POTENTIAL EFFECTS OF ADVANCED CYBERATTACKS ON CYBERSECURITY SOFTWARE BUYERS' BEHAVIOUR

Guy WAIZEL
Alexandru Ioan Cuza University of Iaşi, Faculty of Economics and Business Administration
Iaşi, Romania
guy.waizel@gmail.com

Prof. Adriana ZAIT
Alexandru Ioan Cuza University of Iaşi, Faculty of Economics and Business Administration
Iaşi, Romania
azait@uaic.ro

ABSTRACT

This research paper aims to develop a comprehensive understanding of cybersecurity buyer behavior by integrating multiple theories. Specifically, we examine the Theory of Buyer Behavior, the Theory of Reasoned Action, the Theory of Planned Behavior, the Stakeholder Theory, and their relevance in the context of advanced cybersecurity attacks. The paper proposes a new model, the Cybersecurity Buyer Behavior Effect Model (CB2EM), which synthesizes insights from these theories to predict the potential effect of advanced cybersecurity attacks, including zero-day supply chain attacks and stealth techniques attacks, on cybersecurity buyer behavior. Through a systematic review and analysis of the selected theories, we identify commonalities and complementarities, ultimately creating a unified framework that enriches our understanding of how cyber incidents shape buyer decisions. The CB2EM is expected to provide marketers and cybersecurity vendors with valuable insights to effectively address buyer concerns in a rapidly evolving threat landscape.

Keywords: stealth techniques; buyer behavior; zero-day, supply chain attacks; cybersecurity software

JEL Classification: M3 Marketing and Advertising, M310 Marketing

1. Introduction

Advanced cybersecurity threats are on the rise, with attackers increasingly employing sophisticated techniques such as Living off the Land Binaries and Scripts (LOLBins and LOLScripts), as well as zero-day supply chain attacks targeting vulnerabilities within software systems. The cybersecurity landscape is witnessing a paradigm shift due to these advanced cyberattacks, particularly as they expose data privacy concerns and lead to breaches impacting numerous sensitive organizations concurrently. By leveraging these techniques, attackers can effectively circumvent traditional security measures, including Endpoint Detection and Response (EDR) systems, by exploiting legitimate Windows tools and an array of vulnerabilities present in both IoT devices and computers. The ramifications of such attacks reverberate across various industries in both the public and private sectors, thereby challenging the stability of global economies.

This research paper aims to explore how advanced cyberattacks impact the thoughts and actions of those purchasing cybersecurity software. To achieve this, we thoroughly review relevant existing studies. We then relate the connection between cybersecurity buyer behavior and the landscape of advanced attacks by comparing established theories in buyer behavior. Our analysis incorporates theories such as the Theory of Buyer Behavior, the Theory of Reasoned Action, the Theory of Planned Behavior, and Stakeholder Theory. By combining these theories, we identify important implications and introduce a new model called the Cybersecurity Buyer Behavior Effect Model (CB2EM). This model is designed to predict the potential effects of advanced cybersecurity attacks on the decision-making of cybersecurity software buyers.

Through our research findings, this paper enhances the comprehension of how those buying cybersecurity software interpret and react to the changing threat environment. Moreover, the CB2EM model acts as a valuable resource, predicting the diverse consequences of advanced cyberattacks on the cybersecurity software market. This aids stakeholders in developing well-informed strategies to reduce risks and bolster overall cyber resilience.

2. Literature

2.1 Advanced Cybersecurity Threats - Stealth Techniques

Living Off the Land Binaries (LOLBins) hacking techniques have been in use by hackers for over a decade (Campbell & Graeber, 2013). LOLBins are executable files that come pre-installed as part of the Windows operating system, legitimate utilities, executables, DLLs, and libraries that hackers can exploit for their malicious purposes. In a joint report published in May 2023, CISA (Cybersecurity and Infrastructure Security Agency) and Microsoft highlighted the

use of such techniques in attacks targeting critical infrastructure within the United States (CISA, 2023; Intelligence Microsoft, 2023).

Attackers employ these techniques with the intent to conceal their actions using legitimate tools like Windows PowerShell, effectively evading detection. This concealment strategy has been in practice for years, as evidenced by a 2016 Symantec report (Symantec, 2016). Windows PowerShell, a legitimate utility pre-installed on all Windows operating systems, offers capabilities such as execution directly from memory, rapid remote access, lateral movement potential, and the ability to obfuscate actions. It often blends seamlessly with routine IT administrative tasks, making it an attractive choice for hackers engaging in fileless malware techniques (Sudhakar & Kumar, 2020), such as the downloadstrings technique employing WebClients.

Moreover, hackers utilize techniques like "Invoke expressions" (IEX) within PowerShell, alongside various obfuscation methods achievable through tools like Invoke-Stealth (K, R., 2021) and encryption via msfvenom within Metasploit (Metasploit, 2023). These tactics facilitate the loading of potent tools into memory, such as Redrabbit (Github, 2023), enabling the execution of commands encompassing activities such as scanning, brute forcing, password extraction, encoding and decoding, establishing reverse shells, employing keyloggers, and more. To further evade detection, hackers even resort to renaming LOLBins before execution, thus thwarting endpoint solutions that rely on predefined detection patterns. Research has demonstrated attackers' ability to bypass endpoint protection solutions (Karantzas, G., & Patsakis, C., 2021), presenting a significant challenge for security solutions and Security Operations teams in detecting their movements.

Furthermore, hackers exploit Microsoft's Antimalware Scan Interface (AMSI), a tool designed for software communication that facilitates tasks like requesting scans of files, memory, or streams (Gallagher, S., & Gallagher, S., 2021). Additionally, DLL sideloading techniques are frequently employed to execute malicious code (Labs, T., 2023).

In summary, the utilization of LOLBins and associated stealth techniques underscores the evolving sophistication of cyberattacks. Hackers' adeptness at leveraging legitimate utilities and concealing their actions in complex ways amplifies the difficulty of detecting and countering such threats.

2.2 Advanced Cybersecurity Threats - Zero-day and Supply Chain Attacks

Drawing from documented sources, it becomes evident that malicious actors such as the CL0P group are adept at exploiting vulnerabilities to achieve their objectives.

In a concerning instance, the CL0P group targeted a vulnerability known as CVE-2023-34362 within the MOVEit security file transfer software. This

exploitation led to the breach of hundreds of organizations and thousands of hosts, including high-profile entities such as BBC, British Airways (BA), and Boots, among others, all falling victim to cyberattacks (BBC, 2023). Moreover, other reputable news outlets have reported that the same CL0P ransomware group previously employed a zero-day vulnerability in GoAnywhere, compromising over 130 organizations (Gatlan, S., 2023). Disturbingly, indications of the exploitation of the MOVEit vulnerability were even evident as far back as two years ago (Scott Downie, D., 2023).

The complex dynamics of these attacks highlight significant time gaps in the cybersecurity landscape. Organizations get caught in a cycle involving attackers experimenting with Proof-of-Concept (PoC), vendors revealing vulnerabilities, exploits emerging in the wild, vendors eventually releasing patches, and the patches being applied. This puts IT departments in a constant race against cybercriminals, working to close the gap.

Managing patches becomes a crucial concern here, demanding substantial time and careful attention. IT departments usually test patches in controlled settings to ensure they don't disrupt essential processes before widespread use, protecting productivity. However, vulnerabilities often persist even after patches are issued. Previous research shows that a significant 42% of vulnerabilities continue to be exploited after patches are released. The speed at which exploitation happens is striking, with vulnerabilities targeted within just two days of PoC or exploit code becoming publicly available. Also, the average time vulnerabilities remain critical, from disclosure to patch availability, is around 9 days (Mandiant, 2023).

Considering these difficulties, the MOVEit attack incident stands as a clear example. The discovery of signs of MOVEit vulnerability exploitation, stretching over two years, vividly illustrates the proactive and persistent nature of cyber adversaries (Scott Downie, D., 2023).

2.3 The Theory of Reasoned Action (TRA)

The Theory of Reasoned Action is a psychological model that explains the relationship between attitudes, subjective norms, and behavioral intentions. It suggests that people's behavioral intentions are influenced by their attitudes towards a behavior and the subjective norms related to that behavior. (Fishbein, M., & Ajzen, I, 1977, 2011). By illuminating the dynamic connections between attitudes, subjective norms, and behavioral intentions, this model provides a comprehensive framework for understanding and predicting human actions in a myriad of contexts.

2.4 The Theory of Planned Behavior (TPB)

The Theory of Planned Behavior is a psychological model that extends the Theory of Reasoned Action (TRA). It suggests that behavioral intentions and actions are influenced not only by attitudes and subjective norms but also by perceived behavioral control or the perceived ease or difficulty of performing the behavior. (Ajzen, I. , 1985).

A clear study of how the TPB can be used in cybersecurity shows it can help us understand complex situations better. For instance, Sulaiman et al. (2022) delved into the domain of information security compliance violations, shedding light on employees' behavioral tendencies. Similarly, George et al. (2021) unearthed compelling insights by examining customers' intent to purchase IoT security devices. Their findings revealed that fear of burglars emerged as a positive influence on purchasing intentions, while privacy concerns negatively affected attitudes.

Further amplifying the TPB's relevance, Vafaei-Zadeh et al. (2019) embarked on an investigation that elucidated the intricate nexus between perceived price levels, information security awareness, attitudes, subjective norms, and perceived behavioral control. Their research uncovered an interesting discovery: subjective norms play a crucial role in predicting users' intentions to install anti-malware software. Ansari (2021) unearthed a significant positive correlation between the effectiveness of AI-Based Security Awareness Training programs and employees' risk scores. Aderibigbe and Ocholla (2020) probed the challenges surrounding cyber-ethics behavior in South African universities, adding a valuable layer of understanding to the TPB's contextual application.

In sum, the Theory of Planned Behavior, through its incorporation of perceived behavioral control, emerges as a versatile framework for comprehending the complexities of human behavior within the dynamic landscape of cybersecurity. As demonstrated by the studies highlighted, the TPB not only extends theoretical understanding but also provides actionable insights for fostering enhanced cybersecurity practices.

2.5 The Theory of Buyer Behavior (TOBB)

The Theory of Buyer Behavior is concerned with understanding the behavior of buyers or consumers in the context of making purchasing decisions. It seeks to analyze the factors that influence consumers' choices, such as personal preferences, attitudes, perception of the product, social and cultural influences, and economic factors. (Howard, J. A., & Sheth, J. N., 1969).

2.6 The Stakeholder Theory

The Stakeholder theory is a management and organizational theory that suggests that an organization should consider the interests and needs of all its

stakeholders when making decisions. (Donaldson, T., & Preston, L. E. ,1995). Within the realm of information security and cybersecurity, Washington (2023) embarked on an exploratory journey to investigate the applicability of the Stakeholder theory. The focus of the research was centered on discerning how this theory informs perceptions of an organization's information security policy. By analyzing stakeholders' perspectives, the study adds a layer of nuance to the integration of this theory within the cybersecurity domain.

Interestingly, during the comprehensive literature search, no specific studies were unearthed that delved into the intricate interplay between advanced cyber attacks and cybersecurity buyer behavior while concurrently examining the implications of pivotal theories, namely, the Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), Theory of Buyer Behavior (TOBB), and the Stakeholder theory. This uncharted territory highlights a potential research gap, indicating an interesting path that we are pursuing in this research paper.

3. Methods

Literature Review: An extensive literature review was conducted to identify pertinent theories related to buyer behavior, with a specific focus on cybersecurity buyers and the influence of cyberattacks on their behavior. Key theories selected encompassed the Theory of Buyer Behavior, the Theory of Reasoned Action, the Theory of Planned Behavior, and the Stakeholder Theory. The exploration encompassed studies that delve into cybersecurity buyer behavior and the impacts of cyberattacks on decision-making. Additionally, research linking the aforementioned theories with cybersecurity was also included.

Theoretical Framework Identification: Drawing from the literature review, crucial constructs and variables from each theory that pertained to cybersecurity buyer behavior were identified. This process also revealed gaps and potential overlaps among the theories, serving as a foundation for subsequent integration efforts.

Conceptual Integration: Construct comparison and analysis were undertaken to uncover commonalities and interconnections among the identified constructs from each theory. The aim was to explore how these constructs could harmoniously blend to form a more comprehensive and cohesive model, facilitating a deeper understanding of the ramifications of advanced cyberattacks on cybersecurity buyer behavior.

Development of a New Proposed Model: Guided by insights derived from the theoretical integration process, the Cybersecurity Buyer Behavior Effect Model (CB2EM) was conceptualized. This model delineates the interrelationships and interplays between key constructs, elucidating their impact on cybersecurity buyer behavior in the face of sophisticated cyber threats.

Discussion and Implications: Subsequent discussions centered on the ramifications of the newly proposed CB2EM model for cybersecurity marketers, vendors, and organizations. The model's contributions to comprehending cybersecurity buyer behavior were highlighted, alongside the strategic implications for addressing buyer concerns within an evolving threat landscape.

Conclusion: The paper culminated with a concise summary of findings and contributions. Emphasis was placed on the inherent value of integrating theories to advance the comprehension of intricate phenomena such as cybersecurity buyer behavior. Furthermore, the potential applications of CB2EM were underscored, particularly its role in guiding marketing strategies and influencing cybersecurity investments.

By deploying a methodical approach to theory integration, this research paper aims to introduce an innovative model that sheds light on the interplay between advanced cyberattacks and cybersecurity buyer behavior. In doing so, it contributes to the expanding realm of knowledge within both cybersecurity and marketing research domains.

4. Results

4.1 Theory of Reasoned Action (TRA) and Theory of Planned Behavior (TPB) in the Context of Advanced Cyber Threats on Cybersecurity Buyers

When applying the Theory of Planned Behavior (Ajzen, 1985) to understand the impact of advanced cyberattacks on cybersecurity buyer behavior, we delineate the following categories:

Attitudes: In the realm of cybersecurity, attitudes encompass a buyer's beliefs and evaluations regarding the advantages and disadvantages of investing in cybersecurity solutions. Advanced cyberattacks wield a considerable influence on attitudes. Instances such as severe cyberattacks experienced by businesses or organizations, or high-profile cyberattacks capturing media attention, heighten awareness about the potential repercussions of inadequate cybersecurity measures. Consequently, cybersecurity buyers may develop more favorable attitudes towards investing in advanced cybersecurity solutions, recognizing the benefits of safeguarding their assets and sensitive information.

Subjective Norms: Subjective norms within the cybersecurity context pertain to the perceived social pressures and expectations concerning cybersecurity investments. The occurrence of advanced cyberattacks can evoke a sense of urgency and social pressure among cybersecurity buyers. Media coverage of cyberattacks and public perception of organizations' data security practices hold the potential to shape subjective norms. Positive subjective norms, such as peer

organizations adopting robust cybersecurity measures, can serve as an impetus for buyers to follow suit and make corresponding investments.

Perceived Behavioral Control: Perceived behavioral control denotes a buyer's perception of their capability to enact a desired behavior, specifically investing in advanced cybersecurity solutions. The impact of advanced cyberattacks on this facet of the Theory of Planned Behavior is multi-faceted. For instance, if buyers perceive their organization to lack the requisite resources or expertise to effectively address cybersecurity challenges, it may diminish their intention to invest in advanced solutions. Conversely, if they believe that implementing advanced cybersecurity measures lies within their control and can proficiently safeguard their assets, their intent to invest may be heightened.

Behavioral Intentions: Behavioral intentions encapsulate an individual's motivation and willingness to engage in a specific behavior. In the context of cybersecurity, advanced cyberattacks wield a substantial influence on behavioral intentions. Buyers who perceive a substantial threat emanating from cyberattacks, hold favorable attitudes towards cybersecurity investment, and possess a sense of control over implementing advanced solutions, are more inclined to exhibit robust behavioral intentions to procure and adopt such solutions.

To conclude, the Theory of Planned Behavior acts as a framework to clarify how advanced cyberattacks can impact the behavior of cybersecurity buyers. This occurs through their attitudes, the influence of others' opinions, and their perceived control over their actions. Advanced cyberattacks affect attitudes by making individuals more conscious of the advantages of investing in cybersecurity. They shape subjective norms by creating social pressure and emphasizing the significance of cybersecurity. Moreover, the perceived behavioral control is influenced by how buyers assess their organization's ability to effectively handle cybersecurity challenges. These combined elements shape the behavioral intentions of cybersecurity buyers, motivating them to invest in advanced cybersecurity solutions to protect their organizations against potential cyber threats. We employ a visual representation (Fig. 4.1) to illustrate the core elements of the Theory of Reasoned Action (TRA) and the Theory of Planned Behavior (TPB) within the context of the effect of advanced cyber threats on cybersecurity buyers' behavior.

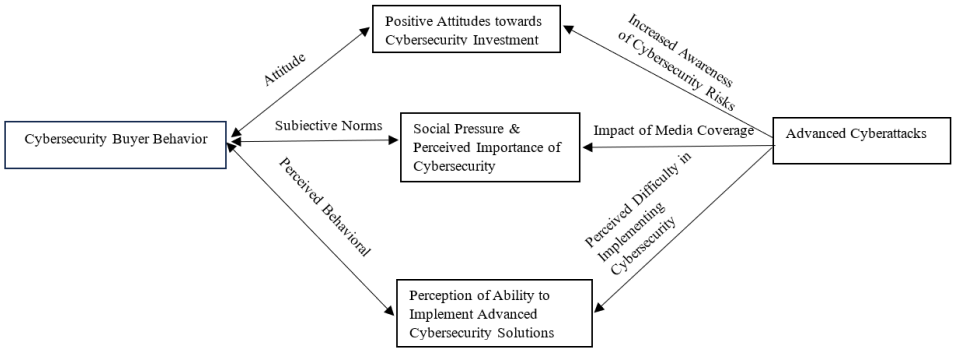

Fig. 4.1: The effect of Advanced Cyberattacks on Cybersecurity Buyer Behavior - Theory of Planned Behavior

4.2 The Theory of Buyer Behavior (TOBB) in the Context of Advanced Cyber Threats on Cybersecurity Buyers' Behavior

When applying the TOBB Theory (Howard, J. A., & Sheth, J. N., 1969) to Understand the Effect of Advanced Cyberattacks on Cybersecurity Buyer Behavior, we define the following elements:

Perception and Motivation: Advanced cyberattacks can significantly influence cybersecurity buyer behavior by shaping their perceptions and motivations. Awareness of high-profile cyber incidents can create a perception of vulnerability and a heightened sense of urgency to protect assets and data. The motivation to invest in cybersecurity solutions increases as buyers aim to mitigate potential risks and safeguard business interests.

Information Processing: Cybersecurity buyers engage in extensive information processing when evaluating potential solutions. Advanced cyberattacks can stimulate the search for more information about cybersecurity products and services. Buyers may conduct thorough research, consult experts, and compare various options to make informed decisions.

Attitudes and Preferences: The Theory of Buyer Behavior emphasizes attitudes in shaping consumer decisions. Cybersecurity buyers' attitudes are influenced by perceived effectiveness and reliability of different solutions. Advanced cyberattacks can lead to more positive attitudes toward advanced and comprehensive cybersecurity products, as buyers seek higher protection levels to avoid breach consequences.

Personal and Situational Influences: Personal factors, like the buyer's needs, experiences, and risk tolerance, play a role in decision-making. Advanced cyberattacks can trigger emotional responses, impacting risk perceptions and

aversion. Situational factors, such as recent attack severity or regulatory changes, can also influence buyer behavior.

Social Influences: The Theory of Buyer Behavior acknowledges social influences on purchasing decisions. In cybersecurity, this can manifest through peer recommendations, testimonials from attacked organizations, or guidance from experts. Positive experiences of other organizations investing in cybersecurity solutions may drive buyers to follow.

Post-Purchase Evaluation: After investing in cybersecurity, buyers engage in post-purchase evaluation. If they experience attacks despite efforts, it can lead to reassessment. Organizations may seek advanced or tailored solutions to address gaps.

In Conclusion, the Theory of Buyer Behavior sheds light on how advanced cyberattacks can affect cybersecurity buyer behavior. Cybersecurity buyers' perceptions, motivations, information processing, attitudes, and social influences are all impacted by these incidents. Understanding these influences helps marketers tailor messaging and offerings to address specific cybersecurity buyer needs in a changing threat landscape.

We Utilize a Visual Representation (Fig. 4.2) to illustrate the main elements of the Theory of Buyer Behavior (TOBB) in the context of the effect of advanced cyber threats on cybersecurity buyers' behavior.

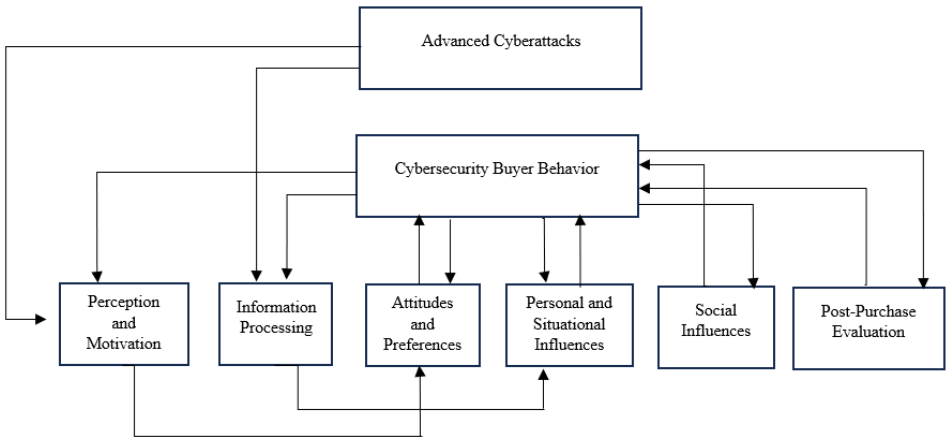

Fig. 4.2: The effect of Advanced Cyberattacks on Cybersecurity Buyer Behavior - Theory of Buyer Behavior

4.3 The Stakeholder Theory in the Context of Advanced Cyber Threats on Cybersecurity Buyers' Behavior

When Applying the Stakeholder Theory (Donaldson, T., & Preston, L. E., 1995) to understand the effect of advanced cyberattacks on cybersecurity buyer behavior, we define the following elements:

Perception of Risk: The occurrence of advanced cyberattacks increases the perception of risk among different stakeholders, including potential buyers of cybersecurity solutions. Customers grow concerned about the safety of their personal information and might hesitate to engage with businesses that have a history of cyber breaches. Employees worry about job security and question the company's ability to safeguard their data. Shareholders become cautious about potential financial losses and harm to the organization's reputation. These risk perceptions can significantly influence cybersecurity buyer behavior.

Trust and Reputation: Advanced cyberattacks can severely harm an organization's reputation and undermine trust with its stakeholders. Buyers are more likely to trust and favor companies with a strong cybersecurity track record. Conversely, organizations that have faced cyber incidents might experience negative perceptions and reduced trust. As a result, cybersecurity buyers tend to seek out trustworthy and reputable cybersecurity vendors to safeguard their interests.

Demand for Robust Solutions: Stakeholder Theory emphasizes the need for organizations to prioritize stakeholders' interests and meet their needs. Advanced cyberattacks elevate the demand for robust cybersecurity solutions from customers, who expect businesses to prioritize data and privacy protection. This heightened demand can drive a shift in cybersecurity buyer behavior, leading them to actively seek out comprehensive and innovative solutions to counter cyber threats.

Regulatory Compliance: Stakeholders, particularly customers, often demand that organizations adhere to relevant cybersecurity regulations to ensure data safety. Advanced cyberattacks can prompt governments and regulatory bodies to tighten cybersecurity requirements, impacting buyer behavior. Buyers may be more inclined to invest in cybersecurity solutions that not only safeguard their interests but also aid them in complying with standards and avoiding potential legal consequences.

Ethical Considerations: The Stakeholder Theory underscores the ethical dimensions of business decisions. Cybersecurity buyers may be influenced by an organization's commitment to ethical practices and data protection. Neglecting cybersecurity responsibilities or inadequately addressing cyber threats may deter potential buyers who prioritize ethical considerations in their purchasing choices.

In Conclusion, the Stakeholder Theory underscores how advanced cyberattacks affect cybersecurity buyer behavior by shaping stakeholders' risk perceptions, trust, reputation, and ethical considerations. Cybersecurity buyers are likelier to seek reliable and robust solutions from reputable vendors to protect their interests and cater to the needs of various stakeholders, including customers,

employees, and regulatory authorities. Organizations that prioritize cybersecurity and demonstrate a commitment to safeguarding stakeholders' interests are poised to attract and retain cybersecurity buyers in an increasingly risk-aware and security-conscious business landscape.

We offer a visual illustration (Fig. 4.3) that outlines the core components, showcasing the impact of advanced cyberattacks on different stakeholders within an organization. This representation aligns with the Stakeholder Theory and showcases the dynamic relationship between stakeholders' concerns and the decisions made by cybersecurity buyers in response to these concerns.

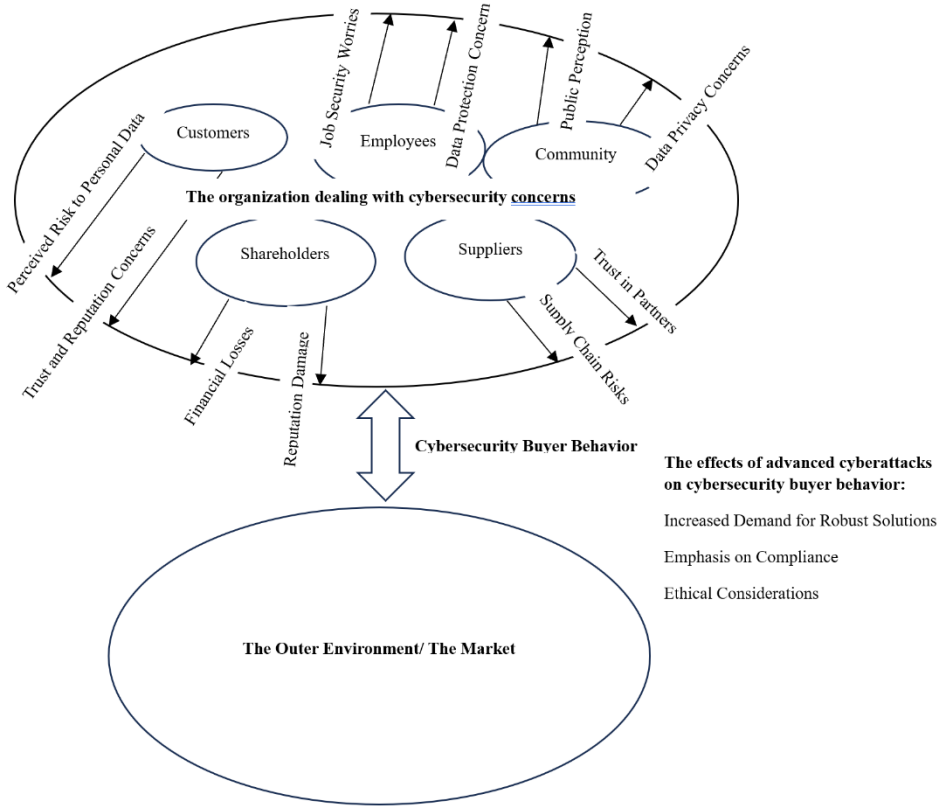

Fig. 4.3: The effect of Advanced Cyberattacks on Cybersecurity Buyer Behavior – The Stakeholder Theory

4.4 The Proposed Integrated Cybersecurity Buyer Behavior Effect Model (CB2EM)

This proposed model aims to predict the potential effect of advanced cyberattacks, Including zero-day supply chain attacks and stealth techniques attacks, on Cybersecurity Buyer Behavior. Here's an Overview of the CB2EM model's elements:

Perceived Threat and Vulnerability: This forms the model's foundation, influenced by the Theory of Buyer Behavior (Howard, J. A., & Sheth, J. N., 1969). Perceived threat and vulnerability are based on cybersecurity buyers' awareness of advanced cyberattacks, including incidents like zero-day supply chain attacks and stealth technique attacks. This factor shapes the entire decision-making process.

Attitudes and Risk Perception: Drawing from the Theory of Reasoned Action and the Theory of Planned Behavior (Ajzen, I. , 1985; Fishbein, M., & Ajzen, I, 1977, 2011), this factor represents cybersecurity buyers' attitudes toward cybersecurity investment. The perception of risk, influenced by the perceived threat and vulnerability, affects buyers' attitudes toward the importance of investing in advanced cybersecurity solutions.

Subjective Norms and Social Influences: Incorporating elements from the Theory of Reasoned Action (Fishbein, M., & Ajzen, I, 1977, 2011) and the Stakeholder Theory (Donaldson, T., & Preston, L. E., 1995), this factor considers the impact of social influences on cybersecurity buyer behavior. Media coverage, industry trends, and peer experiences play a significant role in shaping subjective norms and the perceived importance of cybersecurity investment.

Perceived Behavioral Control and Resource Availability: Based on the Theory of Planned Behavior (Ajzen, I., 1985), this factor examines buyers' perceived ability to implement advanced cybersecurity solutions. It takes into account their resources, expertise, and the feasibility of addressing potential cyber threats.

Trust and Reputation: This factor is influenced by the Stakeholder Theory (Donaldson, T., & Preston, L. E., 1995) and reflects buyers' perceptions of cybersecurity vendors and their trustworthiness. It considers how advanced cyberattacks affect vendors' reputation and how it influences buyer decisions.

Organizational Stakeholders: This factor acknowledges the role of various organizational stakeholders (e.g., customers, employees, shareholders) as influenced by the Stakeholder Theory (Donaldson, T., & Preston, L. E., 1995). The impact of cyberattacks on different stakeholders

can drive cybersecurity buyer behavior, as their interests and needs come into play.

Buyer Decision Process: This represents the collective influence of all the factors mentioned above on the buyer decision-making process. It predicts how cybersecurity buyers' attitudes, subjective norms, perceived behavioral control, and trust culminate in behavioral intentions to invest in advanced cybersecurity solutions.

By integrating insights from the Theory of Buyer Behavior, the Theory of Reasoned Action, the Theory of Planned Behavior, the Stakeholder Theory, and the potential effect of advanced cybersecurity attacks, the CB2EM provides a comprehensive framework for understanding and predicting the potential effects of cyber threats on cybersecurity buyer behavior. It considers both psychological and social factors that influence buyer decisions, providing valuable insights for marketers and cybersecurity vendors seeking to address the evolving challenges posed by advanced cyberattacks.

We Use a Visual Representation (Fig. 4.4) to present the main elements of the integrated model for understanding the potential effect of advanced cybersecurity attacks on cybersecurity buyer behavior.

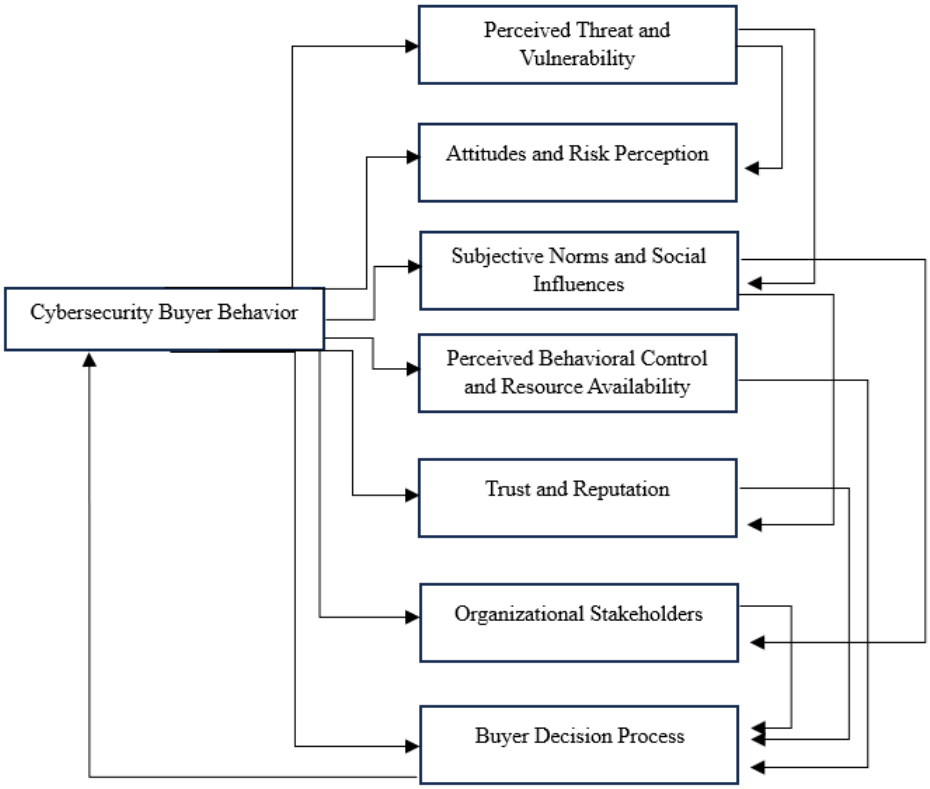

Fig. 4.4: The proposed integrated Cybersecurity Buyer Behavior Effect Model (CB2EM)

5. Discussion

By employing a systematic approach to integrating theories, this research paper offers the CB2EM model (Fig. 4.4), shedding light on the dynamics between advanced cyberattacks and cybersecurity buyer behavior. This contribution adds to the growing body of knowledge in the fields of cybersecurity and marketing research. The proposed model holds value for cybersecurity marketers, vendors, and organizations. Theory integration's significance lies in advancing the comprehension of complex phenomena like cybersecurity buyer behavior. The model serves as a guide for shaping marketing strategies and making informed cybersecurity investments.

Future research is recommended to conduct a case study analysis using real-world examples of organizations that have encountered advanced cyberattacks.

This analysis would examine how the CB2EM model aligns with observed buyer behavior in these cases and the decision-making processes in response to the incidents. Additionally, seeking expert opinions and feedback from cybersecurity professionals and marketers to validate the CB2EM through qualitative data, obtained via interviews and focus groups, can assess the model's practical applicability and identify potential refinements.

REFERENCES

Aderibigbe, N. A., & Ocholla, D. N. (2020). Insight into ethical cyber behaviour of undergraduate students at selected African universities. South African Journal of Information Management, 22(1)https://doi.org/10.4102/sajim.v22i1.1131

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In Action control: From cognition to behavior (pp. 11-39). Berlin, Heidelberg: Springer Berlin Heidelberg.

Ansari, M. F. (2021). The Relationship between Employees' Risk Scores and the Effectiveness of the AI-Based Security Awareness Training Program (Order No. 28961534). Available from Publicly Available Content Database. (2624617545). https://www.proquest.com/dissertations-theses/relationship-between-employees-risk-scores/docview/2624617545/se-2

Donaldson, T., & Preston, L. E. (1995). The stakeholder theory of the corporation: Concepts, evidence, and implications. Academy of management Review, 20(1), 65-91.

Fishbein, M., & Ajzen, I. (1977). Belief, attitude, intention, and behavior: An introduction to theory and research.

Fishbein, M., & Ajzen, I. (2011). Predicting and changing behavior: The reasoned action approach. Taylor & Francis.

Gallagher, S., & Gallagher, S. (2021). AMSI bypasses remain tricks of the malware trade. Retrieved 4 June 2023, from https://news.sophos.com/en-us/2021/06/02/amsi-bypasses-remain-tricks-of-the-malware-trade/

Gatlan, S. (2023). Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day. Retrieved 26 June 2023, from https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/

George, J. F., Chen, R., & Yuan, L. (2021). Intent to purchase IoT home security devices: Fear vs privacy. PLoS One, 16(9)https://doi.org/10.1371/journal.pone.0257601

How to use msfvenom. (2023). Retrieved 1 June 2023, from https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-msfvenom.html

Howard, J. A., & Sheth, J. N. (1969). The theory of buyer behavior. New York, 63, 145.

K, R. (2021). Invoke-Stealth: Simple And Powerful PowerShell Script Obfuscator. Retrieved 1 June 2023, from https://kalilinuxtutorials.com/invoke-stealth/

Karantzas, G., & Patsakis, C. (2021). An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. Journal of Cybersecurity and Privacy, 1(3), 387. doi:https://doi.org/10.3390/jcp1030021

Labs, T. (2023). LOLBins and DLL sideloading. Retrieved 4 June 2023, from https://www.triskelelabs.com/lolbins-and-dll-sideloading

Living Off the Land: A Minimalist's Guide to Windows Post-Exploitation - Christopher Campbell, Matthew Graeber Derbycon (2013) (Hacking Illustrated Series InfoSec Tutorial Videos) . (2023). Retrieved 21 July 2023, from http://www.irongeek.com/i.php?page=videos/derbycon3/1209-living-off-the-land-a-minimalist-s-guide-to-windows-post-exploitation-christopher-campbell-matthew-graeber

MOVEit hack: BBC, BA and Boots among cyber attack victims. (2023). Retrieved 22 June 2023, from https://www.bbc.com/news/technology-65814104

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection | CISA. (2023). Retrieved 30 July 2023, from https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

Scott Downie, D. (2023). MOVEit Transfer Vulnerability (CVE-2023-34362) | Kroll. Retrieved 23 June 2023, from

https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362

securethelogs. (2023). GitHub - securethelogs/RedRabbit: Red Team PowerShell Script. Retrieved 2 June 2023, from https://github.com/securethelogs/RedRabbit

Sudhakar, & Kumar, S. (2020). An emerging threat fileless malware: A survey and research challenges. Cybersecurity, 3(1) doi:https://doi.org/10.1186/s42400-019-0043-x

Sulaiman, N. S., Muhammad, A. F., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review. Social Sciences, 11(9), 386. https://doi.org/10.3390/socsci11090386

Symantec (2016). https://docs.broadcom.com/doc/increased-use-of-powershell-in-attacks-16-en

Think Fast: Time Between Disclosure, Patch Release and Vulnerability Exploitation — Intelligence for Vulnerability Management, Part Two | Mandiant. (2023). Retrieved 26 June 2023, from https://www.mandiant.com/resources/blog/time-between-disclosure-patch-release-and-vulnerability-exploitation

Vafaei-Zadeh, A., Thurasamy, R., & Hanifah, H. (2019). Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior. Kybernetes, 48(8), 1565-1585. https://doi.org/10.1108/K-05-2018-0226

Washington, T. M. (2023). Stakeholder Perceptions of the Organization's Information Security Policy: A Q Methodology Study to Support Evidence-Based Policymaking in the Federal Government (Order No. 30489766). Available from Publicly Available Content Database. (2813827805). https://www.proquest.com/dissertations-theses/stakeholder-perceptions-organization-s/docview/2813827805/se-2