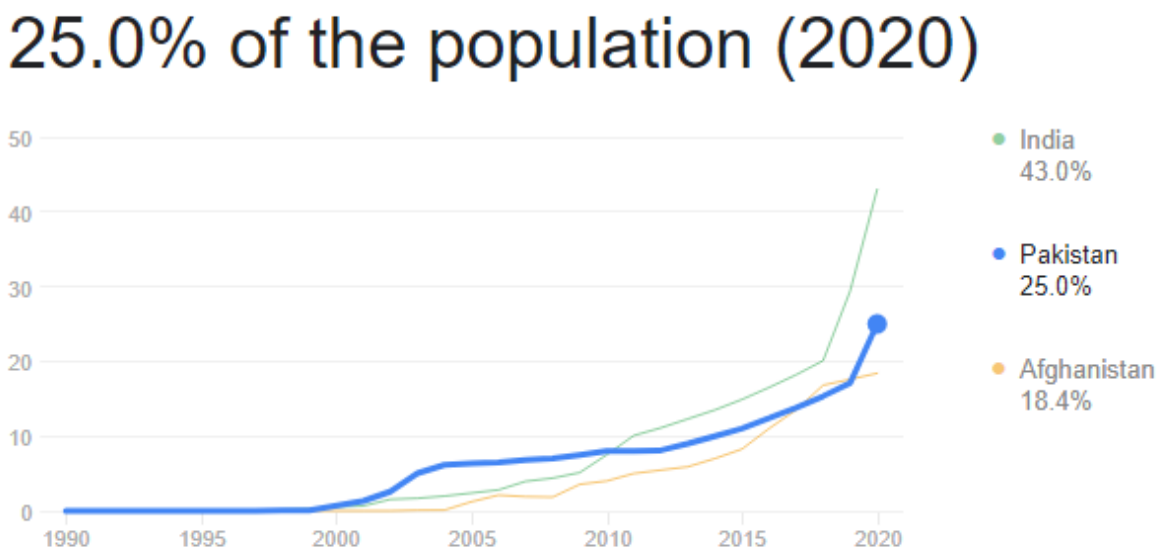
Cyber Security Challenges in Pakistan



(**Users of Internet as per World Bank Data**)

According to the Pakistan Telecommunication Authority's (PTA) 2019 statistics, 55 million people in Pakistan have internet access,

Introduction:

Information and Communication Technologies (ICTs) have played a key role in revolutionizing the world, making it truly a Global Village within the last 2 decades.The growth of technology and dependency on cyberspace offers valuable and essential services for human life's functionality and the environment as well as the challenges and threats. *Cybersecurity is a field that emphasizes protecting computers, servers, information, programs, and networks from unauthorized access, any change or destruction.* Cyber Security requires adequate knowledge of cyber-attacks, and vulnerabilities of ICT, and to know how to improve the critical operating assets in cyberspace.

As revealed by a report by Polish Electronic Firm "Storware", **21st-century world grapples with data privacy concerns and witnesses an average of more than 2,200 cyber-attacks, with about 71.1 million victims of cyber-attacks yearly.** Thus, *Cybersecurity is a massive challenge for several countries as well as Pakistan. Pakistan experiences a fast growing application of the ICT in different sectors but seriously lacks in cyber readiness. However, in 2021, Pakistan formulated its first National Cyber Security Policy, 2021 in order to protect E-Government services, capital markets, corporations, and other businesses Critical defense measures for important cyber services of the country still require a holistic approach.*

Major Cyber Security threats:

1. Ransomware Attacks

It's hacking into the user's sensitive information and denying them access to it until a ransom amount is paid to the hackers. As depicted in the below image where a ransom amount is asked from the user.

2. IoT Attacks (Internet of Things)

The Internet of Things or IoT is the most vulnerable to data security threats. Every digital, mechanical, computing smart device that can transmit data over the internet network are termed as IoT such as; laptop and mobile phones.

In order to access your personal device that contains your sensitive information, hackers use devices surrounding you, such as wearable smartwatches, baby monitors, smart fridges, or smart lights.

3. Cloud Attacks

Cloud computing is the modern age of new technology that has revolutionized the physical world of data storage. Businesses from large to small now utilize cloud services for storing their user-sensitive information.

On the one hand, where adoption of it has reduced the cost and increased efficiency, it has also opened possibilities for data security breaches.

The main reason for compromised data security is the lack of encryption, authentication, and improper configuration of the cloud setups.

4. Phishing Attacks

A phishing attack is a type of social engineering attack that targets users' login details and credit card information. In contrast to ransomware, here the information is used to benefit the hacker.

5. Banking blockchain Attacks

Digital currency or wallets are the most prime target of hackers. Many blockchain attacks have been on the rise due to security breaches.

Importance of Cyber Security:

With hackers constantly trying to find an easy way to make money, it is important to safeguard information that is stored on servers around the world. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. **Computer hackers are unauthorized users** who break into computer systems in order to steal, change or destroy information, often by installing dangerous malware without your knowledge or consent. Through Malwares, hackers gain unauthorized access to your personal information. In absence

of proper cyber security, hackers may

- Gain access to national databases
- Banking softwares and database
- Hijack your usernames and passwords
- Steal your money and open credit card and bank accounts in your name
- Make purchases with other's credit cards
- Use and abuse your Social media accounts
- Sell your information to other parties who will use it for illicit or illegal purposes
- Breach your privacy

Global incidents of Cyber Attacks: facts and incidents;

1. *Globally, According to Cyber Security Statistics, there is an attack every 39 seconds.*

2. *As per Forrester website report,*
   " just three 2 sectors accounted for 80% of all data breaches i.e, technology, government . Government and technology remained major targets of cybercrime in 2017 as well.

3. *Cyber attacks will cost companies $10.5 trillion per year by 2025 (As per EMBROKER INC report)*

4. 90% of data breaches occur as a result of phishing attacks.

5. According to a study by IBM, 95% of cyber security breaches result from human error. This mistake is so overwhelming in cybersecurity that 19 out of 20 cyber breaches result from human error. It includes activities like downloading an infected software and keeping a weak password or through phishing pages.

6. Gartner, a tech advisory firm, stated that spending on information security was total $172 billion in 2022.

Major Attacks (Globally):

Most notable cyber attacks globally are

1) Cyber Attack on US oil pipelines 2021

In 2021, an oil pipeline system was attacked, leading to the largest attack on oil infrastructure in the United States. While the company did work with the FBI and paid the **ransom of $4.4 million**, it still led to a multiple-day shutdown of the system. They also stole 100 gigabytes of data within two-hours.

2. NASA Hacks

In the year 2000, for 21 days of NASA systems offline due to a cyber attack, it impacted two prominent government organizations in the United States known as the Department of Defense (DoD) and NASA.

In 1999, a teenage hacker broke into the networks of the DoD and NASA & downloaded software from NASA worth around $1.7 million.

3. Cyber Attack on Yahoo

In *2013 & 2014*, in a cyber attack, the largest data breach was suffered by yahoo, almost **500 million accounts related data was hacked**. Cases for targeted attacks against high-ranking U.S. Intelligence officials who were impacted by the breach.

4. Cyberattack on SONY playstation network:

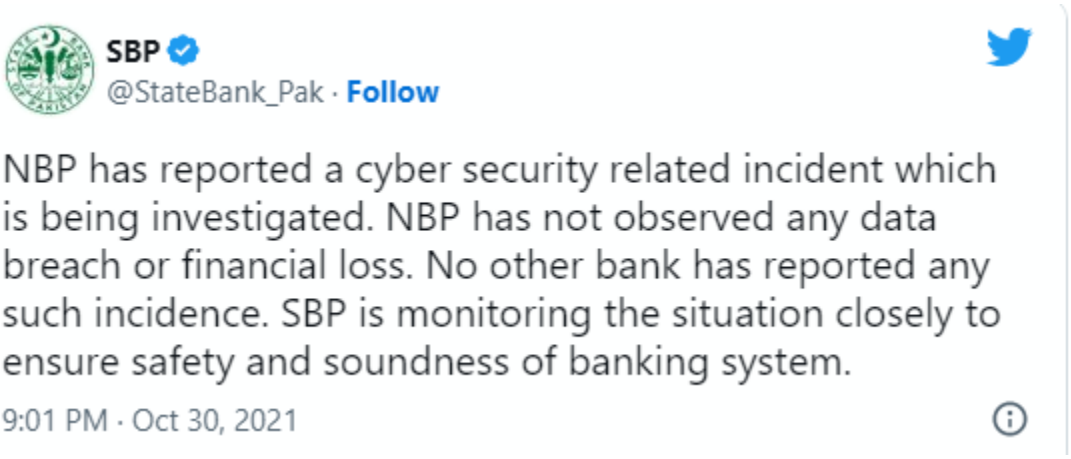
In 2011, Sony Playstation network was under cyber attack, faced 1 month disruption of services and suffered a loss of $170m.

5. Attack on Saudi Aramco:

In 2012, Through the attack, the attackers were able to destroy 30,000 computers' data of the biggest oil producer company of Saudi Arabia by using a virus named "**SHAMOON**" similar to the virus "Stuxnet" which was used to attack Iran's nuclear reactors by Israil.

Cyber Attacks on Pakistan:

1) On National Bank of Pakistan:



2. Daily 9 Lac cyber attacks in Pakistan:

In 2022, Pakistan faced many cyber attacks including on the Sindh High Court website, FBR, PTV Sports and commercial banks

According to **Federal Minister for Information Technology Syed Aminul Haque, over 900,000 hacking incidents take place in Pakistan daily**. Israel is investing heavily in developing cyber weapons and advanced AI systems.

3. Audio Leaks in 2022 ; a very significant cyber security lapse

It was widely tweeted by **Open Source Intelligence Insider @OSINT** that the audio files that have been made public are a collection of discussions that lasted 140 hours. It was for sale on the dark web since August 20th, demanding $3.45 million.

Why Cyber Security is Important for Pakistan:

- ★ As per UNTD report 2017, Pakistan is ranked among top 10 booming digital/internet economies in the world.
- ★ The Global Cybersecurity Index (GCI) placed Pakistan 94th globally having efficient cyber security. According to the report, this poor ranking owes to the country's insufficient measures — legal, technical, organizational, capacity building and cooperation — to upgrade cybersecurity.
- ★ In 2013, Guardian revealed through Snowden's leaks that after Iran, Pakistan was the second most targeted country for surveillance by the US National Security Agency (NSA)

- ☐ Banking system especially SBP data is confidential
- ☐ Indian hackers have previously proved that they could get access to NADRA database and Ministry of Finance data.
- ☐ Emerging trend of mobile wallets and online banking

- ☐ In 2007, Pakistan banks faced more than 200 cyber attacks from India hackers
- ☐ As per World Bank report ,online banking accounts for nearly 75% of all bank transactions, which is increasing, meaning people are leaving cash and cheques and moving to electronic banking, (Hence cyber Security is needed)
- ☐ NADRA holds confidential data of almost all citizens
- ☐ Pakistan's key institutions using **E-Office**
- ☐ Government websites if disrupted by hackers is a challenge to sovereignty and integrity
- ☐ Social Media networks,
- ☐ low awareness in masses of pakistan regarding security protocols, massive computer illiteracy make them vulnerable
- ☐ Most ICT services are based in foreign countries and equipment is imported, there is no mechanism of its examination and forensic that determines whether these are risk-free.
- ☐ Numerous Pakistani organizations, including the Federal Board of Revenue (FBR), Careem, PTV Sports, the website of Sindh High Court, K-Electric, NADRA, Meezan Bank, and Bank Islami, have experienced cyberattacks as well.

Legislation enacted and measures taken by the Government in this Regard:

1) National Cyber Security Policy 2021

NATIONAL CYBER SECURITY POLICY 2021

NCSP 2021 is a comprehensive document emerged as a national policy to tackle cyber security challenges. The objectives of this policy are

- To establish a secure IT-based institutional framework
- To enhance the security of national information systems and infrastructure
- .To create a protection and information sharing mechanism
- To protect National Critical Information Infrastructure
- To create audit mechanism to assess security standards are followed or not
- To ensure the integrity of ICT products, systems, and services by establishing a mechanism of testing, screening and forensics
- To protect the online privacy of the citizens
- To develop public-private partnerships and collaborative mechanisms

- To create a country-wide culture of Cyber Security awareness
- To train skilled Cyber Security professionals through capacity building, skill development
- To encourage and support indigenization and development of Cyber Security solutions through R&D Programs involving both public and private sectors.
- To provide a framework on national-global cooperation and collaborations on Cyber Security.
- Risks related to Cyber Security need to be managed continuously

2) PECA 2016

The government enacted the Prevention of Electronic Crimes Act (PECA), 2016, which lays out penalties for offenders or criminals who are accused of gaining unauthorized access to personal data. It covers a wide range of cybercrimes — cyberterrorism, hate speech, spamming ,fraud and interference with critical infrastructure.

3. NR3C(National Response Centre For Cyber Crime)

National Response Centre for Cyber Crime (NR3C), is introduced by the FIA, primarily to **deal with technology based crimes in Pakistan**. It directly receives complaints and also assists other law enforcement agencies in their own cases.

4. The Electronic Transaction Ordinance 2002 (ETO 2002)

It was enacted to provide legal protection of e-commerce, penalizing violation of privacy and damage to the information system.

5. Instructions of SBP and PTA:

SBP and PTA are entrusted with the responsibility to update relevant stakeholders about the possible cyber security threat and way forward:

Hence, the State Bank of Pakistan (SBP) issues guidelines on Cyber Security for the financial sector, and the PTA has notified the Telecom Computer Emergency Response Team (CERT) to look into the cyber security matters and update the users. ***To undertake academic research, National Center for Cyber Security was established in 2018.*** The **HEC has also formulated new academic degrees that include BS, MS, and Ph.D. Cyber Security** and MS Systems Security programs. However, the demand and supply gap for digital skills

6. Technical bodies of Cyber Security:

Regarding technical measures for cybersecurity, Pakistan has the bodies, namely **Pakistan Computer Emergency Response Team** (Pak CERT) and **Pakistan Information Security Association(PISA),** providing information on cyber threats to provide assistance and capacity building in cybersecurity. **Pakistan launched first-ever National Centre of Cybersecurity (NCCS) at Air University, Islamabad in May 2018**

Challenges:

1. Capacity Issues:

FIA's NR3C can barely deal with cyber attacks as trained/experts' are in want who may be able to trace cyber attacks. According to the official report of the National Response Centre for Cyber Crime , NR3C cannot trace such attacks that are executed by hackers through proxies.

2. Most of the Sophisticated operational and Security softwares are out-sourced to foreign IT firms

Heavy amount is paid to foreign firms but the maintenance and updates required are paid no heed. For instance Accounts and Audit applications often require maintenance and security patches, if not updated timely, billions of rupees funds will be vulnerable to cyber attacks. Indigenous skill development is given no priority.

3. India's emerging Cyber Security capabilities in collaboration with Israel:

India is amongst the top IT related products exporter where it earned more than **$140b** through exports of IT products, more than Saudi Arabia has earned from oil exports. Besides , there are yearly 100000 IT professionals being graduated in India, in the light of these stats, Pakistan is way behind.

4. Low awareness and low computer literacy:

Among masses as well as on an institutional level, low literacy in cyber security make the networks prone to cyber attacks.

5. Low trend of upgrading network security or mobile security:

No culture of paying attention to upgrade security, free anti-virus softwares and applications are preferred, having limited expiry period.

6. Non-Resilient or Non-reliable ICT infrastructure also hampers to digitize the economy and governance:

- ☐ Ministries reluctant to shift to e-filing due to possible security/secrecy breach
- ☐ NSP 2022-2026 favours moving to E-Governance but…
- ☐ Attacks on Pakistan's ICT infrastructure discourage shifting from manual to digitized system
- ☐ Too much reliance on external resources for equipment, systems, softwares and security protocols

7. Weak Enforcement mechanism of Laws:

Self-explanatory, **PAKISTAN IS GOOD AT MAKING EXCELLENT POLICIES BUT WEAK IN ITS IMPLEMENTATION**

Way Forward:

The increasing adoption of ICT requires every country to secure its virtual boundaries in addition to physical boundaries. This is especially true for Pakistan as it experiences fast growing e-government, e-commerce and ebusiness in a security environment which potentially poses serious cyber threats due to volatile regional conflict, extremism and terrorism.Following can be a possible way forward;

1) Adopting Standard Procedures:

As per good practices, the best way to counter cyber-attacks is examine every system including license updates and security risks . So, when a vulnerability is discovered , all affected systems will be timely detected and prevented from damage/breach.

As per NIST cyber security firm of the US helps public and private organization to adapt to updated security protocols and identify the risk by following these steps:

Capability	Description
Identify	What processes and assets need protection?
Protect	Implement appropriate safeguards to ensure protection of the enterprise's assets
Detect	Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents
Respond	Develop techniques to contain the impacts of cybersecurity events
Recover	Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

2. Awareness through print, electronic and social Media:

There has been a rise in mobile phone hacking in Punjab and Sindh, the government can highlight the possible symptoms that can detect whether a phone is possibly hacked: as given below

- *Your phone quickly loses battery.*
- *Your phone is operating unusually slowly.*
- *Your other online accounts show unusual behavior.*
- *You discover strange texts or calls in your logs.*

A possible way forward to protect phones may be ;

- *On your phone, install comprehensive security software.*
- *Updates can close security holes used by thieves to launch their malware-based attacks.*
- *Updates can close security holes used by thieves to launch their malware-based attacks.*
- *Keep a vigilant eye on your phone.*
- *When not in use, turn off your Bluetooth and Wi-Fi.*
- *Avoid using app stores from outside sources.*

These guidelines including some other instructions can be highlighted via media.

3. Sensitizing Masses and Training government employees, private firms, stock market personnels and banking sector regarding security risks and possible way forward.

4. **Promoting cyber Security discipline** within universities of Pakistan as India is one of the leading software exporting countries in the world and produces more than 100,000 IT professionals each year. Pakistan has only 1,50,000 IT professionals available in the market.

5. Securing NADRA Database and Military Assets:

NADRA shares online information of citizens with banks, Election Commission of Pakistan, immigration and passports department, mobile networks and security

departments, these data needs to be secured with proper security protocols. Often, it has been seen, user data are shared with private firms for promotions, this data breach needs to be tackled once and for all.

Furthermore, digitalisation of military assets and nuclear arsenals is the hallmark of their modernisation in the 21st century and Pakistan is no exception in this regard. Though Pakistan has strict security protocols, many countries are skeptical about the security of Pakistan's nuclear weapons. Government can invest in cyber security to build indigenous cyber security mechanisms rather than importing from foreign firms.

6. Preventing Cyber Terrorism:

Terrorists find cyberspace convenient for their cyber terrorism, where they can use cyber space for a number of activities including,communication with other terrorist organizations, propaganda, hate speech, radicalization, recruitment and training via simulations. A strict surveillance is this regard is needed by the law enforcement and intelligence agencies.

Cyberspace is a fifth-generation warfare domain and has recently attracted attention of many developed and developing countries as Cyber Security has led to widespread chaos in the digital world.

7. Countering Indian Cybersecurity capabilities:

According to estimates, 1600 websites were hacked by India from 1999 to 2008. In 2013 Norwegian based firm discovered a cyber attack known as "operation hangover" that originated from India. The purpose was to attack sensitive information and gather militant, government and corporate data.

India-Pakistan cyber-attacks usually occur in the context of important events, such as Independence Day and in a tit-for-tat move. For instance, retaliating to the Indian hackers cyber attack on Pakistan's 40 websites, including that of the State Bank of Pakistan, the Pakistani hackers defaced India's 270 websites, including that of the Central Bureau of Investigation (CBI).

Regarding cyber warfare also needs to be countered:

cyber warfare is a state-sponsored cyber-attack which is usually well-funded, organised and conducted by highly skilled personnel, It is a new form of warfare used to facilitate conventional military attacks. This kind of 'cyber-enabled physical attack' first disrupts critical infrastructures to facilitate a physical attack on a military target. For instance, in *2007, Israel shut down Syria's air defence capabilities using a cyber-attack and launched an air strike on a nuclear reactor in the country,* without being detected. Similarly, Israel damaged Iran's nuclear reactor through a virus called "Stuxnet". The National Security Policy of Pakistan (2022-26) have covered this aspect, hence it should be implemented in letter and spirit.

8. Collaboration and cooperation with China to strengthen our Cyber Security:

India-Israel cybersecurity cooperation under the garb of their comprehensive security cooperation is a threat to Pak's cyber security. The two countries are staunch opponents of Pakistan.Pakistan should go for collaboration and joint venturing in this aspects with friendly countries especially China.

9. Implementation Mechanism of Cyber Security Laws Including National Cyber Security Policy 2021:

As per Symantec report 2018, Pakistan is better in undertaking legal measures for cybersecurity but lacks in capacity building and implementation for countering the cyber-attacks. Hence, proper implementation mechanisms should be our priority.

The NR3C, a unit of the FIA, deals with cybercrimes but there is a problem of institutional capability. The NR3C is deficient in resources and facilities to track down the anonymous activities of the hackers. Pakistan also has some white hat or ethical hackers but their expertise in cybersecurity remain unutilised.

Thank You for Your Attention!