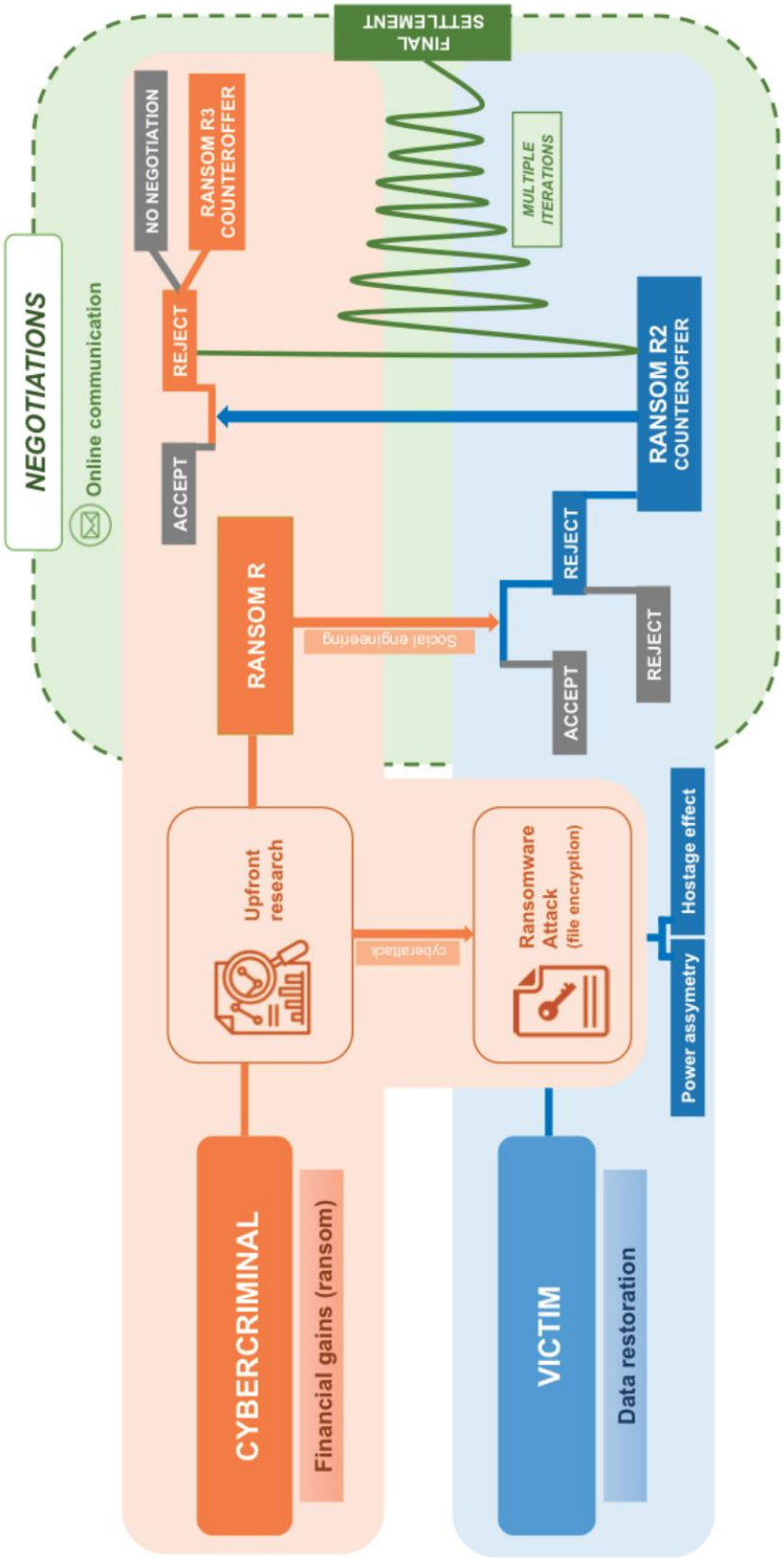
White, J. B., Tynan, R., Galinsky, A. D., & Thompson, L. (2004). Face threat sensitivity in negotiation: Roadblock to agreement and joint gain. *Organizational Behavior and Human Decision Processes*, *94*(2), 102–124. https://doi.org/10.1016/j.obhdp.2004.03.005

Williams, C. R., Robu, V., Gerding, E. H., & Jennings, N. R. (2011). Using Gaussian processes to optimise concession in complex negotiations against unknown opponents. *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence*, 432–438. https://doi.org/10.5591/978-1-57735-516-8/ijcai11-080

Zimba, A., & Chishimba, M. (2019). On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. *European Journal for Security Research*, *4*(1), 3–31. https://doi.org/10.1007/s41125-019-00039-8

APPENDIX A – WANNACRY RANSOMWARE (FAIVRE, 2023, P6)

Adapted from Faivre (2023, P6)



APPENDIX B – THEORETICAL OVERVIEW

Authors, theoretical foundation and research aim	Key-words (when given)	Incorporated findings	Biggest limitations in regard to this study
Bazermann et al. (2000) provide a framework for understanding the process and outcome of negotiations through various factors, namely negotiators' mental models, ethical considerations, the number of parties within a negotiation, the choice of communication medium, and cross-cultural concepts.	Bargaining; Communications media; Culture; Ethics; Mental Models; Multiparty Negotiation.	Bazerman et al. (2000) emphasize the significance of mental models in negotiation. They also highlight the importance of ethical considerations, the impact of communication methods on negotiation outcomes, and the analysis of cross-cultural differences in negotiation across different dimensions.	This paper lacks findings pertaining to crisis negotiation or ransomware negotiation.
Hernandez-Castro et al. (2017) provide an economic analysis of ransomware, including price discrimination and bargaining strategies.	Ransomware; Economy; Analysis; Price Discrimination; Bargaining; Uniform Pricing.	The criminal's profit can be expressed as a summation of all targeted victims, subtracted by the cost of handling ransom money.	Doesn't include negotiation strategies, data selling potential, business continuity impact, threat actor codes of conduct, cultural factors, and the notion of multiple threat actor roles.
Vecchi et al. (2005) review the integration of crisis management and intervention in crisis negotiation, emphasizing the Behavioral Change Stairway Model (BCSM) as a systematic approach for peaceful resolution, and highlighting role-playing's crucial role in	Crisis Negotiation; Hostage Negotiation; Crisis Intervention; Role-playing; Conflict Resolution; Online.	Vecchi et al. (2005) delineate the distinction between hostage situations, motivated by instrumental factors like specific demands, and scenarios where captives are taken for expressive reasons, driven primarily by intense emotional states.	This study solely delves into conventional discourse surrounding crisis and hostage negotiation.

Continues

skill assessment and training.			
Hack and Wu (2021) explore how adversaries use economic models to maximize their profits, what this means for the position of the victim during the negotiation, and what strategies victims can use to even the playing field.		Hack and Wu (2021) augment this profit equation by introducing additional variables, providing a comprehensive structural overview of the factors influencing the modus operandi of threat actors. They outline three price discrimination techniques.	Doesn't include negotiation strategies, data selling potential, business continuity impact, threat actor codes of conduct, cultural factors, and the notion of multiple threat actor roles.
Li and Liao (2020) propose a new model to differentiate between traditional ransomware (ransomware 1.0), which solely demands ransom, and the emerging variant (ransomware 2.0), which involves both selling the data and demanding ransom.	Cyber-security; Ransomware 2.0; Data Selling; Game Theory; Economics.	Ransomware 2.0 is often more profitable than its predecessor, with traditional defenses like data backup and the never-pay-ransom strategy may not suffice. Uncertainties surrounding this new model could impact attackers' reputation and victims' willingness to pay.	Doesn't include negotiation strategies, data selling potential, business continuity impact, threat actor codes of conduct, cultural factors, and the notion of multiple threat actor roles.
Zimba & Chishimba (2019) discuss the technical and economic impacts of the ransomware pandemic, focusing on its effects on businesses, including paid ransoms and lost revenue due to downtime and production loss.	Enterprise Security; Cyberthreat; Crypto-ransomware; Encryption; Cryptocurrency; Bitcoin.	Businesses rely heavily on enterprise information systems (EIS) for core functions. When they're down, this results heavily in utility costs and therefore has implications on the victim's WTP.	Negotiation is beyond the scope of this research.

Continues

Faivre (2022) endeavors to elucidate the complexities of asymmetric ransomware negotiations, offering insights to enhance comprehension and response to this cybersecurity threat.	Ransomware; Cybercriminals; Wannacry; Malicious software; Encryption; Decryption key; Bitcoin ransom; Targeted ransomware; Cyber-negotiations; Unlevel playing field; Predatory motivations; Illegitimate negotiations; Game theory modeling; Information asymmetry; Double-extortion; Dirty Tricks.	Paper explores the strategic tactics of threat actors in ransomware negotiations, emphasizing the calculated nature of ransom demands, the predatory dynamics, challenges in trust-building, and the use of psychological tactics such as urgency-inducing visuals, highlighting the mutual benefit in resolving negotiations.	Doesn't include negotiation strategies, threat actor codes of conduct, cultural factors, and the notion of multiple threat actor roles.
Warikoo (2023) presents a brief history of ransomware, top threat actors employing ransomware, tactics used, and key strategies firms need to deploy to prevent, detect, and respond to ransomware in attacks.	Ransomware; Extortion; Threat Actor Groups; Tactics; Prevention; Detection; Response	Warikoo (2023) identifies three distinct periods: pre-2014, 2015-2017, and post-2017. During these phases, threat actors adapted their strategies, leading to the emergence of personalized pricing models and BGH.	Negotiation is beyond the scope of this research.
Hofmann (2020) outlines the ethical dilemma of whether to negotiate with cybercriminals during ransomware incidents.		Hofmann (2020) outlines the dual considerations of ethics and finances in deciding whether to pay a ransom, and recommends a structured approach involving incident response procedures, negotiation tactics, and strategic payment planning to	Negotiation strategies are beyond the scope of this research.

Continues

		minimize risks and ensure secure recovery.	
Meland et al. (2020) studied darknet markets and forums over a period of two years using a netnographic research approach.	Ransomware; RaaS; Malware; Darknet; Marketplace; Netnography.	Meland et al. (2020) discuss the emergence RaaS on darknet markets, presenting it as a franchise-like model enabling individuals lacking programming expertise to engage in ransomware attacks and profit from the illicit economy.	The research focuses solely on English-speaking markets and forums, which are recognized for their heightened interest in drug-related products and carding services, in contrast to Russian sites.
Griessmair et al. (2015) explore how emotions influence negotiation dynamics both internally, affecting decision-making, and externally, shaping social interactions, particularly in the context of electronic negotiation and decision support systems.	Group Decision; E-negotiation; Emotion; Emotive Decision Systems.	The choice between synchronous and asynchronous digital channels affects real-time interaction and the ability to review exchanges.	Does not incorporate crisis negotiation concepts.
Stoddart (2022) offers a comprehensive examination of cybersecurity threats, encompassing outsider threats, insider threats, Social Engineering tactics, terrorism, cybercrime, organized crime involvement and state-sponsored attacks.	Cybercrime; Terrorism; Hacking; APT; SNA; Cybercrime; Dark Net; Ransomware; Proxy	Stoddart (2022) underscores Russia and China as the primary cyber threats to the West, while also emphasizing the significant involvement of organized crime groups from Eastern Europe, particularly those with ties to Russia.	Negotiation is beyond the scope of this chapter.

Continues

Adair et al. (2004) investigates how culture influences negotiation outcomes by studying the effects of information sharing and power strategies in intracultural negotiations across six cultures with uncertain correlations between cultural values and joint gains.	Russian culture values indirect, nuanced negotiation strategies, reflecting a broader preference for implicit communication and situational cues.	Does not incorporate crisis negotiation concepts.
Kamphuis et al. (2006) investigates how the use of ten different influencing strategies affects the outcome of crisis negotiations and to what extent the effectiveness depends on the type of incident and the negotiation phase.	Kamphuis et al. (2006) categorizes crisis negotiations into three phases, finding that the "Being Equal" strategy is more effective in the initial phase, emphasizing relational strategies' role in pacifying aggressors and co-creating solutions with perpetrators, while noting the lack of support for the hypothesized effectiveness of the commonly used "Being Kind" strategy.	This research does not cover ransomware and e-negotiations, and the sample size is limited to the Netherlands and Belgium.
Rogan and Hammer (1995) investigate patterns of perpetrator and negotiator message affect behavior in three actual crisis negotiation incidents are examined.	Strategies centered on empathy, dignity preservation, and emotional reassurance (Rogan & Hammer, 1995) were hypothesized to improve negotiators' effectiveness by reducing	This research does not cover ransomware and/or e-negotiations, and the sample size is very limited.

Continues

		confrontational stances and fostering a more collaborative environment.	
Wade (2022) outlines an interdisciplinary approach to cybernegotiation combining features of online dispute resolution and terrorist hostage theory.	Ransomware; Cybersecurity; Hostage Negotiation; Dispute System Design; Cryptocurrency	Wade (2022) proposes applying crisis and hostage negotiation theories to the cyber domain, advocating for the "Wade and Seek" methodology to build rapport with hackers by recognizing their expertise and displaying warmth and cooperation, offering a methodological crossover for addressing ransomware incidents.	This research does not encompass the ransomware mental model, ethics, cultural dynamics, the threat actor value chain, or the choice of communication channel.
Grubb (2010) examines the role of hostage negotiation in the 21st century by reviewing historical literature, crisis dynamics, conceptual models, and negotiation strategies.	Hostage Negotiation; Crisis Negotiation; Mental Health; Strategy; Model.	Grubb (2010) emphasizes various negotiation approaches and models, including the "interest-based" approach, the Crisis Bargaining model, S.A.F.E., BISM, the Cylindrical Model of Crisis Negotiation, and STEPS.	This research does not cover ransomware and/or e-negotiations.
Fisher and Ury (1981) introduced principled negotiation, emphasizing an "interest-based" approach to conflict resolution.		Advocates four key principles: separating the person from the problem, focusing on mutual interests rather than individual positions, generating options for	this model has been critiqued for its limited applicability in crisis situations involving individuals in irrational cognitive states, such as

Continues

	mutual gain, and insisting on objective criteria to judge agreements' effectiveness.	severe mental illness or emotional conflict.
Ury (1991) expands upon his earlier work, devising a five-step model for challenging negotiations, including hostage situations.	Ury's negotiation model advises steps like observing without emotional reaction, portraying the hostage taker as an ally, reframing demands for solutions, involving the subject in decision-making, and making it difficult for them to refuse, facilitating successful resolution.	While this model offers a toolkit of techniques for crisis situations, it relies on some degree of cognitive rational processing from both parties, a feature often absent in the mindset of hostage takers.
Donohue et al. (1991) present a model distinguishing between crisis (distributive) and normative (integrative) bargaining strategies employed by hostage negotiators.	Donohue et al. (1991) stress addressing relational and material issues in negotiation, guiding hostage takers towards crisis resolution through normative bargaining.	This model does not cover ransomware and/or e-negotiations.
The S.A.F.E. model, developed by Hammer and Rogan (1997) offers a structured approach to crisis negotiation, drawing from behavioral science research and input from experienced negotiators.	S.A.F.E. identifies four key triggers—Substantive Demands, Attunement, Face, and Emotion—that influence subject behavior during crises. Each trigger represents a communicative frame.	This model does not cover ransomware and/or e-negotiations.

Continues

The Behavioral Influence Stairway Model (BISM), developed by Vecchi (2007), is a crisis negotiation model based on active listening principles, adapted from the Federal Bureau of Investigation Crisis Negotiation Unit (FBI CNU).	BISM emphasizes relationship-building between negotiator and subject to achieve a peaceful resolution. Drawing parallels with Motivational Interviewing, the BISM focuses on skills like empathy, rapport, and active listening to facilitate behavior change.	This model does not cover ransomware and/or e-negotiations.
The Cylindrical Model of Crisis Negotiation, developed by Taylor (2002) emphasizes the complexity of negotiation by focusing on levels of interaction, motivational emphases, and behavior intensity.	Taylor's dynamic negotiation model aims to guide subjects towards cooperation, considering motivational themes and negotiation behavior intensity for successful outcomes.	This model does not cover ransomware and/or e-negotiations.
The Structured Tactical Engagement Process (STEPS) model, developed by Kellin and McMurtry (2007), draws from the Transtheoretical Stages of Change Model (Prochaska & DiClemente, 1986) to provide a framework for managing crisis situations.	The model identifies four stages: Precontemplation, Contemplation, Preparation, and Action, each representing the subject's progression toward behavioral change and peaceful resolution. Negotiators utilize various skills and techniques to guide	This model does not cover ransomware and/or e-negotiations.

Continues

		subjects through these stages.	
Vallano and Compo (2015) review recent empirical literature on rapport-building in investigative interviews, summarizing definitions, techniques, and research on its effects on witness cooperation and the diagnostic value of information from suspects.	Rapport-building; Investigative Interview; Interrogation; Eyewitness recall; Suspect Confessions	Vallano & Compo (2015) explore rapport-building techniques including verbal and non-verbal communication, finding common ground, and providing support to foster productive dialogue in investigative settings, viewing rapport as a productive working relationship essential for achieving investigative objectives.	While Vallano & Compo's (2015) exploration provides valuable insights into rapport-building techniques, it does not delve deeply into the broader domain of relationship-building. Also, research does not cover ransomware and/or e-negotiation dynamics in rapport-building.
Giebels (2002) examines how the use of ten different influencing strategies affects the outcome of crisis negotiations and to what extent the effectiveness of these strategies depends on the type of incident and the phase of negotiation in which they are applied.		In this study, the effectiveness of negotiation outcomes correlated with the use of influencing strategies. Calming strategies were found to be effective in the initial phase, while relationship focus was crucial in the problem-solving phase of soft negotiations. Hard negotiations in the problem-solving phase yielded no significant results. Additionally, providing explicit instructions to the perpetrator was associated with	Research does not cover ransomware and/or e-negotiation dynamics.

Continues

		effectiveness in the decision-making phase.	
White et al. (2004) investigate variations in individuals' sensitivity to face threats (FTS) and examine how a negotiator's role influences the connection between their FTS and negotiation results.	Negotiation; Conflict Resolution; Face; Face Threat Sensitivity; Identity; Politeness Theory	Maintaining a kind and respectful demeanor that preserves the other party's face may improve negotiation outcomes.	Research does not cover ransomware and/or e-negotiation dynamics.

APPENDIX C – CODING TABLE

Adapted from Euwema & Giebels (forthcoming)

Strategy	Underlying principle	Examples of behavior
1. Being kind	Sympathy	A. Active listening B. Show empathy C. Kindly offer something
2. Being equal	Identification	A. Use 'We' instead of 'I/You' B. Stress something you have in common (background, family circumstances, hobbies) C. Emphasize mutual goal/dependence/enemy
3. Being credible	Authority	A. Show reliability (do what you say) B. Emphasize your expertise/experience (you know what you are doing) C. Show you are transparent
4. Emotional appeal	Self-image (heart)	A. Touch upon feelings/ask for sympathy (how it affects you/victims) B. Praise other's behavior C. Boost other's self-respect
5. Intimidation	Deterrence	A. Warnings B. Threats C. Codemn transgression
6. Imposing a restriction	Scarcity	A. Postpone an answer B. Ignore other/not being available C. Offer limited choice (A or B)
7. Direct pressure	Power of fact/repetition	A. Repeat request (planting the seed) B. Share fact C. Give instruction
8. Legitimizing	Legitimacy (external)	A. Reference to formal rules/the law B. Reference to procedures C. Mentioning of moral/social codes
9. Exchanging	Reciprocity	A. Ask for something in return B. Lower your bid C. Exchange proposal
10. Rational persuasion	Consistency (head)	A. Use of arguments B. Provide logic C. Confront with inconsistencies

APPENDIX D – SCATTERPLOTS

Figure 1
Scatterplot Exchanging and Information Exchange

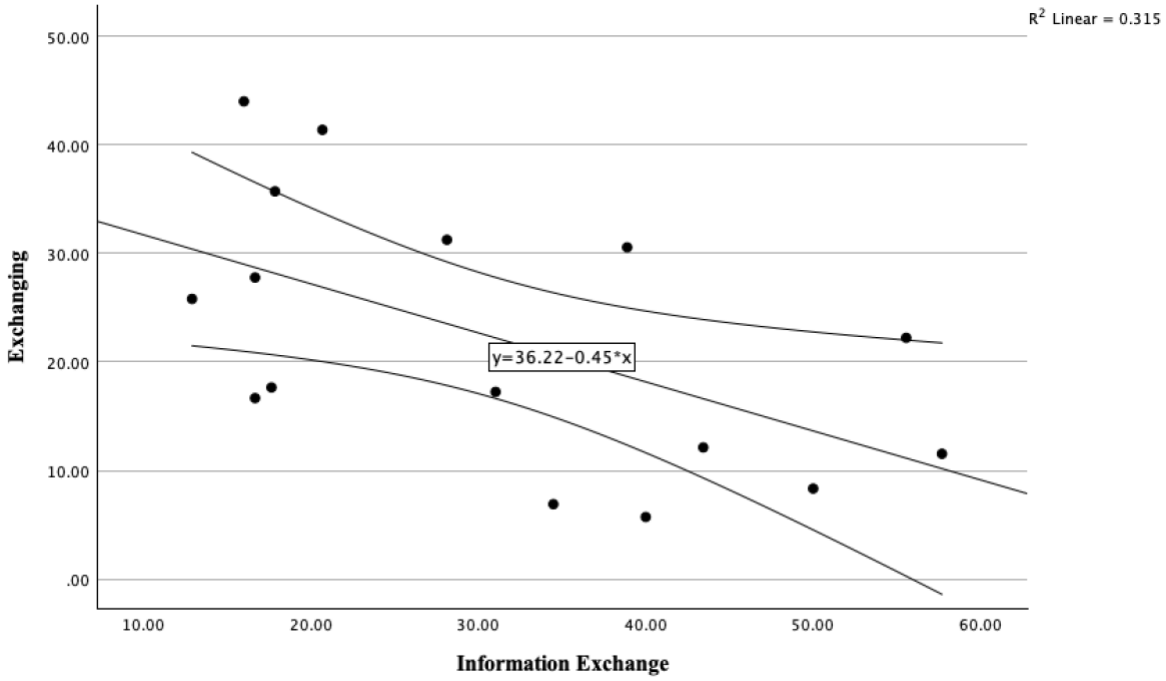


Figure 2
Scatterplot Being Kind on Discount

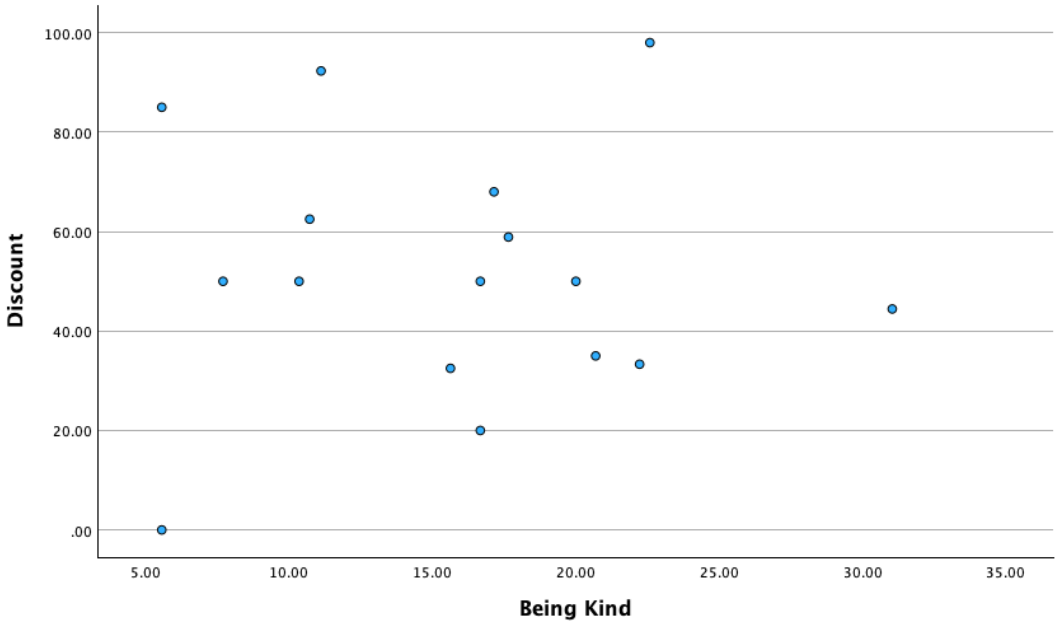


Figure 3
Scatterplot Being Equal on Discount

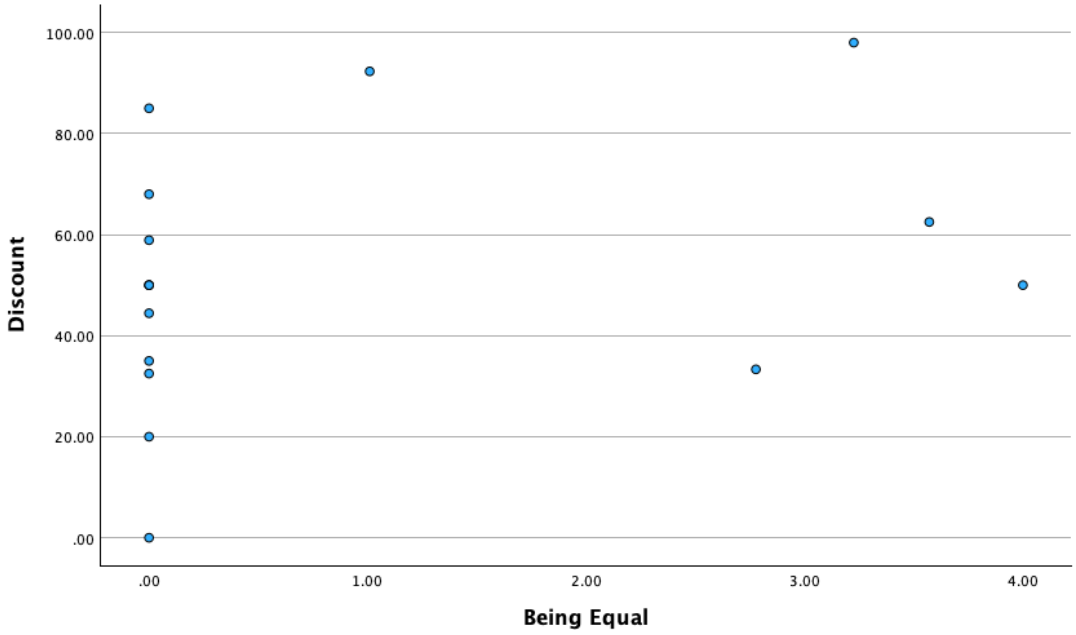


Figure 4
Scatterplot Emotional Appeal on Discount

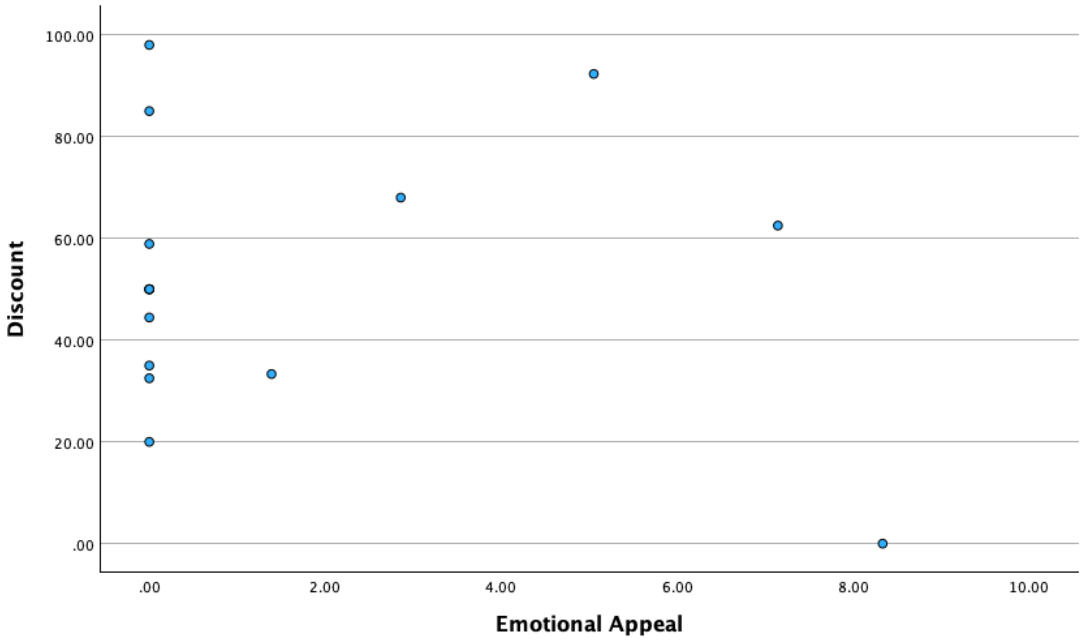


Figure 5
Scatterplot Rational Persuasion on Discount

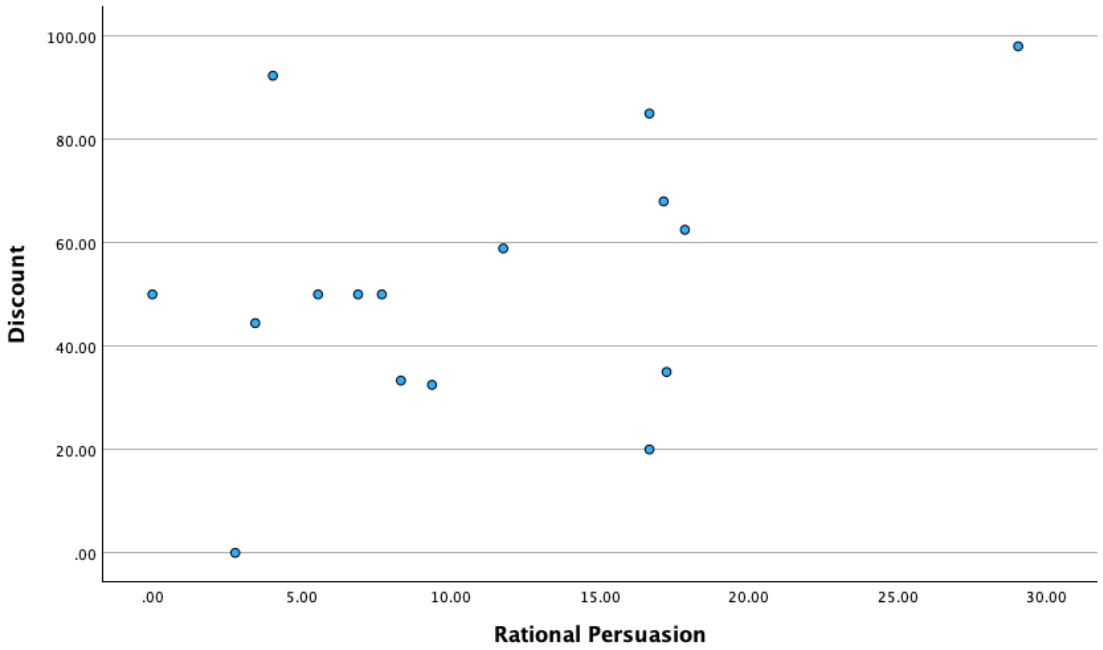


Figure 6
Scatterplot Legitimizing on Discount

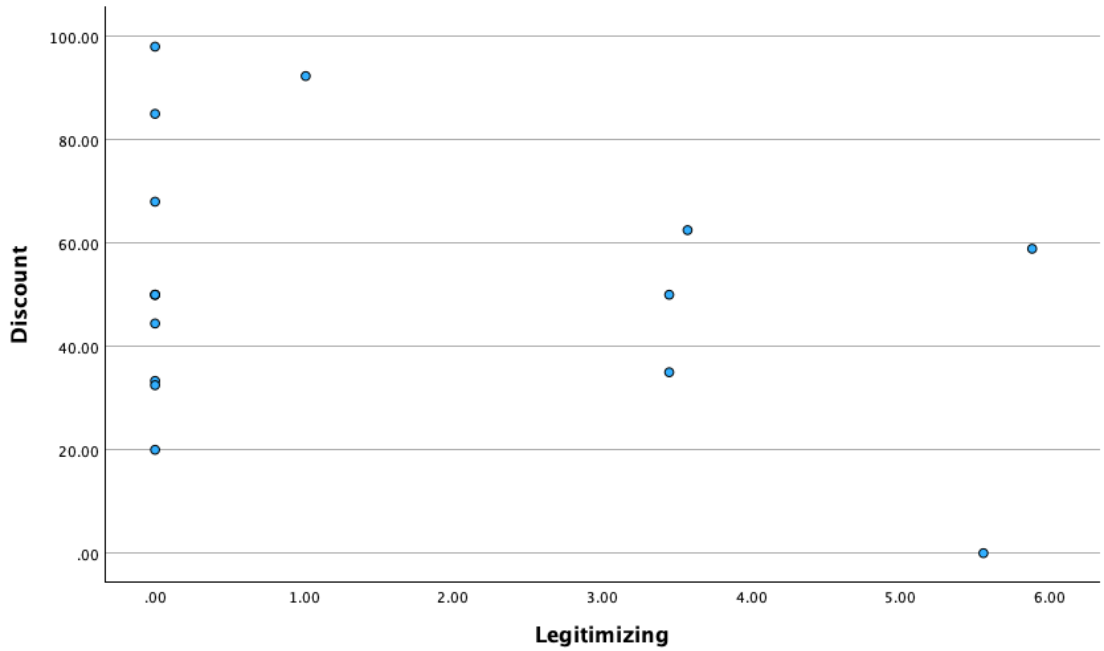


Figure 7

Scatterplot Standardized Residuals on Standardized Predicted Values Being Kind

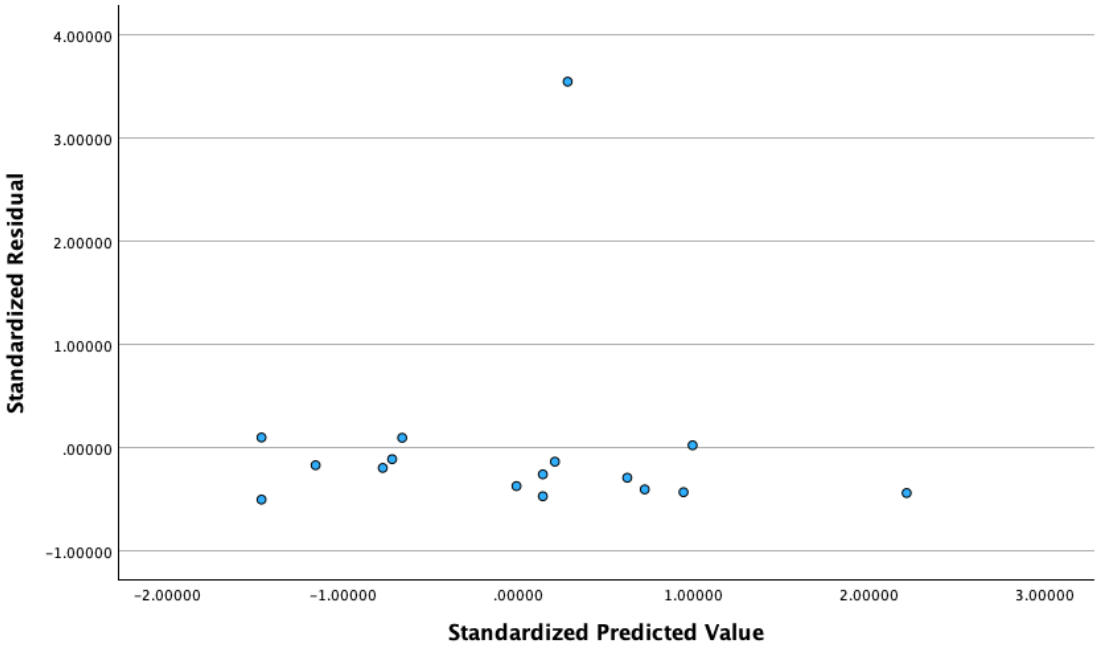


Figure 8

Scatterplot Standardized Residuals on Standardized Predicted Values Being Equal

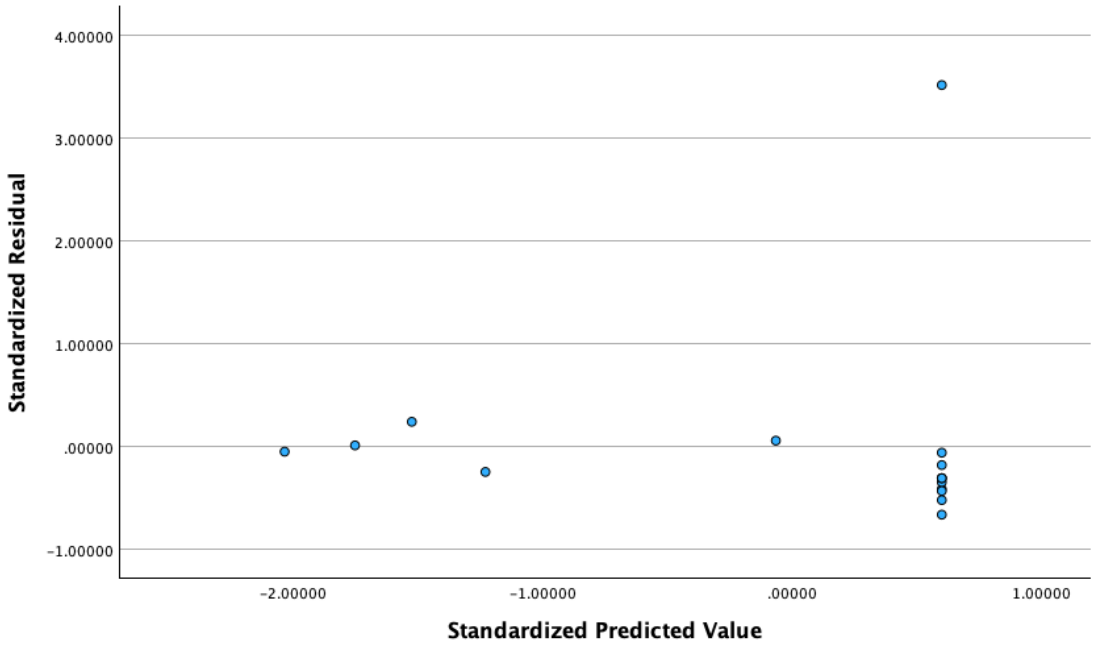


Figure 9

Scatterplot Standardized Residuals on Standardized Predicted Values Emotional Appeal

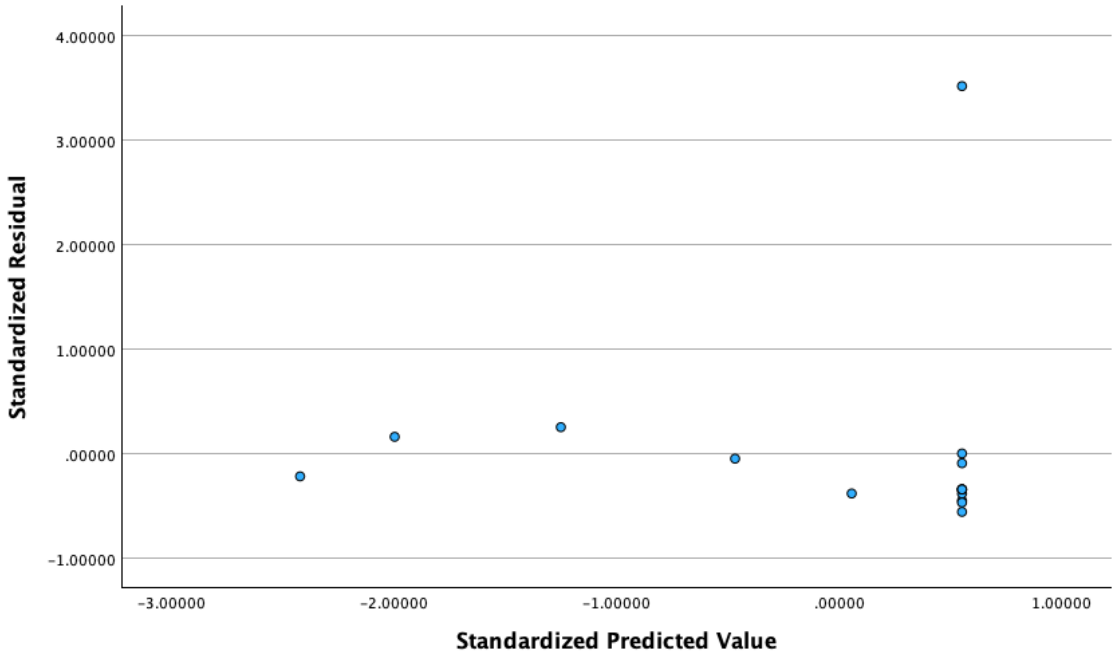


Figure 10

Scatterplot Standardized Residuals on Standardized Predicted Values Legitimizing

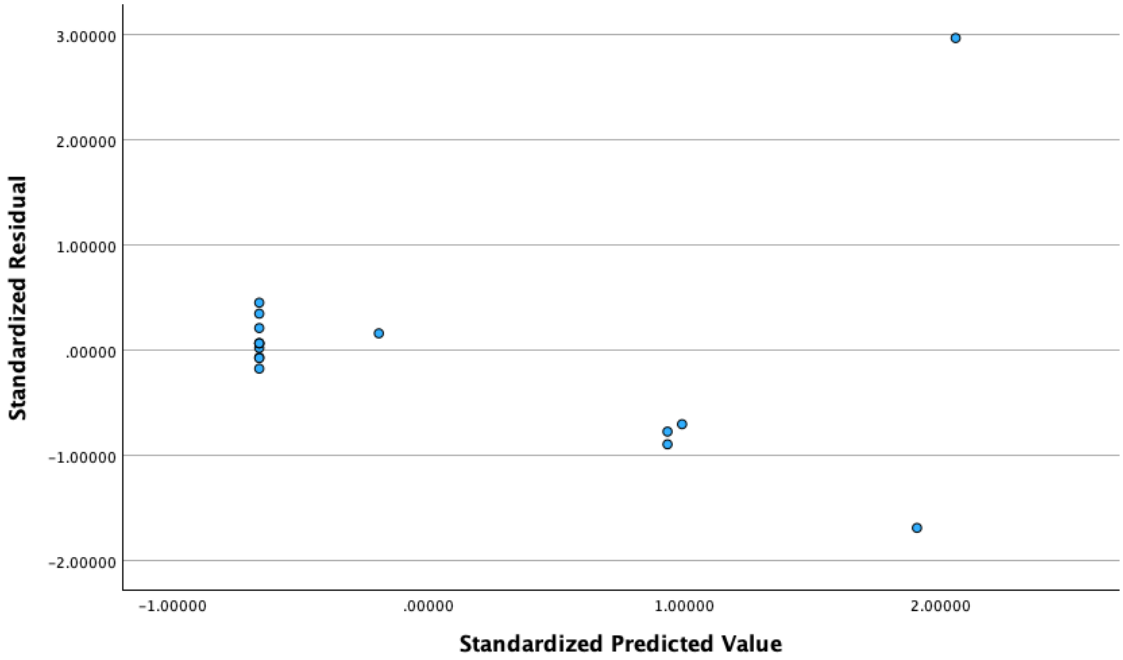
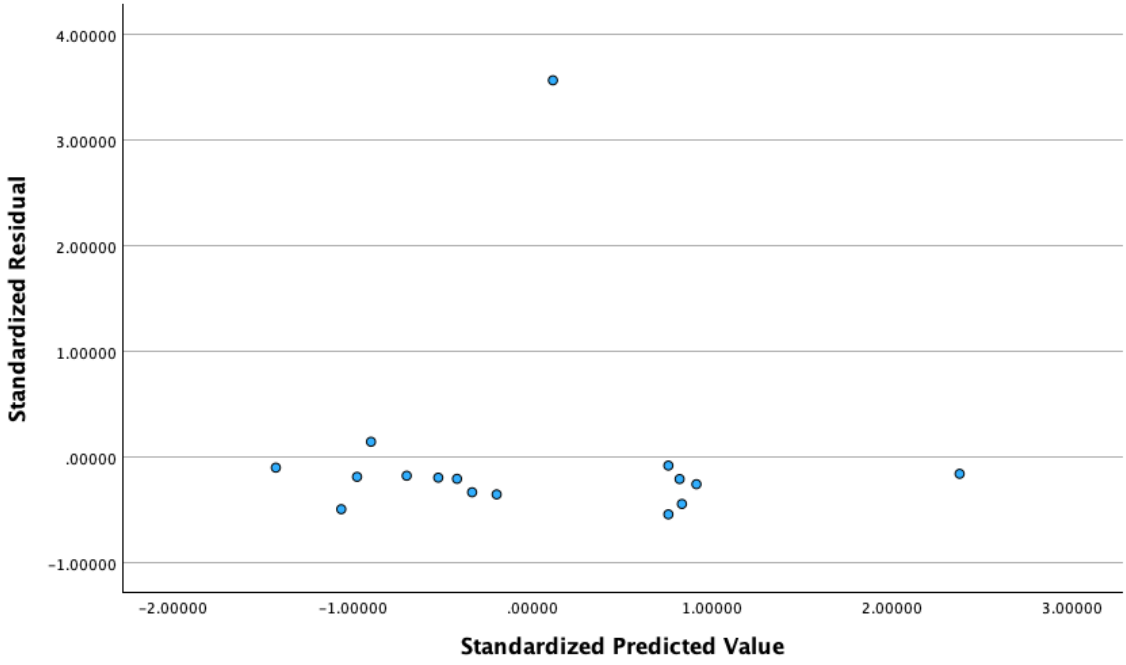


Figure 11

Scatterplot Standardized Residuals on Standardized Predicted Values Rationality



APPENDIX E – BOXPLOTS

Figure 1
Simple Boxplot of Annual Revenue

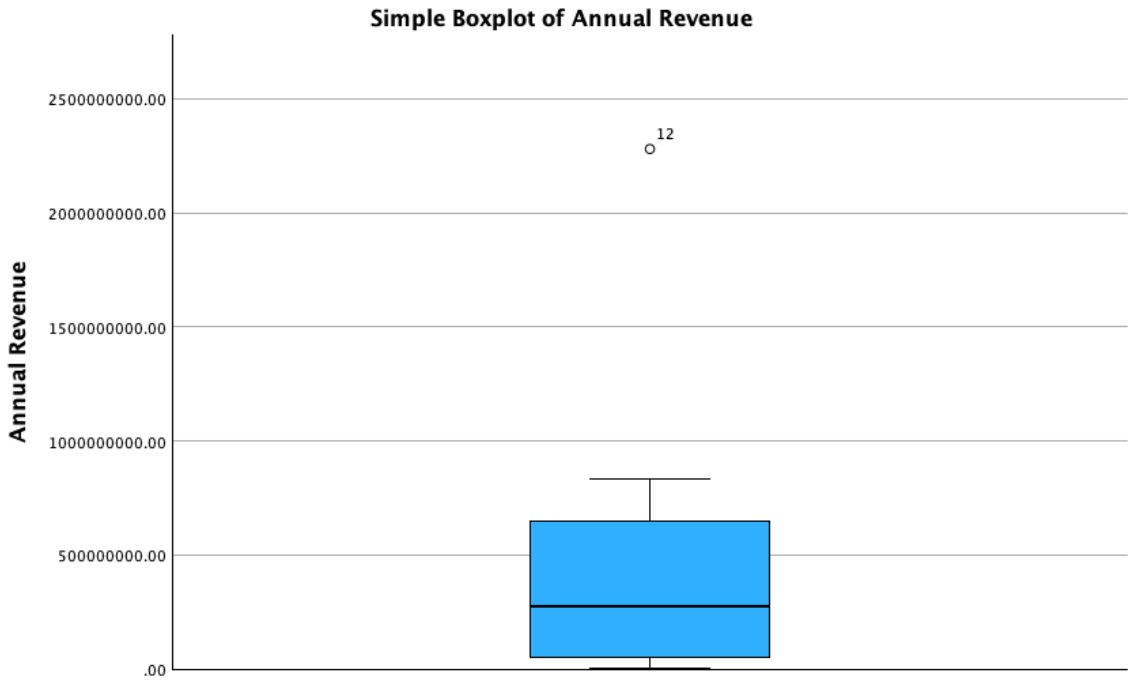
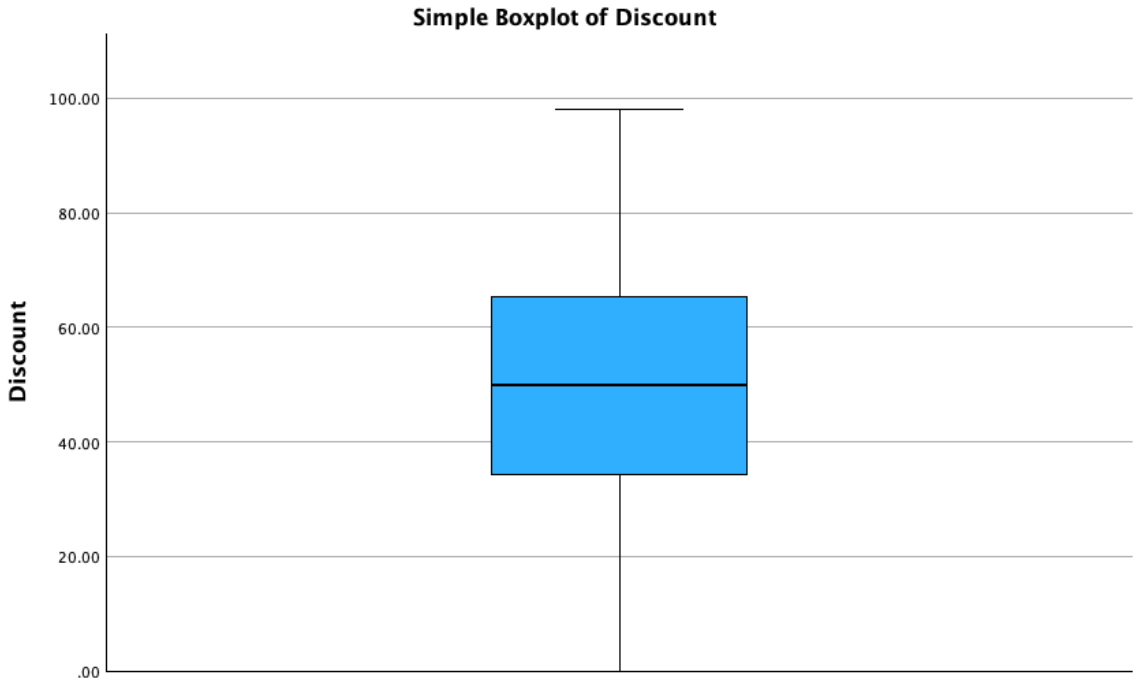


Figure 2
Simple Boxplot of Discount



APPENDIX F: USE OF AI IN EDUCATION AT THE UNIVERSITY OF TWENTE

In crafting this paper, the author utilized AI for enhancing the formal tone of the original text and for addressing coding issues within SPSS. The content, post-utilization of AI, was meticulously reviewed and revised by the author, who assumes complete responsibility for the final work. Moreover, the document underwent a thorough rephrasing for the Green Light version, ensuring the exclusion of any sentences generated by AI. It is important to note that the use of AI tools was not advised by the supervisory team.