International Journal of Business and Management Invention (IJBMI)
ISSN (Online): 2319 – 8028, ISSN (Print): 2319 – 801X
www.ijbmi.org || Volume 13 Issue 5 || May, 2024 || PP: 81-86

Publicly Traded Companies – Mobile Ransomware A Threat?: 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 article discusses the increasing threat of mobile ransomware in corporate environments, particularly in publicly traded organizations in the United States. It explores the impact of institutional security controls and policies on the risk introduced by the utilization of mobile devices in these organizations. The study sheds light on a new threat vector not actively discussed in the information technology sector and provides valuable insights into the significance of mobile ransomware as a risk management problem. The research employs a quantitative ANOVA analysis method, using a survey to collect data from 250 participants. The findings reveal that institutional security controls significantly impact the risk introduced by using mobile devices in the organization. The implications for the public sector industry are highlighted, emphasizing the need for closer attention to mobile device management and security. The article also presents recommendations for further research, including the effectiveness of anti-malware software solutions, user awareness and education programs, and the impact of mobile ransomware attacks on various sectors and industries. Overall, the study contributes to the information security community by addressing a critical gap in research on mobile ransomware and its implications for organizational security.*

KEYWORDS – Mobile, Malware, NIST, Publicly Traded, Ransomware

Date of Submission: 01-05-2024 Date of acceptance: 12-05-2024

I. INTRODUCTION

Due to the growing acceptance and dependence on mobile technology, publicly traded companies have also welcomed using mobile devices. Nonetheless, the increasing use of mobile devices has given hackers additional ways to target and exploit weaknesses.

Mobile ransomware is one such threat. Ransomware is malicious software that compromises mobile devices, encrypts files, and holds the files hostage until a ransom is paid. Due to its ability to damage sensitive data, interrupt vital processes, and negatively affect staff and student productivity, mobile ransomware attacks have become a severe worry for publicly traded organizations.

This research aims to investigate the growing threat of mobile ransomware in publicly traded companies. It will explore the several ways that cybercriminals attack mobile devices, the possible outcomes of these attacks, and the tactics that publicly traded organizations can adopt to lessen the dangers related to mobile ransomware. Publicly traded institutions can defend their mobile infrastructure and essential resources from ransomware attacks by comprehending the nature of this danger and putting appropriate preventive measures in place.

II. PROBLEM STATEMENT

The issue is that there are not enough security measures and regulations to stop the growing threat of mobile ransomware from spreading. Even though mobile devices are becoming increasingly utilized for various reasons, publicly traded institutions often fail to realize the potential threats of ransomware due to inadequate security measures. Mobile devices can be the target of ransomware attacks for both individuals and organizations. According to Checkpoint research, mobile ransomware assaults against businesses surged by 123 percent in 2020.

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. The problem is that publicly traded 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.

III. BACKGROUND

According to recent data, 99.9% of mobile malware discoveries were made through third-party app stores (PurpleSec, 2020)[1]. Nevertheless, according to Haas (2015)[2], 57% of mobile consumers are unaware that protection software protects them from mobile risks. When individuals use Wi-Fi or another method to connect a device to the network, they may not be aware that this could unintentionally transmit viruses or other risks (Kazmeyer, 2016)[3]. Behavioral controls must be used to help modify user behavior around downloading software onto their devices (Haas, 2015; Kazmeyer, 2016)[2],[3].

Ransomware has recently emerged as one of the fastest-growing threats in the mobile space, primarily due to its profitability (Mohan & Kumar, 2017)[4]. McAfee discovered these applications and reported them to Google. Shortly after, the applications disappeared from the Google Play Store (Samuels, 2017)[5]. Publicly traded organizations are subject to different security restrictions, and these criminal applications and compliance rules face increasing difficulty. With the Apple and Android space growing and mobile users continuing to bring their devices into the office and freely connecting their devices to corporate Wi-Fi, these publicly traded companies are continually at Risk (Paterson, 2014)[6].

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)[4]. 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, many times unmanaged, and not corporate-owned (Bullock, 2019)[7]. Ransomware is malicious software that can encrypt, lock, or lock the files on the target device (Fruhlinger, 2018)[8]. These attacks can generate mobile ransomware or ransomware from phishing emails and target mobile devices on corporate networks.

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)[9]. This quantitative regression analysis study aims to answer the following questions: to what extent do institutional security controls impact risk introduced by the utilization of mobile devices in the organization, and to what degree do institutional security policies impact vulnerabilities caused by using mobile devices in the organization?

IV. SIGNIFICANCE OF STUDY

The corporate environments in this study are publicly traded corporations in the contiguous United States. The rationale behind these types of organizations is that these types of organizations are more likely to follow NIST as a risk management framework. They are more likely to have mobile devices that require management through “bring your own device” (BYOD) policies or mobile device management platforms, sometimes a combination of both, depending on the corporation.

The business problem is that organizations often lack proper security controls and policies regarding their mobile devices; as a result, mobile ransomware is an active threat vector (Green, 2007)[10]. This business problem addresses the following questions: To what extent do institutional security controls impact risk introduced by the utilization of mobile devices in the organization? and To what degree do institutional security policies impact vulnerabilities caused by using 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. The researchers can contribute to the Information Security community with new information and bring to light a new threat vector not currently at the forefront of the community. This academic study will give the researchers additional knowledge of how and why mobile ransomware is installed on devices, although multiple behavioral controls are in place to prevent such behaviors. The academic community will discuss a new topic in the cybersecurity business because of this study. While ransomware is a primary discussion topic within the cybersecurity industry, mobile ransomware frequently goes undetected, leaving a significant gap in research capabilities.

V. LITERATURE REVIEW

Since 2014, the ransomware attack rate has steadily increased, according to the information security industry. It rose from 3.2 million in 2014 to 204.24 million in 2018. (Statistia, 2019)[11]. Malicious ransomware software targets computers, laptops, smartphones, and other mobile devices (Fruhlinger, 2018)[8]. The gadget may be locked, encrypted, or cryptographically locked in exchange for a ransom fee (Fruhlinger, 2018)[8]. That is how ransomware first appeared (Fruhlinger, 2018)[8]. As its name implies, lock restricts file access (Fruhlinger, 2018)[8]. The files are encrypted using crypto, limiting access (Mohan & Kumar, 2017)[4]. Data or the device can be encrypted and locked inside a crypto locker. Both types of malware have assaulted the mobile space (Fruhlinger, 2018)[8].

Many people use cellular or mobile equipment today (Pew Research, 2019)[12]. Over 5 billion individuals are thought to own mobile devices, with smartphones accounting for over half of those (Silver, 2019)[13]. Because the typical user of these gadgets does not care about protecting their mobile device, this opens up a new threat vector for adversaries (Haas, 2015)[2]. Due to the portability and constantly evolving technology of mobile devices, individual users and businesses have compelled their staff to rely extensively on these electronic items (Tripwire, 2016)[14]. Mobile devices now perform several daily tasks thanks to their expanded functionality, including access to the internet, making appointments, creating reminders, exchanging files, instant messaging, video chatting, and mobile banking (Tripwire, 2016)[14]. Mobile devices have many features, but they are incredibly vulnerable to online threats because of their portability and vulnerability to physical attacks (Tripwire, 2016)[14]. 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)[14].

IT professionals have little understanding as to why people who own and use these devices can download these harmful apps even though they know they are dangerous (Haas, 2015)[2]. There were 5,321,142 malicious mobile installation packages found in 2018, which was 409,774 less than what was found in 2019. (Chebyshev, 2019)[15]. Chebyshev (2019)[15] says that although malware is becoming less common, the number of attacks using malicious mobile software doubled in 2018. There were 116.5 million of these attacks (against 66.4 million in 2017). As such, technologists must set up security controls and policies to stop users from downloading malicious software onto their devices.

Corporate entities did not have to worry about the security of mobile devices until the Blackberry came out on March 7, 1984 (O'Boyle, 2020)[16]. The Blackberry was the first smartphone in how we think of them today. Ransomware for mobile devices did not become a problem until FakeDefender hit the Android market in 2013. (NJCCIC, 2016)[17]. This malware showed users fake security alerts to get them to buy an app to eliminate fake threats (NJCCIC, 2016)[17]. Malware has sometimes stopped users from getting rid of it and opening other programs (Power, 2018)[18].

Before 2013, there was malware for mobile devices. In 2004, a virus called Cabir was called Mosquitos-Trojan.Mos, a mobile malware game that came out 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)[19]. 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)[18]. 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)[18].

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)[2]. 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)[2],[1]. Many apps will also use the auto-update feature to send more malware or ransomware attacks to these devices (PurpleSec, 2020)[1]. It's important to know that ransomware is on the user's device, even if they don't realize it (Haas, 2015)[2]. 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)[1]. AndroidOS.Asacub is a malicious program (PurpleSec, 2020)[1]. 98 percent of malware for mobile devices goes after Android devices (PurpleSec, 2020)[1].

The most important way to attack is through people (Jang-Jaccard & Nepal, 2014)[19]. 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)[19]. 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)[19]. The adversary pursues an individual when they click on a link to install malicious software or visit a risky website, which is where the issue originates. (Fruhlinger, 2018)[8].

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)[20]. The scenario presented previously requires more robust security policies and controls to prevent the behavior, where UTAUT (Unified Theory of Acceptance and Use of Technology) 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)[21]. 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 fulfill these goals, NIST recommends protecting mobile devices against multiple risks.

The CIA triangle, or Confidentiality, Integrity, and Availability, is essential to cybersecurity. When considering confidentiality, consider a sensitive document such as a social security number. This information should only be accessed by those authorized to access it. Confidentiality is equivalent to privacy, and action must be taken to ensure that only those needing data access can access it (Rouse, 2020)[22]. Data integrity is where the data must remain the same during the entire transit between one point and another. For example, the social security number from before; this sensitive data cannot change between one end and the endpoint. If it does, that social security number will become a different person. Integrity ensures unauthorized persons cannot alter data during transit (Rouse, 2020)[22]. Availability is also better defined as uptime or guaranteeing that hardware systems become patched automatically and that the operating system is free from software disputes (Rouse, 2020)[22]. The CIA triangle continues to be utilized in the NIST framework during implementation.

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)[9]. 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.

VI. 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:

$H1_0$: Institutional security controls do not have a significant impact on risk introduced by using mobile devices in the organization.

$H1_a$: 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.

VII. METHODOLOGY

The dependent variable for these research questions and topical hypotheses is the degree of risk introduced by mobile devices. The dependent variable is the risk index. The average numerical/ordinal response to the seven questionnaire questions can be used to determine this continuous numerical variable. The control factors are categorical variables, meaning each has a range of unique possible values. These variables include demographics, organizational characteristics, and the existence or application of institutional security controls and policies. The statistical technique known as univariate analysis of variance (ANOVA) uses deliberate sequential model-building to (a) create a predictive risk model and (b) analyze the correlations between the dependent variable and the control factors and their

The researchers conducted an online poll and gathered replies using SurveyMonkey, a popular online survey platform, to collect information. Only closed-ended questions were included in the poll to gather quantifiable responses. The responses to the closed-ended questions provided detailed insights into the participants' experiences and perceptions of mobile ransomware and were utilized for statistical analysis.

The survey was distributed through various channels, including social media, online forums, email lists, and targeted advertisements, to ensure high response rates and a representative sample.

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 corporate environments.

VIII. DATA COLLECTION/DATA ANALYSIS

After data cleansing, there were 12 categorical control factors (CFs), each with varying levels (values), each corresponding to a single item in the questionnaire. The CFs included the following:

Question 5: sector to which the participant belonged (used only for sorting the data)

Three demographic or organizational CFs:

Question 7 (organization size)
Question 10 (computer operating system)
Question 26 (respondent gender)

The following questions identified risk:

Question 8: program to stop ransomware
Question 12: knowledge of ransomware
Question 14: anti-malware use in the organization
Question 15: effectiveness of anti-malware software
Question 16: the ability to identify/avoid ransomware attacks
Question 18: organization’s concern with being a ransomware victim
Question 19: previous knowledge of mobile ransomware
Question 20: frequency of mobile device updates

We tested the null hypotheses for the final model (no difference in Dependent Variable (DV) means for each level of that factor) using a level of significance equal to the variable inclusion criterion (.20). For each CF in the final model, I rejected the null hypothesis. I concluded that there is a difference in mean values of risk for different levels of Question 7, Question 8, Question 10, Question 12, Question 14, Question 15, Question 18, and Question 19.

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) [10]. 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: 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 public 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 publicly traded 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 or government 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.

Analyze how well MDM systems work to protect mobile devices and reduce the likelihood of ransomware infestations. Examine ransomware attacks’ effects on mobile devices in various sectors and industries. Examine ransomware outbreaks’ financial, operational, and reputational impact to determine the actual cost and ramifications for businesses. Analyze how ransomware attackers change their strategies and methods to target mobile devices. Keep up with the most recent tactics and trends threat actors use to create proactive defenses and efficient counters.

Examine how artificial intelligence and machine learning algorithms may be used to identify and stop mobile ransomware threats. Investigate the use of predictive models and sophisticated analytics to find trends in ransomware and improve threat detection. Evaluate how well recovery and backup plans work to lessen the damage caused by ransomware attacks on mobile devices. Examine several recovery procedures and backup options to ensure businesses can promptly restore their data and systems in case of an attack. Lastly, investigate the legal and regulatory ramifications of ransomware on mobile devices. Examine the regulatory frameworks and compliance standards businesses must follow to safeguard their data, prevent ransomware attacks, and maintain privacy.

X. CONCLUSION

In conclusion, the study highlights the significant impact of institutional security controls on the risk introduced by using mobile devices in publicly traded organizations. The findings emphasize the need for closer attention to mobile device management and security, particularly in the face of the growing threat of mobile ransomware. The study contributes valuable insights to the information security community and underscores the importance of implementing robust security measures to safeguard against mobile ransomware attacks. Further research is recommended to explore the effectiveness of anti-malware software solutions, user awareness and education programs, and the impact of mobile ransomware attacks on various sectors and industries.

REFERENCES

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

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

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

[4] 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.

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

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

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

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

[9] 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.

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

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

[12] Pew Research. (2019, June 12). Demographics of mobile device ownership and adoption in the united states. https://www.pewresearch.org/internet/fact-sheet/mobile/.

[13] Silver, L. (2019, February 5). Smartphone ownership is growing rapidly around the world, but not always equally. https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/.

[14] Tripwire. (2016, November 29). How to secure your mobile device in six steps. https://www.tripwire.com/state-of-security/security-data-protection/secure-mobile-device-six-steps/.

[15] Chebyshev, V. (2019, March 5). Mobile malware evolution 2018. Secure List. https://securelist.com/mobile-malware-evolution-2018/89689/

[16] O'Boyle, B. (2020, February 3). The history of Blackberry: The best blackberry phones. https://www.pocket-lint.com/phones/news/137319-farewell-blackberry-os-here-are-the-23-best-blackberry-phones-that-changed-the-world.

[17] NJCCIC. (2016, November 8). FakeDefender. https://www.cyber.nj.gov/threat-center/threat-profiles/android-malware-variants/gazon.

[18] Power, J.-P. (2018, April 13). Maliciously mobile: A brief history of mobile malware. https://medium.com/threat-intel/mobile-malware-infosec-history-70f3fcaa61c8.

[19] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

[20] Datta, S. (2019, November 26). Information security: Corporate-owned devices vs employee-owned devices. https://securityboulevard.com/2019/11/information-security-corporate-owned-devices-vs-employee-owned-devices/.

[21] Zurkus, K. (2019, January 7). Is it time for enterprises to bid farewell to byod? https://securityintelligence.com/is-it-time-for-enterprises-to-bid-farewell-to-byod/.

[22] Rouse, M. (2020, April 7). What is the cia triad? https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA.