Exploring students' perceptions of FUD marketing strategies by cyber security companies

Sofia Vesajoki

Degree Thesis

Degree Programme

2024

Degree Thesis

(Author) Sofia Vesajoki

Exploring students' perceptions to FUD marketing strategies by cyber security companies.
Arcada University of Applied Sciences: International Business, 2024.

Abstract:

This study delves into the intricate intersection between marketing strategies and cybersecurity concerns, aiming to shed light on the effectiveness and implications of Fear, Uncertainty, and Doubt (FUD) marketing tactics employed by cybersecurity companies. Through focus group interviews, this study investigates how students aged 20-25 perceive FUD marketing strategies, navigating through the complexities of their reactions to fear-inducing stimuli. Drawing on existing literature, this study examines previous research on FUD marketing in cybersecurity contexts discerning variations in FUD strategies among different companies. With recent studies suggesting a shift from fear-based marketing towards more constructive approaches, transparency and consumer-centric solutions in cybersecurity marketing are becoming ever more favoured by marketers. Through analysis of visual perception and cognitive processing theories this study provides insights into the students' responses to sensory stimuli and fear appeals. The study acknowledges limitations, including participant biases, language barriers, and the absence of extensive prior research in this specific domain. Nevertheless, the findings suggest a growing scepticism towards unrealistic fear-based marketing tactics, highlighting the importance of authenticity and trust in cybersecurity marketing efforts. Ultimately, this study concludes that the students in this demographic perceive FUD marketing tactics as outdated, which leads to an undeniable lack of trust towards the companies.

Keywords:

FUD, Fear, Uncertainty, Doubt, perception, cyber security, marketing, fear-appeal, trust

Opinnäyte

(Tekijä) Sofia Vesajoki

Exploring students’ perceptions to FUD marketing strategies by cyber security companies.

Yrkeshögskolan Arcada: Kansainvälinen liiketalous, 2024

Tiivistelmä:

Tämä opinnäytetyö tarkastelee markkinointistrategioiden ja kyberturvallisuuden monimutkaista yhteyttä pelolla markkinoinnin näkökulmasta. Syventyen kyberturvayritysten käyttämään Fear, Uncertainty, Doubt (FUD) markkinointitaktiikkaan ja tarkastellen sen tehokkuutta ja vaikutusta kohderyhmään. Hyödyntäen kvalitatiivista tutkimusmatodia, fokus ryhmä haastatteluiden perusteella tutkitaan, kuinka 20-25 vuotiaat opiskelijat käsittävät FUD-markkinointistrategiat, eritellen osallistujien reaktiot palkoa aiheuttaviin ärsykkeisiin. Tarkastellen aiempia tutkimuksia FUD-markkinointiin kyberturvan kontekstissa, tämä tutkimus jäsentää pelkoa-aiheuttavien strategioiden vaihteluita valittujen yritysten välillä. Viimeaikaiset tutkimukset viittaavat siirtymiseen pois pelkoon perustavista markkinointistrategioihin, painottaen rakentavien, läpinäkyvyyttä ja kuluttajakeskeistä asennetta hyödyntävien, lähestymistapojen tärkeyttä. Hyödyntämällä visuaalisen havainnon ja kognitiivisen prosessoinnin teorioita, tämä tutkimus tarjoaa oivalluksia opiskelijoiden reaktioista aistiärsykkeisiin ja pelon vetoomuksiin. Tutkimus tunnistaa potentiaaliset rajoitukset muun muassa osallistujien ennakkoluulot, kielimuurit ja puutteet aikaisemmista alan tutkimuksista. Tulokset viittaavat kuitenkin kasvavaan skeptisyyteen epärealistisista pelkoon perustuvista markkinointistrategioista, korostaen aitouden ja luottamuksen merkitystä kyberturvallisuudessa. Tutkimuksen tuloksena on ymmärrys siitä, että opiskelijat pitävät FUD markkinointistrategioita vanhentuneina, mikä johtaa kiistattomaan luottamuksen puutteeseen kyberturva yrityksiä kohtaan.

Contents

1 INTRODUCTION

In a world greatly swayed by misconceptions and fake news, Fear, Uncertainty, and Doubt (FUD) become a factor influencing a person's everyday life decisions. Through the fear of what-ifs and scenarios fuelled by uncertainty, companies are plausibly able to influence a potential customer's perception and purchase decision (Tharakan, 2019).

When considering FUD, the question of ethics quickly arises. FUD is mainly based on anecdotes (Lai, 2019) negative and fake information that encourage the audience to respond in a certain way. One could even venture to compare this method to blatant manipulation. However, where there is research leading us to believe FUD is unethical, others discover it can be used in a constructive and ethical way, for instance to add healthy pressure on uncertain customers to make their purchase decision (Tharakan, 2019). Nevertheless, the controversy of this simply leads us to the question of how people end up perceiving said strategies.

Although there are a lot of controversies surrounding FUD in marketing communications, they are not always baseless. Statements such as: "Mystery threats lurk unseen—stay vulnerable or choose our shield today!" may play on the idea of a hidden and mysterious threat, but it also reflects the undeniable risks and uncertainties of the cybersecurity landscape.

The overarching idea of this study is to navigate the complex landscape where marketing strategies cut across cybersecurity concerns. With the vision to contribute insights to both domains, this study embarks on a journey to advance the understanding of FUD marketing in cybersecurity contexts providing insights to companies on the effectiveness of their marketing strategies.

1.1 Problem statement

Motivated by the interest in analysing marketing strategies prompted by negative emotion used in the cybersecurity industry, this thesis endeavours to answer the question of how students perceive FUD marketing strategies by cybersecurity companies?

In the light of previous studies, such as Bryan Pfaffenberger's article titled "The rhetoric of dread: Fear, uncertainty, and doubt (FUD) in information technology marketing" (2000), the nature and legality of FUD is examined. Originated by IBM, yet most notably implemented by Microsoft, FUD is exercised in order to acquire and maintain a dominant position in a given field of industry.

While the thesis investigates how FUD marketing is perceived by the demographic, students in this case, it also examines how previous studies have explored FUD marketing in the context of cybersecurity? Furthermore, the thesis seeks to discern variations in FUD strategies among the different companies chosen.

1.2 Aim of the study

The aim of the study is to understand "how students perceive FUD marketing strategies by cybersecurity companies". This is done by investigating how the students, aged 20-25, react to fear, uncertainty, and doubt marketing tactics exercised by cybersecurity companies. Based on the marketing material posted on the companies YouTube channels, students describe their perceptions, influential moments, and emotions that the videos watched provoked.

1.3 Demarcation

Employing desk research and focus group interviews, the study explores the emotional responses to FUD marketing. The research intentionally excludes other marketing strategies in cybersecurity, focusing on a dominant trend of marketing within the field and concentrating solely on this demographic due to the probability of entry into fields of work requiring cybersecurity implementation.

Regarding the chosen demographic, the author has chosen students from various academic backgrounds, placing them in mixed groups to ensure insightful conversations and results.

Recognizing that these students will become future decision-makers, the study seeks to unravel how FUD influences their perceptions, offering valuable insights into potential

long-term effects on their attitudes towards cybersecurity products and services. Additionally, the tech-savvy nature and heightened cybersecurity concerns of this demographic make them a critical group to study. By addressing the gap in research, the study endeavours to contribute both a theoretical and practical understanding, shedding light on the nuanced impacts of FUD marketing on this specific segment.

1.4 Definitions

FUD also known as Fear, Uncertainty, and Doubt is a marketing strategy widely used by cybersecurity companies to convince people to act in a certain way or purchase a certain product. The FUD marketing strategy is based on utilizing fear, uncertainty, and doubt by spreading negative and false information to coax the target to purchase based on the fear this approach causes. This marketing strategy is surprisingly effective since negative emotions work typically as an incentive for action (Bobbert, 2021).

Cybersecurity encompasses the comprehensive security measures designed to safeguard the applications, devices, networks, software, and hardware of both organisations and individuals. The primary objective of cybersecurity is to shield these critical components form various cyber threats such as viruses, worms, and malware. Among the most prevalent cyber threats ransomware stands out as a particularly notorious adversary. In a nutshell, cybersecurity aims to protect, fortify, and research the digital landscape to counteract the evolving cyber threats. (IBM, 2024)

2 THEORY

This chapter expands on the topic of FUD and perception, analysing previous research and introducing theories and methods that can be used in understanding the relationship between fear strategies and perception of recipients. Previous research widely debates the usage of FUD in marketing and theories for and against FUD strategies have been reviewed to build a holistic understanding of FUD in cybersecurity. This chapter finishes by analysing customer behaviour through the fear appeal theory, an extensively studied psychological theory on the persuasive messages that aim to arouse fear (Maddux & Rogers, 1983).

2.1 Previous findings

It was Franklin D. Roosevelt who famously remarked, “The only thing we have to fear is fear itself” (The White House, 2022). Yet Fear, Uncertainty, and Doubt (FUD) have long been recognized as a potent marketing strategy, characterized by its aggressive nature and the potential to sway prospects' perceptions. According to Lai (2019), FUD tactics can manifest in various forms, from subtly insinuating doubts about competitors to directly pressuring prospects into making purchases. As such, Lai (2019) stated that a more sustainable approach to winning over prospects would involve building stronger, long-term relationships, rather than resorting to fear-based tactics.

In the context of competing with rival companies, FUD marketing is often seen as a defensive manoeuvre, aimed to prompt competitors to retreat. To effectively combat these strategies, it is imperative for businesses to not only prepare their customers but also equip their employees with appropriate responses (Lai, 2019). One effective countermeasure is to actively engage satisfied customers, leveraging their positive experiences to counteract the fear and doubt propagated by competitors (Lai, 2019).

Recent research suggests a growing consensus against the use of fear-based marketing, particularly in cybersecurity, where ethical and constructive approaches are increasingly favoured over fraudulent methods such as FUD (Bobbert, 2021).

2.1.1 FUD; A subject of debate

Matias (2023) argues that as cybercrime evolves, FUD strategies are becoming increasingly ineffective in raising awareness about threats. Instead, they offer simplistic solutions that fail to address the complex and evolving nature of cyber threats (Matias, 2023). This leads to a level of oversimplification when considering a problem, which is part of a rather typical human reaction also known as the generalisation instinct (Rosling, p.146, 2011). Moreover, FUD tactics tend to prioritize short-term alignment over long-term solutions, overlooking the nuanced needs of customers (Matias, 2023).

In contrast to fear-based marketing, which seeks to unite customers against a perceived enemy, the emphasis should be on providing personalized solutions tailored to individual needs (Div, 2015). Decisions based on FUD are described as inherently

volatile and often fail to align with customers' values, such as security, user experience, and affordability (Matias, 2023). Ultimately, fostering transparent and healthy relationships with customers and prospects is paramount in order to achieve long-term success in cybersecurity marketing.

Despite a considerable amount of research highlighting the negative implications of fear-based marketing, there are arguments in favour of the effectiveness of FUD. Indeed, sales results prove the undeniable fact that FUD simply works. This demonstrates remarkable persistence and potency of fear-based marketing in driving sales, hence more often than not outperforming the more positive marketing strategies.

2.1.2 The risk of fear-based marketing

In the cybersecurity industry, fear-based marketing becomes particularly prevalent, given its focus on preventing business disruption and financial loss (Peiffer, 2022). However, the effectiveness of FUD yet again varies among recipients. Mann's study (2023) suggests that individuals' responses to fear-based strategies can be categorized into adopters and non-adopters, with the former showing high involvement and adapting to the message, while the latter remain indifferent or disengaged.

Moreover, Pfaffenberger's research (2000) sheds light on how companies utilize FUD to compete for market share, with examples like Microsoft asserting their dominance with the belief that their fair share of the market is total. This underscores the pervasive nature of fear-based strategies in the competitive landscape (Pfaffenberger, 2000).

While FUD may yield short-term gains in sales and decision-making, its long-term effects on brand trust and consumer relationships are subject to debate. Despite its effectiveness, fear-based strategies risk alienating certain segments of the audience and eroding trust over time. Thus, marketers must carefully weigh the benefits and drawbacks of employing FUD in their campaigns, considering the potential impact on brand reputation and consumer perception.

Ultimately, understanding the nuances of fear-based marketing and its effects on consumer behaviour requires a multidisciplinary approach, integrating insights from

psychology, marketing, and communication studies. By examining the varied responses to fear-based messaging and considering the ethical implications, marketers can develop more informed and responsible strategies to engage their audience effectively.

2.2 Countering FUD

Recent research suggests a notable paradigm shift away from fear, uncertainty, and doubt (FUD) strategies in marketing, with an increasing emphasis on constructive and customer-centric approaches (Bobbert, 2021). One such strategy gaining traction is the BAD approach, an acronym for Brave, Assuredness, and Daring, which encourages leaders and employees to confront challenges with courage and confidence (Bobbert, 2021). This approach fosters innovation and resilience within organizations, promoting a proactive stance towards addressing digital security issues, among other challenges.

Fear-based marketing has long been known to elicit exceptionally intense emotional responses, often comparable to positive emotions like happiness and excitement (Fritscher, 2023). This observation prompts a crucial question: could marketing strategies emphasizing positive emotions effectively counter fear-based approaches (Fritscher, 2023)?

Moving beyond fear-based strategies, Kajendran (2017) introduces the 4R's of cybersecurity: reality, response, resilience, and rehearse. This comprehensive framework advocates for acknowledging the inevitability of cyber threats, preparing robust responses, building organizational resilience, and continuously rehearsing and educating stakeholders to mitigate risks (Kajendran, 2017). Additionally, Tharakan (2019) offers a set of practical tactics aimed at alleviating FUD, including guarantees, education initiatives, trial periods, authoritative endorsements, client testimonials, behind-the-scenes access, and detailed product demonstrations (Zarate, 2024).

Ethical concerns surrounding fear-based marketing in cybersecurity are raised by Thomas (2023), addresses trust-building through education and empowerment of consumers. Thomas argues that while fear-based tactics may initially drive sales, they can erode trust and credibility in the long run (Thomas, 2023). This sentiment underscores the growing consensus within the marketing community on the importance

of ethical practices and transparent communication in fostering enduring customer relationships.

In addition to ethical considerations, Funk (2020) proposes alternative marketing strategies such as content marketing and search engine optimization (SEO), highlighting the significance of credibility and education in attracting and retaining prospects. By providing valuable content and educational resources, companies can establish themselves as trusted authorities in their respective industries, thereby mitigating the need for fear-based tactics to drive sales.

In navigating competitive challenges, it is critical for businesses to anticipate and counter FUD tactics effectively. This entails redirecting focus to strong selling points, providing evidence to refute claims, and pre-emptively showcasing organizational strengths (Zarate, 2024). As the marketing landscape continues to evolve, embracing customer-centric approaches and ethical standards will be crucial for long-term success and sustainability.

2.3 Perception and interpretation

Gibson (1966) introduces a theory proposing that perception directly reflects the information provided by the environment, without necessarily relying on past knowledge (Study Smarter, 2024). This theory emphasizes a bottom-up process of perception, where sensory information drives the interpretation of the environment, independent of prior experiences or interpretations. In contrast, the top-down theory argues that perception is heavily influenced by past experiences and expectations (Study Smarter, 2024).

Gregory (2005) introduces the constructivist theory of perception, which posits that sensation alone provides ambiguous and incomplete information about the environment, necessitating interpretation to construct a mental image (Study Smarter, 2024). This perspective suggests that perception is an active process, wherein individuals actively construct their understanding of the world based on sensory inputs and cognitive processes.

Krishna's study (2012) delves into sensory marketing, revealing how sensory cues shape consumers' emotions and thoughts about products or services. Sensory marketing can tap into subconscious triggers, creating associations and characteristics in consumers' minds, influencing their perceptions, and buying decisions (Krishna, 2012).

Understanding the impact of sensory cues on consumer behaviour is crucial for marketers, as it allows them to strategically use visual, auditory, olfactory, gustatory, and tactile stimuli to evoke desired responses.

Solomon (2019) emphasizes the significance of visual perception in consumer behaviour, particularly the influence of colours on emotions and associations. Colours can evoke specific emotions and associations, varying across cultures and contexts, impacting consumer responses and brand perceptions (Lange, 2023, & Solomon, 2019). For example, the colour red is often associated with excitement and passion, while blue is associated with trust and reliability. Marketers leverage these colour associations to evoke desired emotions and perceptions in consumers, influencing their purchasing decisions.

Table 3.1 Marketing applications of colours

Colour	Associations	Marketing applications
Yellow	Optimistic and youthful	Used to grab window shoppers' attention
Red	Energy	Often seen in clearance sales
Blue	Trust and security	Banks
Green	Wealth	Used to create relaxation in stores
Orange	Aggressive	Call to action: subscribe, buy or sell
Black	Powerful and sleek	Luxury products
Purple	Soothing	Beauty or anti-ageing products

Source: Adapted from Leo Widrich, 'Why Is Facebook Blue? The Science Behind Colors in Marketing', *Fast Company* (6 May 2013), http://www.fastcompany.com/3009317/why-is-facebook-blue-the-science-behind-colours-in-marketing?partner=newsletter (accessed 23 August 2018).

Figure 1 Marketing applications of colours (Solomon, p.90, 2019)

In a study by Rathee and Rajain (2019), colours were found to play a crucial role in influencing consumer behaviour and differentiating companies from their competitors. Colour choices in branding and marketing efforts can evoke specific emotions and

perceptions, contributing to brand identity and market positioning. For instance, fast-food chains often use red and yellow in their branding to evoke feelings of energy and urgency, while luxury brands may use black and gold to convey sophistication and exclusivity.

Understanding consumer perceptions of colour associations requires consideration of cultural and demographic factors (Rathee &Rajain, 2019). However, such perceptions remain largely hypothetical, given the subjective nature of individual interpretations (StudySmarter, 2024). Cultural differences in colour symbolism can lead to contrasting interpretations of colours across different regions and demographics, highlighting the importance of cultural sensitivity in marketing strategies.

Preity (2016) highlights the constant bombardment of stimuli our brains receive from the environment, with only a fraction consciously processed due to attentional limitations. Interpretation of sensory stimuli varies among individuals, influenced by personal meanings and associations (Solomon, 2019). Therefore, marketers must consider the subjective nature of perception when designing marketing campaigns, tailoring messages, and visuals to resonate with their target audience's unique perceptions and preferences.

In conclusion, perception is a complex process influenced by various factors, including sensory inputs, past experiences, cultural norms, and individual interpretations. Marketers can leverage insights from perceptual theories and sensory marketing research to create impactful marketing campaigns that resonate with consumers on a subconscious level. By understanding how sensory cues shape consumer perceptions and behaviours, marketers can effectively differentiate their brands, evoke desired emotions, and ultimately drive purchase decisions.

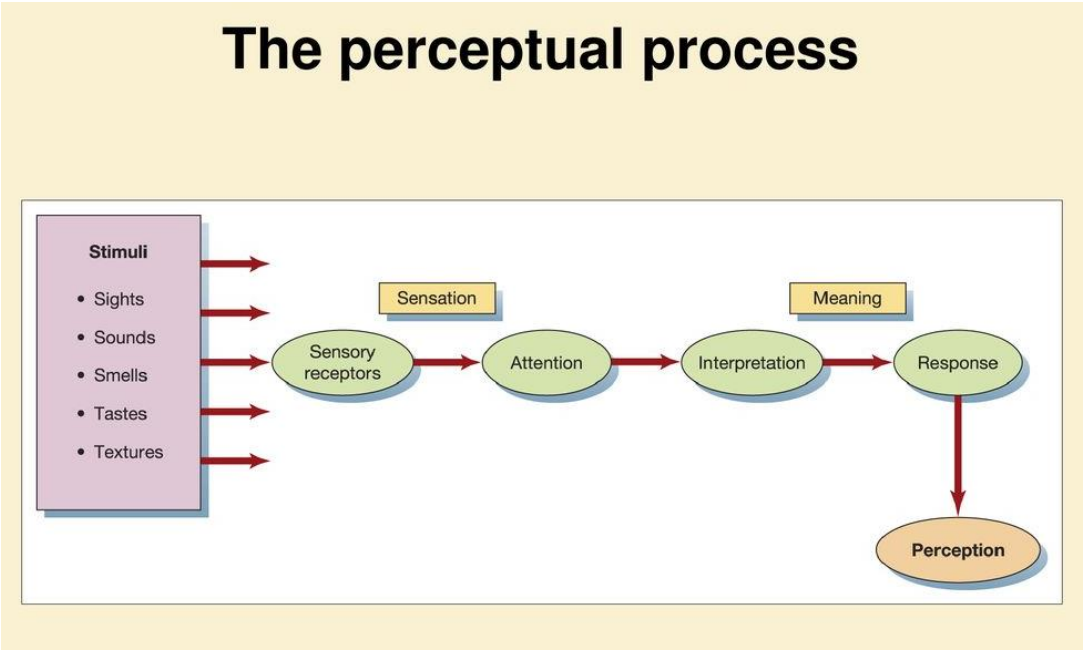

Figure 2 An overview of the perceptual process, Solomon (p.86, 2019)

2.4 The fear appeals theory

The fear appeals theory, as explained by Sreenivasan and Weinberger (2018), revolves around persuading individuals by highlighting the potential harm they may face if they refrain from purchasing a specific product or service. This theory comprises three main components: the message, the audience, and the recommended behaviour. The message aims to instil sufficient fear to prompt the recipient to take the desired action, offering instructions on how to mitigate the perceived risk. However, striking the right balance is crucial in fear appeals; excessive fear may lead to avoidance rather than action, especially in cybersecurity marketing where recipients may lack the expertise to gauge the severity of the threat, resulting in fear of the unknown.

Fear appeals tap into strong emotional connections, as indicated by Tannenbaum et al. (2015), who found positive effects on attitudes, intentions, and behaviours, particularly when accompanied by efficiency statements or calls to action. However, fear arousal, as highlighted by Ruiter et al. (2014), may trigger defensive reactions such as risk denial and biased information processing, influencing how individuals attend to messages. Fear arousal creates an unpleasant emotional state in response to perceived threats, underscoring the role of perception in human reactions to stimuli.

The theory posits two types of information: presenting a severe threat to which the recipient is susceptible and illustrating a neutralizable or avoidable threat with certain actions (Ruiter et al., 2014). Both approaches aim to evoke strong emotions and persuade recipients to favour the initiator's choice. While fear appeals are widely employed across various domains, including cybersecurity, ethical concerns arise regarding their use to motivate action (Dupuis & Renaud, 2020).

In cybersecurity, fear appeals are seen as necessary by marketers despite being disliked by recipients, as noted by Dupuis and Renaud (2020). However, ethical dilemmas emerge concerning the demonization of specific subgroups and the potential for complacency among unaffected individuals. The manipulation and ethicality of fear appeals raise questions about the justification of deception and the responsibility of cybersecurity companies in ensuring the transparency and feasibility of recommended actions.

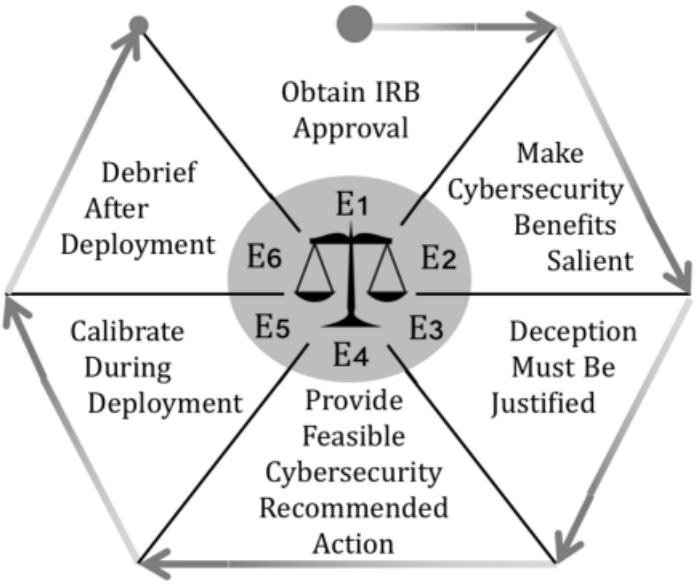

Figure 3 Cybersecurity fear appeal ethical principles for informing their design and deployment by Depuis and Renaud (p.277, 2020)

To navigate these ethical concerns, Dupuis and Renaud (2020) propose several guidelines for cybersecurity companies, including obtaining approval, justifying deception, providing feasible recommendations, and making cybersecurity benefits

clear. Calibration during deployment and debriefing at the conclusion of experiments are also essential to ensure the ethicality and effectiveness of fear appeals tactics.

3 METHOD

Research methodology can be divided into two: qualitative and quantitative. While the author decided on the former method for this study the latter was discarded due to the mathematical approach which does not cover the necessary bases of a study focused on perceptions. Quantitative research would fail to provide data deep enough to understand the intricate scenes playing out in a person's mind.

Qualitative methodology revolves around gathering and analysing non-numerical data and identifying patterns within. This data can be in the form of audio, video, photo, or text, which focuses primarily on the participants beliefs and responses. Qualitative data is particularly useful when a company wants to understand a customer's or target group's feelings around a service or product (Girardin, 2023). Qualitative research aims to understand concepts, experiences, and opinions and it is used to gather in-depth insights into a problem, sufficiently generating new ideas for research (Bhandari, 2020). In the light of this the author has decided upon this approach for its good fit in understanding and gathering the necessary data.

Nevertheless, like any method qualitative research has its limitations which widely revolve around the different bias and unreliability in uncontrolled factors that an author may stumble upon (Bhandari, 2020).

Qualitative research has been a valuable tool for exploring complex phenomena and uncovering insights within. Qualitative research allows this study to dive deeper into the nature and nuances of fear and how it can be perceived. Through the recipients' personal narrative, the author is able to understand to an extent which audio-visual aspects generate emotional responses in the participants. In conclusion, qualitative meets the requirements for the aim of this study by pinpointing patterns and themes of emotional responses in the recipients to uncover the overall perception that is then formed in the minds of the recipients that can in turn influence responses and actions.

3.1 Focus group interviews

Qualitative methodology has different approaches that can be used to generate data. For this study, the author has decided upon interviews to gather as much insight as possible into the recipients' thought processes. Interviews generate large amounts of data through their typically open-ended questions that serve well in explaining thoughts, actions, and responses.

Interviews can be roughly divided into three categories: structured, semi-structured, and un-structured. While structured interviews prove to be too rigid for discussing personal experiences and un-structured undoubtably make it easy to stray from the root of the questions, the author decided upon a semi-structured interview, which aims to create a relaxed setting where discussions can thrive.

A semi-structured interview is commonly used, providing a thematic approach with a flexible structure that encourages participants to elaborate on their perceptions and ideas while allowing them to express themselves freely (Barclay, 2018). The perks of semi-structured interviews have allowed the author to create a loose framework for the questions making sure the sequence is logical yet flexible and leads in the desired direction without dominating the flow of conversation and allowing greater reflection to discover the underlying responses.

Narrowing down the field of interviews the author has decided upon focus group interviews which are most commonly used when conducting semi-structured interviews. The decision to utilise focus group interviews for this research stems from its alignment with the research question and is supported by existing literature focusing on reactions, emotions, and perceptions. At the heart of focus group interviews lies the need to answer questions of "why" and "how" (Bhat, 2023). Generally held in groups of four or five participants in the target group, focus group interviews generate rich discussion bolstered by the comments of each participant.

For this study the focus group interviews are relevant due to the level of deep inquiry they generate. Primarily focus group interviews conducted this study combine participants of various backgrounds to create parallels and possible confrontations of opinions (Krueger,

2002). The explorative nature of focus group interviews allows the participants to build a holistic understanding of their responses to fear-based marketing, and while discussing them, pinpoint and verbalize their own perceptions bolstered by comments shared in the focus group.

The focus groups allow a natural dynamic between participants to form giving them a chance to reflect on what they have seen and experienced, highlighting aspects that can generate further analysis on the subject within the group. Moreover, this type of interview generates rich qualitative data in the form of observations, notes, transcripts, and recordings (Bhat, 2023).

3.2 Respondents

The selection of respondents for this study was carefully considered to provide valuable insights into the future consumer base of cybersecurity solutions. By focusing on current students, who will eventually become the target audience for these solutions, the study aims to understand their attitudes and behaviours towards FUD marketing tactics. Uncovering these perceptions lends this study a futuristic approach while still adding depth to the research by examining the reactions of individuals with varying levels of exposure to the cybersecurity domain.

The selection criteria included diversity in recipient backgrounds to ensure a varied perspective on FUD marketing tactics. Students with different levels of familiarity with cybersecurity concepts offer a range of insights, enriching the analysis and interpretation of the data.

In the table below the respondents of each focus group are represented, dividing them based on gender, age, and nationality.

Table 1 Focus groups from 1 to 4

Focus group 1	**Gender**	**Age**	**Nationality**
Person 1	Female	20	Finnish
Person 2	Female	23	Finnish

Person 3	Female	22	Finnish

Focus group 2	**Gender**	**Age**	**Nationality**
Person 3	Female	23	Finnish
Person 4	Female	23	Finnish
Person 5	Female	23	Finnish
Person 6	Female	23	Finnish
Person 7	Female	23	Finnish

Focus group 3	**Gender**	**Age**	**Nationality**
Person 8	Female	21	Russian
Person 9	Female	22	Finnish
Person 10	Female	20	Vietnamese
Person 11	Female	20	Vietnamese

Focus group 4	**Gender**	**Age**	**Nationality**
Person 12	Female	25	British
Person 13	Female	24	British
Person 14	Female	24	British
Person 15	Male	25	British
Person 16	Female	21	Finnish

3.3 Interview guide

The questions for the focus group interviews were designed around the aim of understanding perceptions through study of emotions. Aiming to pinpoint the most prevalent emotions the videos raise in the participants at the very beginning of the interview. The interview then circles through underlying senses, trust, and influence to return to the study of emotions. This type of approach proves to generate relevant discussion that works towards the recipients better understanding the underlying emotions that might not have been identifiable at the beginning of the interview.

The questions lean heavily on the study of perceptions, touching upon aspects such as colours, tones, and expressions that the videos aim to highlight. Guiding the recipients to identify influential or striking aspects in the videos and describe the feeling they created. Like many marketing videos, all chosen videos strive to elicit action of some sort. Noting this, some of the questions in the interview bring up the appeal of action through discussing the sense of urgency or action, reflecting back to the study on how fear appeals.

By structuring the questions into open-ended ones and providing prompts, the discussion is kept on subject, allowing participants to articulate their perceptions with greater ease and accuracy. (see appendix 2)

3.3.1 Video description

The selected videos are sourced from three prominent companies operating in the Finnish cybersecurity market, hereafter referred to as company Torrent, Tide, and Wave. While one of these companies is Finnish based, the other two have headquarters abroad but maintain a significant presence in Finland. This deliberate selection allows for a nuanced examination of each company's marketing strategies and the subtle incorporation of Fear, Uncertainty, and Doubt (FUD) tactics in their videos.

To start off the interviews, there is a short, humorous advertisement from company Torrent for their Point Gen V service called “Without the Best Security, Bad Things Happen” (2019). While the video does not employ dark or brooding colours, it effectively conveys panic when a virus is detected on the protagonist's computer. The spreading of the virus to other computers, coupled with a countdown indicating impending damage, heightens the urgency of the situation. This video is strategically positioned first to assess how well participants perceive fear tactics disguised in a friendly manner (see appendix 3).

The second video, "The Hacker," (2023) crafted by company Tide, presents a hacker's perspective, depicting hackers as formidable and capable of infiltrating systems undetected. Despite featuring predominantly light and inviting colours, the video instils a sense of unease, suggesting that hackers could be anyone. This portrayal evokes a

level of paranoia, which some argue is beneficial in promoting a Zero Trust security approach in cybersecurity (see appendix 3).

The final video, courtesy of Wave, adopts a more informative approach than its predecessors. The video titled “Live Security” (2019) employs darker tones and provides an overview of the threat landscape, highlighting the challenges of safeguarding company data from cyber threats. Key terms such as 'breach' and 'devastating' underscore the severity of potential attacks, eliciting a sense of despair. The advertisement concludes optimistically, presenting a futuristic solution exclusive to the company, bolstered by “*award-winning technologies*” and “*seasoned consultants*” (see appendix 3).

The variation in content and FUD subtlety across the chosen videos offers a rich dataset for analysis, facilitating a comprehensive exploration of how fear, uncertainty, and doubt are utilised in cybersecurity marketing. Each video presents unique perspectives and messaging strategies, enabling a deeper understanding of their impact on viewers' perceptions and emotions.

3.4 Research approach

Before the interview commences, the interviewer must obtain informed consent from the participants via an online form. The consent form begins with the participant explicitly consenting to being recorded, with the understanding that the recording will be transcribed later. Additionally, the consent form provides a brief overview of the interview content and a summary of the research objectives and questions. Only after the interviewee comprehends and provides consent can the interview proceed.

The focus group interviews span over a week, the first focus group taking place on March 14th and the last one concluding on Sunday, March 24th. Sessions are primarily scheduled in the evenings, starting at 19:00, with an anticipated duration of 30 minutes. An exception is made for Sunday, March 17th, and March 24th with the focus group interviews set for 15:00 for the former and at 17.00 for the latter.

Convenience and accessibility heavily influenced the decision to conduct the interviews online via Microsoft Teams. Participants, potentially residing in diverse locations, benefit from the elimination of commuting constraints, likely enhancing participation rates, and reducing dropouts, thus ensuring higher data quality. Additionally, the flexibility afforded by Microsoft Teams, including features like screen and document sharing, real-time chat, and transcription capabilities, enhances the seamless execution of interviews.

Online interviews provide a level of anonymity and comfort that encourages participants to express their opinions and emotions candidly. This anonymity extends to the reporting stage, with participant identities withheld in results, discussions, and conclusions. This fosters honest responses and deeper insights into students' perceptions of FUD marketing strategies.

Efficiency is another advantage of online focus group interviews, as researchers can simultaneously gather data from multiple participants, maximising productivity. This enables the collection of a larger volume of data within a shorter timeframe, facilitating comprehensive analysis of the phenomenon.

Moreover, Microsoft Teams' recording functionality enables the capture of discussions for later review, ensuring the retention of nuanced insights that may have been overlooked during the live session. This feature contributes to accurate data collection and analysis, enhancing the overall quality of the research.

3.5 Analysis of the data

Qualitative data analysis typically follows a five-step framework: organizing and preparing the data, reviewing and exploring the data, developing a data coding system, assigning codes to the data, and identifying recurring themes. The qualitative data analysis can be addressed through several more specific approaches such as content analysis, thematic analysis, textual analysis, or narrative analysis. In this study the relevant findings can best be analysed through thematic analysis (Bhandari, 2020).

The data has been gathered in two ways. Through desktop research, data regarding previous studies has been gathered and summarized. The data used in the focus group

interviews, the videos, have been carefully picked from previously decided companies YouTube pages. The criteria for them being that they must portray FUD tactics to a certain level.

The data generated through the focus group interviews varies in analysability due to the language the interview has taken place in. For English language interviews the recordings and transcripts have been automatically generated, the Finnish interviews have been recorded and based on the recordings transcribed by hand to spot the patterns with greater ease.

The data analysis process is based on manually going through the transcripts, recordings, and notes taken during the focus group interviews. Implementing thematic analysis allows the identification of patterns and reoccurring themes between the interviews (Crosley, 2021). These patterns will be divided into categories based on the theory that has been gathered earlier in the study. The idea behind identifying subcategories is the act of combining and separating them when it is beneficial for the study while comparing them between each other. These findings will then be summarized into a cohesive whole for conclusions to be drawn based on them.

Thematic analysis involves identifying, analysing, and interpreting patterns or themes within qualitative data (Crosley, 2021). Given that this research aims to understand how students perceive FUD marketing tactics, thematic analysis allows systematic identification of recurring themes or patterns in their responses. Through the categorizing process, conclusions can be drawn on similar emotional responses and interpretations. In conclusion, thematic analysis provides a flexible approach that accommodates the diverse range of perspectives enabling various pairings between subcategories resulting in an organized and multidimensional conclusion (Crosley, 2021).

3.6 Validity and reliability

Validity and reliability are used to evaluate the rigor of research designs and methods. While validity pertains to the accuracy and meaningfulness of research findings reliability connects to their consistency and stability.

Validity refers to the degree to which the study accurately measures what it is intended to measure. Validity assesses whether the research method is in fact capturing the phenomenon under scrutiny. Validity is crucial in order to ensure that the observed effects are due to the research questions being studied and not the confounding variables (Heath, 2023).

In this study validity has been addressed in designing the interview questions, ensuring that the questions align with the overall research goal. The qualitative method chosen for this research also validates this study due to the undeniable compatibility between theory and method.

Reliability stands for the consistency, stability, and repeatability of research findings. It portrays the extent to which the same results could be obtained if they were to be replicated under similar or the same conditions (Middleton, 2023). Reliability is essential for ensuring that research is dependable and trustworthy. Reliability can be divided into several different categories such as test-retest reliability, inter-rater reliability, and internal consistency reliability.

The study conducted is reliable due to the information given on the participants. By addressing the background, age, and gender of the participants, as well as disclosing the number of participants for each focus group and the number of focus groups the study is reliable to the extent that should one want to replicate the study with a similar group of participants the results will be aligned.

To warrant as much validity and reliability as possible, this study uses triangulation, which indicates that the data has been gathered from multiple sources, in this case the three different focus groups. The data has been gathered by standardized procedures, comparing it to previous findings and searching through various research to ensure that there is sufficient unanimity in the results.

3.7 Ethics

To safeguard the ethics in this research, all recipients and their answers have been kept anonymous. Furthermore, the names of the companies have been changed to pseudonyms.

The participants for the focus group interviews filled an online consent form before attendance. The consent form, following the official guidelines, made sure the interviewees had an understanding on the proceedings of the interview, their explicit consent to be recorded and the recordings used for transcription.

4 RESULTS

Following the five-step framework of thematic analysis, the recordings and transcripts generated in the focus groups were carefully reviewed so that patterns and themes became identifiable. These patterns have been placed in categories and subcategories in order to cohesively understand and analyse the results this study yielded.

While the questions did not ask respondents to rank based on fear, uncertainty, or doubt many recipients found that to be an easy way to compartmentalize their perceptions, which led to easily identifiable patterns between groups. The videos that generated the more fruitful discussions were the second “The Hacker” and the third “Live Security”.

The majority of the recipients roughly ranked the videos from least to most fear-generating, ranking them as follows: video 1, video 2, video 3. Participants who ranked the videos as such were concordant in their trust and emotions regarding the videos. Focus group 3, which had the majority of participants from outside Europe, stood out with the greatest number of different opinions. Focus group 3 considered video 2 as the most influential.

In short, the patterns and themes were clearly recognizable, especially through key words the participants used to describe them. Table 2, below, portrays the adjectives most commonly used to describe the videos based on the transcripts and recordings of each focus group. These exact adjectives have been used in every focus group.

Table 2 Videos described in a couple of adjectives.

Video 1, Torrent	Funny	Humorous	Out-dated	Oversimplified

Video 2, Tide	Charismatic	Funny	Laid-back	Exciting
Video 3, Wave	Severe	Convincing	Boring	Info-dumping

In light of previous experiences and knowledge on the matter, the top-down theory (Study Smarter, 2024) applies for this study. All responses were heavily coloured by the participants past experiences or expectations. The focus group participants fell into two categories based on previous experience, one group, group 3, which had no previous understanding of cybersecurity whatsoever, and a second group, group 4, that was surprisingly well acquainted with cybersecurity. Another notable factor in the top-down theory became apparent during the interviews when respondents admitted to having prejudice towards cybersecurity due to its perceived boring nature.

> "*Well, I could say, Wave, the third one, has of course like, been around for a long time and has a big reputation. The second one was Tide, haven't heard as much of them, but they are big in the IT industry. And the first one I don't even remember what it was. I just remember tacos*." (Person 16)

4.1 Perception

Centring on perception, the focus groups gave good analysis on how various elements presented in the videos stood out and why.

A common theme that arose in the interviews was the general bombardment of stimuli. Because the focus groups began by watching the three short advertisement videos, it quickly became evident that the messages of the videos blended together. As Preity (2016) explains the human brain is constantly receiving a plethora of information out of which only a fraction is processed in the conscious mind. In the light of this, the author chose to approach the questions in a manner that would circulate back to the start while pinpointing emotions and moments that stood out.

Within the matter of a sensory overload the third video stood out more than rest. Many participants complained on the length of the video as well as the information overflow

that was presented in it. More often than not the video went over their head and was overall difficult to understand. Here the participants with previous cybersecurity knowledge truly stood out due to their understanding on the basics and through that focus on the minor details that the third video brough forth.

Through the discussion around perceptions, many participants found it easy to identify the techniques the videos used to generate fear, uncertainty, and doubt. Stating some aspects as clearly manipulative, led to two distinct approaches: denial of the fear factor and appeal. Considering the denial, it was clear some students did not react emotionally to the videos, denying the fear factor by cold logic of "that is not how cybersecurity or -attacks work." The recipients who were attracted to the fear ranked the scariest video as the best video justifying their choices by perceived professionality and influence.

In short, a recipient can either act or neutralize themselves against the fear appeals. Out of the two the latter was more common in the focus groups, where many participants did not have a keen sense of action. Many did, however, ponder upon their lack of knowledge that then spiralled into so to say self-inflicted fear. Other notable situations where when someone was particularly aware of the threats and could bring that to the next level, for example in AI posed threats.

Through study of perceptions, subcategories within became evident. Dividing the subcategories into roughly two: colour and audio, the recipients' perceptions became analysable from a more profound vantage point.

4.1.1 Colour and audio

In the book Consumer Behaviour (Solomon, 2019) the significance of visual perception is studied in detail, using respondents from around the world. It is stated that colours can evoke specific emotions and as such contribute to the brand identity and market positioning. While marketers are well aware of the significance colour plays in associations, there is of course no guarantee a certain colour elicits the same response in all customers. Studying colour in visual perceptions solidified this as answers widely varied.

> "*You know, gets the cybersecurity, you know, mindset in dark colours and blue. Very hacker. But it wasn't green. But blue is good enough, you know. Really, I remember blue. Also, it was darkness, and that is very cyber of them."* (Person 16)

Within perceptions the subcategory of colour and audio was easily identifiable. Variation between subconscious and conscious attention to colour and audio was clearly seen, as some of the students never mentioned either colour or audio, even when other students in their group were discussing them. The students who highlighted aspects such as colour and audio were remarkably unanimous in their assessments.

The first video was widely defined as chipper and colourful due to the multiple vibrant colours that popped up. This was observed as non-threatening and child-like.

Reflection on the filming style of the first video was also brought to attention, stating that it was the only video where there was monologue without breaking the fourth wall. However, none of the participants noted this aspect as relevant and rather paid attention to the warning sirens that accompanied the video. While noticeable, the sound of the alarm and sirens did not come across as influential, and recipients tended to have a neutral response to it. In short, many mentioned it as a failed technique of creating urgency and fear.

> *"I noticed this when there were more colours, especially bright colours and made it seem like it's child's play."* (Person 7)

In the second video, participants highlighted the blue colour theme that was prominent throughout the video. This was often mentioned in association to the colour of the company logo. While it cannot be directly related to a sense of trust that blue colour typically creates, the second video was still found rather trustworthy by roughly half (9) of the participants.

Many participants (11) also paid a lot of attention to the audio of the second video noting how the chipper tunes took away from the fear aspect that the video was still

trying to uphold. This fact also helped in keeping the attention of the participants on the video and making it a more pleasing experience as a whole.

> "*The second one had a very fast tempo with a lot of different aspects that drew the attention of the viewer, a lot of audio and sound effects for instance the rushing sound when the scene changed."* (Person 1)

> "*The second video had upbeat tunes that kept the focus better and made the watcher more alert."* (Person 9)

The responses regarding the third video all had a similar tone. Yet again participants noted the huge sift in filming style and colour since it stood out as the most severe video from the three. According to recipient analysis, the style of the video suggested the matter addressed in it as serious, and the assertion was supported by visual and audio inputs. This resulted in many of the participants reported this video as the most fear inducing out of all three.

> *"I have a feeling that the colours black, white, and red affected on how seriously the video or advertisement should be taken."* (Person 7)

The analysis on colour in the video was brought up by person 15, who explained how the colour red is almost universally considered the colour of danger, backing this statement up by the basic human psychological response to colour stimuli. This accompanied by the audio and the narrator explaining how a person could be already compromised due to an attack, was considered as a clear fear factor that in some recipients induced fear and others built a sense of urgency.

> "*Video 3 had a scary audio."* (Person 8)

4.2 Moments and emotions

In order to better understand the emotions, the videos created in the participants, some of the questions revolved around pinpointing moments that stood out within the videos.

These influential moments varied between participants and were driven by various emotions and feelings.

> "*The first two were quite theatrical… Clearly also manipulative in the sense that you are forced to think that you need the services the companies are providing."* (Person 3)

Many participants also noticed the warning noise in the first video as a moment that stood out to them. Aside from this, it quickly became apparent that the video was viewed as old fashioned, dated, and oversimplified, which resulted in the inability to take the video seriously. The majority of the participants were sufficiently well aware of cybersecurity threats, easily categorising the first video into something unrealistic.

While no one outright contradicted this, it was noted by Person 2 that there are all kinds of funny little ways a person might end up being hacked.

> "*The underlying feeling that, yeah, you actually should worry about your security was there."* (Person 2)

As an overview, the first video received a very positive emotional response by everyone stating how humorous or funny it was. While urgency was a feature highlighted in the video and noted by many participants (13) the wry nature of the advertisement led to a single-minded conclusion not to take it seriously. The recipients stated that it also made the company look ill prepared through the lack of explanation, professionalism, and a slapstick attitude to a more complex and severe issue.

For the second video there were a couple of things participants noted as memorable moments, associated with a pinpointable emotion. Here three main aspects were recognized: appeal of the antagonist, walking through walls, and audio.

The first factor is the actor chosen for the role of the hacker had a very pleasant outward appearance instead of looking like a villain. Some (3) noted how that little factor played well into the thought of how hackers could be anywhere and anyone.

> "*I noticed that in the second video they had chosen a charismatic and generically handsome man as the protagonist."* (Person 5)

The second noticeable factor from "The Hacker" (2019) video were the scenes where the hacker was shown walking straight through walls, which most viewers described as unsettling. The fact that he was able to get anywhere created a sense of disturbance in many of the participants. Emotions such as paranoia, uncertainty, and annoyance were brought up. Some participants (5) noted how the protagonist of the video seemed unstoppable, resulting in a lack of control. When asked to elaborate the participants explained how a situation as indicated in the video could quickly spiral out of control even through one's best efforts to prevent it.

> "*It was just like when is this going to end? I don't want to see this man no more. Like that? That's how it seemed to me. It was kind of like stalker going in and especially about him looking at into the camera most of the time and just smiling, like this is normal, just everyday stuff…"* (Person 14)

The third factor, as already addressed above, was the soundtrack for the video. With an upbeat and pleasant tune, the video created a sense of false security that typically took away from the sense of fear and uncertainty, participants concluded.

> "*And I think the second they mentioned something about stay connected and to stay safe. Like if I'm not connected with the Internet, am I in trouble then? Yeah, I suppose so."* (Person 12)

A couple of participants also mentioned places the hacker went. While not necessarily due to previous knowledge person 7 pointed out the scene where the hacker was pictured in a hospital looking at patient information.

Aside from the hospital scene, participant 15 noted how the hacker was filmed taking a picture of confidential business plans in a conference room.

> "*In the second one, when he was in the boardroom and took a selfie with graphs and charts that were on the screen… That is the biggest way someone can*

accidentally compromise a company… Taking pictures and not paying attention to what is in the background of it." (Person 15)

The third video provided all participants with a clear focus: the skull. Out of the participants who were drawn to the skull a couple stated that the skull added to the sense of fear or disturbance. The skull was also described as having a weird and scared appearance. As stated above many (13) found this video more distressing than the earlier ones. Participants mentioned that the colours, audio, and visual expressions all indicated that this video was very serious.

"*I remember a whole the brain and the skull and the head of the person and all the digital stuff around it. Yeah. Professionalism, seriousness."* (Person 12)

While the information provided in the video was too much for some of the participants, others saw that as a sign that the company had actually done a lot of research on the matter and knew what they were talking about. Influenced by grand words such as "seasoned specialists" the moments that stood out for the participants created a sense of fear and uncertainty, in some, and highlighting the professionalism of the company in others. The more sceptical participant, person 3, concluded that the use of words such as "seasoned" came off as impudent, discriminating against those viewers that do not know enough about the subject to understand the terms used.

4.3 Trust

While the main focus in the interviews was on the emotions, perceptions and feelings, the matter of trust naturally arose. The focus group interviews concluded with seeing if the tactics used in the advertisement videos gained the trust of the students when it came to the company's knowledge of cyber threats as well as the capabilities to mitigate these threats they portrayed in the videos.

Discussing trust led to fluctuating results that were heavily influenced by the earlier aspects of colour theory, influential moments, and emotions. Few of the students stated that a deep level of trust was established and that while they might not have the required knowledge to make an educated argument to why it was justified with the lack of

information given in some of the videos and the frankly unprofessional way, especially the first company, delivered their video.

> *"From the first two videos I got the feeling that they don't even have anything trustworthy and good to offer."* (Person 6)

Through discussing the lack of trust, participants reminisced to the fact that all the videos fell short of actually explaining what they are doing to alleviate the cyberthreats.

> "*The first two how to sense that they can protect you and your technology to a certain point but not further."* (Person 2)

Others concluding that there would be no way they would trust the first company with their security. In conclusion, the first video and the company behind it succeeded in creating a wide 'no trust' reaction in recipients.

Reflecting on the second and the third video, levels of trust were generally higher. Participants noted how the videos were shot in a clear and professional way the companies already establish a level of trust through showing that they know what they are doing. Colour played a role in this as well, with the blue being a rememberable and soothing colour in the second video.

> *"I think the second one builds like a stronger sense of trust between the like potential consumer and the company."* (Person 9)

Concordantly all the participants agreed that the third video generated the most overall trust. While some (2) based on previous knowledge of the company, others (6) stated that although the overly informative nature of the video they clearly know what they are doing and are even ahead in the game by applying machine and AI aspects.

> "*The third created a trust in their capabilities*." (Person 10)

> *"I think the reason I trust the third one the most is because they lay it out and they speak more professionally. They also show what they do, the steps, whereas in the*

other two, they're like "we stopped it, done! You don't need to know how we do it or who's working on it..." (Person 13)

Interestingly a participant, person 3, stood out stating that they had no trust in any of the companies, the reasoning behind this statement was highly motivated by the understanding of manipulation tactics which could be seen in each video and the way all the companies delivered their advertisements did not convince them. This participant believed that none of the companies would be a viable solution when regarding cybersecurity.

5 DISCUSSION

This discussion chapter addresses and analyses the various patterns and themes that were brought up in the results chapter. Confiding in the models referred to in the theory chapter, the results have been discussed through critical analysis of the method.

5.1 Bias in perception

A viable issue for this study is the existence of biases. Participants may have had previous knowledge on the companies that were introduced in the videos and based on that they may have portrayed previous preferences, trust, or mistrust towards the companies.

While qualitative research has the benefit of being easily conducted and approached it also has drawbacks which many are due to research bias. These biases, the Hawthorne effect and recall bias to name a few, may impact the overall objectiveness of the research due to the reliance of partial objectivity of the participants.

The Hawthorne effect refers to the tendency people have of behaving in a different way when being observed, this act of not representing the 'normal' behaviour threatens the validity, internal and external, of the research (Nikolopoulou, 2022). The recall bias, as the name indicates, refers to the inability of individuals to recall an event or past behaviours correctly and accurately, which was seen at the beginning of some interviews. Participants lamented the inability to correctly recall what had come to pass in the videos they had seen and what were the emotions they created. This issue, however, was solved

largely by the nature of the focus group interviews themselves, with participants helping each other to accurately recall the proceedings in the videos.

While the interviews greatly relied on personal perceptions in which the matter of bias undoubtedly played a huge part, bias also somewhat clouded the judgement of the participants. This was seen when a certain moment of a video became etched in the minds of the recipients and ended up generating one barefaced understanding on the videos, which correlates to the reaction of stimuli Solomon (2019) has outlined portraying how the student's attention gets drawn in to the most influential factor seen or heard.

The most prominently biased video was video one, which many participants quickly slotted into the unsignificant, outdated, and stupid category, not being able to analyse it much further than the initial image that was created in their mind in the first few seconds of the video. Most notably participants struggled to pinpoint factual moments in the first video that worked in an influential way. The results that came back were very heavily tinted with humorous responses revolving around the taco that so many of the participants noted as a memorable moment.

5.2 Background

Reflecting on the results of this study the diversity of the responses was clearly affected by the participants backgrounds. While gender and age did not play a clear, significant role in the responses, previous knowledge and nationality made some participants stand out. Deeper and more nuanced analysis was generated by students who specifically mentioned previous knowledge of the companies in question or the subject in general. Those who mentioned not knowing anything about cybersecurity ended up having similar responses and perceptions. More than this it was clear that some of the students with previous knowledge also had an interest in the subject and as such discussed the matters in a very throughout manner.

Nationality widely determined recipients' perceptions during the focus group interviews. Since nationality can be measured more accurately than previous knowledge the author considers this a key element in how fear, uncertainty, and doubt were perceived. According to a study by Rathee & Rajain, (2019) nationality can also influence colour

associations. While not confirmed in this study it leads to the conclusion that the subjective nature of the participants individual perceptions has also influenced the colour associations of this study.

As it is evident in table 2 recipients of focus groups 3 and 4 were mostly from outside of Finland. While participants from Brittain did not have largely differing opinions on the videos, focus group 3 stood out as a group with most drastically contradicting perceptions and opinions regarding fear. The second video creating the most fear in the participants in this group, and the threats portrayed in the video regarded as realistic and worrisome. Based on the comments of participants, the video presumably attracted their attention due to the TV commercial type of sequence of scenes and the worrisome yet entertaining nature of the video.

Focus group 3 stood out due to the strict difference of fear perception. Since most other focus groups regarded the third video as the most fear inducing, worrisome, and severe, the responses of group 3 leads to the conclusion that the difference lies in the culture and nature of the nation the participants grew up in. This would imply that long and informative videos would not work in generating emotional responses from recipients from such backgrounds, leading us to effectively assume that recipients from Northern Europe find informative videos much more appealing.

5.3 Fear and trust

Considering the threat of eroding trust in the long run, through fear-based marketing tactics the results of this study would indicate that to be correct. As stated before, the videos in general yielded limited levels of trust. While the third video was mostly considered the scariest it still indicated a semblance of trust in the recipients, the same could not be said on the second. Fear and trust did not correlate when analysing the second video, with the approach the company implemented resulted in it being unconstructive for the company and brand reputation. Aligning with a study by Ruiter et al. (2014) this shows how risk denial, and defensive reactions were triggered in response, something well portrayed by person 3, and showing how a defensive reaction can lead to the complete loss of trust in recipients.

In the same category the results would indicate that students are more recipient to happy and exciting videos that grasp the focus of the viewer. The brighter colours and chipper tunes were always notable aspects stated by the participants, yet again proving the colour theory provided by Solomon (2019) to hold merit. However, it cannot be concluded based on this that a more positive approach in advertisements would have a longer and more memorable effect on the viewers. Noting this, the results did point towards the usefulness of having memorable visual aspects in the videos in order to generate higher levels of attention.

Finally, the results of the focus groups suggested that students prefer to have a realistic approach on matters like cybersecurity. Regarding the 4R's mentioned by Kajendran (2017) reality is one of the key factors that needs to replace FUD in the long run. This would be backed up by the student's inertia and blatant disregard towards the marketing tactics that were seen as unrealistic and oversimplified, a common result of FUD marketing as many theories indicates. In summary, students demand that the company shows the reality and their competence in cybersecurity before a true semblance of trust can be fabricated.

5.4 Discussion of method

The method chosen for this study was focus group interviews, a qualitative method which allowed the careful consideration of the recipient's perceptions to commerce through well placed questions. While the method fit the purpose of the study excellently, the conundrum was to create questions and an atmosphere where students had time and space to take apart their thought process and analyse the intricacies in detail. This being a difficult task in itself, some of the recipients struggled to pinpoint valuable thoughts at the beginning. After noticing this the questions were switched around for the following interviews creating a circle like structure where the first question was asked twice. Once at the beginning and again, while differently worded, at the end. This proved to be an applicable strategy which ended up generating exceedingly deep reflections.

The participants were generally cooperative due to the selection process where the aims of the research were explained, and consent of participants was confirmed. This fact meant that all participants had an understanding on the topic of the thesis and the

proceedings of the interviews themselves, which ultimately made them cooperative and responsive. Nevertheless, difference was seen between dynamics in focus groups, group 2 in particular being rather quiet and needing prompting. Although not all participants knew each other well from the beginning that never raised any issues and at length worked in favour of fruitful reflection.

Notably focus group 2 struggled the most in understanding and answering the question. This meant that the interviewer needed to adjust and reframe the questions a couple of times which made the focus group interview last longer. Aside from focus group 2 all other groups succeeded in answering the question clearly and explaining their reasoning for their answers. Those participants who struggled to answer questions felt comfortable asking for guidance and explanations when needed, these explanations were occasionally given by the interviewer, but mostly other participants showed their understanding by explaining the details to their fellow participants.

The method chosen proved its value time and again during the interviews themselves but also during presenting and dividing the results into themes. Regarding the level of detail gained through the usage of this method, it is unlikely that any other chosen method could have produced as nuanced results.

While validity has been generated through meticulously designed questions based on the theory and the aim to answer the research question, the level of validity can be questioned by the influence of human error. Misunderstandings and personal biases can all result in reduced validity. The significant issue validity faces is the possibility that the participants have not entirely understood the questions or the aim making it possible that results do not hold true validity. As it is, the study is based on an unreliable factor of perceptions which cannot be entirely measured, influenced by minute details they might change significantly in a short period of time.

Noting the issues in validity, the study meets the requirements to be reliable due to the information on the background of the participants, making it possible to in theory replicate the study.

6 CONCLUSIONS

This study has embarked on a mission to better understand how do students perceive FUD marketing by cybersecurity companies, successfully executing focus group interviews in which the subject was studied through questions revolving around perceptions, resulting in nuanced responses that were then categorized using thematic analysis and as such creating a summarised conclusion on students' perceptions.

The conclusion, this study has reached is that many of the fear-based marketing tactics are perceived as unrealistic and outdated resulting in a compromise of trust regarding the companies' abilities to meet the requirements and standards of security in the cyber domain.

6.1 Limitations of the study

The limitations and drawbacks of this study start with the lack of previous research in this particular field. While cybersecurity itself is not a new industry and sees continuously new research within, the study of marketing in cybersecurity is remarkably less researched, making students perceptions even less so. This has limited the study through the lack of a beginning or foundation on which to base the study, as it is the first in its field.

Another limitation this study faces is the inability to generalize the results achieved in the focus groups. The method chosen adds more limitations to this study through the influence of external factors, previous knowledge, and personal biases as mentioned above. This led to the lack of objectivity in many students and discussions heavily tinted by preference. While limiting it does not invalidate the study, simply demonstrating the volatility of perceptions.

Finally, the issues communication pose can greatly limit the study. As many of the focus groups were held in English, which was not the preferred language to communicate for some, it could have resulted in a difficulty in adequately expressing emotions and perceptions, leaving it up to the author to interpret.

6.2 Suggestions for further studies

This study has taken the first step in attempting to understand the perceptions students have towards fear-based marketing strategies. Nevertheless, this area of study still presents a great opportunity to conduct more comprehensive research. The study can be re-created with a different target group, were it changing age, nationality of respondents, or industry in which the marketing takes place.

Another possibility for future studies can be taking apart the fragments addressed in this study and further studying their interconnections. Through the foundation this thesis gives, research regarding the difference between perceptions and nationality can be studied as well. Finally, comparisons between fear-based and excitement-based marketing strategies can be further studied.

In short, this study is merely a small piece of a wider picture and as such can be significantly furthered through various studies diving deeper into the subject in order to gain a wider view of fear and perceptions.

References

Bhandari P., 2020, *What Is Qualitative Research? Methods and Examples*, https://www.scribbr.com/methodology/qualitative-research/

Barclay, 2018, *Semi-Structured Interviews*, https://know.fife.scot/__data/assets/pdf_file/0028/177607/KnowHow-Semistructured-interviews.pdf

Bhat Adi, 2023, *Qualitative Research Methods: Types, Analysis+ Examples*, https://www.questionpro.com/blog/qualitative-research-methods/

Bobbert Yuri, 2021, *Why FUD fails and BAD prevails in Digital Security*, https://www.antwerpmanagementschool.be/en/blog/fud-fails-bad-prevails-digital-security

Checkpoint, 2019, *Without the Best Security, Bad Things Happen*, https://www.youtube.com/watch?v=8jhwAesNcVk

Cisco, 2023, *The Hacker*, https://www.youtube.com/watch?v=JNMuuV3o_DU

Crosley Jenna, 2021, *What (Exactly) Is Thematic Analysis?* https://gradcoach.com/what-is-thematic-analysis/

Div Lior, 2015, *Advanced Persistent Threats And The Board: Moving Past FUD*, https://www.forbes.com/sites/frontline/2015/12/03/advanced-persistent-threats-and-the-board-moving-past-fud/

Dupuis & Renaud, 2020, *Scoping the ethical principles of cybersecurity fear appeals*, https://link.springer.com/article/10.1007/s10676-020-09560-0

Fritscher Lisa, 2023, *The Psychology of Fear*, https://www.verywellmind.com/the-psychology-of-fear-2671696

F-Secure, 2019, *Live Security*, https://www.youtube.com/watch?v=Cn1P6vVAZpw

Funk John, 2020, *Cybersecurity Marketing Tactics That Actually Work*, https://www.sevenatoms.com/blog/cyber-security-marketing-tactics-that-actually-works/

Gibson & Robinson, 2005, *The intersection between systems theory and grounded theory: the emergence of the grounded systems observer*, https://www.researchgate.net/publication/236325251_The_intersection_between_systems_theory_and_grounded_theory_The_emergence_of_the_grounded_systems_observer

Girardin 2023, *What is Qualitative Research? Methods and Examples*, https://www.theforage.com/blog/skills/what-is-qualitative-research

Heath Cathy, 2023, *Validity in research: a guide to measuring the right things*, https://dovetail.com/research/validity-in-research/

IBM, 2024, *What is cybersecurity?* https://www.ibm.com/topics/cybersecurity

Kajendran Jeremy, 2017, *Cyber Security: From FUD To The 4Rs*, https://inforisky.com/2016/03/07/cyber-security-from-fud-to-the-4rs/

Krishna, 2012, *An integrative review of sensory marketing: Engaging the senses to affect perception, judgement, and behaviour*, https://deepblue.lib.umich.edu/bitstream/handle/2027.42/142108/jcpy332.pdf?sequence%3D1%26isAllowed%3Dy

Krueger, 2002, *Designing and Conducting Focus Group Interviews*, https://www.eiu.edu/ihec/Krueger-FocusGroupInterviews.pdf

Lai Johnson, 2019, *What is FUD Marketing?* https://www.linkedin.com/pulse/what-fud-marketing-johnson-lai-mba/

Lange Charles, 2023, *The Science of Colour in Marketing: How to Use Colour Psychology to Boost Your Brand*, https://bootcamp.uxdesign.cc/the-science-of-color-in-marketing-how-to-use-color-psychology-to-boost-your-brand-299db0c8a3b2

Maddux James E., Rogers Ronald W., (1983) *Protection motivation and self-efficiency: A revised theory of fear appeals and attitude change*, Journal Volume 19, Issue 5, pages 469-479, https://www.sciencedirect.com/science/article/abs/pii/0022103183900239

Mann Ashwinder, 2023, *Investigating Factors Related to Fear, Uncertainty, and Doubt (FUD) in End-User Cryptocurrency Behaviours*, https://repository.library.carleton.ca/concern/etds/8s45q988k

Matias Rebecca, 2023, *Cyber Security Vendors Need to Move Past FUD: Here's Why and How*, https://www.callboxinc.com/growth-hacking/cyber-security-vendors-need-move-past-fud/

Middleton, 2023, *Reliability vs. Validity in Research: Difference Types and Examples*, https://www.scribbr.com/methodology/reliability-vs-validity/

Nikolopoulou, 2022, *What Is the Hawthorne Effect? Definition and Examples*, https://www.scribbr.com/research-bias/hawthorne-effect/

Peiffer Anna R., 2022, 2 *Ways Cybersecurity Marketers Can Have Fun with FUD*, https://www.linkedin.com/pulse/2-ways-cybersecurity-marketers-can-have-fun-fud-williams-peiffer

Pfaffenberger Bryan, (2000, *The rhetoric of dread: Fear, uncertainty, and doubt (FUD) in information technology marketing*, https://link.springer.com/article/10.1007/s12130-000-1022-x

Preity, 2016, *Stimuli & Consumer Behaviour*, https://www.linkedin.com/pulse/stimuli-consumer-behaviour-preity-iiyerr

R. Rathee & P. Rajain, 2019, *Role Colour Plays in Influencing Consumer Behaviour*, https://www.researchgate.net/publication/338430636_Role_Colour_Plays_in_Influencing_Consumer_Behaviour

Rosling Hans, 2011, *Factfulness*, book p.146

Ruiter et al, 2014, *Sixty years of fear appeal research: current state of the evidence*, https://pubmed.ncbi.nlm.nih.gov/24811876/

Solomon Michael R., 2019, *Consumer Behaviour*, book, 7th edition, pages 86-90

Sreenivasan & Weinberger, 2018, *Fear Appeals: An approach used to change our attitudes and behaviours*, https://www.psychologytoday.com/us/blog/emotional-nourishment/201809/fear-appeals

Study Smarter, 2024, *Gibson's Theory of Direct Perception*, https://www.studysmarter.co.uk/explanations/psychology/cognition/gibsons-theory-of-direct-perception/

Tannebaum et al, 2015, *Appealing to fear: A meta-analysis of fear appeal effectiveness and theories*, https://psycnet.apa.org/record/2015-48611-002

Tharakan Kurian M., 2019, *What is the meaning of FUD?* https://strategypeak.com/fud-fear-uncertainty-doubt/

The Interaction Design Foundation, 2015, *Elaboration Likelihood Model Theory: How to0 Use ELM*, https://www.interaction-design.org/literature/article/elaboration-likelihood-model-theory-using-elm-to-get-inside-the-user-s-mind

The White House, (2022) *Franklin D. Roosevelt*, https://www.whitehouse.gov/about-the-white-house/presidents/franklin-d-roosevelt/

Thomas, 2023, *Overcoming the cybersecurity FUD problem: Addressing Fear, Uncertainty, and Doubt*, https://hackwarenews.com/overcoming-the-cyber-security-fud-problem-addressing-fear-uncertainty-and-doubt/

White H. Allen, 2011, *Elaboration Likelihood Model*, https://www.oxfordbibliographies.com/display/document/obo-9780199756841/obo-9780199756841-0053.xml

Zarate Alejandra, 2023, *FUD: How to Use It, Abuse It, and Thwart It*, https://www.scholesmarketing.com/scholes-knows-marketing-blog/fud-how-to-use-it-abuse-it-and-thwart-it

Appendix

Appendix 1: Consent form:

- I give permission for the data collected to be used for scientific research.
- I understand that I can pull out of the study at any time, and I do not have to provide reasons for doing so.
- I understand that the data will be stored for a period of 10 years according to VSNU guidelines.
- I have received information on the study and as such understand what this study entails.
- Signature, time, and place.

Appendix 2: Focus group interview questions:

1. What kinds of emotions do these videos create?
2. Where there any specific moments or elements in the videos that stood out to you?
3. Do you feel a sense of urgency and need to do something based on these videos?
4. Do these videos create a sense of trust in the capabilities of the companies?
5. How are these cyber threats portrayed in your understanding?
6. What caused the feeling of distrust if there was no trust?
7. Can you identify any features or techniques used in the videos to evoke emotions or influence perceptions?

8. Circling back could you pinpoint a couple of top emotions that rose to the top when watching the videos?

Appendix 3 Video links:

Company Torrent:

Checkpoint, 2019, *Without the Best Security, Bad Things Happen*, https://www.youtube.com/watch?v=8jhwAesNcVk

Company Tide:

Cisco, 2023, *The Hacker*, https://www.youtube.com/watch?v=JNMuuV3o_DU

Company Wave:

F-Secure, 2019, *Live Security*, https://www.youtube.com/watch?v=Cn1P6vVAZpw