Human Factors in Cybersecurity: Humans as a Weak Link to Malware Distribution

Alqarni Sami
Doctorate Student
Marymount University

ABSTRACT
This study investigates the impact of human factors in the context of malware distribution within the organization. Malware is often used to exploit human elements by making use of social engineering techniques. The paper explores the interplay between human elements and malware distribution. The study examines the psychological elements that makes it easier for bad actors to exploit humans into distributing the malware. The analysis of secondary research provides vital insights that will lead to the implementation of effective mitigating strategies. The findings of the selected studies demonstrate the fundamental ground truth. Human factors are the most neglected factors when compared to the technical elements when it comes to implementation of strategies that protect against cybersecurity attacks. The ground truth is supported by the fact that technical defenses are not often targeted because humans are easier to penetrate than the technical aspects. The findings demonstrate the need to implement a multi-approach that integrates technological strategies and gaining an understanding of how human vulnerabilities make it easier for bad actors to use social engineering techniques to distribute malware in a system.

Keywords
Malware, human behavior, vulnerabilities, human factors

1. INTRODUCTION
The cybersecurity landscape has changed because of new threats and focus on technical factors and ignoring the human factors. Malware is being deployed by attackers because they find it easier to use humans as a vulnerability rather than technical aspects which are hard to infiltrate [1]. Bad actors use social engineering to lure individuals into accepting malware on the systems. The link between human error and malware distribution creates the need to address human vulnerabilities. As much as there re technological defenses implemented to deal with the increased number of cybersecurity vulnerabilities, humans are the weakest link when it comes to dealing with issues on malware distribution.

Many cybersecurity incidents arise from lack of awareness [2]. It is easier for a personal to click a link sent to their email attachment without authenticating whether it is a malicious link or not. Some of the social engineering methods used by bad actors involves the use of emails, which use the identity of trusted persons or organizations. Once the malware is distributed in the targeted system, the bad actors will try to manipulate the cybersecurity security features for their gain. Understanding human factors is important in ensuring that the rising cases of malware attacks are mitigated. Integration of a multidisciplinary approach is important in mitigating the risks that might arise from malware distribution. There is need to create training programs within the organization that will ensure employees have awareness on how they can deal with risks related to malware. Moreover, the cybersecurity leadership should encourage employees to report any error that is likely to lead to a threat.

This paper seeks to investigate the role of human factors vulnerabilities and malware distribution. The particular area of focus is social engineering and ways it is used to exploit unsuspecting employees to distribute the malware. Organizational and cultural aspects will also be investigated to determine how individuals are susceptible to cyberattacks. The paper will use secondary research to provide insights on how human vulnerabilities can lead to malware distribution. Creating awareness and training employees on the importance of accountability of actions will assist to mitigate the use of social engineering tactics to target organizations.

In the digital era, cyberattacks are becoming unique and the human factors are the weakest link in maintaining a robust cybersecurity environment. To address the malware vulnerabilities, there is need to develop a multi-approach that involves the combination of technological and human elements. This research will investigate how humans are the weakest link in malware distribution.

The following are research questions for this study:

1. How does human vulnerabilities lead to the deployment of malware?
2. What are the human factors that are exploited to distribute malware?
3. What role does awareness training do in mitigating the challenges caused by malware distribution?

The questions seek to explore the elements of human factors that make it easier for bad actors to infiltrate the system. The questions will also help to identify specific factors such as awareness and bad practices in adhering to cybersecurity practices.

2. LITERATURE REVIEW
According to research studies, there are many vulnerabilities that are used by bad actors to distribute malware [3]. Emotional manipulation and behavioral aspects are some of the ways threat actors use to exploit employs into installing and distributing malware without suspecting. The reliance of authority individuals within the organization makes it easier for bad actors to instill fear or create trust that clicking a link that has been sent on email is safer to click. Persuasion is a key strategy that has been used to advance social engineering; the use of pop-ups and adverts makes it easy for employees to click the malicious links. Organizational culture is also another element that has seen malware distribution a common occurrence within the organization. Most organizations have weaker cybersecurity strategies which makes it easier to advance social engineering. The article demonstrates the importance of developing robust security measures to mitigate cybersecurity risks. There are different attack scenarios used to make use of human vulnerabilities; pretexting and phishing are some of the common attack methods that are employed by bad actors to exploit human vulnerabilities.

In addition, research demonstrates how attackers use technical and human elements in making their attacks successful [3]. Social

engineering is an effective strategy that attackers use as an entry point; once a malware has been distributed, the attacker will use payloads to maximize on the goals meant for the breach. The connection between human and technological factors demonstrates the importance of looking at ways human factors are the weakest link in advancing malware vulnerabilities. The paper provides recommendations that can be used to address the vulnerabilities. Implementation of training initiatives will help to educate persons on the importance of paying attention to their emotional underpinnings if they are to overcome the manipulation strategies employed by the bad actors. The study advocates for the importance of employing technical and human-centered approaches to deal with the threats caused by social engineering techniques.

Research explores the connection between human vulnerabilities and malware distribution [4]. The study employs a clinical trial in identifying how malware infections can have negative implications on an organization. The study specifically addresses the role of human behavior and how the technological elements have made it easier for the bad actors to advance their objectives. The study demonstrates the different ways user interactions create an enabling environment for malware to be distributed. For instance, most individuals fail to verify the authenticity of the sources that send them links on their emails. The failure to verify whether the links are malicious or not exposes an organization to heightened risks. The use of human psychology has made it easier to dupe employees into performing actions that create an enabling environment to deliver malware. A critical aspect noted is the lack of awareness among employees. Lack of awareness is undertaking an action without understanding its implications on the cybersecurity posture. While organizations use technical safeguards against malware threats, they fail to acknowledge the role humans play in exposing an organization to malware attacks. Weak passwords and visiting unsafe sites are often ways that malware attackers use to exploit systems. Many users also use single factor authentication and adoption of best practices, a reluctance that makes it easier for malware attackers to infiltrate the systems. The implementation of training programs will help to mitigate the rising cases of malware attacks due to human vulnerabilities.

Another research provides viable insights on the methods used by malware attackers to infiltrate the system [5]. Social engineering tactics such as phishing and pretexting are common methods that have been used in exploitation of emotions and urgency of the unsuspecting users. In most cases, the attackers will impersonate themselves into trusted entities. The attackers often take the advantage of the trusted entities to dupe unsuspecting individuals into performing an action that later creates an avenue for vulnerability of a system. The other method is the use of clickjacking using the pop-ups on the browsers. This method is most used to dupe individuals into installing malicious malware. The article demonstrates the role human factors play in creating an environment which makes it easier for attackers to infiltrate the system. It is important for organization to address the human vulnerabilities in cybersecurity posture of the organization by highlighting the importance of creating awareness and training that will enhance steadfast on actions that will likely jeopardize the security of the organization.

Research demonstrates the role of human factors and facilitation of an environment that makes it easier to distribute malware [6]. The research dwells on how human factors and limited cybersecurity protocols remain to be a major challenge to protect the organization against cybersecurity attacks. The study focuses on the healthcare sector, particularly how the attackers take advantage of impersonation to access healthcare systems. The attackers target healthcare settings because it is a high-stress sector, where making a rush decision might lead to a security lapse. The other thing is that most healthcare institutions do not have clear cybersecurity hygiene practices. Some of things that makes it easier to infiltrate the system is not limited to weak passwords and failure to confirm the authenticity of a person who sent an email. Lack of awareness and limited training opportunities have made it easy for attackers to target systems. There is need to develop cybersecurity measures that will help to deal with the intrusion of malware on a system. Having structured training programs will make it hard for attackers to exploit human vulnerabilities. Undertaking regular security updates will also make it hard for the attackers to exploit the system. It is important for organizations to encourage the implementation of cyber hygiene practices that will help in handling sensitive information, which is critical in addressing the cybersecurity risks. The findings of this study demonstrate the role of human factors and the proliferation of malware in the organization. Policy reform and investment in education programs will assist to enhance cybersecurity resilience within the organization.

Another study demonstrates the impact of cyberattacks in the evolving digital era [7]. The study terms humans as the weakest link that is exploited to gain access to sensitive information. Due to the widespread of internet usage and emerging technologies, attackers use malware for profit making ventures. Limited awareness on security issues has made it easier for attackers to stage the phishing scams. Cyber attackers stage phishing attacks on unsuspecting employees who end up performing actions that makes it easier to gain access to the systems. The study is study will add to the existing knowledge on ways organizations can position themselves to protect against cyber threats. To deal with malware distribution, organizations should integrate multi-factor authentication methods, network behavioral analysis, and regular updates on the system.

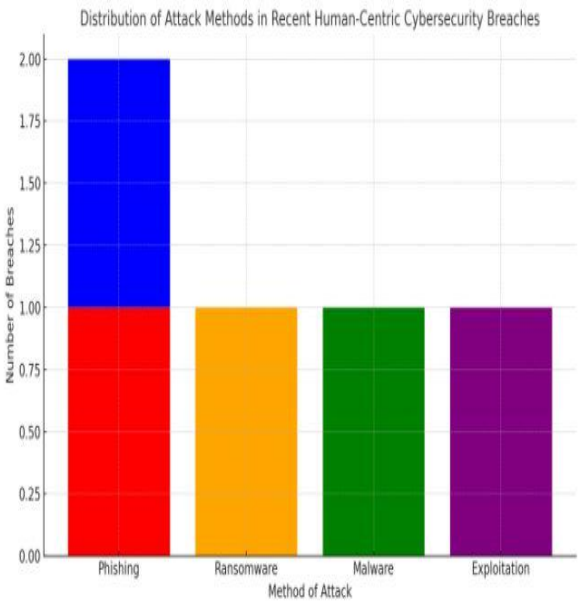

Figure 1: Attacks methods used by bad actors in cyberattacks

Research has shown that human factors in cybersecurity are important to address because the prevalence of human errors have become common [8]. The implementation of adequate security features is essential in ensuring that ensuring human factors are the least of concerns in causing cybersecurity vulnerabilities.

Cultivating a strong security posturing is vital in improving incident response and handling of cybersecurity breaches. Cybercriminals choose the type of attack to implement when they target individuals. The types of cybercrimes depend on the intentions of cybercriminals. Cyberattackers often target unsuspecting persons who often act without due diligence. Trickery and deceit are some of the social engineering techniques used by bad actors to achieve their objectives. The intention of the attackers is often to deceive and misdirect persons towards helping them achieve their end goal. For instance, a bad actor breaks into a phone provider account in 5 minutes. This is achieved by making a phone to the cell provider and impersonating the target, let say a wife to the person. In the background, there is a child crying to make sure the other person from the other end will have empathy and make it easier to manipulate the person on the class to provide unauthorized access.

Human factor is becoming a challenge because they contribute to the increased number of cybersecurity threats. Social engineering is often used by attackers to manipulate unsuspecting individuals into providing personal information by using social engineering methods [9]. The attacks often used psychological weaknesses to infiltrate systems that are well protected. Phishing is also another common technique that is employed by cyberattackers. In most cases, bad actors use deceptive emails that are used to trick persons into giving personal information. Despite the development f technology, phishing is still a threat that needs to be addressed. Another key factor to consider is the weak password practices. Many persons use weak and easy passwords in different accounts. This is easier for attackers to use in penetrating systems that are considered impossible to infiltrate.

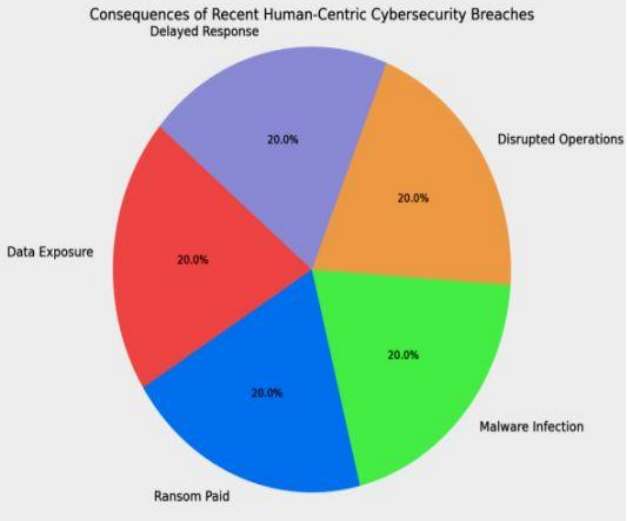

Figure 2: Human-Related Breaches in Organizations

The image illustrates the distribution of different attack techniques that are used in cybersecurity attacks.

3. METHODOLOGY

This section of the research study provides a detailed description of the sources used in this research. The study employs secondary research and integrates five articles from 20 articles that were analyzed; the articles selected provide key themes on how human vulnerabilities contribute to the integration of malware in the system. The selected articles were selected based on their relevance to the selected topic. The title and abstracts of the selected articles were evaluated to determine whether the research problem aligned to the topic under research. Articles selected were a great fit because the demonstrated different gaps that ought to be addressed and the foundation in which research is built upon.

The study examines the human factors that make it easy for attackers to infiltrate the cybersecurity environment. Research scholars provides viable insights through clinical-trials [4]. The study uses the clinical-trial to investigate how human elements in cybersecurity can lead to malware attacks. Exploring the human behaviors has demonstrated how users are exposed to different malware scenarios and the interactions between human and technical vulnerabilities. Another research conducts a systematic review which discusses the mechanisms that are used to advance social engineering and maps out how human vulnerabilities can be used in distribution of malware [3].

Research scholars critically evaluates the impact of human factors in the healthcare environment [6]. The study demonstrates how malwares are used to exploit the unique healthcare system. Nurse (2018) also conducts a systematic review of the methodologies that attackers use to exploit specific human behaviors when they want to distribute malware. Finally, another study illustrates the implications that human factors can have on the environment, especially the impact of human factors in advancing malware intrusion [7]. The dataset of the study is informed by the limitation of time to collect data using other methodologies.

The study uses secondary research as a method to collect key themes that relate to the study. In this context, the five sources were used to draw key patterns pertaining to human vulnerabilities that advance the distribution of malware in the system. This method proved efficient as it allowed for synthesis of key themes and ensuring a deeper understanding of key themes without having to undergo the hustle of primary collection of data. For this study, systematic reviews, journal articles, and conference papers were used as primary means to collect data. The collected methods were useful in providing evidence on the role of human factors in cybersecurity. The choice of the method is informed by the limitation of time. The secondary research provided a wealth of information within a short period of time. The application of secondary research allowed the analysis of ways human factors lead to the distribution of malware in the cybersecurity environment. It also ensures the insights shared provided ground truth based on the holistic perspective. The analysis of the research proved vital in that it allowed the analysis and discussion of solutions that will help mitigate the cybersecurity risks associated with the distribution of malware in the cybersecurity environment.

The research questions guided how the data drawn from the secondary research was analyzed and helped to draw the key themes. After ensuring the sources align with the identified research questions for the study, the researcher assessed the credibility and relevance of the secondary sources. The sources were categorized into peer-reviewed, systematic reviews, and conference papers. Data categorization was also done, whereby the selected articles were grouped into different focus groups such as human factors, social engineering, and organizational culture. This was a vital aspect when it came to identification of patterns across different sources.

Undertaking a thematic analysis also helped to identify some of the trends and common patterns on malware distribution owing to the vulnerabilities caused by humans. The comparison of common themes on human behavior and other systematic elements proved vital for the research. Another strategy used was to analyze the existing differences and similarities between the selected articles. For instance, some studies used experimental simulation while others used theoretical frameworks to demonstrate how human vulnerabilities was a breeding ground for malware intrusion in the organization.

Other scholars also looked at individual and group risks that affect

the ease at which vulnerabilities are exposed to the organization. The secondary research also benefitted from the qualitative and quantitative analysis. The combination of the two approaches was important in demonstrating how human factors can affect the infiltration of malwares in the system. Summary of key themes and synthesizing it across the selected sources prove vital in answering the research questions. Overall, the analysis of the sources involved the development of a structured way of evaluation and categorizing insights drawn from different literature studies. The integration of the findings proved vital in understanding the role that human factors have in infiltration of malware.

It is important to note that all the articles selected for the study were evaluated rigorously and their contribution counterchecked with the intext-citations used. Some of the studies were also selected because they provided clinical-based evidence on the impact of human error in decision-making and how it leads to increased cybersecurity vulnerabilities. Some of the studies also contextualized different attacks and best strategies that can be implemented to deal with cybersecurity vulnerabilities.

Credibility and reliability are also something that was considered for the selection of the articles. Peer-review articles and systematic reviews were integral in ensuring that the findings of the study are credible. The use of qualitative and quantitative findings in the study was integral in highlighting and understanding of how human vulnerabilities can affect the cybersecurity posture of an organization.

The methodology section also used a systematic approach to organize the collected data and perform an analysis of the research outcomes. The categorization of the articles in different themes was made to identify different points of agreement. The analysis of human vulnerabilities highlighted different vulnerabilities and research gaps that need to be addressed,

4. RESULTS

Research studies demonstrates that human factors are the major cause of malware distribution (Wang et al., 2021). Attackers are likely to exploit individual's cognitive biases and the emotional triggers that will make it easier for them to exploit the systems. A clear demonstration of the emotional response is the use of phishing attacks which use human trust in deceiving individuals into installing malicious links to the system. Methods such as pretexting and phishing have been repeatedly used by malware attackers to infiltrate a system [3]. Scholars term organizational elements as the main factors that lead to vulnerabilities [6]. Weak policies and inadequate cybersecurity measures have created cybersecurity environments that make it hard to recognize threats. One particular sector that is prone to cybersecurity threats, is the healthcare sector. In situations where legacy systems are integrated, cybersecurity threats are common because delivery of service is considered important than security policies. Scholars cite user interface as one of the factors that make it easier for attackers to distribute malware in the system [4]. Users often find it hard to navigate the complex interfaces, which make it possible to make an error. The poor decisions lead to security loopholes which can be exploited. Another study demonstrates the ways cultural and psychological elements lead to risky cybersecurity behaviors [7]. The human elements are important in demonstrating why malware attacks succeed even with deployment of technical defense. Malware often works bests when human targets are involved. Human provide easy access to the system by bypassing the different security measures.

Psychological factors have made it easier for attackers to exploits humans into installing malware into the system. Some of the common vulnerabilities includes click baits on some of the websites. The exploitation is often fruitful because it overcomes the logical process. The limited training programs have made it hard for organizations to deal with increased malware threats within the organization. Employees with lack of awareness are easily targeted. Technology aspects such as the design of the system can make it hard for the users to use the system.

The findings of the selected studies demonstrate the fundamental ground truth. Human factors are the most neglected factors when compared to the technical elements when it comes to implementation of strategies to protect against cybersecurity attacks. The ground truth is supported by the fact that technical defenses are not often targeted because humans are easier to penetrate than the technical aspects. Pretexting and phishing are common vulnerabilities which enable attackers to infiltrate the system [3]. The other element is that humans are easier targets because of the behaviors. It is easier for attackers to predict the behaviors of the attackers thus making it harder for the organization to deal with such threats.

Organizational issues have made it easier for bad actors to infiltrate systems using malwares. The implementation of weak cybersecurity policies has made it difficult for organizations to handle issues related to malware attacks [6]. In some organizations, cybersecurity is not viewed as a collective responsibility among employees rather it is viewed as a shared responsibility. This means, in case of a cybersecurity incident, some employees are likely to ignore any suspicious activity. The other key issue is that bad actors continue to change their skills on how they exploit humans. Attackers are now using artificial intelligence to stage attacks in the cybersecurity environment. Attackers are now developing personalized malwares which make it hard for employees to detect [5]. The use of AI has made it even harder to detect the phishing attempts because even the fake audio appears to be legitimate.

The human role in creating a vulnerability environment continues to be overlooked. The manipulation of human behavior and organizational challenges have made it easier for threat actors to thrive. It would be vital if every stakeholder concerned with cybersecurity could focus on education. Creating awareness and training programs will help employees to handle cybersecurity threats. The findings of the study demonstrate why it is important for organizations to integrate a holistic approach that will go a long way in dealing with the cybersecurity challenges.

5. CONCLUSION

This research study has added to the body of knowledge on the impact of human factors on the increased number of malware attacks. There are several issues such as psychological and organizational aspects that demonstrates why humans are the weakest link to cybersecurity vulnerabilities. The following table demonstrates key issues that make it easier for attackers to infiltrate the system.

Table 1: Table illustrates key themes related to cybersecurity risks

Theme	Key issues	Tactics	Psychological Factor	Mitigation strategy
Social engineering	Exploit user trust	Phishing emails	Trust in individuals with leadership	Awareness programs
Lack of awareness	Limited knowledge on cybersecurity risks	Clicking malicious links	Ignorance of actions	Training employees
Organizational culture	Weak cybersecurity policies	Complacent	Lack of accountability	Policy revisions
Technological factor	Outdated systems	Exploit outdated systems	Use of outdated systems	Regular audits and updates
Advanced methods	AI enabled attacks	Personalized attacks	Trust in personalized information which is not authentic	Advanced detection methods
Urgency and intimidation	Manipulation of user emotions	Urgent emails	Fear	Scenario simulations
System design	Complicated systems	Personalized attacks	Users lack of knowledge on how system works can undertake any action.	New user-friendly designs

The table demonstrates how attackers are manipulating specific aspects which are not limited to human factors and organizational culture. Employees will likely undertake an action if they receive an email that seems to be from a legitimate entity. Phishing is the most common technique that attackers use to dupe a person into allowing a malware into the system. Organizations need to build a security conscious workplace culture to mitigate the increased risks. Training programs will ensure organizations have way they can mitigate threats and respond to evolving attacks. Simplification of user interfaces will also ensure the errors within the system are minimized and attackers cannot capitalize on errors. The contribution of the study demonstrates how humans can also be used as integral assets to mitigate malware attacks. The contributions of the study have an impact on policy implementation and structuring of training programs.

The limitation of this study is the use of secondary research to provide insights in the topic and answering of the research questions. The insights provided can be applied in any sector as human vulnerabilities can be exploited at any level by the bad actors. The insights are drawn from theoretical perspectives. While most studies provide important insights, they lack empirical validation. There is not presentation of all geographies and a wider culture, something that might point to possible bias. The generalizability of the results might also be affected because there are differences when it comes to integration of technology. The volving nature of threats also makes it hard to develop a perspective and maintain relevance in the long run. This study will be integral to organizations which have placed emphasis on technical aspect while overlooking the human factors in terms of their role in distribution of malware.

6. REFERENCES

[1] J. Edwards, "Malware Defenses. In Critical Security Controls for Effective Cyber Defense: A Comprehensive Guide to CIS 18 Controls.," pp. 277-308, 2024.

[2] F. Ugbebor, O. Aina, M. Abass and D. Kushanu, "Employee cybersecurity awareness training programs customized for SME contexts to reduce human-error related security incidents.," Knowledge Learning and Science Technology, pp. 2959-6386, 2024.

[3] Z. Wang, H. Zhu and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods.," pp. 11895-11910., 2021.

[4] F. Lévesque, S. Chiasson, A. Somayaji and J. Fernandez, "Technological and human factors of malware attacks: A computer security clinical trial approach. ACM Transactions on Privacy and Security," 2018.

[5] J. Nurse, "Cybercrime and you: How criminals attack and the

human factors that they seek to exploit.," 2018.

[6] S. Nifakos, K. Chandramouli, C. Nikolaou, P. Papachristou, S. Koch, E. Panaousis and S. Bonacina, " Influence of human factors on cyber securitywithin healthcareorganisations: A systematic review," Security Science Journal, vol. 2, 2021.

[7] E. Kadena and M. Gupi, "Human factors in cybersecurity: Risks and impacts.," Security science, vol. 2, pp. 51-64., 2021.

[8] L. Thirupathi, B. Vasundara, D. Sundaragiri, R. Gugulothu and R. Pulyala, "Understanding and Addressing Human Factors in Cybersecurity Vulnerabilities. In Human Impact on Security and Privacy: Network and Human Security, Social Media.," 2025.

[9] G. Ayodele, L. Abdulrahman, J. Alebiosu, G. Egdebion and O. Akinbolajo, "Human-Centric Cybersecurity: Addressing the Human Factor in Cyber Defense Strategies.," 2025.