RESEARCH & INNOVATION DIVISION
IJIST

Securing Pakistan's Cyberspace Cyber Counter Intelligence Strengths, Weaknesses and Strategies

Noman Habib[1], Sajid Hussain[1], Syed M. Ali Uddin Hafee[2]
[1]Institute of Industrial Electronics Engineering
[2]Pakistan Telecom Authority
*Correspondence. nomanhabib@iiee.edu.pk, sajid@iiee.edu.pk, syedmuhammadaliuddin@gmail.com

Citation | Habib. N, Hussain. S, Hafee. S. M. A. U, "Securing Pakistan's Cyberspace Cyber Counter Intelligence Strengths, Weaknesses and Strategies", IJIST, Vol. 06 Issue. 04 pp 1586-1605, Oct 2024
DOI | https://doi.org/10.33411/IJIST/993
Received | Aug 15, 2024 **Revised |** Sep 28, 2024 **Accepted |** Oct 04, 2024 **Published |** Oct 08, 2024.

Cyberspace is fundamental in the contemporary world for economies, societies and politics. It has many advantages with plenty of disadvantages. The evolution of digital technology in Pakistan has given advancement and improved investment in information technology but it has also instigated numerous cyber threats to national security, economic grounds and infrastructure. These threats are not straightforward and as a result, a strong and more importantly integrated strategy for Critical Cyber Infrastructure (CCI) is necessary. Before embarking on the recommendations, this research aims to describe the current state of CCI in Pakistan and the key involved. They take into consideration weak points in essential infrastructures, the problems of data security and other matters of concern in the growing threat domain. One of the key findings of the study relates to the need to integrate other governments, companies and intelligence organizations to deal with these cyber threats. CCI has been developed in Pakistan to some extent; however, there are significantly vulnerable areas. Terminated businesses like electricity, finance and telecom face this problem because their technology is old and security is inadequate. While Pakistan has recently adopted legislation on the protection of personal data, the country is not very efficient when it comes to implementing such legislation. Therefore, eradicating these problems from the roots of Pakistan requires a comprehensive and multiple-faceted strategy that requires changes in policies, people, technology and international cooperation. The essence of the present paper is the proposition that if Pakistan has a CCI plan that is progressive synchronistic and comprehensive, it can safeguard its strategic assets and serve the safety of its economy and the nation's security from the threats posed by the Information Age.

Keywords. CCI, Cyber Security, Cyber Space, Pakistan, Cyber risks, vulnerable.

IPIndexing Indexing Portal
CiteFactor Academic Scientific Journals
RESEARCHBIB ACADEMIC RESOURCE INDEX
IDEAS
Scientific Journal Impact Factor TOGETHER WE REACH THE GOAL
JOURNALS MASTER LIST
ROOTINDEXING
Scilit
INFOBASE INDEX
DRJI
Crossref
ResearchGate
WIKIDATA
HEC

Introduction.

Due to the globalization of digital technology, countries have experienced unprecedented connectivity, progress and advancement. The world has embraced technology in growth and Pakistan embraced innovations to boost its economy, education and governance. Nevertheless, this situation has made the country connect several technologies it adopted to numerous cyber threats that are beyond the geographical limitations and conventional security systems [1]. Thus there is a dire need for Pakistan to develop a proper CCI system because with time and development threats are emerging [2][3].

The authors in [4] reported an incident of data exposure occurred involving information from the FIA, prompting the government to consider enhancing cybersecurity measures for safeguarding electronic data. In the same year, a cyber-related financial loss of approximately $6 million was reported by a bank, highlighting areas for improvement in the cybersecurity infrastructure of Pakistan's banking sector (https://www.dawn.com/news/1443970). K-Electric also faced a disastrous ransomware assault, which resulted in the interruption in their services for hours [7]. Data breaches from Pakistan International Airlines (PIA) and a cyber-attack on the National Bank of Pakistan (NBP) highlighted the requirement of strong infrastructure, regulations and laws related to cyber security in the country [8][9]. These incidents reflect the magnitude of cyber-attacks on Pakistan's civil and banking sectors and the need for a sophisticated cybersecurity system.

Background.

E-commerce has grown at a fast pace in Pakistan in the recent past; with an increased public internet connection and more use of mobile phones and various web tools in organizations [10][11]. Although it has helped to boost the nation's economy, improve communication and make information more reachable, it has also brought out risks such as cyber that are a threat to the nation's security [12][13].

In Pakistan, cyber threats range from state-sponsored attacks to sophisticated cybercriminal activities, covering a wide spectrum of malicious efforts aimed at compromising national and organizational security [14]. These attacks use sophisticated methods and tools to attack the vulnerabilities of the sectors that comprise critical infrastructures, retrieve private data and disrupt necessary services. Acknowledging such threats, the country has an urgent necessity for a properly constructed and efficient CCI.

Rationale for the Study.

This research is relevant because, without a well-integrated and effectively managed (CCI), cyberspace remains vulnerable to substantial hostile interference [15]. Threats from the virtual world may pose an imminent danger to a nation's security, economy and people. This paper aims to determine the contributions and shortages of the current CCI system in the country and gives suggestions to ameliorate the Pakistani position in the domain of cyberspace and fill the existing gaps.

Objectives of the Study.

This comprehensive study aims to.

- **Analyze.** To analyze the current position of CCI infrastructure.
- **Assess.** Assessing the strengths and weaknesses of the CCI infrastructure based on the analysis of data.
- **Identify.** Identifying the gaps and deficient areas that require improvements.
- **Evaluate.** Evaluation of data privacy laws and their capacity to penalize the responsible.
- **Examine.** Examining the modernized threats and tools e.g state-sponsored threats.
- **Develop.** Based on the assessment, examination and analysis propose a more efficient strategy for CCI in Pakistan.

Structure of the Research.

This research aims to provide the general viewer with a survey of the current scenario of CCI and measures to improve its effectiveness. It assesses the opportunities and threats of Pakistan's CCI system, identifies threats related to specific sectors of the critical infrastructure, tackles the issue of data security and considers new trends of cyber threats [16]. The paper aims to outline the necessary recommendations that would allow to address the identified shortcomings and enhance overall cybersecurity. Finally, this research aims to raise awareness among policymakers, security professionals and other stakeholders about the importance of establishing a strong CCI system to protect cyberspace from advanced cyber threats.

Methodology.

Research Design.

An empirical and exploratory approach was employed, utilizing both quantitative and qualitative research methodologies [17][18]. It makes it possible to gain a substantially deeper understanding of CCI as an organization taking into account to gauge the strengths and weaknesses.

Data Collection.

In this context, quantitative data was collected from open sources reports [19] [20][21] [22]. The time frame analyzed covered the years 2020 to 2023, offering insights into the latest trends and developments in cyber threat activities. The data was transformed and sorted according to categories that need to be examined in the course of research. Quantitative data was collected from sources selected based on the following criteria.

- **Open Sources.** Chosen for their credibility and relevance, including reputable news outlets, academic journals and industry reports.
- **Official Reports.** Selected from publications of government departments, international organizations and research institutions to ensure comprehensive and reliability of data.

In the quantitative study, data was retrieved from public dossiers and datasets. We ensured that data was acquired from official reports on all categories of cyber incidents that were publicly available.

Data Analysis.

Quantitative information was analyzed using statistical measures to obtain significant findings about the level of cybersecurity threats [23]. Quantization was performed by using frequencies, averages and percentages to present the number and the impact of different cyber briefs. The comparisons of collected data for various industries, different organizations, or at different time intervals exhibit the trends and patterns.

- **Frequencies.** Counting the instances of various cyberattacks to find prevalent dangers.
- **Averages (Mean).** To identify patterns and to figure out the average annual number of cyber incidents.
- **Percentages.** Illustrating the proportionate frequency of attacks against particular industries (banking, government, etc.).

Trend Evaluation.

The data was smoothed down to emphasize long-term trends. Correlation analysis and comparative analysis are methods were used to evaluate the links between variables, such as attack frequency and cybersecurity investment.

Deductive Statistics.

Information Visualization.

Data linkages, distributions and trends were visualized using charts and graphs.

Comparative analysis. Comparing performance to industry benchmarks is known as "comparing against standards." These steps support data analysis to spot trends, evaluate security flaws and develop cybersecurity plans.

Qualitative Data Analysis.

The themes were grouped to afford an idea of the pros, cons as well as shortcomings in the current state of affairs of the CCI [24]. This analysis sharpens our awareness of factors influencing CCI applicability and efficiency on the human and situational levels. The following methodical procedure was used to identify and classify themes in the qualitative data analysis.

- **Data Familiarization.** To comprehend the entire content and spot reoccurring themes or patterns, the data were carefully examined through different research studies.
- **First coding.** The data was divided into segments and particular codes or labels were applied to each segment to represent its main idea such as "challenges," "strengths," or "areas needing improvement."
- **Subject Identification.** These codes pertain to "training needs" and "resource limitations" that could be combined under a subject such as "Challenges in CCI."

Research Studies Criteria.

The research area has been selected based on the following criteria;

- Specially focused on cyber security and cyber counterintelligence.
- Strategic or system formulation related to cyber security and cyber counterintelligence.
- Must be related to some more vulnerable areas like the banking sector, law enforcement agencies and state institutions.

Framework for Analysis.

The study of CCI in Pakistan was organized into three main categories.

- **Strengths and Weaknesses.** A breakout of the current status of CCI in general, specific entities, educational awareness and technological milieu.
- **Vulnerabilities and Gaps.** This includes such factors as the identification of vulnerable or lacking sections in critical areas such as power, money, or medication. Hypotheses consist of incidence rates, the seriousness of the incidents and the absence of countermeasures.
- **Data Protection.** Exploring the current data protection policies, breach reports, companies and individuals affected and response time.

Ethical Considerations.

The study involves the typical consideration to improve the overall cyber threat landscape of Pakistan specifically in a public sector.

Limitations.

The data has been retrieved from public resources therefore their exists probability threat the exact no of cases, may not accurately represent the exact number of incidents. Thus, the data is rather dynamic, as the nature of cyber threats is dynamic and changes all the time. The incidents considered in the research are limited to those that have been covered by the media [25].

Results and Discussion.

Strengths of CCI in Pakistan.

The level of understanding of the risks related to cybersecurity is increasing at the governmental and business levels. Expenditures on awareness programs indicate that it is not passive that organisms understand the new tendencies of the cyber threat and the importance of not being reactive regarding them.

The threatening advancements in Pakistan's cybersecurity technologies and infrastructure have been striking lately [26]. The country has made significant investments in cybersecurity, allowing it to effectively detect and mitigate potential threats. By leveraging modern technologies, the protection of critical infrastructure has been strengthened. These enhancements signify a positive step towards the relative development of a coherent framework of cyber

counterintelligence capabilities. However, it should be noted that these strengths should be used to correct the weaknesses and risks that have been pointed out, resulting in the formation of a stronger and more efficient cybersecurity shield.

The nation's capacity to identify and address cyber threats has improved as a result of modern advancements, as well as the use of AI-driven threat detection systems, expanded cybersecurity awareness initiatives and international partnerships. These initiatives are significant advances in Pakistan's direction of developing a stronger cybersecurity infrastructure.

Weaknesses of CCI.

Despite its strengths, several issues hinder the effectiveness of CCI [27].

- **Limited Resources.** Lack of funds and the use of old technologies limit the organizations in their capability to fight new threats. It also insists upon the massive investment in modernizing technology and providing appropriate financial assistance.
- **Lack of Collaboration.** This has the effect of hindering systematic assessment of threats and an integrated approach in the assessment and combating of threats among the CCI stakeholders. Meeting this then calls for a more coordinated and integrated structure.
- **Weak Legal Framework.** Basically, the existing legal approach to cybercrime is wholly unsuitable having regard to the present legal regimes for dealing with particular cybercrime offenses. It is thus necessary to enhance the legal system for combating the problem of cybercrime.
- **Public Awareness Regarding Cyber Security.** Lack of awareness of threats and general preventive measures makes the general public vulnerable to threats including phishing and social engineering, hence its vulnerability to cyber threats.

Vulnerabilities and Gaps in CCI:

Aspirations are being made by security experts over the flaws and vulnerabilities relating to important infrastructural zones. These are crucial sectors of society and encompass energy, finance and healthcare among others.

Energy Sector.

Thus, the number of cyberattacks is high; they lead to power outages and affect the stability of the energy supply. This sector is at a high risk of being attacked due to the embrace of advancement in technology and poor protection.

Finance Sector.

Sagas arising from the leakage of data have been associated with massive losses. To avoid such incidents, data protection must be improved.

Healthcare Sector.

Medical care has been impersonated and patient information has been hacked causing its impact to be enormous. There is no doubt that upgrading the settings of cybersecurity is the key to healthcare facilities' protection. Thus, weak identities of incident response plans and communication procedures in some areas make them susceptible to cyber threats. This unpreparedness aggravates the effects of attacks and therefore, there should be more focus in efforts aimed at enhancing responsiveness.

Data Protection Challenges.

Pakistan's system for managing personal data has significant weaknesses, leading to violations of privacy and a lack of accountability. These flaws expose individuals' personal information to risks such as hacking, misuse and breaches, making sensitive data highly vulnerable. The lack of rules that provide for notification of data breaches contributes to the situation where timely responses and remedial action cannot be initiated, thus increasing the effects of breaches. Explorations from the official organizations show the extent of the issue. Fifteen data breaches occurred in the year 2022 affecting two million clients. Already in the year

2023, 10 breaches have occurred and the number of resulting incidences is 1.5 million people. The following numbers depict how important it is to enhance data protection to ensure it shields critical data [28] [29].

Response Times.

The FIA's National Response Centre for Cyber Crime (NR3C) typically responds to critical cyber incidents within 48 hours, though response times depend on the case's severity and complexity. The NCSC primarily provides advisory and coordination support for cybersecurity efforts, with no publicly defined response time metrics, focusing on prevention and collaboration with other national agencies. [29].

Targeted Sectors.

The NCSC focused on finance, energy and government sectors, while the FIA prioritized telecom, healthcare and education. It also indicates how rampant cyber-attacks are and how different concentrated organizations act based on these patterns. In other words, for the situation to be more effective and to call further for cooperation between various organizations needed to fight cyber threats, the reporting and evaluation also have to be standardized. International criteria, such as those set by NIST and ENISA, recommend responding to high-severity incidents more quickly—ideally within a few hours. Targeted industries, which are found through incident reports and threat information, frequently include energy, healthcare and finance. These industries are important worldwide targets that are frequently targeted. Pakistan should strive to improve in these crucial areas by reducing reaction times and strengthening security measures in line with global norms for increased cybersecurity efficacy.

Results & Analysis.

Here's a comparison of cyber-attack types in Pakistan (2020-2023) across various sectors, including the number of attacks and official sources.

Table 1. Comparison of cyber-attack types in Pakistan (2020-2023) across various sectors

Sector	Year	Type of Attacks	No. of Attacks	Source (2020)
Government	2020	Phishing, Malware	45	FIA, Dawn
Financial	2020	Banking Trojans, Phishing	50	FIA, Express Tribune
Healthcare	2020	Ransomware, Phishing	30	FIA, Dawn
Education	2020	Phishing, DDoS	20	FIA, Express Tribune
Telecom	2020	Phishing, Malware	25	NSC, Dawn
E-commerce	2020	Phishing, DDoS	35	FIA, Business Recorder
Energy	2020	Phishing, Malware	15	NSC, Dawn
Government	2021	Ransomware, DDoS	60	FIA, Tribune
Financial	2021	Ransomware, Phishing	75	FIA, Dawn
Healthcare	2021	Data Breach, Ransomware	50	NSC, Geo News
Education	2021	Data Breach, Ransomware	35	FIA, Dawn
Telecom	2021	DDoS, Ransomware	45	NSC, Express Tribune
E-commerce	2021	Data Breach, Phishing	50	FIA, Dawn
Energy	2021	Ransomware, DDoS	30	FIA, Express Tribune
Government	2022	Ransomware, Data Breach	70	NSC, Dawn
Financial	2022	Data Breach, Phishing	80	FIA, Business Recorder
Healthcare	2022	Ransomware, Data Breach	65	NSC, Express Tribune
Education	2022	Ransomware, Phishing	40	FIA, Geo News
Telecom	2022	Phishing, Data Breach	55	NSC, Geo News
E-commerce	2022	Phishing, Malware	60	FIA, Express Tribune
Energy	2022	Phishing, Data Breach	40	NSC, Business Recorder
Government	2023	Phishing, APTs	85	NSC, Geo News

Financial	2023	Phishing, Ransomware	90	FIA, Express Tribune
Healthcare	2023	Phishing, Ransomware	70	NSC, Business Recorder
Education	2023	Data Breach, Phishing	55	FIA, Dawn
Telecom	2023	DDoS, Ransomware	65	NSC, Business Recorder
E-commerce	2023	Ransomware, Phishing	75	FIA, Geo News
Energy	2023	APTs, Ransomware	50	NSC, Dawn

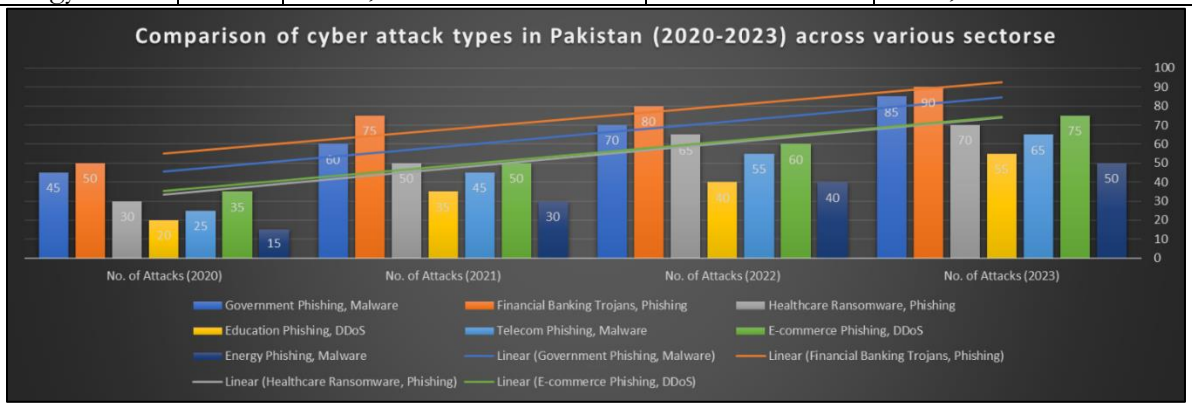


Figure 1. Comparison of cyber-attack types in Pakistan (2020-2023) across various sectors

Key Observations.

- **Government Sector.** They are consistent and diverse threats and the attack scale grows from 45 attacks in 2020 to 85 in 2023. [Sources. Daily FIA, Dawn, Tribune, NSC, Geo News.
- **Financial Sector.** A high propensity of attacks; the number of attacks progressively increases from 50 in 2020 to 90 in 2023, underlining the sector's openness. [Sources. The following dailies were used in this study. Financial Information Agency, Express Tribune, Dawn and Business Recorder.
- **Healthcare Sector.** Rising strikes such as ransomware and data breaches; from 30 in the year 2020 to 70 in the year 2023. Sources. FIA, Dawn, NSC, Geo News, Express Tribune and Business Recorder.
- **Education Sector.** An attack number that increases over time from 20 cases in 2020 to 55 in 203 with a focus on greater exposure or risk. Sources. There are five sources namely FIA, Express Tribune, Dawn and Geo News.
- **Telecom Sector.** An increase in the constant attack from 25 in 2020 to 65 in 2023, including various kinds and types of attacks, of which 54% were DDoS attacks and 27% of ransomware attacks. Sources. Source selection was based on their circulations in Pakistan [Newspaper. NSC, Dawn, Express Tribune, Geo News, Business Recorder
- **E-Commerce Sector.** From 35 in 2020 to 75 by the end of 2023 using phishing, DDoS and malware types of attack. [Sources. An analysis of the specified news sources will, therefore, include FIA, Business Recorder, Dawn, Express Tribune and Geo News.
- **Energy Sector.** Sustained or increased rates of attacks from 15 in the year 2020 to 50 of attack in the year 2023 portraying a growing interest of the adversaries in the cyber domain. Sources. Newspaper sources included NSC, Dawn, Express Tribune and Business Recorder.

Table 1 provides a comprehensive overview of how specific vulnerabilities in different sectors correlate with the types of cyberattacks they experience. The increasing ratio of incidents highlights the growing threat landscape, with varying degrees of social, economic and financial impact across sectors. Each sector's unique vulnerabilities and attack types underscore the need for tailored cybersecurity strategies.

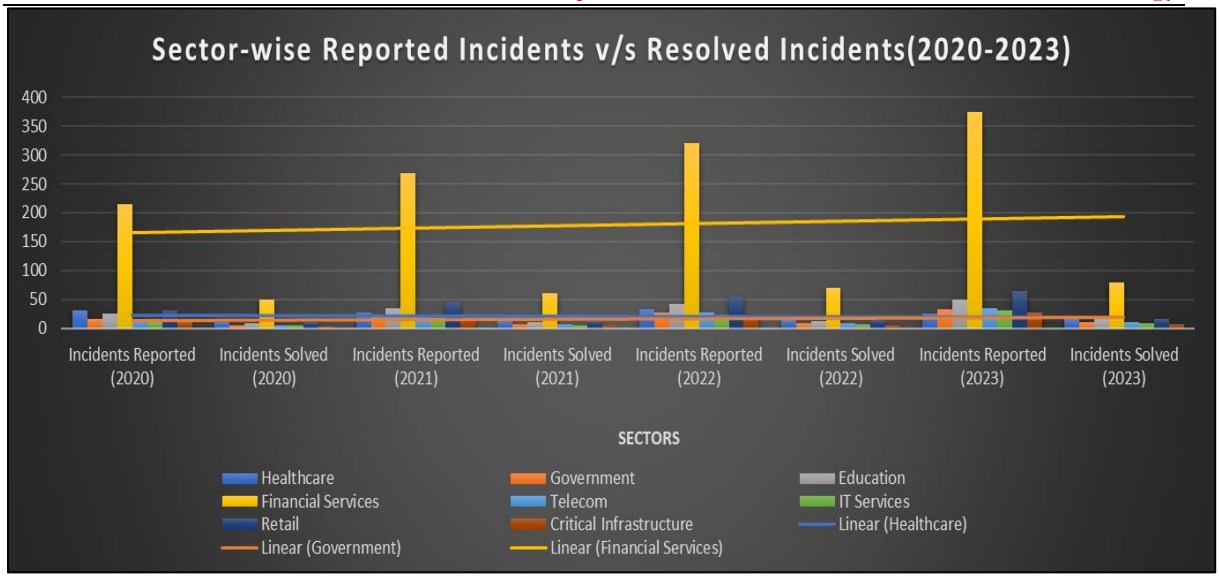


Figure 2. Comparison of cyber-attack types in Pakistan (2020-2023) across various sectors

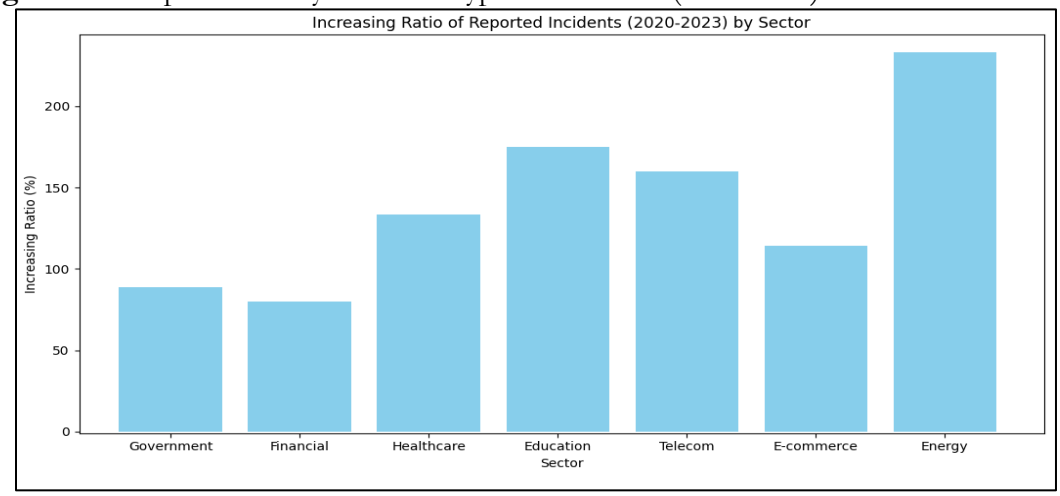


Figure 3: Increasing Ratio of Reported Incidents (2020-2023) by Sector

Key Factor Analysis.

Government Sector.

Attack Types. Phishing, Ransomware, Data Breach.

Correlation. Outdated systems and insufficient funding make the government sector highly vulnerable to these attack types. Phishing and ransomware are particularly prevalent, leading to significant social and economic disruptions.

Impact. Financial losses stem from increased cybersecurity expenses and the interruption of public services.

Financial Sector.

Attack Types. Phishing, Banking Trojans, Ransomware.

Correlation. The complexity of IT infrastructure and the sensitivity of financial data make this sector a prime target for phishing and ransomware attacks, resulting in increasing incidents.

Impact. Economic instability and significant financial losses due to breaches and recovery efforts.

Table 2. Sector-wise Reported Incidents v/s Resolved Incidents (2020-2023)

Sector	Incidents Reported (2020)	Incidents Solved (2020)	Incidents Reported (2021)	Incidents Solved (2021)	Incidents Reported (2022)	Incidents Solved (2022)	Incidents Reported (2023)	Incidents Solved (2023)
Healthcare	30	10	27	12	32	14	26	16
Government	15	5	22	6	28	8	32	10
Education	25	8	35	10	42	12	50	15
Financial Services	215	50	268	60	320	70	375	80
Telecom	15	5	21	6	28	8	35	10
IT Services	12	4	17	5	23	6	30	8
Retail	30	10	45	12	55	14	65	16
Critical Infrastructure	10	3	18	4	22	5	27	6

This table presents a detailed year-by-year comparison of reported and solved incidents for various cyberattack types and their impact on different sectors in Pakistan from 2020 to 2023.

Table 3. Sector Vulnerabilities, Attack Types and Correlation with Reported Incidents (2020-2023)

Sector	Vulnerabilities	Attack Types	Reported Incidents (2020-2023)	Increasing Ratio (%)	Social Impact	Economic Impact	Financial Impact	Sources
Government	Outdated systems, Insufficient funding	Phishing, Ransomware, Data Breach	45 (2020) to 85 (2023)	89%	Disruption in public services, loss of trust	Delays in government projects, increased spending on cyber defenses	Financial losses due to interrupted services and increased cybersecurity expenses	FIA, Dawn, NSC, Geo News
Financial	High data sensitivity, Complex IT infrastructure	Phishing, Banking Trojans, Ransomware	50 (2020) to 90 (2023)	80%	Loss of customer trust, potential personal financial losses	Economic instability due to large-scale financial breaches	Huge financial losses from theft, ransomware payments and recovery costs	FIA, Express Tribune, Dawn, Business Recorder
Healthcare	Lack of cybersecurity awareness, Critical nature of services	Ransomware, Data Breach, Phishing	30 (2020) to 70 (2023)	133%	Compromised patient data, disruptions in critical care	Increased healthcare costs, delays in medical procedures	Financial burdens due to ransomware payments, data recovery and potential lawsuits	FIA, NSC, Geo News, Express Tribune, Business Recorder
Education	Low-security awareness, High user turnover	Phishing, Data Breach, DDoS	20 (2020) to 55 (2023)	175%	Loss of personal data, disruption of	Increased costs for improving cybersecurity, loss of reputation	Financial losses due to data breaches and necessary security upgrades	FIA, Dawn, Geo News, Express Tribune

					educational activities			
Telecom	Critical infrastructure dependency, Complex network systems	DDoS, Phishing, Ransomware	25 (2020) to 65 (2023)	160%	Disruptions in communication services, loss of customer trust	Economic impact due to downtime in communication services	Financial losses from DDoS attacks, ransom payments and repair costs	NSC, Dawn, Express Tribune, Geo News, Business Recorder
E-commerce	The high volume of transactions, Customer data sensitivity	Phishing, DDoS, Malware	35 (2020) to 75 (2023)	114%	Loss of customer trust, identity theft, disruption of online services	Reduced economic activity in the online market, loss of consumer confidence	Financial losses from theft, fraud and increased cybersecurity investments	FIA, Business Recorder, Dawn, Express Tribune, Geo News
Energy	Critical infrastructure, Outdated technology	Phishing, Ransomware, APTs	15 (2020) to 50 (2023)	233%	Disruptions in energy supply, potential public safety risks	Widespread economic impact due to energy outages, increased costs for upgrading security	Financial losses from operational disruptions, potential ransom payments and increased security costs	NSC, Dawn, Express Tribune, Business Recorder

Healthcare Sector

- **Attack Types.** Ransomware, Data Breach, Phishing.
- **Correlation.** The lack of cybersecurity awareness in critical services correlates with a sharp rise in incidents, particularly ransomware and data breaches.
- **Impact.** The sector faces increasing financial burdens due to recovery costs and potential lawsuits, with severe social impacts on patient care.

Education Sector.

- **Attack Types.** Phishing, Data Breach, DDoS.
- **Correlation.** Low-security awareness and frequent user turnover contribute to a steep rise in
- incidents, with phishing and DDoS attacks being particularly common.
- **Impact.** Financial losses result from the need for security upgrades and handling data breaches, with significant social impacts on educational activities.

Telecom Sector.

- **Attack Types.** DDoS, Phishing, Ransomware.
- **Correlation.** The telecom sector's dependency on complex network systems makes it vulnerable to DDoS and ransomware attacks, leading to a substantial increase in incidents.
- **Impact.** Economic and financial losses are incurred due to downtime and the costs of mitigating attacks.

E-Commerce Sector.

- **Attack Types.** Phishing, DDoS, Malware.
- **Correlation.** High transaction volumes and sensitive customer data make this sector susceptible to phishing and DDoS attacks, resulting in a significant increase in incidents.
- **Impact.** Financial losses arise from theft, fraud and the costs of enhancing cybersecurity measures, with social impacts on consumer trust.

Energy Sector.

- **Attack Types.** Phishing, Ransomware, APTs (Advanced Persistent Threats).
- **Correlation.** The critical nature of energy infrastructure and outdated technology correlate with a dramatic rise in incidents, particularly APTs and ransomware.
- **Impact.** The sector experiences severe financial losses from operational disruptions and ransom
- payments, with widespread social and economic consequences due to energy outages.

Table 4. Provides a clear and organized summary of the key terms and metrics used throughout the research, helping to maintain consistency and clarity.

Term/Metric	Description
Reported Incidents	The total number of cyberattacks officially recorded in various sectors from 2020 to 2023.
Resolved Incidents	The number of incidents successfully addressed by cybersecurity authorities indicates response effectiveness.
Attack Types	Categories of cyber threats such as Phishing, Ransomware, DDoS and Data Breaches, classifying the nature of the attacks.
Response Time	The time taken by organizations to respond to reported incidents.
Vulnerabilities	Specific weaknesses within sectors that make them prone to cyber threats are correlated with the frequency of attacks.
Years (2020-2023)	The time frame of the study was used to track trends and patterns in cyber incidents.
Economic Impact	The effect of cyberattacks on the economic stability of affected sectors, particularly Finance and Healthcare.
Social Impact	The broader societal implications of cyberattacks include loss of public trust and disruption of essential services.
Financial Impact	The direct financial losses incurred due to cyberattacks, especially in sectors like Finance and E-commerce.
Sectors	The different industries analyzed in the study, such as Government, Finance, Healthcare and Energy.
Quantitative Data	Numerical data (e.g., number of attacks, statistics) used for statistical analysis and trend identification.
Qualitative Data	Insights gathered from research studies, media related to cyber-attacks, counter cyber intelligence and others.
Sources	References to data origins, such as FIA, NSC and major news outlets, ensure credibility and traceability.

Table 5. Detailed Comparative Analysis of Sector-Specific Vulnerabilities and Response Effectiveness

Sector	Reported Incidents (2020)	Resolved Incidents (2020)	Reported Incidents (2021)	Resolved Incidents (2021)	Reported Incidents (2022)	Resolved Incidents (2022)	Reported Incidents (2023)	Resolved Incidents (2023)	Increase in Incidents (2020-2023)	Increase in Resolved Incidents (2020-2023)	Resolution Ratio (2020)	Resolution Ratio (2023)
Healthcare	30	10	27	12	32	14	26	16	+21%	+60%	33.3%	61.5%
Government	15	5	22	6	28	8	32	10	+113%	+100%	33.3%	31.3%
Education	25	8	35	10	42	12	50	15	+100%	+87.5%	32.0%	30.0%
Financial Services	215	50	268	60	320	70	375	80	+74.4%	+60.0%	23.3%	21.3%
Telecom	15	5	21	6	28	8	35	10	+133%	+100%	33.3%	28.6%
IT Services	12	4	17	5	23	6	30	8	+150%	+100%	33.3%	26.7%
Retail	30	10	45	12	55	14	65	16	+116%	+60.0%	33.3%	24.6%
Critical Infrastructure	10	3	18	4	22	5	27	6	+170%	+100%	30.0%	22.2%

This detailed analysis provides a comprehensive view of sector-specific vulnerabilities and the effectiveness of response measures over the years, highlighting trends and areas for improvement.

Healthcare Sector.

The sector's resolution ratio improved dramatically from 33.3% to 61.5%, with a 21% increase in reported events and a 60% increase in cases that were resolved. The increase in attacks emphasizes the necessity of continuous cybersecurity improvements to safeguard patient data.

Government Sector.

The number of reported events in the government sector increased by 113%, while the number of cases resolved increased by 100%. However, the resolution ratio fell marginally from 33.3% to 31.3%. This shows that there are increasing weaknesses that need to be fixed to protect national security.

Education Sector. An increase of 87.5% was seen in resolved events, while reported occurrences doubled. The resolution ratio decreased from 32.0% to 30.0%, indicating that stronger security protocols are required to protect educational data.

Financial Services industry.

The number of reported events and resolved cases in the financial industry increased by 74.4% and 60%, respectively. The resolution ratio decreased from 23.3% to 21.3%, indicating the necessity of more robust protection against cyberattacks related to finance.

Telecom Sector.

The reported events in the telecom sector increased by 133%, while the number of handled cases increased by 100%. The resolution ratio decreased from 33.3% to 28.6%, suggesting that more protection is required to preserve network integrity.

IT Services Sector.

There was a 150% increase in reported events and a 100% increase in resolved incidents. The resolution ratio fell from 33.3% to 26.7%, highlighting the necessity of better incident handling.

Critical Infrastructure Sector.

The resolution ratio decreased from 30.0% to 22.2% due to a 170% increase in reported events and a 100% increase in cases that were resolved. The surge in attacks targeting vital infrastructure underscores the pressing requirement for strengthened security.

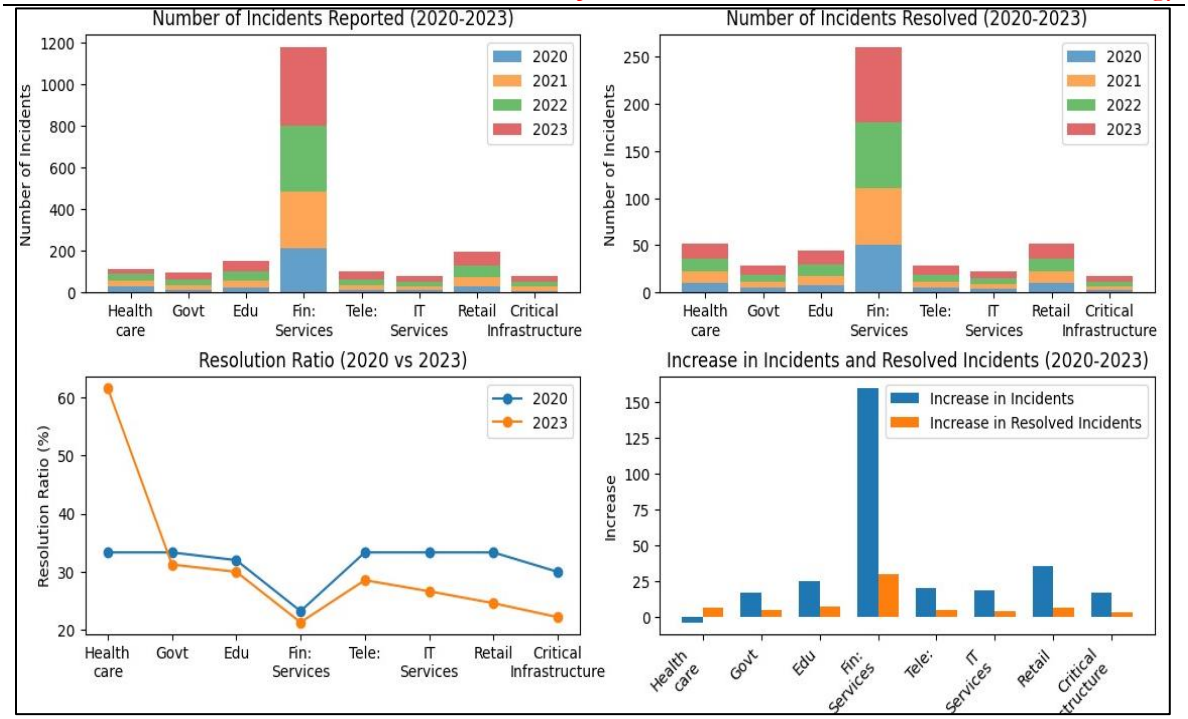


Figure 4: Comprehensive and Discusses the Implications of Increasing Attack Ratios

Recommendations.

To enhance Pakistan's Cyber Counter Intelligence capabilities, the following recommendations are proposed.

Standardized Reporting.

It is suggested that the cyber security departments should collectively prescribe a standard reporting & analysis mode to measure and report cybersecurity breaches. This will help to create awareness regarding Pakistan's cyber threats, which can be followed by designing proper countermeasures. Standardizing reporting and assessment procedures amongst cyber security department is essential to strengthen Pakistan's cybersecurity posture. By putting in place a uniform reporting system, you can guarantee reliable data gathering and make accurate cyber threat analysis for reaction plans. Standardization will improve cooperation, give more precise insights into threat patterns and simplify countermeasure coordination. Pakistan may enhance its cybersecurity framework and effectively tackle new threats by implementing a unified reporting and evaluation strategy.

Enhanced Coordination.

It is crucial to emphasize the ability to work close-knit among the stakeholders dealing with Cyber counterintelligence. Establishing well-defined channels for interaction will help in extensive threat analysis and co-ordinate with cyber threats.

Legal Framework Enhancements.

Review and strengthen the cybercrime laws to put in check the new emerging threats. Equip the police forces with latest tools to fight hackers and prosecute them. It is imperative to have a strong legal framework to secure confidential data, guarantee corporate responsibility and foster customer confidence. Robust regulations enforce stringent security protocols, expedite timely reaction to breaches and discourage cybercrime, ultimately augmenting cybersecurity and cultivating a safe and secure digital landscape.

Public Cybersecurity Education.

There should be advocacy for the critical steps in cyber security. Post all the educational resources to make people less vulnerable to social engineering and phishing attacks. Public awareness initiate statewide campaigns across media platforms, arrange educational seminars

and workshops, collaborate with tech businesses to provide resources, develop interactive online tools and include cybersecurity education into the curriculum to increase public knowledge of cybersecurity concerns.

International Collaboration.

It is necessary to become member of international cybersecurity organizations and reflect on the issues of the country's cybersecurity situation in forums to obtain technical assistance and develop cooperation in joint cyber operations.

Cybersecurity Awareness.

Pakistanis have limited awareness of basic cyber threats and protection techniques, making them vulnerable to theft or fraud. The absence of information security education and adequate learning resources contributes to this issue.

International Cooperation.

Pakistan is endeavoring to establish strong linkages global cybersecurity partners to access to critical data, and to set support and collaborative opportunities. Pakistan needs to actively engage in international collaborative initiatives in the domain of cybersecurity. Joining forums, sharing information and working with other nations will improve the understanding of global threats, new technologies and various aspects of CCI.

Evolving Cyber Threat Landscape.

Pakistan's cybersecurity environment is dynamic requiring prompt and proactive attention at all times. The actors and non-governmental organizations use sophisticated methods to interfere, infiltrate, or attack important structures..

Understanding Threats.

- **State-Sponsored Attacks.** Cyber warfare sponsored by other countries are possible threat to Pakistan's core infrastructures similar to energy facilities and government networks. These attacks can be from nearby countries or groups with strategic world interests.
- **Non-State Actors.** Terrorists, criminals and their groups also present a major threat in cyberspace. Some of them may attack websites to write messages on their web pages or post virus links, stealing information, or stop services from running to meet their parochial goals.
- **Insider Threats.** Disgruntled employees or contractors are likely to hold a negative attitude toward their organization and may decide to act negatively with the intent to harm that organization. Even these internal threats should also be looked at and prevented as they are part of internal and extensive security threats.

Counter-Cyber Intelligence Strategies.

- **Implement Advanced Detection Systems.** The public sector should focus on AI and ML implementation to detect irregularities in the network traffic at the moment accordingly rules & regulations and policies should be implemented as per regulatory authorities' directives.
- **Foster Collaboration.** Pakistan should provide inputs about threats to friendly countries and world cyber organizations so that they get a snapshot of future threats.
- **Enhance Cyber Defenses.** Industries such as defense, finance and energy cannot afford to have their databases and computer systems breached as prone to having their security checked, updated security software and complex encryptions among others.
- **Fostering Cybersecurity Professionals.** Organizations should ensure the presence of well-trained and certified personnel in cybersecurity to set up a competent workforce for counterintelligence. They should be proficient in the processes of putting in place and managing strong security features.

- **Legal Framework for Cybersecurity.** Legal frameworks should be developed as measures to reduce cybersecurity risks. These policies should incorporate the cybersecurity standards as well as should prescribe the severe consequences in case of cyber-attacks.
- **Public Cyber Literacy**. One approach is to educate the general population about various cyber threats and provide guidance on how individuals can protect themselves from becoming easy targets for attacks. To enhance the level of knowledge among users, awareness campaigns should be based on phishing, social engineering and other frequently used forms of exploitation.

To sum up, Pakistan needs to advance the respective plans to enhance the general capabilities in the cyberspace of a nation to react and prevent the negative impacts of cyber incidents. These should contain specific details on what communication, containment and corrective action plans are. Thus, increased development of cyber intelligence is required to preserve the security of Pakistan as a result of new cyber threats. The nation needs to protect itself from hostile governments and even outcome individuals by embracing the newest technologies, developing international relationships and creating efficient cybersecurity legislation. In this case, through training the personnel and sensitizing the public, much can be done to provide Pakistan with the right defense against cyber criminals hence creating room for a secure cyberspace in the country.

Correlation between Vulnerabilities and Attack Types.

Healthcare Industry.

- **Vulnerabilities.** Outdated security procedures and insufficient encryption lead to data breaches.
- **Attack Types** that target patient records include ransomware and data theft.
- **Cybersecurity Strategies.** Put in place strong encryption, frequent security updates and phishing and social engineering awareness training for staff members.

Sector of Government.

- **Vulnerabilities** include antiquated legacy systems and inadequate security for sensitive data.
- **Attack Types.** Advanced Persistent Threats (APTs) and state-sponsored cyber espionage.
- **Cybersecurity Strategies i**nclude regular penetration testing, improving Multi-Factor Authentication (MFA)and upgrading legacy systems.

Education Sector.

- **Vulnerabilities.** Inadequate student data protection and weak network security.
- **Attack Types.** Ransomware and phishing attempts directed at educational establishments.
- **Cybersecurity Strategies.** Boost network security, put in place thorough access controls and give staff and students cybersecurity training.

Financial Services.

- **Vulnerabilities** include weak fraud detection systems and vulnerable financial transactions.
- **Attack Types**. Ransomware and financial fraud are targeted against private financial information.
- **Cybersecurity Techniques.** Install sophisticated fraud detection systems, make sure all transactions are encrypted and update security procedures regularly.

Telecom Industry. Weak network architecture and insufficient communication channel protection are examples of vulnerabilities.

- **Attack Types.** Data breaches and Denial-of-Service (DoS) attacks directed against communication networks.
- **Cybersecurity Strategies.** Use DDoS prevention techniques, strengthen network resilience and encrypt communication channels.

IT Sector.

- **Vulnerabilities** include insufficient patch management and insecure software.
- **Attack Types** include malware and zero-day exploits that make use of software flaws.
- **Cybersecurity Techniques.** Use cutting-edge threat detection tools, enforce strict patch management and carry out frequent security assessments.

Retail Industry.

- **Vulnerabilities** include inadequate security measures for online transactions and inadequate protection of client payment information.
- **Attack Types.** Cybersecurity breaches and credit card fraud.
- **Cybersecurity Techniques.** For transactions, use robust encryption, improve payment security protocols and conduct frequent vulnerability assessments.

Critical Infrastructure Sector.

- **Vulnerabilities.** Outdated security measures and inadequate protection of critical services.
- **Assault types** that target critical infrastructure include sabotage and disruptive attacks.
- **Cybersecurity Strategies.** Put in place strong security procedures, evaluate risks frequently and make sure backup and redundancy mechanisms are in place.

Developing successful cybersecurity strategies requires an understanding of the relationship between attack types and vulnerabilities particular to a certain industry. Adapting defenses to these weaknesses lowers risks and improves security posture generally across several industries.

Increasing Sophistication of Cyberattacks.

Currently, Pakistan, along with many nations worldwide, is witnessing a consistent rise in complex cybercrimes. These complex threats are affecting nations and core institutions of a country's social structure, as well as the commercial enterprises in the private sector. It strongly threatens national security, economic development and people's trust. The aforementioned intricate cyber threats need to be recognized and dealt to have an efficient cybersecurity approach.

Attributes of some of the advanced cyberattacks are as follows.

- APTs which are intricate and time-consuming cyber threats intended to procure confidential data, including privileged information and jeopardize business operations. The governmental and infrastructural entities of Pakistan are frequently in the crosshairs of APTs that aim to steal relevant information or perform selective sabotage.
- Zero-day exploits are types of cyberattacks that involve vulnerabilities which have been recently discovered and have not yet been fixed. Presently, Pakistan depends heavily on digital technologies and hence is exposed to what is referred to as zero-day vulnerabilities, which can result in large-scale privacy intrusions before the release of the corresponding security fix.
- **Ransomware Evolution.** Hacker have started using ransomware to encrypt data and ask for a ransom. Two forms of pressure are applied to the victim. 1) it proves that the attacker is capable of extorting money from the victim and 2) it is that the attacker is capable of attacking the victim's clients.

- **Fileless Malware.** This makes it hard to detect by standard means. - Advanced malware that counteracts the antivirus companies and does not alert the owner upon entering a business house.
- **AI and Machine Learning.** This results in pinning AI and machine learning-aided phishing and critical evading frontier that brings challenges to Pakistani cybersecurity.

Impact of Cyber Attack.

- **Financial Consequences.** It makes the computers and other related properties vulnerable to theft and may disrupt business operations and tendencies, besides the costs associated with attacks incidences across private and public firms.
- **National Security Threats.** Targeting such important systems as the power supply, communication and defense most definitely is a potential threat to the security of any given nation. They can result in acts such as spying, destruction of facilities and products and general harming of organizational plans and initiatives.
- **Reputation Erosion.** There is a possibility that external threats pose a risk to Pakistani businesses since cyber breaches may cause Pakistani businesses to lose of reputation inclusive of loss of customer trust not to mention the legal obligations.
- **Intellectual Property Theft.** Pakistani companies may be vulnerable to such cyber attackers that seek to steal intellectual property from the companies and place such organizations in a disadvantaged position making the economy suffer.

Economic Impacts.

- **Financial Losses.** Some of the financial impacts witnessed in the Bank Islami cyber heist that happened in 2018 and the National Bank of Pakistan (NBP) hack in 2022. These episodes revealed a vulnerability in Pakistan's financial sector, disrupted the operations of banks and corroded the client's trust. Apart from indications of shrinking short-term revenues, long-term damage to branding hampers the attraction of foreign investments and economic growth.
- **Disturbance of Essential Services.** Cyber threats are also capable of making the critical infrastructure company completely non-operational, or unusable, as was evidenced in the ransomware attack by K-Electric in the year 2020. Many more millions of customers were affected by the extensive dislocations in electronic operations as well as in billing by the attack. Besides posing economic losses in the short run, these disruptions also bring out the risks of future attacks on essential services leading to un-specified economic.
- **Data Breaches and Intellectual Property Theft.** The Data breach at Careem, for example, saw the details of more than 14 million consumers' information leaked to the public in 2018 thus eroding consumer trust in digital services. Additionally, the economic competitiveness of Pakistan is under threat from cyber espionage against the country's government and business establishments; putting the possibility of getting hold of intellectual assets and discrete trade secrets at risk.

National Security Impacts.

- **Government and diplomatic communications are compromised.** It can be recalled that in April 2019, Pakistan's Ministry of Foreign Affairs was hacked as a reminder of the possibility of cyberespionage targeting government institutions. To put the country's foreign policy in danger and compromise relations with other nations, the attackers wanted to gather sensitive information and wiretap diplomatic communications.
- **Potential for Cyber Warfare.** The frequency of incidents and increased complexity of the cyber threats are revealed by daily attempts of hacker. Cyber vulnerabilities can be exploited by trusted actors for regime change, disrupt national defense systems, or even

for a long-synchronized attack on strategic facilities, thus threatening the security of States.

Pakistan has no other option but to build a robust CCI that would serve the best interest of the nation and its security by enhancing the institutions capability to detect, prevent and counter cyber threats. In today's world where everything is gradually getting connected the future requires establishing strong, well-equipped and trained cybersecurity mechanisms and global cooperation.

Strategies for Combating Sophisticated Cyber Attacks:

- AI and ML are applied to improve cybersecurity for Pakistani businesses because they analyze and neutralize different complicated threats in real-time mode.
- Supervisory control of operating network traffic and system performance will identify the behavior that resembles advanced threats. This prevents the admittance of problems that may be dangerous to students, staff and faculty members.
- Some of the benefits accruing from the successful adoption of patch management include timely updates, deployment of security patches and protection of areas that are in the awareness of the hackers hence minimizing the probability of breaches.
- As described by the participants, effective incident response plans help Pakistani companies to quickly mitigate cyber threats causing little disruption in business.
- Stress on cyber threats and best practices in line with "check and balance" training procedures for the staff helps to avoid instances of phishing or social engineering attacks.
- Additional countermeasures and threat recognition can be achieved through cooperation with institutions from around the world, regional counterparts, as well as cybersecurity specialists. One of the benefits of information sharing is the sending of early warning signals and coordinated action against cyber assailants.

Conclusions.

Analyzing the anti-CCI scenario Pakistan has been steadily progressing for establishing institutions, increasing awareness and research on cyber defense technologies. Nevertheless, there are many drawbacks, critical security vulnerabilities and desires to preserve data confidentiality. Nonetheless, it is noteworthy that a comprehensive, well-funded and legally mandatory CCI framework is needed to meet these hurdles effectively. This study suggests some measures that can be employed to strengthen.

References.

[1] J. P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehaband M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," Microprocess. Microsyst., vol. 77, p. 103201, Sep. 2020, doi: 10.1016/J.MICPRO.2020.103201.

[2] D. R. Winston, "Narco-Insecurity, Inc", [Online]. Available: https://deepportal.hq.nato.int/eacademy/wp-content/uploads/2022/05/Narco-Insecurity-Inc..pdf

[3] U. ESCAP, "National study on digital trade integration on Pakistan," 2021, [Online]. Available: https://www.unescap.org/sites/default/d8files/knowledge-products/National study on digital trade integration of Pakistan 1.pdf

[4] "Pakistan's banking system witnesses another cyberattack." Accessed: Sep. 09, 2024. [Online]. Available: https://tribune.com.pk/story/1836466/pakistans-banking-system-witnesses-another-cyberattack#google_vignette

[5] "Major cyber attack by India targeting devices of govt, military officials identified: ISPR." Accessed: Sep. 09, 2024. [Online]. Available: https://www.geo.tv/latest/302479-major-cyber-attack-by-india-targeting-devices-of-govt-military-officials-identified-ispr

[6] "Ministry of Foreign Affairs website hacked, inaccesible in several countries - DAWN.COM." Accessed: Sep. 09, 2024. [Online]. Available: https://www.dawn.com/news/1464217

[7] "K-Electric struck by 'ransomware' - Business - DAWN.COM." Accessed: Sep. 09, 2024. [Online]. Available: https://www.dawn.com/news/1578882

[8] "Cyberattack disrupts National Bank of Pakistan services; recovery by Monday likely - Business - DAWN.COM." Accessed: Sep. 09, 2024. [Online]. Available: https://www.dawn.com/news/1655059

[9] "Pakistan International Airlines data breach underscores sharp rise in illicit sales of access credentials | CSO Online." Accessed: Sep. 09, 2024. [Online]. Available: https://www.csoonline.com/article/570117/pakistan-international-airlines-data-breach-underscores-sharp-rise-in-illicit-sales-of-access-crede.html

[10] Shoaib Imtiaz, 김동진and Syed Hassan Ali, "E-Commerce Growth in Pakistan: Privacy, Securityand Trust as Potential Issues," Culin. Sci. Hosp. Res., vol. 26, no. 2, pp. 10–18, Feb. 2020, doi: 10.20878/CSHR.2020.26.2.002.

[11] "Challenges of E-Commerce Adoption Experienced by Pakistani SMEs: A Qualitative Analysis. | International Review of Entrepreneurship | EBSCOhost." Accessed: Sep. 09, 2024. [Online]. Available: https://openurl.ebsco.com/EPDB%3Agcd%3A2%3A1067714/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A163786118&crl=f

[12] X. Liu et al., "Cyber security threats: A never-ending challenge for e-commerce," Front. Psychol., vol. 13, p. 927398, Oct. 2022, doi: 10.3389/FPSYG.2022.927398/BIBTEX.

[13] I. D'adamo, R. González-Sánchez, M. S. Medina-Salgadoand D. Settembre-Blundo, "E-Commerce Calls for Cyber-Security and Sustainability: How European Citizens Look for a Trusted Online Environment," Sustain. 2021, Vol. 13, Page 6752, vol. 13, no. 12, p. 6752, Jun. 2021, doi: 10.3390/SU13126752.

[14] E. U. Haque, W. Abbasi, S. Murugesan, M. S. Anwar, F. Khanand Y. Lee, "Cyber Forensic Investigation Infrastructure of Pakistan: An Analysis of the Cyber Threat Landscape and Readiness," IEEE Access, vol. 11, pp. 40049–40063, 2023, doi: 10.1109/ACCESS.2023.3268529.

[15] "CYBERSECURITY AND CHALLENGES FACED BY PAKISTAN." Accessed: Sep. 09, 2024. [Online]. Available: https://www.researchgate.net/publication/361218515_CYBERSECURITY_AND_CHALLENGES_FACED_BY_PAKISTAN

[16] M. Hijji and G. Alam, "A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats during the COVID-19 Pandemic: Challenges and Prospective Solutions," IEEE Access, vol. 9, pp. 7152–7169, 2021, doi: 10.1109/ACCESS.2020.3048839.

[17] A. K. Torres, "Assessing the New Type of Cyberwar: A Qualitative Exploratory Study of Technology Dependence Facilitating the Current Rise of Cyberterrorism," Color. Tech. Univ., 2024.

[18] F. J. Haberl, "Jihadi Intelligence and Counterintelligence," 2023, doi: 10.1007/978-3-031-24744-6.

[19] M. M. Khurshid, "Open government data adoption model for public sector organizations in Pakistan," 2022, Accessed: Sep. 09, 2024. [Online]. Available: http://dms.library.utm.my:8080/vital/access/manager/Repository/vital:150591

[20] "Civil Military Cooperation (CIMIC) in Cyber Security Domain." Accessed: Sep. 09, 2024. [Online]. Available: https://www.humapub.com/admin/alljournals/gsssr/papers/U7ZF3gFIxi.pdf

[21] N. J. L. R. Zahoor, R., "Review, Analyzing the Cyberspace Laws to Protect Data Privacy in Pakistan," Univ. Bras., vol. 13, no. 2, pp. 42–55, 2021.

[22] S. A. Jaffery, "An Empirical Analysis to Control Product Counterfeiting in the Automotive Industry's Supply Chains in Pakistan," Doctoral, Jan. 2021, doi: https://doi.org/10.21427/EC7E-KD93.

[23] S. A. A. Bokhari, "A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan," Soc. Sci. 2023, Vol. 12, Page 629, vol. 12, no. 11, p. 629, Nov. 2023, doi: 10.3390/SOCSCI12110629.

[24] "The Cyber Defense Review - vol. 7 No. 2 Spring 2022." Accessed: Sep. 09, 2024. [Online]. Available: https://www.researchgate.net/publication/360745730_The_Cyber_Defense_Review_-_vol_7_No_2_Spring_2022

[25] J. S. Hiller and R. S. Russell, "The challenge and imperative of private sector cybersecurity: An international comparison," Comput. Law Secur. Rev., vol. 29, no. 3, pp. 236–245, Jun. 2013, doi: 10.1016/J.CLSR.2013.03.003.

[26] "The Cyberthreat in the Contemporary Era Challenges for the security of Pakistan." Accessed: Sep. 09, 2024. [Online]. Available: https://www.researchgate.net/publication/358845313_The_Cyberthreat_in_the_Contemporary_Era_Challenges_for_the_security_of_Pakistan

[27] "EFFECTIVE ENFORCEMENT OF CYBER LAWS IN PAKISTAN | Babar Saeed - Academia.edu." Accessed: Sep. 09, 2024. [Online]. Available: https://www.academia.edu/9884036/EFFECTIVE_ENFORCEMENT_OF_CYBER_LAWS_IN_PAKISTAN

[28] T. Yamin and I. He, "Cyberspace Management in Pakistan," Gov. Manag. Rev., vol. 3, no. 1, p. 47, 2018.

[29] K. S. Paul Cichonski, Tom Millar, Tim Grance, "Computer Security Incident Handling Guide," NIST Spec. Publ., pp. 1–79, 2012, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf



Copyright © by authors and 50Sea. This work is licensed under Creative Commons Attribution 4.0 International License.