International Journal of Business and Management Invention (IJBMI)
ISSN (Online): 2319 – 8028, ISSN (Print): 2319 – 801X
www.ijbmi.org || Volume 13 Issue 3 || March, 2024 || PP—123-130

Reducing Risk on Mobile Devices in Academics: A Quantitative Study

Nicole Hoy[1], Dr. Douglas Capellman, CISSP[2]
[1](Capitol Technology University, United States)
[2](Capitol Technology University, United States)

ABSTRACT: *The paper "Reducing Risk on Mobile Devices in Academics: A Quantitative Study" delves into the growing menace of mobile ransomware in academic institutions and explores the various methods cybercriminals use to target mobile devices. It discusses the potential consequences of such attacks and the strategies educational institutions can employ to mitigate the risks associated with mobile ransomware. The study aims to answer the research question: to what extent do institutional security controls impact risk introduced by using mobile devices in the organization? The paper also provides insights into the significance of the study, hypothesis, literature review, methodology, data collection, and analysis and concludes with a discussion of the findings and recommendations for further research. The study is significant as it addresses a threat vector not actively discussed in the Information Technology sector and contributes to the Information Security community by providing new information.*

KEYWORDS – *Academics, Mobile, Malware, NIST, Ransomware, Risk Management*

Date of Submission: 15-03-2024 Date of acceptance: 30-03-2024

I. INTRODUCTION

With the increasing popularity and reliance on mobile technology, academic institutions have also embraced using mobile devices for educational purposes. However, this widespread adoption of mobile devices has opened new avenues for cybercriminals to exploit vulnerabilities and launch attacks.

One such threat is mobile ransomware, malicious software that infiltrates mobile devices, encrypts files and holds them hostage until a ransom is paid. Mobile ransomware attacks have become a significant concern for academic institutions, as they can disrupt critical operations, compromise sensitive data, and impact the overall productivity of students and staff.

This paper aims to explore the growing menace of mobile ransomware in academic institutions. It will delve into the various methods cybercriminals use to target mobile devices, the potential consequences of such attacks, and the strategies educational institutions can employ to mitigate the risks associated with mobile ransomware. By understanding the nature of this threat and implementing effective preventive measures, academic institutions can safeguard their mobile infrastructure and protect their valuable resources from the clutches of ransomware attacks.

II. PROBLEM STATEMENT

The problem is that there are not enough security controls and policies in place to prevent mobile ransomware from spreading, which is a threat that is growing more and more. According to the 2021 Mobile Threat Report published by McAfee, the number of ransomware attacks occurring on mobile devices rose by 54 percent in 2020 compared to the previous year (McAfee, 2021) [1]. Due to insufficient security measures, academic organizations frequently fail to recognize the potential dangers of ransomware, although mobile devices are increasingly dependent on it for various purposes. Individuals and businesses alike are susceptible to ransomware attacks on mobile devices. In 2020, the number of mobile ransomware attacks carried out against organizations increased by 123 percent, as stated in a report by Check Point (Checkpoint, 2021) [2]. There is a possibility that sensitive information, financial data, and the functionality of mobile devices could be compromised due to this issue.

For this reason, it is necessary to have a comprehensive understanding of the characteristics of mobile ransomware and its potential impacts and to put robust security measures in place to protect mobile devices from these kinds of attacks. The general issue is insufficient security controls and policies to safeguard against mobile ransomware, which is becoming an increasingly dangerous threat. As a result of inadequate security measures, academic organizations frequently fail to recognize the potential dangers posed by ransomware, putting sensitive information, financial data, and the functionality of mobile devices at Risk (Green, 2007) [3]. The problem is that academic organizations frequently do not have adequate security controls and policies for

their mobile devices, which leaves them open to ransomware attacks. Mobile ransomware is often not considered to be a significant threat by the security controls and policies that are currently in place. As a result, a lack of coverage is necessary to prevent attacks of this nature (Green, 2007) [3].

III. Background

Every eleven seconds, a ransomware attack takes place, and each one of these attacks costs victims, on average, nineteen days of network downtime and a payout of more than $230,000. In 2021, the global costs associated with ransomware recovery exceeded $20 billion (Lubin, 2022) [4]. Many mobile users do not use antivirus software, are unaware of the dangers associated with mobile platforms, and frequently do not take measures to protect themselves (Haas, 2015) [5]. The total number of app downloads reached 178.1 billion in 2017 alone (Koyuncu & Pusatli, 2019, p. 1) [6].

According to the most recent data, third-party app stores were responsible for 99.9 percent of all mobile malware discovered (PurpleSec, 2020) [7]. On the other hand, 57 percent of mobile users are unaware that protection software shields them from security risks associated with mobile devices (Haas, 2015) [5]. It is possible for users to unknowingly spread any number of viruses or threats when they connect a device to the company's network using Wi-Fi or another method. This poses a risk to the company's network security. Furthermore, users can perpetuate these dangers on their own. This is because users are not aware of the potential risks involved within the system (Kazmeyer, 2016) [8]. When this is considered, it is necessary to protect mobile devices from ransomware (Kazmeyer, 2016) [8]. It comes to downloading applications on their devices and implementing behavioral controls to encourage users to change their behavior (Haas, 2015; Kazmeyer, 2016) [5], [8].

Recently, ransomware has emerged as one of the threats in the mobile space, and it is growing at the fastest rate, primarily because it is potentially profitable (Mohan & Kumar, 2017) [9]. A piece of ransomware known as LeakerLocker for Android devices was released on the Google Play Store in 2017. (Samuels, 2017) [10]. Wallpapers Blur HD, an application that alters wallpapers, and Booster and Cleaner Pro, which boosts memory, were the two applications it concealed behind (Samuels, 2017) [10]. LeakerLocker did not encrypt the devices; instead, it locked them and threatened to spread any sensitive information discovered on them (Samuels, 2017) [10]. These applications were discovered by McAfee, who then alerted Google to their existence. Almost immediately after that, the applications were removed from the Google Play Store store (Samuels, 2017) [10]. Academic organizations are subject to different security restrictions, and these criminal applications and compliance rules face increasing difficulty. With the growth of Apple and Android space and mobile users continuing to bring their devices into the office and freely connect to Wi-Fi, these academic organizations are continually at risk (Paterson, 2014) [11].

For Android users, the problem is compounded due to the open nature of the Android platform and its support for open app marketplaces. The growing shift towards a mobile-first approach has elevated the importance of securing the vast mobile attack surface (Mohan & Kumar, 2017, p. 115) [9]. The open architecture nature of Android is particularly crucial for businesses to understand from a technological standpoint. Many enterprises have cellular devices on the corporate organizational infrastructure that are often unpatched, unmanaged, and not corporate-owned (Bullock, 2019) [12]. Ransomware is malicious software that can encrypt, lock, or lock the files on the target device (Fruhlinger, 2018) [13]. These attacks can generate mobile ransomware or ransomware from phishing emails and target mobile devices on corporate networks.

When considering technical controls against ransomware, Oberly (2019) [14] says that performing regular system backups on the corporate network is one of the best practices for preventing ransomware. Specifically, Oberly has found backups of networked devices such as laptops, desktops, and servers, not cellular devices. Oberly finds that the company can effectively restore from a backup without paying the ransom from the attacker with proper backups. While this technical security control works most of the time, sometimes, backups may not be enough of a technical control (Harris, 2010) [15].

Technical security controls are only half of the equation. The other half of the equation includes behavioral controls and understanding how to incorporate those into the corporate networks. The National Institute of Standards and Technology (NIST) discusses behavioral controls in publication 800-53, rule number PL-4, where it discusses that an organization must provide rules and guidelines for how a person must handle systems and the expected behavior regarding those systems (National Institute of Standards and Technology, 2015) [16]. This quantitative ANOVA analysis study aims to answer the following questions: to what extent do institutional security controls impact risk introduced by using mobile devices in the organization?

IV. Significance of Study

The business problem is that academic organizations often lack proper security controls and policies regarding their mobile devices; as a result, mobile ransomware is an active threat vector (Green, 2007) [3]. This business problem addresses the following questions: To what extent do institutional security controls impact risk introduced by utilizing mobile devices in the organization?

The significance of the study is that it provides a view into a threat vector that is not currently actively discussed in the information technology sector. In addition to bringing to light a new threat vector that is not currently at the forefront of the community's attention, the researcher has the potential to contribute to the Information Security community by providing new information. Even though several behavioral controls are in place to prevent such behaviors, the additional significance of this academic study is that it will provide the researcher with a better understanding of how and why mobile ransomware is installed on devices. The findings of this study will lead to the discussion of a novel subject within the realm of cybersecurity within the academic community. Although ransomware is a primary topic of debate within the cybersecurity industry, mobile ransomware frequently goes undetected, which results in a significant gap in research capabilities.

V. Hypothesis/Research Questions

The research question is to what extent do institutional security controls impact risk introduced by the utilization of mobile devices in the organization?

The hypothesis is:

H10: Institutional security controls do not have a significant impact on risk introduced by using mobile devices in the organization.

H1a Institutional security controls do have a significant impact on risk introduced by using mobile devices in the organization.

The purpose of this question and hypothesis is to drive the quantitative study directly. Additionally, this question will guide the research and how the researcher will ultimately perform the overarching analysis.

VI. Literature Review

The UTAUT, or Unified Theory of Acceptance and Use of Technology model, argues that the actual use of technology is determined by the individuals' intentions regarding their behavior. It is necessary to consider the direct impact of four fundamental constructs to ascertain the perceived likelihood of adopting the technology. These constructs are performance expectancy, effort expectancy, social influence, and facilitating conditions. The impact of predictors is moderated by factors such as age, gender, experience, and the degree to which use is voluntary. (Venkatesh et al., 2003; Marikyan, D. & Papagiannidis, S. 2023) [17]; [18]The reason for utilizing the UTAUT vs. Technology Acceptance Model (TAM) or another model is that UTAUT performs a deeper analysis of human behavior.

According to the information security industry, the rate of ransomware attacks has been steadily increasing since 2014. It has increased significantly from 3.2 million in 2014 to 204.24 million in 2018. According to Statista (2019) [19], Computers, laptops, smartphones, and other mobile devices are the platforms targeted by malicious ransomware software (Fruhlinger, 2018) [13]. The device may be locked, encrypted, or cryptographically locked in exchange for a ransom payment. These options are possible (Fruhlinger, 2018) [13]. Ransomware was initially introduced this way (Fruhlinger, 2018) [13]. As its name suggests, the lock restricts file access (Fruhlinger, 2018) [13]. Information or the device can be encrypted and stored in a crypto locker for safekeeping. Mobile space has been penetrated by malicious software (Fruhlinger, 2018) [13].

Many people use cellular or mobile equipment today (Pew Research, 2019) [20]. Over 5 billion individuals are thought to own mobile devices, with smartphones accounting for over half of those (Silver, 2019) [21]. Because the typical user of these gadgets does not care about protecting their mobile device, this opens a new threat vector for adversaries (Haas, 2015) [5]. Individuals who use mobile devices and businesses have been forced to rely heavily on these electronic items because of the portability of these devices and the fact that their technology is constantly evolving (Tripwire, 2016) [22]. The increased functionality of mobile devices has enabled them to perform various previously inconceivable tasks. These tasks include accessing the internet, scheduling appointments, generating reminders, exchanging files, instant messaging, video chatting, and mobile banking. Individuals who use mobile devices and businesses have been forced to rely heavily on these electronic items because of the portability of these devices and the fact that their technology is constantly evolving (Tripwire, 2016) [22]. The increased functionality of mobile devices has enabled them to perform various previously inconceivable tasks. These tasks include accessing the internet, scheduling appointments, generating reminders, exchanging files, instant messaging, video chatting, and mobile banking (Tripwire, 2016) [22]. Mobile devices have many features, but they are incredibly vulnerable to online threats because of their portability and vulnerability to physical attacks (Tripwire, 2016) [22]. Malware with a specific mobile device

design is among the security risks. Data extraction from mobile devices is possible through viruses and malware, unauthorized access, phishing scams, and theft (Tripwire, 2016) [22].

IT professionals do not understand why people who own and use these devices can download these harmful apps even though they know they are dangerous (Haas, 2015) [5]. There were 5,321,142 malicious mobile installation packages found in 2018, 409,774 less than in 2019. (Chebyshev, 2019) [23]. Chebyshev (2019) [23] says that although malware is becoming less common, the number of attacks using malicious mobile software doubled in 2018—116.5 million of these attacks (against 66.4 million in 2017). So, technologists must set up security controls and policies to stop users from doing these things.

Ransomware for mobile devices did not become a problem until FakeDefender hit the Android market in 2013. (NJCCIC, 2016) [24]. This malware showed the user fake security alerts to get them to buy an app to eliminate counterfeit threats (NJCCIC, 2016) [24]. Malware has sometimes stopped users from getting rid of it and opening other programs (Power, 2018) [25].

Before 2013, there was malware for mobile devices. In 2004, a virus called Cabir was called Mosquitos-Trojan.Mos is a mobile malware game that appeared soon after Cabir for Symbian devices in 2004. Skuller, which was annoying malware that hurt and made it hard to use the device, was also released in 2004. (Clooke, 2016) [26] In 2005, Symbian devices could use CommWarrior. In 2006, RedBrowser was the first mobile device malware that worked on multiple platforms. It worked on any phone that could run Java 2 Mobile Edition (Power, 2018) [25]. FlexiSpy came out in 2007 and claimed to be able to spy on someone's partner. However, once downloaded, this software collected SMS messages, recorded phone calls from the affected phone, and sent the information to the attacker (Power, 2018) [25].

Ransomware has been known to get on mobile devices through apps that look safe in the Apple Store or the Google Play Store. This is similar to how other types of malware get on mobile devices (Haas, 2015) [5]. Even though these apps look safe, they contain malicious code that waits to run when the app is opened or downloaded onto the target device (Haas, 2015; PurpleSec, 2020) [5]; [7]. Many apps will also use the auto-update feature to send more malware or ransomware attacks to these devices (PurpleSec, 2020) [7]. It is essential to know that ransomware is on the user's device, even if they do not realize it (Haas, 2015) [5]. This dangerous software can often stay dormant on a device, whether an Apple or an Android. Recent statistics show that mobile malware is on the rise. In 2018, new malware variants grew by 54 percent, 99.9 percent of mobile malware was found in third-party app stores, and Trojan-Banker attacked over 250,000 users (PurpleSec, 2020) [7]. AndroidOS.Asacub is a malicious program (PurpleSec, 2020) [7]. 98 percent of malware for mobile devices goes after Android devices (PurpleSec, 2020) [7].

The most important way to attack is through people (Jang-Jaccard & Nepal, 2014) [27]. Since people are involved, the need for security controls and policies keeps growing. When malicious actors go after a business, they go after the person first, not the computer or the phone (Jang-Jaccard & Nepal, 2014) [27]. Cybercrime victims are also increasing at a high-speed rate. A survey by Symantec talked to 20,000 people from 24 countries. Of those people, 69% said they had been the victim of a cyber incident at some point. Symantec also found that 14 people are attacked online every second, adding up to more than a million daily attacks (Jang-Jaccard & Nepal, 2014) [27]. The enemy goes after a person because that person clicks on the link to install the dangerous software or goes to the hazardous site, where the problem starts (Fruhlinger, 2018) [13].

When individuals download a ransomware application, they can pay the ransom or lose their phone to the adversary. If the device is corporate-owned, this poses a more considerable risk to the organization, and this needs further investigation by the corporation (Datta, 2019) [28]. The scenario presented previously requires more robust security policies and controls to prevent the behavior, where UTAUT becomes imperative.

In the information security field, mobile ransomware is actively being studied. The mobile device itself is a risky hazard that businesses must work to mitigate or risk potential security breaches owing to a lack of safeguards (Zurkus, 2019)[29]. This problem appears to be a risk management problem. Many private-sector companies use the risk management framework developed by NIST. This approach enables these businesses to implement security rules that are both measurable and mature. The NIST risk management framework, detailed in NIST document 800-124, explains how to handle mobile devices. According to the National Institute of Standards and Technology, connected devices such as smartphones and tablets must generally satisfy various security objectives: confidentiality, integrity, and availability. To meet these goals, NIST recommends protecting mobile devices against multiple risks.

NIST's term "connected device" refers to any associated device attached to the network. This term refers to mobile devices, PDAs (Personal Digital Assistants), or tablets (National Institute of Standards and Technology, 2015) [30]. These are not conference phones, desktop computers, security cameras, laptops, or servers, which also can connect to the network. The NIST Publication, 800-124, mentions the CIA triangle and the connected devices to support multiple security objectives, specifically referencing Mobile Device Management (MDM). This reference indicates that an organization should employ an MDM program to handle its mobile devices, PDAs, or tablets. Additionally, many organizations in the United States are using the NIST

framework to create more robust security policies and robust security controls and to work through any barriers they encounter regarding user behavior.

Using a quantitative ANOVA analysis method to perform this study allows for those who are current practitioners to provide insight into research and drive change within the Information Security community. For this quantitative ANOVA analysis study, the structure is a survey. This survey collected data from 250 participants.

Before contemplating whether to utilize risk management or implement constraints around behavioral controls and, more specifically, how to enforce NIST suggestions about mobile devices, NIST makes recommendations and suggestions on the sensitivity of the item, among other considerations that should be discussed before implementation.

NIST has another publication, 800-53, which speaks directly to the technical controls. The above-referenced publication is specific to guidelines and speaks to the best practices when handling mobile devices in the corporate environment.

Mobile ransomware has emerged as a significant cybersecurity threat, targeting individuals and organizations. As the usage of mobile devices continues to grow exponentially, the risk of ransomware attacks also increases. This literature review explores the current state of knowledge on mobile ransomware, explicitly focusing on the insights provided by the National Institute of Standards and Technology (NIST) through their publications and collaborations.

Detecting mobile ransomware attacks requires identifying the source of the affected systems and collecting sufficient data for impact analysis (Franklin et al., 2019) [31]. NIST's Cybersecurity Practice Guide addresses this by providing a reference design for enterprise-class protection for mobile devices accessing corporate resources (Franklin et al., 2019) [31]. The guide offers practical solutions based on standards and best practices, enabling organizations to implement an effective enterprise mobility management solution.

Risk Assessment and Mitigation Techniques: To mitigate the risks posed by mobile ransomware, organizations need appropriate actions during a detected data integrity attack (Cawthra et al., 2020) [33]. NIST's collaboration with industry organizations, government agencies, and academic institutions through the NCCoE facilitates the development of solutions that detect and respond to data integrity attacks (Franklin et al., 2019) [31]. These solutions aim to guide how to respond to ongoing cybersecurity events and enhance an organization's ability to act during an attack.

NIST acknowledges the increasing complexity of cyber threats and emphasizes the need for organizations to have the necessary tools to combat these attacks (Franklin et al., 2019) [31]. Through collaborations with vendors like Cisco, Glasswall Solutions, and Symantec, NIST's NCCoE develops and implements best practices for detecting and responding to mobile ransomware attacks (Franklin et al., 2019) [31]. These collaborations ensure that the solutions provided are based on commercially available products and are practical for real-world implementation (Franklin et al., 2019) [31].

Mobile ransomware significantly threatens the integrity and security of an organization's infrastructure and data. Organizations remain vulnerable to these attacks without proper detection and response solutions (Franklin et al., 2019) [31]. NIST's guidance and research on mobile ransomware help organizations understand the evolving threat landscape and implement adequate security measures.

Ransomware targeting mobile devices is becoming an increasing concern for individuals and organizations. Utilizing the insights provided by the National Institute of Standards and Technology (NIST) through their publications and collaborations is essential to better understanding mobile ransomware and implementing effective security measures. Organizations can develop appropriate actions, evaluate risks, collaborate with industry partners, and adopt best practices to detect, respond to, and mitigate the threat of mobile ransomware attacks if they follow the guidance provided by the National Institute of Standards and Technology (NIST).

VII. Methodology

The risk level introduced by mobile devices is the dependent variable for these research questions and hypotheses about the topic. The index of risk is the dependent variable. It is a continuous numerical variable that can be calculated as the average numerical/ordinal response to the seven questions in the questionnaire. The control factors (related to demographics, organizational attributes, and the presence or utilization of institutional security controls and policies) are categorical variables, meaning that each factor has a set of possible values specific to that variable alone. Utilizing purposeful sequential model-building, the statistical method known as univariate analysis of variance (ANOVA) is used to (a) develop a predictive risk model and (b) compare the relationships between the dependent variable and the control factors and their two-factor interactions.

To collect information, the researcher used SurveyMonkey, a well-known online survey platform, to conduct an online poll and collect responses. To collect quantitative responses, the survey only contained

closed-ended questions. The answers to the closed-ended questions were used for statistical analysis and provided in-depth insights into the participants' experiences and perceptions of mobile ransomware.

The survey was distributed through various channels to ensure that it received a high response rate and a representative sample. Platforms for social media, online forums, email lists, and targeted advertisements are examples of the utilized channels.

Following the conclusion of the phase devoted to data collection, the information obtained was analyzed utilizing statistical techniques. The quantitative data from the closed-ended questions was analyzed using descriptive statistics and inferential analysis to identify patterns and relationships between the variables. These findings will provide insights into the prevalence of mobile ransomware and contribute to understanding how cellular devices are used in academic environments.

VIII. Data Collection and Data Analysis

The original data set for the academic sector comprised n = 46 respondents. This number was insufficient for conducting ANOVA with 11 categorical predictors. Therefore, the analysis was run using bootstrapping with 10,000 samples.

We ran an initial ANOVA with the complete set of CFs to perform a preliminary test of assumptions, using the SPSS General Linear Model & Univariate method (one Dependent Variable (DV)). We selected the numerical DV (Risk) and the 11 categorical CFs as fixed factors. We built the model terms and chose the Type III sum of squares. We selected post hoc homogeneity tests (Levene's test) and saved unstandardized residuals.

We tested the null hypotheses for the final model (no difference in DV means for each level of that factor) using a significance level equal to the variable inclusion criterion (.20). For each CF in the final model, we rejected the null hypothesis. We concluded that there is a difference in mean risk values for different levels of Question 7, Question 16, Question 18, and Question 20.

Predicted values of the DV can be compared to actual values from the data set to validate the predictive, mathematical model. As an example, risk can be predicted for the case when Q7 (organization size) = SML (small), Q16 = GREAT (a great extent), Q18 = X_NEUTR (neutral), and Q20 = X_WKLY (weekly).

IX. Data Discussion and Recommendations for Further Research

This article discussed the problem statement: mobile ransomware is often not considered a threat due to current security controls and policies; however, many policies lack the coverage necessary to prevent mobile ransomware. (Green, 2007) [3]. It also addressed the hypothesis that was H10: Institutional security controls do not significantly impact risk introduced by using mobile devices in the organization. H1a Institutional security controls do have a significant impact on risk introduced by using mobile devices in the organization.

The null hypothesis was presented and found to be false. In this case, the alternative was confirmed, which is that the security controls have a significant impact on risk introduced by using mobile devices in the organization. We tested the null hypotheses for the final model using a significance level equal to the variable inclusion criterion (.20). For each CF in the final model, we rejected the null hypothesis.

The implications for the academic sector industry are that organizations must start paying closer attention to their mobile devices and how they are managed. Mobile devices present a more significant attack vector than previously discovered, and the risk associated with these devices is not tiny. The fact that academic organizations do not often have policies to mitigate the risk is an area of study that can be continued with further research. Additionally, other sectors can be investigated, such as the non-profit sector, their utilization of mobile devices on their networks, and the implications that they may have.

Additional recommendations for future research include investigating the effectiveness of different anti-malware software solutions in preventing mobile ransomware attacks. Compare their detection rates, response times, and overall performance to identify the most reliable options. Explore the impact of user awareness and education programs on reducing the risk of mobile ransomware. Assess the effectiveness of training initiatives in improving user behavior and promoting safe mobile device practices.

Examine the role of organizational security policies and controls in mitigating the risk of mobile ransomware. Analyze the effectiveness of different policy frameworks and control measures in preventing and responding to ransomware attacks. Investigate the relationship between mobile device updates and vulnerability to ransomware attacks. Assess the frequency and timeliness of updates and their impact on device security and resilience against ransomware threats. Explore the effectiveness of mobile device management (MDM) solutions in preventing and detecting ransomware attacks.

Evaluate the features and capabilities of MDM platforms in securing mobile devices and mitigating the risk of ransomware infections. Investigate the impact of mobile ransomware attacks on different industries and sectors. Analyze ransomware incidents' financial, operational, and reputational consequences to understand the actual cost and implications for organizations. Examine the evolving tactics and techniques used by ransomware attackers targeting mobile devices. Stay updated on threat actors' latest trends and strategies to develop effective countermeasures and proactive defense mechanisms.

Investigate the potential of machine learning and artificial intelligence algorithms in detecting and mitigating mobile ransomware attacks. Explore using advanced analytics and predictive models to identify ransomware patterns and enhance threat detection capabilities. Assess the effectiveness of backup and recovery strategies in mitigating the impact of mobile ransomware attacks. Analyze different backup solutions and recovery processes to ensure organizations can quickly restore their systems and data in the event of an attack. Finally, explore the legal and regulatory aspects related to mobile ransomware. Investigate the legal frameworks and compliance requirements organizations must adhere to to protect themselves from ransomware attacks and ensure data privacy and security.

X. CONCLUSION

In conclusion, the paper sheds light on the critical issue of mobile ransomware in academic institutions and emphasizes the need for robust security controls and policies to safeguard against this growing threat. The study's findings have debunked the hypothesis that institutional security controls do not significantly impact the risk introduced by using mobile devices in the organization, highlighting the importance of effective security measures. The literature review provided insights into the Unified Theory of Acceptance and Use of Technology model, the increasing complexity of cyber threats, and the significance of NIST's guidance in combating ransomware attacks. The methodology employed a quantitative ANOVA analysis, and the data collection and analysis revealed patterns and relationships between variables, providing valuable insights into the prevalence of mobile ransomware. The paper concludes by recommending further research in this area and emphasizes the significance of addressing mobile ransomware as a critical cybersecurity concern in academic institutions.

REFERENCES

[1] McAfee (2021) https://www.mcafee.com/content/dam/global/infographics/McAfeeMobileThreatReport2021.pdf

[2] Checkpoint (2021) https://resources.checkpoint.com/cyber-attack-prevention-kit/ransomware-attacks-continue-to-surge-hitting-a-93-increase-year-over-year

[3] Green, A. (2007). Management of security policies for mobile devices. Proceedings of the 4th Annual Conference on Information Security Curriculum Development - InfoSecCD '07. ACM. 10.1145/1409908.1409933

[4] Lubin, A. (2022) The Law and Politics of Ransomware https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=4065&context=facpub

[5] Haas, P. D. (2015). Ransomware goes mobile: An analysis of the threats posed by emerging methods (dissertation).

[6] Koyuncu, M., & Pusatli, T. (2019). Security awareness level of smartphone users: An exploratory case study. Mobile Information Systems, 2019, 1–11. https://doi.org/10.1155/2019/2786913

[7] PurpleSec. (2020, August 6). 2019 cyber security statistics trends & data. PurpleSec. https://purplesec.us/resources/cyber-security-statistics/

[8] Kazmeyer, M. (2016, October 26). Can viruses spread over Wi-Fi? Small Business. https://smallbusiness.chron.com/can-viruses-spread-over-wifi-75136.html

[9] Mohan, J. C., & Kumar, R. C. (2017). On the efficacy of android ransomware detection techniques: A survey. International Journal of Pure and Applied Mathematics, 115(8), 115–120.

[10] Samuels, M. (2017, July 11). New leakerlocker ransomware puts Android users at risk. Security Intelligence. https://securityintelligence.com/news/new-leakerlocker-ransomware-puts-android-users-at-risk/

[11] Paterson, J. (2014, November 7). 3 ways your mobile device is putting your company at risk. Zimperium. https://blog.zimperium.com/is-your-mobile-device-putting-your-company-at-risk/

[12] Bullock, L. (2019, January 21). The future of BYOD: Statistics, predictions and best practices to prep for the future. Forbes. https://www.forbes.com/sites/lilachbullock/2019/01/21/the-future-of-byod-statistics-predictions-and-best-practices-to-prep-for-the-future/

[13] Fruhlinger, J. (2018, December 19). Ransomware explained. How it works and how to remove it. CSO Online. https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

[14] Oberly, D. J. (2019). Best practices for effectively defending against ransomware cyber attacks. Intellectual Property & Technology Law Journal, 31(7), 17–20.

[15] Harris, R. (2010, May 28). Why backup isn't enough. ZDNet. https://www.zdnet.com/article/why-backup-isnt-enough/

[16] National Institute of Standards and Technology. (2015, January 22). NIST special publication 800-53 (rev. 4). https://nvd.nist.gov/800-53/Rev4/control/PL-4

[17] Venkatesh, V., Thong, J., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. Journal of the Association for Information Systems, 17(5), 328–376. doi:10.17705/1jais.00428

[18] Marikyan, D. & Papagiannidis, S. (2023) Technology Acceptance Model: A review. In S. Papagiannidis (Ed), TheoryHub Book. Available at https://open.ncl.ac.uk / ISBN: 9781739604400

[19] Statistia. (2019, January). Number of ransomware attacks per year 2018. Statista. https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

[20] Pew Research (2019). https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/

[21] Silver, L. (2019, February 5). Smartphone ownership is growing rapidly around the world, but not always equally.

[22] Tripwire. (2016, November 29). How to secure your mobile device in six steps. Tripwire. https://www.tripwire.com/state-of-security/security-data-protection/secure-mobile-device-six-steps/
[23] Chebyshev, V. (2019, March 5). Mobile malware evolution 2018. Secure List. https://securelist.com/mobile-malware-evolution-2018/89689/
[24] NJCCIC. (2016, November 8). FakeDefender. NJCCIC. https://www.cyber.nj.gov/threat-center/threat-profiles/android-malware-variants/gazon
[25] Power, J.-P. (2018, April 13). Maliciously mobile: A brief history of mobile malware. Medium. https://medium.com/threat-intel/mobile-malware-infosec-history-70f3fcaa61c8
[26] Clooke, R. (2016). A brief history of mobile malware. Retail Dive. https://www.retaildive.com/ex/mobilecommercedaily/a-brief-history-of-mobile-malware
[27] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. doi:10.1016/j.jcss.2014.02.005
[28] Datta, S. (2019, November 26). Information security: Corporate-owned devices vs employee-owned devices. Security Boulevard. https://securityboulevard.com/2019/11/information-security-corporate-owned-devices-vs-employee-owned-devices/
[29] Zurkus, K. (2019, January 7). Is it time for enterprises to bid farewell to byod? Security Intelligence. https://securityintelligence.com/is-it-time-for-enterprises-to-bid-farewell-to-byod/
[30] National Institute of Standards and Technology. (2015, January 22). NIST special publication 800-53 (rev. 4). https://nvd.nist.gov/800-53/Rev4/control/PL-4
[31] Franklin, J., Bowler, K., Brown, C., Dog, S. E., Edwards, S., McNab, N., & Steele, M. (2019, February 5). Mobile Device Security. NIST SPECIAL PUBLICATION 1800-4B. https://www.nccoe.nist.gov/publication/1800-4/VolB/