Implementation of Zero Trust Security to Reduce Ransomware Attacks in the Philippines: A Literature Review

Eric Blancaflor *, Angelo Dominic D. Abat, Kyle Matthew A. Degrano, Ma. Cassandra M. Lindio, and Andrei Daniel A. Pamoso

School of Information Technology, Mapua University, Makati, Philippines;
Email: adtdeguzman@mymail.mapua.edu.ph (A.D.D.A.), kmadegrano@mymail.mapua.edu.ph (K.M.A.D.), mcmlindio@mymail.mapua.edu.ph (M.C.M.L.), adapamoso@mymail.mapua.edu.ph (A.D.A.P.)
*Correspondence: ebblancaflor@mapua.edu.ph (E.B.)

***Abstract*—Zero Trust Security is an architecture that, as the name implies, trusts no one. This type of architecture is used by several firms globally due to its robust security. The Zero Trust security implementation in the Philippines is very low and it shows by looking at the number of cyberattacks that Philippine companies experience. A prominent form of cyberattack is ransomware that endangers that sensitive information that most companies hold. Ransomware attacks are common, and this is where attackers would lock certain files and will only be unlocked when the victim would pay the appropriate ransom for the information. The Philippines has been deemed by international firms as a risky venture since the cybersecurity levels are low. There are also reports that major companies in the Philippines are victims of large-scale ransomware attacks. This study aims to give an in-depth explanation of Zero Trust and see its fundamental aspects that makes it a better option. This exploratory study considers the possible capabilities of the said architecture to combat ransomware in the context of the Philippines.**

***Keywords*—zero trust security, architecture, security, cyberattacks, ransomware**

I. Introduction

As the world faces a global pandemic, many businesses had to find alternatives to ensure that their operations continue amidst the restrictions of government-issued protocols. A noticeable trend is the shift of many enterprises to online modes of conducting business. This new business model opens up numerous opportunities where most transactions rely on the internet to connect with clients. This online mode of interaction presents opportunities of both positive and negative kinds. It became positive since online transactions are convenient for users, and automated processes can help optimize the business' workflow. The negative side is that many of these transactions handle sensitive information, and an online mode of business transaction is vulnerable to various attacks. One common form of attack is ransomware that threatens the clients' confidential information. A ransomware infection encrypts the data on infected computers and demands a ransom payment, typically made in Bitcoins, from the user in order to restore full access to the compromised system [1]. When it comes to compromised Android devices, the ransomware initially tries to obtain administrative privileges by begging for them or by using social engineering techniques. Another method of obtaining administrative rights is to request that the user install software updates, click on phony update pop-ups, or update their antivirus software. A common additional step used by ransomware is to request app-level permissions, which are necessary to carry out crucial operations. In most cases, a mobile application that requests permissions that are unrelated to the task at hand is engaging in malicious activities [2]. Fig. 1 shows a screenshot of a ransomware attack victimized device.

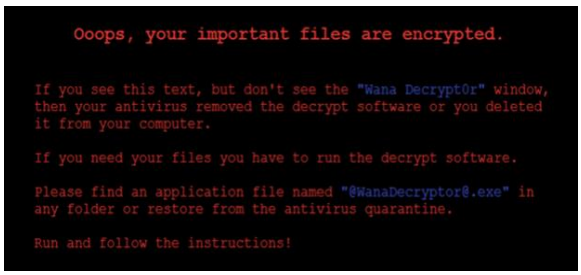

Figure 1. A message from an infected computer with the WannaCry ransomware [3].

These heavily affected various companies, universities, government, healthcare, and more. This incident resulted in chaos as sensitive information crucial to sustaining business operations was forced to a halt as this ransomware locked essential files. A way to combat ransomware is the implementation of Zero Trust security. The Zero Trust has a different approach to network security as this comprehensive security model essentially trusts no one hence the name [4]. The Zero Trust architecture heavily guards against access from outside the network while being strict to users inside. This

Manuscript received August 23, 2022; revised October 23, 2022, accepted December 5, 2022; published September 18, 2023.

security approach is extreme against attackers outside the network trying to gain access but giving considerable ease of access to users within, thus ensuring no performance drop. This architecture emphasizes the importance of credential verification and can limit the access of verified users within the network [4]. Every data resource within this model would require authenticated access from its users, adopt the least privilege model, and inspect and log all the activities related to the network and the information within.

The Philippines has numerous companies that now focus on online transactions, and some of them deal with sensitive information. Numerous considerations must be considered because ransomware is one of the fastest-growing types of cybercrime, with recent estimates indicating that the damage costs will exceed $20 Billion by 2021. In the context of the Philippines, a Kaspersky report shows that the Philippines ranked 4th in Southeast Asia when it comes to ransomware attempts during the first quarter of 2020. Additionally, over 7000 companies in the country were targeted by ransomware in the same year [5]. The Philippines face some of the noted issues as a noticeable lack of countermeasures for ransomware attacks makes companies vulnerable. Implementing the Zero Trust security would theoretically prove to be more robust than the traditional models currently existing in the Philippines.

This review paper aims to create exploratory research that shows analysis on the effectiveness of the Zero Trust model when it comes to combating ransomware attacks. This study discussed the fundamentals of the Zero Trust architecture and explore organizations that adapted the said framework. Moreover, this paper covers discussions about its benefits and presents factual data on the performance of other companies using Zero Trust.

II. Literature Review

A. Ransomware

Ransomware can infiltrate a computer in a lot of different ways. As shown in Fig. 2, ransomware is delivered by sending a phishing scam or email. This kind of delivery system sends an email to a victim that contains attachments that could take over the victim's computer by encrypting whole or most parts in the victim's device. The attacker shall demand for a ransom and once settled, the files will be decrypted.

Figure 2. Stages of Ransomware [5].

There are several things that the malware can do once it has taken over a victim's computer. One of them is file encryption, making some or all the victim's files inaccessible unless a ransom is paid, which is commonly Bitcoin, for the decryption key. The impacts of ransomware can be detrimental to its victims as it can lead to permanent or temporary loss of data. In a corporate context, a ransomware attack can cause adverse ramifications as loss of data may lead to a possible shutdown of company operations, thus losing potential revenue in return [6]. Statistics indicate the gravity of ransomware's detrimental effects as 75% of ransomware victims lose access to their personal data for more than two days, whilst 67% of businesses affected permanently lose either parts or the totality of their confidential data [6]. Table I presents a comprehensive list of notable ransomware attacks (2015–2017) [7].

TABLE I. Popular Ransomware Attacks [7]

Ransomware	Year	Type	Target devices and systems
LockerPin	2015	Locker ransomware	Mobile devices
TeslaCrypt	2015	Crypto ransomware	Data encryption on disk
Chimera	2015	Malvetisement	Data encryption on disk
LowLevel04	2015	Crypto ransomware	Remote desktop computers
7ev3n	2016	Crypto ransomware	Data encryption on disk
Ransomware32	2016	Locker ransomware	Computers
SamSam (SAMAS)	2016	Crypto ransomware	Computers
Locky	2016	Downloader	Computers
Petya	2016	Locker ransomware	Windows computers
KeRanger	2016	Crypto ransomware	Mac computers
Jigsaw	2016	Crypto ransomware	Windows computers
Maktub	2016	Crypto ransomware	Data encryption on disk
Cryptxxx	2016	Crypto ransomware	Windows operating system
PowerWare	2016	Locker ransomware	Windows operating system
ZCryptor	2016	Crypto ransomware	Data encryption on disk
GoldenEye	2016	Locker ransomware	Windows operating system
Crysis	2016	Crypto ransomware	Data encryption on disk
zCrypt	2016	Cryto ransomware	Data encryption on disk
WannaCry/WannaDecryptor	2017	Cryptoware	Data encryption on disk

From this, ransomware attacks are grave cyber threats with widespread ramifications that can adversely impact any kind of victim. Implementing a Zero Trust network security model may combat such a threat to mitigate the damaging effects of ransomware on people and corporations.

B. Zero Trust Security

Zero Trust is a network security model that is based on the idea that no one should automatically be trusted—either from inside or outside a network. The framework of Zero Trust indicates that only the authenticated and authorized users and devices can access the applications

and data and ensures the safety of the applications and users from advanced threats on the internet [8]. The model of Zero Trust was first introduced by John Kindervag from Forrester in 2009, with the principle of "Never Trust, Always Verify" [9]. Even though the model is not an entirely new theory, it gradually became essential for the modern-day digital transformation and business network security architecture [8].

One of the primary principles behind the inner workings of the Zero Trust security model is the continuous monitoring and validation of users. As the model inherently assumes that attackers are present both outside or inside of the network, zero trust is given to active users or machines. Zero Trust security continuously verifies user identity and privileges as well as the identity and security of the devices utilized. From this, logins and connections within a network timeout periodically upon establishment—forcing the users and devices employed to be constantly re-verified [10].

Another principle that established the efficacy of the Zero Trust security model is the implementation of least-privilege access. Users and machines will only have access within networks in accordance with their needs and motives. This indicates that no user should have potent privileges within to contain their access and bolster security. Having a least-privilege access can minimize every user's exposure to the sensitive parts of a network—possibly mitigating detrimental cyber threats such as ransomware attacks which can cause adverse damage. In a Zero Trust security model, implementing a least-privilege access suggests carefully managing user permissions to contain their entry within a network [10].

Alongside the implementation of least-privilege access, the Zero Trust security model employs device access control as a central part of its methodologies. The model requires strict control over the devices utilized for accessing the network. As such, it is expected to monitor how many different devices are accessing a certain network to determine their credibility and security. Constant monitoring of the devices ensures that they are authorized as well as determining whether they have been compromised or not. From this, zero trust's device access control can further minimize the attack surface of a given network [10].

This model also incorporates micro-segmentation within its functionalities. It allows the model to divide security perimeters into much smaller and contained segments or zones to maintain separate access for users across distinct areas of the network [10]. In a business context, corporations that utilize data centers with micro segmentations to store their confidential files may have dozens of separate security zones to contain their data. Such a feature strengthens the Zero Trust security model as users will only be given access to certain zones in accordance with their needs. Accessibility to other zones will not be granted for entering users unless a separate authorization is granted or permitted—thus bolstering the strength of a network.

Once an attacker's presence is identified within a network, the compromised device or account will then be immediately quarantined from communicating to other segmented zones to mitigate the damage done—efficiently refining the security of a network. With such a feature, the Zero Trust Security model can outperform the Castle-and-Moat security model as a lateral movement for unauthorized users is one of its biggest flaws which Zero Trust solves. As such, the model can be considered as a competent and innovative upgrade from much older models as it ensures top-notch security for networks and data servers.

Amongst the features that make up zero trust security's functions, Multi-Factor Authentication (MFA) is one of the core values essential to its efficacy. MFA has been a recurring authentication method also found in online platforms such as Facebook and Google. MFA ensures that more than one piece of evidence is entered by a user to authenticate their identity before being granted permission to access [10]. Such a method refines the security of a certain network from intruders as imitating or hacking an authorized user to infiltrate their networks will become a much arduous task for attackers. In addition to that, MFA can also bolster the security for a certain network by requiring a separate generated code sent to a user's mobile device to add an extra step to zero trust's authentication process.

The Zero Trust Security model can be regarded as a robust and efficient framework to combat a plethora of adverse cyber threats. With the various features it provides upon implementation to a network, it can offer a myriad of advantageous benefits for corporations and even individuals. The first among its impactful effects is its capability to reduce business and organizational risk. As Zero Trust assumes that all applications, users, devices, and services are hostile, it can reduce risk as it uncovers the contents within a network and how assets communicate through such [11]. Zero Trust Security has the capacity to provide invisibility which makes it simpler to demonstrate compliance with privacy standards and other regulations and results in fewer findings in audits.

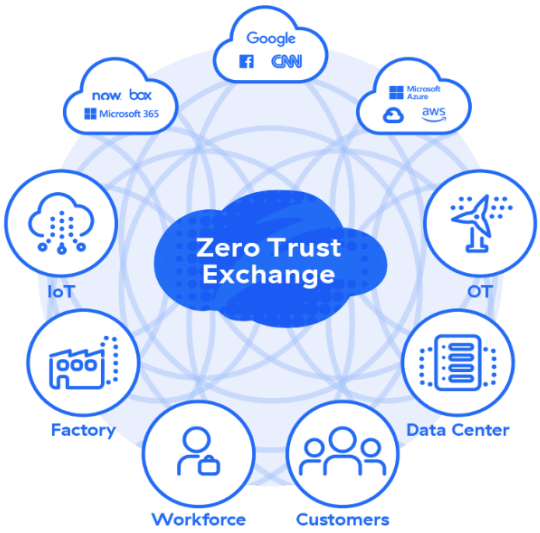

Figure 3. Zscaler zero trust exchange [11].

One vendor that offers a zero-trust platform created for cloud companies and born in the cloud is Zscaler. Zscaler is frequently recognized as a leader in the most esteemed analyst reports and rankings in the sector, and their flagship platform is the Zscaler Zero Trust Exchange, shown in Fig. 3 [11].

Based on the least privilege principle, the Zscaler zero trust exchange creates trust through context, including a user's location, the security settings on their device, the content being shared, and the program being requested. Without ever being connected to the network directly, employees receive quick, dependable connectivity once trust has been established [11].

C. Zero Trust to Combat Ransomware

The Zero Trust Security will not eliminate the ransomware threat in its entirety, but it will minimize the possibility of being attacked; that is why it is effective against Ransomware if it is implemented well. Since fundamentally, human error will always be the root cause of all cyberattacks, Zero Trust emphasizes the use of user identity and access management. It reduces the attacks significantly by hiding resources that are only accessed by authorized personnel. Zero Trust also provides monitoring, detection, and threat inspection which are necessary to prevent exfiltration of sensitive data and ransomware attacks [12].

The Zero Trust architecture requires companies to continuously monitor a user and the device used if it is validated and has the right privileges and attributes. It also requires enforcement of a policy that includes the risk of the user and their device, along with other requirements to consider before permitting a transaction of any kind [13]. On a Zero Trust Security, organizations must look over and know all of their service and privileged accounts and set up controls to where they connect. These requirements can block out any unwanted and unauthorized users from reaching the data and information of the company.

With the continuous verification of Zero Trust, which always verifies any access all the time for any resource can minimize the chances of any breach imaginable, but it also uses identity-based segmentation that in case a breach occurs it will cut down the impact of the breach since it limits the path for the attacker, which gives time for the system and personnel to respond and mitigate the attack [13].

D. The Situation of Organizations with Zero Trust

In a study by John Grady, a senior analyst revealed the situation of organizations that implemented zero trust. The study conducted a survey that shows how well their organizations has managed with Zero Trust, how they perceive Zero Trust, and how they implemented it.

Most organizations that implemented zero trust identify and inventory all devices on their network, and employ multiple factors of authentication, use analytics to identify anomalous behavior. While some of them restricts and controls their employees to only have access to sufficient information to do their work, in a chance of having a leak [14].

Most Organizations that implemented zero trust strategy for two or more years prefers the zero trust to be implemented across their organization than for a specific use, while most organizations that implemented zero trust for less than two years prefers the zero trust to be implemented only for a specific case than be implemented across their organization [14]. It was not implied that even if you have implemented zero trust for more than two years, you must apply it across your organization since zero trust can take a lot of thought even after years of implementation.

46% of implementations of Zero Trust were very successful, 39% of implementations were successful but with some minor problems, and 15% of implementations were not as successful but with room of improvements [14].

According to the research survey on how well their implementation of Zero Trust is, the results were: 43% of organizations have reduced the number of cyber incidents, 43% has improved the efficiency of security, 41% simplified their compliance efforts, 41% has reduced the number of breaches, 38% made their organizations more agile, 36% increased their employees' productivity, 34% has increased user satisfaction, and 31% has reduced security costs [14].

E. Steps to Optimize Zero Trust Strategy

An organization should improve the collaboration between security operations, IT operations, and the other lines of the business was one of the best ways to optimize Zero Trust in an organization. An organization should also implement stronger authentication controls, authorization and accounting to safeguard its assets.

According to an article from the International Trade Administration, the Philippines, a country with a social media savvy population, has very few data protection protocols, thus making it vulnerable to a plethora of cyber-attacks [15]. Overall, the article emphasizes the lack of preventive measures for cyberattacks in the Philippines. With the benefits of Zero Trust, widely known by most international businesses, the news article states that the Philippines has the lowest adoption of said security, yielding only 5%. For context, neighboring countries adopted 32% for Japan, 17% in Hong Kong, 13% in Malaysia, 11% in Australia, and 10% for South Korea and Indonesia [16].

The Philippines has been subjected to a mass migration of its IT infrastructure to cloud and digital systems. This quick migration however, resulted in the immediate purchase of new technologies and adoption of new systems. Considering the immediate purchase and transitions, businesses became vulnerable to various cyberattacks [17]. As a summary, most businesses, organizations, and firms see the benefit of Zero Trust security. They see it as a robust system, but this is just the general idea that most business owners hear.

F. Implementation Strategy of Akamai Technologies

Akamai Technologies, Inc. offers cloud services for Internet content and business application delivery, optimization, and security. Security, online performance,

media distribution, and network operator are among its products. Frank T. Leighton, Jonathan Seelig, Randall S. Kaplan, and Daniel M. Lewin established the firm headquartered in Cambridge, MA [18]. As Akamai IT assumed, a network-centric approach to control and access is no longer adequate for securing corporate resources. An increased risk of unwanted remote access to critical data and access to all company network applications is one of the security concerns of conventional Virtual Private Networks (VPNs). As a result, the said company adopts a Zero Trust security approach to eradicate traditional corporate VPN. Its goal is to secure the data and applications of the company, restrict lateral network movement, and provide a better user experience. Akamai IT has also modified its security protocols to reflect the principles of Zero Trust, where no system or user would be trusted by default [19].

To migrate away from the VPN, Akamai IT implemented Enterprise Application Access. This cloud-based access solution secures the corporate network by permitting only dial-out access to apps behind the firewall. Access is exclusively determined by entitlement, identification, and location. Authentication and authorization are performed on a per-application basis, notwithstanding where apps are hosted. Akamai IT has reduced the risk and further increased their overall security posture as they used Kona Site Defender. It is a web application firewall of Akamai to safeguard internal applications against Structured Query Language (SQL) injection attacks and other advanced persistent threats, including ransomware, emerging from formerly "authorized" hosts. The strategy taken by Akamai lowered the costs and complications generally involved with safeguarding application access [19].

Another critical component in completing Akamai's move to a Zero Trust model is leveraging device posture for dynamic access choices. The said aspect improves and integrates authorization, authentication, reporting capabilities, and access control rules. Some of the benefits of migrating to a Zero Trust Security strategy in companies, as stated in the case study of Akamai implementing the said approach, are reducing the risk by granting solely relevant apps access rather than entire corporate network access and mitigating the IT infrastructure and workflow overhead involved with granting access to newly acquired company employees. In addition, save expenses by allocating IT resources more efficiently; reduced hours spent upgrading, operating, and maintaining network infrastructure implies an additional opportunity for strategic priorities [19].

III. Conclusions

Organizations are increasingly relying on networking technologies and computerized systems, which are subject to attack and gain unauthorized access due to the COVID-19 pandemic. Remote working regulations have increased the necessity for a secure architectural framework that would mandate multi-factor authentication for accessing critical data. One of the prevalent threats worldwide is ransomware, a form of malicious software that locks and encrypts data on a victim's digital device before demanding a ransom to regain access. Thereby, implementing the Zero Trust security is a way to combat ransomware. The pandemic has made organizations recognize the importance of a zero-trust environment in securing their sensitive information. The IT security environment has changed significantly, with people working remotely and relying on vulnerable networking equipment. It has also been mentioned that major data-related incidents have happened in the country, particularly about the Commission of Elections. Relating to the current state of the country's protection protocols, it shows how susceptible the country is to cyberattacks, specifically ransomware. Since Zero Trust Security is being implemented across regions and even the neighboring countries of the Philippines, the country is known to have the lowest adoption of the said security.

The principle of Zero Trust Security is "Never Trust, Always Verify", which was created by John Kindervag. A ransomware threat will not be effectively eradicated by the said model, rather it will reduce the likelihood of being attacked. It has been mentioned that the root cause of all cyberattacks is human error. With that being said, the Zero Trust security approach guarantees that only authorized personnel have a distinct level of access, which is regularly assessed without increasing friction for the user.

In conclusion, the Zero Trust security has been implemented to most organizations offshore and it shows that 46% of all the implementations were successful. As a result, the number of cyberattack incidents was reduced according to 43% of the organizations who implemented the said approach, while 41% has reduced the number o breaches. Furthermore, it has also helped increase their employees' productivity, as well as enhanced user experience. One of the companies which implemented this security approach is Akamai Technologies. They have benefited well from the said implementation as their overall security posture increased, along with their workforce's productivity and user experience across all devices. They were also able to alleviate the risks of cyber threats and cut expenses for IT resources. Thus, Zero Trust security should be implemented in the Philippines as an immediate response to the numerous ransomware attacks and data breaches that happened as it increased during the pandemic. It would help stop the recurring threats and incidents encountered as well as strengthen the country's security posture in different organizations.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, E.B., A.A., K.M.D., and C.L.; methodology, C.L., A.D.P., A.A., and K.M.D.; writing—review and editing, E.B., A.A.; All authors have read and agreed to the published version of the manuscript.

ACKNOWLEDGMENT

First and foremost, the authors would like to thank the God Almighty for giving them the strength, knowledge, ability, and opportunity to undertake the study and complete it. Secondly, the authors wish to thank Dr. Eric Blancaflor, Professor of the School of Information Technology Mapua University, for his guidance on this research work.

REFERENCES

[1] S. Aurangzeb, M. Aleem, M. A. Iqbal, and M. A. Islam, "Ransomware: A survey and trends," *Journal of Information Assurance and Security*, vol. 6, issue 2, pp. 48–58., 2017.

[2] H. Luo, Z. Chen, J. Li, and A. Vasilakos, "Preventing distributed denial-of-service flooding attacks with dynamic path identifiers," *IEEE Transactions on Information Forensics and Security*, 2017.

[3] Secure List Kaspersky. (2017). WannaCry ransomware used in widespread attacks all over the world. [Online]. Available: https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/

[4] Musarubra US LLC. (2022). What Is Zero Trust Security? [Online]. Available: https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-zero-trust.html

[5] NewPost Tech Desk. (2019). Ransomware attacks continue; Philippines ranks 4th in SEA for most attempts. [Online]. Available: https://newpost.com.ph/ransomware-attacks-continue-philippines-ranks-4th-in-sea-for-most-attempts/

[6] Ascend IT Solutions, Inc. The Impact of Ransomware. [Online]. Available: https://www.ascenditsolutions.com/blog/executive-summary/65-the-impact-of-ransomware#:~:text=The%20impacts%20of%20a%20ransomware,generating%20operations%20being%20shut%20down

[7] I. Yaqoob, E. Ahmed, M. H. Rehman, A. I. A. Ahmed, M. A. Al-Garadi, M. Imran, and M. Guizani, "The rise of ransomware and emerging security challenges in the Internet of Things," *Computer Networks*, vol. 129, no. 2, pp. 444–458, 2017. doi: 10.1016/j.comnet.2017.09.003

[8] A. Technologies. (2022). Zero Trust security. [Online]. Available: https://www.akamai.com/resources/zero-trust-security-model?gclid=Cj0KCQiA2sqOBhCGARIsAPuPK0h_kOXpow2b9ZShgtVN2YiJpWxq3Ou5vwAeV2tMiYzaTaLT5NByyPgaAvUcEALw_wcB&utm_source=google&utm_medium=cpc&utm_campaign=F-MC-52610&utm_term=zero%20trust&utm_content=ASEAN&ef_id=Cj0KCQiA2sqOBhCGARIsAPuPK0h_kOXpow2b9ZShgtVN2YiJpWxq3Ou5vwAeV2tMiYzaTaLT5NByyPgaAvUcEALw_wcB:G:s

[9] C. Cunningham. (2020). A look back at zero trust: Never trust, always verify. [Online]. Available: https://www.forrester.com/blogs/a-look-back-at-zero-trust-never-trust-always-verify/

[10] Cloudflare Inc. (2022). Zero trust security. What is a zero trust network? [Online]. Available: https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/

[11] Zscaler Inc. (2022). What is zero trust? [Online]. Available: https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust

[12] S. Durbin. (2021). Zero trust: An answer to the ransomware menace? [Online]. Available: https://www.darkreading.com/vulnerabilities-threats/zero-trust-an-answer-to-the-ransomware-menace-

[13] K. Raina. (2021). Zero trust security explained: Principles of the zero trust model. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

[14] J. Grady. (2021). The state of zero trust security strategies. [Online]. Available: https://info.menlosecurity.com/rs/281-OWV-899/images/ESG-eBook-Menlo-Zero-Trust.pdf

[15] International Trade Administration, U.S. Department of Commerce. (2020). Philippine Cybersecurity. [Online]. Available: https://www.trade.gov/market-intelligence/philippine-cybersecurity

[16] J. V. Cabuenas. (2021). Philippines has lowest "zero trust" adoption in Asia Pacific, says study. [Online]. Available: https://www.gmanetwork.com/news/scitech/technology/806145/philippines-has-lowest-zero-trust-adoption-in-asia-pacific-says-study/story/

[17] Malaya Business Insight. (2021). Study reveals PH leads region in zero-trust implementation. [Online]. Available: https://malayaph.com/news_special_feature/study-reveals-ph-leads-region-in-zero-trust-implementation/

[18] Forbes Media LLC. (2022). Akamai Technologies (AKAM). [Online]. Available: https://www.forbes.com/companies/akamai-technologies/?sh=6e5d74433851

[19] Akamai. (July 2019). How akamai implemented a zero trust security model—Without a VPN: Akamai case study. [Online]. Available: https://www.akamai.com/content/dam/site/en/documents/case-study/how-akamai-implemented-a-zero-trust-security-model-without-a-vpn.pdf