Al-Qirtas القرطاس
http: https://al-qirtas.com/index.php/Al-Qirtas
E(ISSN): 2709-6076
P(ISSN): 2709-6068

A Comprehensive Analysis of Pakistan's Cybersecurity Landscape and its Solutions

Abdullah Shahrose
Lecturer at HITEC University, Taxila
Yousra Zafar
Lecturer at HITEC University, Taxila
Hira Khalid
Lecturer at HITEC University, Taxila
Agha Muhammad Yar Khan
Software engineer at HITEC University, Taxila

Citation: Abdullah Shahrose, Yousra Zafar, Hira Khalid, & Agha Muhammad Yar Khan. (2024). A Comprehensive Analysis of Pakistan's Cybersecurity Landscape and its Solutions. Al-Qirtas, 3(3), 73-80. Retrieved from https://al-qirtas.com/index.php/Al-Qirtas/article/view/321

Abstract:

This scholarly research article overviews the current and growing concept of cybersecurity in Pakistan, pointing out the importance of employing strong security measures as threats rise due to the growing technology. This paper starts with the discovery of open weaknesses in cybersecurity in Pakistan, including ignorance, old-age facility and equipment, fewer experts in the area, and geopolitics. These weaknesses make the nation vulnerable to many cyber risks such as theft of data, sabotage of its infrastructure, cyber spying and many more such as the social engineering scams. The threats are identified to have pedestrian economic and national security consequences to Pakistan and therefore the call to comprehensively and urgently approach the improvement of the country's cybersecurity. Speaking of the problem of weaken cybersecurity and its possible consequences mentioned in the article, it states that the lack of proper security measures may result in rather severe outcomes including significant information theft, disruption of the services that are critical to public health, and crushing loss of intellectual property. The discussion also touches on the possibilities for elevated cybercrime-rates: especially the spread of online scams and social engineering, which can take advantage of the population's general ignorance on security measures. These threats also affect the individual as well as the organizations, but they also result in threats to the nation's stability and its economy. While evaluating the risks of the identified threats, the article focuses on potential impacts on the economic and national security aspects and, thus, the necessity to strengthen cyber protection measures. The article is devoid of concrete suggestions, yet it outlines quite a number of possible measures and approaches to the problem and ways of building up robust Pakistan's cybersecurity. These include: The passing and implementation of effective cybersecurity laws for the country, enhancement of the general technological frameworks utilized in most organizations, creation of nationwide cybersecurity programs which can be under taken by organizations and institutions, general enhancement of cybersecurity education and training among professionals in the field and others. Further, international cooperation and information exchange are also underlined as the ways to use the world's best practices and assets. Thus, by following the outlined strategies, Pakistan can put an end to the existing cybersecurity threats and move to the sphere of digital security.

Keywords: *Cybersecurity, Digital Future, National Security, Digital Threats, Targeted Education*

Al-Qirtas القرطاس
http: https://al-qirtas.com/index.php/Al-Qirtas
E(ISSN): 2709-6076
P(ISSN): 2709-6068

Introduction

In the present technological age, cybersecurity has turned out to be the most significant issue for different states because of the advancement of digital technologies and apparent dependence on internet systems. The IoT, the Cloud and Artificial Intelligence have changed the ways societies function: people are more connected and, to some extent, facilities are even more convenient, but the security issues have emerged. Given the fact that governments, businesses, and individuals are moving to the digital age by incorporating the digital solution in their functional activities, they are increasing the possibility of cyber threats. Thus, digital transformation has increased the demand for strong cybersecurity to keep the data secure, prevent tampering of networks and personal data, and guarantee privacy. Higher occurrence and complexity of cyber threats prove that it is high time to enhance the cybersecurity approaches to minimize the risks and protect the information infrastructure (Anderson & Moore, 2020).

Today, the main problem, the main enemy of the digital world is a large number of various cyber threats, including the withdrawal of data, ransomware, cyberattacks by states and others. Cyber threats are rapidly on the rise posing a threat to the security of nations, its important infrastructure and causing high losses to nations' economies. For example, the WannaCry crypto worm attack of 2017 touched over 200,000 computers in over 150 countries disrupting businesses and resulting in a loss in the billions (Hussain & Priya, 2018). Likewise, hacking interference with elections and voting, financial structures, and the healthcare industry demonstrated that modern societies are not immune to digital structures' flaws. For instance, the use of new techniques by the cyber adversaries then make the threat environment highly dynamic, meaning there is always new strategies in the market, meaning a proactive and forceful approach to cyber security (Lewis, 2019).

This research paper is an attempt to make a systematic evaluation of Pakistan's cybersecurity threats and risks while outlining the possible ways for improving the security in this context. A look at Pakistan and some of the challenges that are likely to be common in many developing nations is also important. These factors include; technological facilities that are dated, inadequate cybersecurity workforce, and low knowledge of cybersecurity measures among citizens. In addition, threats such as geopolitical rivalry and specific cyber threats only deepen these problems, which threaten national security and economic development. It is with the aim of providing specific propositions for the enhancement of Pakistan's cybersecurity and the establishment of a safe digital environment for future advancement that this article overviews these threats and discusses potential strategic initiatives (Khan, 2021; Rafiq, 2022)..

Pakistan's Cybersecurity Landscape

The current scenario of cybersecurity in Pakistan gives an account of a territory that is teeming with strenuous issues and risks. Even though there is increasing computerization, the country has remained poorly equipped to manage contemporary forms of cyber threats. Several industries such as government, banking, healthcare and telecommunications have long admitted to being in the receiving end of recurrent cyber-attacks implying that there are existing structural

vulnerabilities in cybersecurity (Rafiq, 2022). Currently, it was observed that FIA- NR 3C responds to these threats, but evidently the framework for managing Cybersecurity is still in its infancy in Pakistan. Further, despite the fact that Pakistan has made efforts towards passing some of the cybersecurity regulations like the Prevention of Electronic Crimes Act (PECA) 2016, the execution and overall systematic strategies remain a problem (Khan, 2021). This is also evidenced in the Global Cybersecurity Index (GCI) where Pakistan is ranked pretty low below many other countries and hence the need for a better enhanced cybersecurity strategy.

Various aspects explain the state of cybersecurity in Pakistan. It can be seen that one of the most significant challenges is the inability of the common populace and organizations as a whole to actively participate in maintaining adequate cybersecurity. Today, very few organizations' often offer various training programs, especially in relation to cybersecurity awareness and often, the workforce remains very vulnerable with little or no understanding of such threats (Hussain & Priya, 2018). This lack of knowledge and awareness renders the entities vulnerable to various forms of attacks; for instance, phishing, social engineering, malware among others. Furthermore, it is deemed that such vulnerabilities are aggravated by the aged facilities and technological gaps. A great number of critical systems are based on old software to which updated security patches are no longer released, providing IP addresses for attackers (Lewis, 2019). This archaic technology not only deprecated the operations throughout a company and all its subsidiaries but it also greatly compromises the security concerns of a system or firm, therefore underlining the importance of modernization and upgrading of technologies for security.

Another issue which affects the Pakistan's cyber security is the dearth of qualified skilled cyber security experts. This is probably one of the largest gaps in the supply and demand of cybersecurity experts in the country at the moment. This shortage greatly limits the capacity of organizations to install and maintain credible security systems. Furthermore, the existing educational institutions are deficient of programs and curriculum in cybersecurity and this makes the available workforce very limited in addressing today's complex cyber threats (Anderson & Moore, 2020). This disadvantage is extended by the brain drain action whereby proficient experts search for better employment in other nations, and consequently, Pakistan lacks adequate cybersecurity competent professionals (Khan, 2021). To tackle this problem, more efforts have to be made in both increasing the cybersecurity awareness training as well as the measures to keep cybersecurity talents in the country.

External attributes such as geopolitical threats also influence Pakistan's cybersecurity environment and targeted cyber-attacks add to the existing problems. This nation is often attacked by cybercriminals hired by other countries with which it has hostile relations (Rafiq, 2022). These attacks' major objectives are destruction of vital facilities, theft of data and confidential information, and threats to the country's security. For instance, the cyber espionage cases that have been directed towards the government ministries and military bases have been escalated and such features demonstrate the importance of cybersecurity from the geopolitical perspective (Hussain & Priya, 2018). Moreover, the increasing use of the highly developed cyber

Al-Qirtas القرطاس
http: https://al-qirtas.com/index.php/Al-Qirtas
E(ISSN): 2709-6076
P(ISSN): 2709-6068

warfare techniques around the world impose the necessity for Pakistan to be geared to counter essentially all kind of complex existing threats. Meeting these challenges needs not only a national but an international approach to cooperate in the sharing of intelligence, as well as the ideas, experience, and innovations at the global level (Lewis, 2019).

Challenges and Consequences of Weak Cybersecurity

The risks of no stringent cybersecurity measures in Pakistan are wider and more complex; they bring about severe threats to national security and economic stability. Lack of strong protection exposes systems and networks to numerous and severe cyber-attacks, and vital data gets stolen from governments, businesses, etc. It not only erodes the confidence of people and businesses in the protection of one's personal information, and the security of proprietary information but also in digital processes. Lack of protection may result in the disruption of essential facilities like electricity, the financial sector, which impacts the society in many ways and losses. For example, a successful cyberattack to the finance sector can cause the stagnation of banking services and, consequently, financial instability and lack of trust from the public (Lewis, 2019). Such exposures reveal the imperativeness of the need for Pakistan to improve its readiness for cyber-security as a way of avoiding such disruptive, not to mention catastrophic incidents.

Hacking is another major of concern that Pakistan might experience due to poor cyber security adopted in the country. Hackers seeking sensitive information attack databases with people's data, finances, and governmental information. Such breaches cause identities theft, financial scams, and unlawful release of sensitive information with lifelong impacts on the affected people and countries (Anderson & Moore, 2020). Among these, interference of important structures is another dreadful issue. A cyber-attack on the power grid, water supply systems, or healthcare facilities will disrupt crucial services with millions of human impacts and economic/societal losses. For instance, an attack against the power distribution system which may result in a long duration of power outages that affect businesses, healthcare, and everyday life; this shows the relevance of strong cybersecurity measures in these industries (Rafiq, 2022).

This paper examines cyber espionage, and intellectual property theft as threats that affect Pakistan's economic and strategic interests. The cyber espionage is sponsored by any nation in order to gain some competitive edge for its government, military, or industrial establishments in relation to others. Such activities are dangerous because they expose classified information on defense procedures and strength (Cherribi, 2010). While cybercrime slows the process of development through causing losses, IP theft slows the process through affecting innovations and competitiveness. For instance, if trade secrets such as engineering, technologies, and brands are stolen or hacked, it will take a toll on the competitive advantage of the key industries leading to financial losses and slow economic development as indicated by Khan (2021). These threats address the need to protect information through better cybersecurity measures and global collaboration on cyber espionage.

Phishing schemes and cyber frauds are always associated with attacking human characteristics, thus, by-passing technical barriers. These attacks trick the victim into providing

Al-Qirtas القرطاس
http: https://al-qirtas.com/index.php/Al-Qirtas
E(ISSN): 2709-6076
P(ISSN): 2709-6068

some sensitive details or execute something that is not safe. For instance, phishing attacks make the users release their passwords or financial details, thus compromising their money and data (Hussain & Priya, 2018). The effects that are both economic and national security based are massive. Cybercrime proves to have financial repercussions to organisations, thus necessitating loss of consumers' confidence and increased costs of doing business. Nevertheless, national security is also at stake, which identifies with threats to its information resources and disruptions that undermine governmental performance and citizens' trust. To overcome these threats, it is essential to engage in a multi-pronged strategy of aware public, strict cybersecurity policies, and better partnership between the government and the populace for defending Pakistan's cybersecurity perimeter (Lewis, 2019).

Potential Solutions and Strategies

It is thus crucial to take a comprehensive approach to relieve the pressure on this country's cybersecurity by aiming at the technical measures along with the human factor. First of all, the subject area requires the strong and all-encompassing legislation on cybersecurity. The kind of legislation that should be passed should lay down acceptable practices and policies on cyber security, require security scans to be conducted periodically and penalties to be administered to non-compliance. There is the Prevention of Electronic Crimes Act (PECA) passed in 2016 that can be used to tackle the problem, although the Act requires enhancement and more serious implementation to cover current threats (Khan, 2021). More legislation should also be drafted with an aim of accelerating the formation of a national cybersecurity body, responsible for the supervision and management of cybersecurity in the various fields. Besides strengthening legal and regulatory provisions, this approach nurtures the states' responsibility and increased awareness regarding cyber security measures (Lewis, 2019).

Another major strategy involves refurbishing the infrastructures and the secure technologies. Most of the laid down systems in Pakistan are inadequate because most of them do not incorporate modern security features hence prone to cyber-attacks. The improvement of these systems to include new security measures can greatly lessen these risks; new firewalls, improved intrusion detection systems, and new encryption standards. Also, the implementation of proxy technologies such as block chain in strategic operations can improve data validity and security (Rafiq, 2022). However, such investments need large capital investment and both national and international collaboration from the government and other business organisations. The factors include not only the costs, which organizations already have shown that they cannot abide, but also the institutional resistance likely to greet attempts to something new. However, the short-term barriers which include the above challenges are outweighed today by the advantages of lower risks and better cybersecurity (Anderson & Moore, 2020).

Assessing citizens' awareness of cybersecurity and encouraging cybersecurity programs in society remains paramount in creating a strong cybersecurity culture. Another form should provide information about different types of threats agents may encounter online, for example, phishing and social engineering and teach people how to protect themselves and organizations'

data. In this regard, such programs can be initiated in the form of workshops, online courses and public campaigns (Hussain & Priya, 2018). Companies should also be urged to carry out periodic sensitization of the employees on how they are likely to encounter such threats and how they should deal with them. The issues arise in the area of coverage and maintaining random respondents' turnout. Besides, awareness to the cyber trends and their susceptibilities are raised making the environment safe from hackers' attacks (Lewis, 2019).

According to the present unavailability of expertise in Pakistan, it is important to build a proficient workforce in cybersecurity experts. This can be attained through increasing the understanding of the general public and Improving or expanding the type of educational programs in universities and technical institutes which should encompass full functional cybersecurity courses. Scholarships and grant programs for trying to get students for cybersecurity can also assist in attracting talent as well to the field (Khan, 2021). Also, job training via internships and partnerships with companies and organizations may help obtain the practical experience. International cooperation and information exchange with other nations may also promote the improvement of the situation with the cybersecurity of Pakistan. These global projects and alliances can be a way through which Pakistan can get updated information and knowledge, techniques, and other related information and technologies (Rafiq, 2022). The challenges include; funding of the education programs and finding suitable partners at the international level. Nevertheless, the advantages of the availability of a skilled workforce to enhance the country's ability to handle cyber threats are enormous, leading to a stronger and better national cybersecurity architecture (Lewis, 2019).

Recommendations and Conclusion

In light of the above research, the following conclusions have been established about Pakistan's cybersecurity; Despite its advancements in the Information technology sector, Pakistan faces many cybersecurity issues because of the factors like, poor awareness and training for cybersecurity, old infrastructure in most organizations, a short supply of cybersecurity professionals, and the geopolitical conflict that increases the threat of cyberattacks. These risks make the nation more prone to dangerous hazards like cyber theft, sabotage of infrastructures, espionage, and trickery which are always common in the cyber world. If organizations fail to protect themselves, they might increase the risk that cybersecurity threats pose to national security, economic staple, and citizens' trust in digital systems. Solving these problems, it is necessary to develop complex strategies including legislative, technological, educational and international ones.

The following is a set of recommendations for improving the state of cybersecurity of Pakistan: First of all, it is necessary to support and implement high-quality legislation regulating the sphere of cybersecurity. The legal framework against cyber threats will be provided when the Prevention of Electronic Crimes Act (PECA) will be updated, and its enforcement will be intensified (Khan, 2021). It is also necessary to determine the department responsible for the control and implementation of the measures as well as create a national cybersecurity authority

as a focal point for the actions. Second, the areas that need to be focused in this regard are updating infrastructures and implementing secure technologies. The paths include updating old systems and installing new security features; the security threats will be lowered by a great deal (Rafiq, 2022). Third, it is imperative to stress upon plans on raising cybersecurity awareness. Conducting awareness programs for the citizens and organizations involving the social media accounts and educational classes about the threats and measures would increase the total cybersecurity awareness (Hussain & Priya, 2018).

Another important recommendation that has been made is the need to cultivate a pool of skilled workforce with competencies in the area of cybersecurity or security information and network administration. Improving the content of cybersecurity education in educational centers and offering bonuses like scholarships and grants will encourage talented individuals to work in this sphere. Internship programs or cooperation with economy institutions will strengthen practical skills still more and readiness for work (Anderson & Moore, 2020). Also, there is the need to support international partnership and research dissemination. Participation in global cybersecurity programmers and partnerships will avail the best information, innovations, and measures enhancing Pakistan's cybersecurity realm (Lewis, 2019). These recommendations call for a holistic approach at the heart of systemically and multifaceted characteristics of cybersecurity threats. The following strategies have to be duly executed through joint efforts of governmental & private sectors, schools, colleges and universities, and the international community.

Thus, it can be stated that building strong cybersecurity is crucial for Pakistan's further development. The importance of the presented theme in contemporary contexts offers with the development of new digital technologies and the constant growth of threats is evident. In general, improving legislation, upgrading facilities, increasing awareness among the population, creating competent personnel, and cooperation with foreign countries are also significant factors that should be a part of the cybersecurity plan. If the above-mentioned risks are managed today and the recommendations are put into practice, the safety of Pakistani cyberspace will be strengthened, and threats will be minimized. Cybersecurity is no longer limited to the defense of data and systems but is a necessity in the security, growth, and credibility of nations of the world as many functions of the society shift to the online realm (Rafiq, 2022; Lewis, 2019). The coordinated approach toward building up the cybersecurity will help Pakistan to build up a secured and prosperous future in the digital environment.

References

Anderson, R., & Moore, T. (2020). "The economics of information security." Science, 367(6483), 1246-1251.

Cherribi, S. (2010). *In the House of War: Dutch Islam Observed*. Oxford University Press.

Haddad, Y. Y. (2006). *Not Quite American?: The Shaping of Arab and Muslim Identity in the United States*. Baylor University Press.

Al-Qirtas القرطاس
http: https://al-qirtas.com/index.php/Al-Qirtas
E(ISSN): 2709-6076
P(ISSN): 2709-6068

Hussain, A., & Priya, R. (2018). "Cybersecurity awareness and its impact on digital Pakistan." Journal of Cybersecurity Research, 4(2), 101-115.

Khan, M. (2021). "Cybersecurity in Pakistan: Challenges and opportunities." International Journal of Cyber Studies, 5(1), 45-60.

Köse, A. (1996). *Conversion to Islam: A Study of Native British Converts*. Routledge.

Lewis, J. (2019). "Cybersecurity and national power: A strategic framework." Journal of Strategic Studies, 42(6), 853-870.

Lofland, J., & Skonovd, N. (1981). "Conversion motifs." *Journal for the Scientific Study of Religion*, 20(4), 373-385.

Poston, L. (1992). *Islamic Da'wah in the West: Muslim Missionary Activity and the Dynamics of Conversion to Islam*. Oxford University Press.

Rafiq, S. (2022). "The state of cybersecurity in Pakistan: An in-depth analysis." Asian Journal of Information Technology, 21(3), 225-240.

Rambo, L. R. (1993). *Understanding Religious Conversion*. Yale University Press.

Roald, A. S. (2004). *New Muslims in the European Context: The Experience of Scandinavian Converts*. Brill.

Schimmel, A. (1992). *Islam: An Introduction*. SUNY Press.