International Journal of Advanced Engineering, Management and Science (IJAEMS)
Peer-Reviewed Journal
ISSN: 2454-1311 | Vol-9, Issue-10; Oct, 2023
Journal Home Page: https://ijaems.com/
DOI: https://dx.doi.org/10.22161/ijaems.910.3

Implementation of Cyber Security in Corporate Sector of Pakistan

Yousuf Jamil Baig

Received: 08 Sep 2023; Received in revised form: 14 Oct 2023; Accepted: 21 Oct 2023; Available online: 27 Oct 2023

Abstract— *We live in a time when knowledge is easily accessible and people are connected throughout the world. The technological improvements that modern states use to advance include streamlined online bill payments, improved healthcare systems, sophisticated transportation networks, the use of artificial intelligence, cutting-edge communication systems, and technological warfare. Despite the fact that technology has made it possible to break down geographical borders, the widespread use of technology has led to the emergence of new challenges and concerns. Hacking, bank fraud, money laundering, data breaches, unauthorized acquisition of state secrets, and targeted attacks on critical infrastructure are just a few of the criminal activities and threats that plague the digital world today. These crimes have all emerged as major facets of modern cyber warfare. Such threats can affect both wealthy and developing countries, creating a challenging situation for national security. Among these countries, Pakistan and other emerging nations are particularly at risk. The nation has a sizable population of business users who are unfamiliar with information technology, which makes it more difficult for governmental and legislative authorities to regulate the nation's digital environment. Recent catastrophic cyberattacks on Pakistani institutions' most essential websites have successfully breached significant digital installations. Legislators in Pakistan have responded by introducing cyber legislation, but it doesn't seem like they fully address the variety of online threats. This study paper is focused on creating a framework for the adoption of cyber security in Pakistan's corporate sector and investigating workable solutions to serious cybersecurity issues. In order to generate findings, a qualitative research methodology was used, gathering information from both primary and secondary sources. Finally, the study makes a number of suggestions on how Pakistan's corporate sector may implement cyber security.*

Keywords— ***Cyber Security, Corporate Sector, Implementation in Pakistan.***

I. INTRODUCTION

Fundamentally, cybersecurity is putting into place a series of policies and strategies to protect a company's critical systems and sensitive data from online attacks and breaches. The environment of cyber-attacks is becoming more complex as hackers find it simpler to get beyond traditional security measures by using cutting-edge techniques including AI and social engineering. Businesses must increase their cybersecurity precautions in line with the adoption of new technology. A strong cybersecurity strategy includes numerous levels of protection to protect your company from different types of cybercrime, such as attempts to hack into, alter, or compromise data, extort money from customers or the company, or disrupt daily operations.

Cyber strategies should consider the following elements:

- Safeguarding infrastructure
- Enhancing network security
- Strengthening application security
- Ensuring information security
- Securing cloud systems
- Providing employee security training and fostering awareness
- Establishing disaster recovery and business continuity plans

Cybercrime is now more prevalent than ever, and assaults are becoming more complicated, targeted, and frequent. Information theft is developing as the most expensive and quickly rising category of cybercrime, with criminal elements increasingly focusing on the data repositories of corporations. The increase in organizations using cloud services to store personally identifiable information only serves to exacerbate this trend and increase its vulnerability. It is important to understand, however, that theft is not always the intent; some of the offenders choose to manipulate or destroy information in an effort to create mistrust inside businesses or governments.

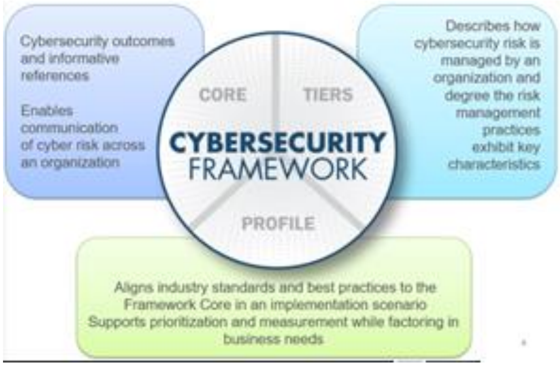
Cybersecurity outcomes and informative references
Enables communication of cyber risk across an organization
CORE
TIERS
CYBERSECURITY FRAMEWORK
PROFILE
Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics
Aligns industry standards and best practices to the Framework Core in an implementation scenario
Supports prioritization and measurement while factoring in business needs

Fig.1: Cyber Security Framework

(Source: https://jeremy-swenson.com/2018/05/06/key-updates-to-the-nist-cyber-security-framework/)

Ransomware and phishing assaults are common ways to compromise a company's vital systems or networks, but social engineering is still the easiest way to carry out a cyberattack. The risk posed by third parties is also increasing, as criminals target these vendors—including IT service providers—in order to acquire unlawful access to organizations to which they are connected. Collectively, these trends highlight the necessity for businesses to recognize and take cybersecurity extremely seriously.

II. LITERATURE REVIEW

Over half of the world's population may now exchange data over connected networks thanks to cyberspace, a conduit that humans have developed for international communication and infrastructure interconnection. Cyberspace risks are always changing, posing fresh problems for all civilizations with the potential to jeopardize personal security (Hussain, 2022). The debate over cyber dangers began in the late 1980s, picked up steam in the 1990s, and then spread to different countries. Due to the reliance of industrialized economies and national security on a trustworthy, globally interconnected software system, cyber dangers first appeared on political agendas in the middle of the 1990s. Cyber threats now pose a threat to cultural ideals, economic stability, and overall well-being. A new, nameless foe that transcends state lines was introduced by internet-connected computers carrying out cyberattacks. This threat paradigm extends to critical infrastructure, turning relatively minor incidents into serious security concerns due to the availability of user-friendly and sophisticated hacking tools for easy download (Cavelty, 2010).

Although the terms "internet" and "cyberspace" are sometimes used interchangeably, the internet is simply one part of the larger concept of cyberspace (Cavelty, 2015). The world has become a "virtual global village" because to the internet (Yamin, 2014). Basically, "communication through an electronic medium, such as websites and emails, involving computer command and control" is what is meant by the term "cyberspace" (Futter, 2016). Different definitions of cyberspace have developed over time, falling short of a common understanding and neglecting some crucial elements (Lorents & Ottis, 2010). A thorough description of cyberspace as a network of linked, time-dependent information systems and the people interacting with them was put out by Lorents and Ottis (2010).

Cyberspace is a brand-new area that is essential to the daily lives of states, groups, people, enterprises, and organizations—all of which are competing for dominance. Conflicts have emerged in cyberspace, taking the form of cyber conflict, which pits different entities against one another there while one launches a cyberattack on the other. Depending on the players' goals, such as the acquisition of sensitive information, nefarious financial gain, or the rapid damage of an adversary's vital infrastructure, the nature of cyber conflict can change (Lorents & Ottis, 2010).

The vulnerabilities it creates necessitate immediate attention from those in positions of authority given the growing reliance of a nation's key infrastructure on cyberspace, since unchecked vulnerabilities could undermine Pakistan's sovereignty (Khan, 2019; Shad, 2017). Cyberthreats and cybercrime incidents are both on the rise. Over the past three years, Pakistan's social media platforms have seen a considerable increase in cybercrimes such harassment, financial fraud, bogus profiles, hacking, defamation, and blackmail. The second-highest category of cybercrime in the nation is harassment complaints. Among the most frequently used platforms for cybercrimes include Facebook, email, and WhatsApp (Abbasi, 2021).

Although both developing and developed countries rely significantly on the internet for e-services to improve the lives of their population, vulnerabilities and cyber dangers still exist (Sharma, 2010). For instance, financial transactions are susceptible to cyber theft, when offenders use computer code instead of firearms to commit robbery and exploit weak passwords. Additionally, malicious hackers have the ability to access or alter confidential military data, jeopardizing national security and vital public infrastructure, and negatively affecting people who frequently communicate online. Traditional security methods are ineffective against these non-traditional cyber security threats (Harknett & Stever, 2011).

Billion-dollar sums are transported or stolen illegally, private data is revealed, state secrets are jeopardized, and crucial public infrastructures are breached in the field of cybersecurity (Syed, Khaver & Yasin, 2019). In line with international trends, Pakistan has to deal with cyberthreats and challenges such as hacking, serious and organized cybercrime, cyberterrorism, and cyber warfare (Shad, 2017), computer malware, identity theft, economic data breaches, cyber fraud, and espionage attempts on critical infrastructures (Rafiq, 2017), as well as ransomware, spyware, social engineering, and tampering with physical devices (Syed, Khaver, & Yasin, 2019). The media's inaccurate portrayal of cyber security initiatives, the lack of pertinent institutions, the length of security debates, a traditional security culture, and the exclusion of the audience from the discourse are additional obstacles to Pakistan's successful securitization of cyberspace (Rafiq, 2017). Additionally, different e-government services face a variety of difficulties, such as technical difficulties, human factors, and problems with service delivery (Awan, Memon, Shah, & Awan, 2016). A high-level organizational structure was proposed by Tariq, Aslam, Rashid, and Waqar (2013) for setting up crucial cybersecurity bodies at various levels that would be in charge of protecting the nation's cyberspace.

These organizations include the Ministry of Information Technology's Computer Emergency Response Team, the National Response Centre on Cyber Crimes, and the National Cyber Security Division, all of which, though now working, may use more efficiency. According to Tariq, Aslam, Rashid, and Waqar (2013), academics agree that it is urgent to identify cyber threats and their possible effects as well as put in place efficient reaction systems to protect against these threats.

III. CORPORATE CYBER SECURITY

Significant cyberattacks can affect a wide range of business entities and types of businesses. For instance, a large volume of private and sensitive data is managed by financial institutions and insurance companies, needing strict security procedures. This emphasizes how crucial cybersecurity is in the business world. The idea of optimizing the use of information technology in several stages of commercialization and operational duties is the foundation of digital advancement, which goes by different names across industries. The developing and increased requirement for information and technology security is one result of this digital transition. As diverse systems communicate, new difficulties arise. Big Data, the Internet of Things, and API technologies have advanced technology, making it simple to develop ground-breaking solutions without running into technological challenges. Since everything is connected, it is possible to store and process all data to produce extra value.

Fig.2: Role of Corporate Cyber Security

The ability of a business to effectively use technology to automate repetitive operations, simplify reporting, and harness data for better strategic decision-making is key to maintaining its competitive edge in the modern day. However, as a company relies more on information technology, it is more vulnerable to security breaches carried out by criminals experienced at locating flaws in the organization's IT infrastructure. Malware, phishing, endpoint security breaches, and ransomware are typical cybersecurity risks. The biggest threat facing corporate entities right now is probably the rise in cybersecurity events. A corporation may go bankrupt if a catastrophic disaster occurred in addition to the financial losses brought on by a breach due to operational disruption and reputational harm.

It is essential for companies and their IT divisions to develop information security policies. In the past, installing firewalls and antivirus software was sufficient. This is no longer the case, though. In order to prevent future attacks, modern businesses must proactively identify and reduce risks at an early stage.

Regulations and norms governing businesses are becoming more detailed. The likelihood of assaults, data breaches, interruptions, and breaches should decrease as a result of these steps. The guidelines underscore the essential security protocols that must be created and implemented to reduce the IT and security risks that financial institutions must deal with, among other directives. It is essential to understand that these regulations have legal effect, requiring the covered businesses to justify any variation from their application.

In reality, businesses must invest in comprehensive cybersecurity policies that protect staff communications, customer contacts, and relationships with outside vendors and suppliers. Every online activity and social media engagement adds a new cyber danger because of how intertwined modern commercial supply chains are. Businesses need to put in place improved procedures that will allow them to spot and stop sophisticated hostile activity before any potential harm is done, maintaining operational continuity and preventing data breaches. The availability of hacking tools and software has made it possible for hackers of all skill levels to successfully compromise business computer systems. In the current global environment, there are more internet-connected gadgets than ever before; predictions indicate that 27.1 billion devices will be globally connected this year. If these devices don't have proper security measures, cybercriminals trying to get into a company's networks and steal sensitive data may be able to take advantage of them.

Corporate Security Best Practices

In order to identify, mitigate, and avoid future cybersecurity threats, your company's risk management policies can be improved by adhering to best practices. Understanding the exact dangers your firm confronts is crucial before addressing cybersecurity issues. Start this process out with a thorough evaluation of potential dangers. Start by defining the information that has to be protected within your organization. This can be done more easily by reviewing pertinent compliance standards that are specifically customized to your industry. To avoid unwanted access, make sure that sensitive data is stored in a highly secure setting. Security professionals should also frequently backup this data, and backups should be kept in a different, equally safe location.

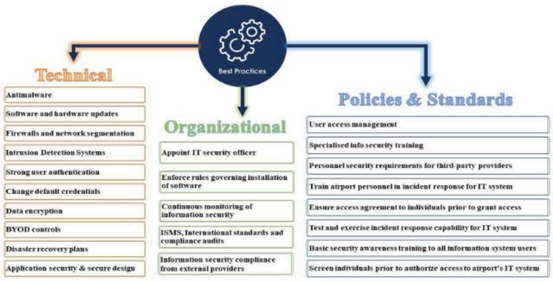
Best Practices
Technical
Antimalware
Software and hardware updates
Firewalls and network segmentation
Intrusion Detection Systems
Strong user authentication
Change default credentials
Data encryption
BYOD controls
Disaster recovery plans
Application security & secure design
Organizational
Appoint IT security officer
Enforce rules governing installation of software
Continuous monitoring of information security
ISMS, International standards and compliance audits
Information security compliance from external providers
Policies & Standards
User access management
Specialised info security training
Personnel security requirements for third-party providers
Train airport personnel in incident response for IT system
Ensure access agreement to individuals prior to grant access
Test and exercise incident response capability for IT system
Basic security awareness training to all information system users
Screen individuals prior to authorize access to airport's IT system

Fig.3: Best Practices Classification

(Source: Lykou, Georgia & Anagnostopoulou, Argiro & Gritzalis, Dimitris. 2018. Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience. 1-6. 10.1109/GIOTS.2018.8534523)

Cybercriminals have a great opportunity to compromise your infrastructure while using outdated software. A simple way to close this particular vulnerability in your company is to update all programs on a regular basis, especially if security products are being used. Many forward-thinking companies have implemented 2FA (two-factor authentication) to strengthen access control since they realize that passwords alone are no longer sufficient to protect user information. This is simply made possible by user-friendly applications that are accessible on employees' mobile devices for authentication approval, guaranteeing that access requests are valid.

You can strengthen your defenses by creating a mandated security policy that specifies the level of password complexity required. It is crucial that every person in the business is aware of and follows cybersecurity policies. Employees can learn about company security standards through required training sessions, and acknowledgment forms can be used to track their compliance.

Consider replacing BYOD (Bring Your Own Device) regulations with security measures that demand the usage of company-approved, secure devices and private Wi-Fi networks for work-related tasks if your workers work remotely. Expect the best, but be ready for the worse, as the saying goes. Your organization's capacity to respond and keep running after a cyberattack depends on adequate planning for all possible outcomes.

Determine probable dangers throughout your risk assessment, then create precautions to prevent any negative effects. Using technology to support your organization's cybersecurity program and experienced third-party service providers may be necessary to put these best practices into practice. Depending on the size, resources, and specific risk profile of your company, either advanced software, security experts, or both may be necessary.

Furthermore, relying simply on cybersecurity software won't guarantee success over the long run. It's crucial to implement a risk management solution that keeps your business ahead of developing risks in response to changing security threats. As threats change, risk management and cybersecurity coexist. Risk management, which tackles possible hazards across multiple parts of organizational activity, is crucial for managing short-term risks. The best way to protect your business from cyberattacks is thus to integrate both programs.

IV. PAKISTAN'S CORPORATE CYBER SECURITY

The cyber threat environment of a state or organization is strongly shaped by how vulnerable its ICT-dependent facilities are. The technical and social environment both have an impact on this susceptibility. A state that struggles with a hostile sociopolitical environment brought on by internal or external conflicts and lacks effective cybersecurity measures is more vulnerable to numerous cyber threats, including cyberwarfare. In this context, Pakistan's increasing reliance on internet-based governance and service delivery, combined with its susceptibility to cyber risks due to inadequate cybersecurity preparedness and the difficult socio-political environment it faces domestically and regionally, shape Pakistan's cyber threat landscape.

Pakistan is one of the growing nations where both governmental and commercial organizations are gradually implementing online administration and service systems. The National Database and Registration Authority (NADRA), which serves as the main repository for the national Identity Documents (ID) database of Pakistani nationals, is noteworthy for its crucial role as a sensitive public body. Banks, the Pakistani Election Commission, the departments of immigration and passports, mobile networks, and security agencies are just a few of the organizations with whom NADRA distributes the internet information of its users.

A number of Pakistan's state enterprises are increasingly providing e-services in a range of economic, social, and security areas in an effort to modernize and increase efficiency. The Pakistan Computer Bureau's merger with the E-Government Directorate in 2014, which was founded in 2002 under the IT Ministry and later renamed the National Information Technology Board, highlights the expanding use of ICT-based services in the nation's economic sector. This includes the implementation of internet banking, online payment methods, and digital stock markets in addition to Automatic Teller Machines (ATMs). Additionally, some social sectors in Khyber Pakhtunkhwa, such as educational institutions, hospitals, and police departments, are offering e-government services.

Pakistan needs an integrated institutional framework that integrates the infrastructures and services of relevant agencies and promotes coordination and collaboration between them in order to handle difficulties. Pakistan should also place a high priority on raising internet users' computer savvy and understanding of cybersecurity. The former calls for the efficient use of trained human resources, while the latter entails teaching and raising awareness of cybersecurity among the general public. Political, social, and private boundaries are not exempt from the spectrum of cyber vulnerability. Our development is inextricably linked to cyberspace as the globe moves into a more technologically advanced and economically intertwined period. Nations are paying closer attention to cyber laws and policies due to the rapidly changing standards and technologies. Pakistan has increased its emphasis on cybersecurity both at home and internationally. The nation faces similar difficulties in the world of online as the global community does. These dangers are rising and taking on more complex patterns. These attacks have also targeted the military and other public institutions. To address these problems and obstacles, a variety of tactics and methods have arisen globally.

Cyber dangers are predicted to continue to be prevalent as Pakistan develops and increases its online presence. Pakistan has actively contributed to the growth and development of cyberspace over the years. However, extensive legislation and regulations are still needed to properly actualize the success of such efforts. Effective management of Pakistan's cyber domain requires a deliberate focus on law and policy creation, as well as cooperative efforts and community commitment.

V. IMPLEMENTATION RECOMMENDATIONS

Here are some suggestions for putting cyber security into practice in Pakistan's corporate sector:

- Develop and implement thorough training programs for staff members at all levels to better their knowledge of cybersecurity best practices, such as threat identification, prevention, and response procedures.
- Regular Security Audits and Assessments: To find weaknesses in the company's network and systems, conduct routine security audits and assessments. To remain ahead of potential risks, this should also include penetration testing and risk evaluations.
- Advanced Encryption and Authentication Protocols: To secure sensitive data and stop illegal access to corporate systems and databases, implement strong encryption and multi-factor authentication techniques.
- Establish Cyber Incident Response Plans: To reduce the impact of possible cyber-attacks, develop thorough and efficient cyber incident response plans. A defined line of command, rules for communication, and tactics for containment and recovery should all be part of this.
- Adoption of Security Frameworks and Standards: To build an organized approach to cybersecurity and ensure compliance with worldwide best practices, adopt internationally recognized cybersecurity frameworks and standards, such as ISO 27001.
- The most recent security patches and fixes should be applied to all software and applications on a regular basis to address any known vulnerabilities.
- Implement reliable data backup and recovery procedures to guard against data loss in the case of a cyber-incident. Test these precautions' effectiveness on a regular basis to ensure prompt data restoration.
- Employee Vigilance and Awareness: Promote a culture of cybersecurity awareness among staff members through ongoing instruction and training. Encourage staff members to be on the lookout for phishing scams, social engineering tricks, and other typical cyber risks.

- Fostering collaboration with government organizations and law enforcement agencies can help you remain current on the most recent cybersecurity risks and will make it easier to respond quickly to any potential cyber crises.
- Investment in Advanced Security Technologies: To defend the corporate network from complex cyber threats and attacks, make an investment in advanced cybersecurity technologies such as intrusion detection systems, firewalls, and endpoint protection solutions.

The corporate sector in Pakistan may dramatically improve its cybersecurity posture and better safeguard its crucial assets and sensitive data from new online threats by putting these recommendations into practice.

VI. FUTURE RECOMMENDATIONS

It is crucial to concentrate on a number of critical areas in order to guarantee a strong and efficient implementation of cyber security in the corporate sector for the future. The corporate sector should first and foremost place a high priority on ongoing, focused training programs that keep staff members up to date on the most recent cybersecurity threats and best practices. To quickly identify and mitigate any security breaches, proactive steps are required, such as the adoption of real-time threat monitoring systems and frequent security audits. In order to prevent unauthorized access to sensitive data, it is essential that strong data encryption techniques and strict access restrictions be integrated. Adopting AI-driven security solutions can also greatly improve the cybersecurity framework's overall resilience and threat detection capabilities. To stay current on the newest trends and best practices in the cybersecurity field, collaboration with peers and industry professionals is essential. Additionally, it is essential to incorporate thorough incident response plans that specify precise measures for containment, mitigation, and recovery in the case of a cyber-attack. Allocating funds for the purchase and adoption of cutting-edge security tools and technologies that provide heightened protection against sophisticated cyber-attacks is also essential. To keep the confidence of stakeholders and customers, compliance with international compliance standards is essential. Creating a resilient and secure cyber environment for the business sector will depend on encouraging regular employee engagement in cybersecurity projects and actively seeking input to continually enhance the security architecture and procedures.

REFERENCES

[1] Abbasi, K. (2021). Cybercrime increases by 83pc in three years. The News. Retrieved from https://www.thenews.com.pk/print/884453-cybercrime-increases-by-83pc-in-three-years

[2] ACS. (2016). Cybersecurity – Threats Challenges Opportunities. Sydney: Australian Computer Society.

[3] Awan, J.H., Memon, S., Shah, M.H., & Awan, F.H. (2016). Security of Egovernment Services and Challenges in Pakistan. SAI Computing Conference (pp. 1082-1085). London: IEEE.

[4] Bowen, G. (2009). Document Analysis as a Qualitative Research Method. Qualitative Research Journal, 9(2), 27-40.

[5] Cardno, C. (2018). Policy Document Analysis: A Practical Educational Leadership Tool and a Qualitative Research Method. Educational Administration: Theory and Practice, 24(4), 623-640.

[6] Cavelty, M.D. (2010). Cyber-threats. In M.D. Cavelty, & Victor Mauer, The Routledge Handbook of Security Studies (pp. 180-188). London: Routledge.

[7] Cavelty, M.D. (2015). Cyber secueity. In A. Collins, Contemporary Security Studies (4th ed., pp. 400-415). Oxford: Oxford University Press.

[8] Council of Europe. (2020, March 27). Cybercrime and COVID-19. Retrieved from Council of Europe portal: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19

[9] Federal budget. (2020-21). Federal budget. finance division. Islamabad: Government of Pakistan.

[10] Frost, & Sullivan. (2018). Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World. Microsoft Asia News Center. Microsoft and Frost & Sullivan. Retrieved from https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats- to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses/

[11] Futter, A. (2016). Is Trident Safe from Cyber Attack? European Leadership Network, 1-7.

[12] Frisby, J. (2020). global cyber security exposure index. California: PasswordManagers.co. Retrieved from https://passwordmanagers.co/cybersecurity-exposure-index/#global

[13] Global Innovation Index. (2020). Global Innovation Index. SC Johnson college of Business and World intellectual property organization, Who will finance innovation? Retrieved from https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020.pdf

[14] Harknett, R.J., & Stever, J.A. (2011). The New Policy World of Cybersecurity. Public Administration Review, 455-460.

[15] Hassan, R.T. (2018). Cyber security: A non-traditional security threat. Expert legal review. Retrieved from http://expertlegalreview.com/cyber- security-non-traditional-security-threat/

[16] Hussain, A. (2022, January 16). Should Pakistan have a cyber army? The Express Tribune. Retrieved from https://tribune.com.pk/story/2338876/should-pakistan-have-a-cyber-army

[17] International Institute of Strategic Studies. (2021). Cyber Capabilities and National Power: A Net Assessment. London: The International Institute for Strategic Studies.

[18] GCI. (2017). Global Cybersecurity Index. Geneva: International Telecommunication Union.

[19] Global cyber security index. (2018). International Telecommunication Union. Global cyber security index & cyberwellness profiles. Geneve: ABI research telecommunication development sector. Retrieved from www.itu.int.

[20] Global Cybersecurity Index. (2021). Global Cybersecurity Index 2020: Measuring commitment to cybersecurity. Geneva: International Telecommunication Union.

[21] Khan, M.I. (2019). Cyber-warfare: Implications for the national security of Pakistan. NDU Journal, 117-132.

[22] Khan, U.P., & Anwar, M.W. (2020). Cybersecurity in Pakistan: Regulations, Gaps and A Way Forward. Cyberpolitik Journal, 5(10), 205-218.

[23] Khilji, U. (2022). Rise in cybercrime. Dawn. Retrieved from https://www.dawn.com/news/1668802

[24] Knill, C., & Tosun, J. (2012). Public Policy: A New Introduction. London: Palgrave Macmillan.

[25] Nabeel, F. (2018). Need of a Robust Cybersecurity Regime for Pakistan. Centre for Strategic and Contemporary Research. Retrieved from https://cscr.pk/explore/themes/defense-security/cybersecurity-pakistan/

[26] McAfee. (2007). One Internet, Many Worlds. Sage, 2(1). Retrieved from http://downloadcenter.mcafee.com/products/pdf/sage_2008.pdf

[27] Morgan, S. (2020, November 13). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybersecurity Ventures. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by- 2021/

[28] Nasir, J. A. (2021). Cyber security challenges and response. The Express Tribune. Retrieved from https://tribune.com.pk/story/2328017/cyber- security-challenges-and-responsel

[29] Naiyer, F. (2020). Pakistan outlook 2020: Politics, economy & security. Islamabad: Islamabad policy institute.

[30] NCSP. (2021). Government of Pakistan, Ministry of Information Technology & Telecommunication, National Cyber Security Policy 2021, Islamabad. NR3C. (2007). National Response Center for Cyber Crime. Federal Investigation Agency. Retrieved from https://nr3c.gov.pk/about_us.html Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and Implications. 5th International Conference on Information Warfare and Security (pp. 267- 270). Dayton: Academic Publishing Limited.

[31] Qadeer, M.A. (2020, June 6). The Cyber Threat Facing Pakistan. The Diplomat. Retrieved from https://thediplomat.com/2020/06/the-cyber- threat-facing-pakistan/

[32] Rafiq, A. (2017). Challenges of Securitising Cyberspace in Pakistan. Strategic Studies, 90-101.

[33] Safdar, A. (2020). The emerging threat of Indian cyber warfare against Pakistan. Daily times. Retrieved from https://dailytimes.com.pk/660092/the- emerging-threat-of-indian-cyber-warfare-against-pakistan/

[34] Sapru, R.K. (2004). Public Policy: Formulation, Implementation and Evaluation. New Delhi: Sterling Publishers.

[35] Statista Global Survey. (2020). Value of expenditure towards cyber security in India in 2019 and 2022. Statista. Retrieved from https://www.statista.com/statistics/1099728/india-expenditure-towards- cyber-security-by-sector/

[36] Shah, S.A. (2021). Cybersecurity through laws in Pakistan. The Express Tribune. Retrieved from https://tribune.com.pk/story/2329721/cybersecurity-through- laws-in-pakistan

[37] Sharma, A. (2010). Cyber Wars: A Paradigm Shift from Means to Ends. Strategic Analysis, 34(1), 62-73.

[38] Siddiqui, N. (2020, August 12). Indian cyber-attack targeting gadgets of govt officials, military personnel identified: ISPR. Dawn. Retrieved from https://www.dawn.com/news/1574034

[39] Syed, R., Khaver, A.A., & Yasin, M. (2019). Cyber Security: Where Does Pakistan Stand? Islamabad: Sustainable Development Policy Institute.

[40] Shad, M.R. (2019). Cyber Threat Landscape and Readiness Challenge of Pakistan. Strategic Studies, 39(1), 1-19.

[41] Tariq, M., Aslam, B., Rashid, I., & Waqar, A. (2013). Cyber threats and incident response capability - a case study of Pakistan. 2nd National Conference on Information Assurance (pp. 15-20). IEEE.

[42] Tagert, A.C. (2010). Cybersecurity Challenges in Developing Nations. Carnegie Mellon University.

[43] The Express Tribune. (2021, September 17). Cyber Security Policy on the cards. The Express Tribune. Retrieved from https://tribune.com.pk/story/2320589/cyber-security-policy-on-the-cards World Economic Forum. (2020). The Global Risks Report 2020. Geneva: World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

[44] Rafiq, A. (2017). Increasing cyber threats to Pakistan. Institute of strategic studies. Retrieved from https://issi.org.pk/wp-content/uploads/2017/10/IB_Aamna_October_13_2017.pdf

[45] Yamin, T. (2014). Developing Information-Space Confidence Building Measures (CBMs) between India and Pakistan. New Mexico: Sandia National Laboratories.