THE CYBER THREAT LANDSCAPE BEYOND THE PANDEMIC

Farooq Naiyer

The impact of the pandemic and the rapid acceleration of digital initiatives in a short time resulted in an increase in the attack surface. It forced nations and businesses to control and manage disruptions at all levels. As security and risk management leaders handle the recovery and renewal phases from the past three years; The evolving threat landscape provided no rest for the weary. In the face of massive disruption brought about by the COVID-driven social, economic and technological shifts of 2020, adversaries refined their tactics, techniques and procedures to become even more sophisticated.

This resulted in a series of high-profile attacks that disrupted many sectors and governments. As organizations scrambled in 2021 and 2022 to protect supply chains and interconnected systems in the face of the incredibly sophisticated cyber-attacks, adversaries exploited zero-day vulnerabilities and architectural limitations in legacy systems like Microsoft to leave many reeling. At the same time, eCrime syndicates refined and amplified big game hunting (BGH) ransomware attacks that ripped across industries, sowing devastation and sounding the alarm on the frailty of our critical infrastructure, which can be brought down like a house of cards.

For any consolation, the security teams already dealing with an ongoing skills shortage, and these issues proved challenging enough on their own. However, there is never a perfect situation in the world of cybersecurity.

2022 was a year of political and economic instability. It wasn't any different when it comes to the state of cybersecurity in the country. The country experienced a surge in cyber incidents in the banking and telecom sector. Whether it is the Judiciary, State run institutions, PTV Sports or commercial banks, almost every industry in the country had been a target of a cyberattack/incident.

Whereas a wave of audio and video leaks raised on the political realm raised concerns on the state of security controls within key institutions

Pakistan's Cybersecurity Readiness

Pakistan's ranking on the Global Cybersecurity Index stands at 80 as of Feb'2023. A key contributing factor to this a low score in the area of cyber threat analysis, contribution to global cybersecurity and military cyber operations; this can be attributed to the delays in setting up a cert by the government.

A score of nil cybersecurity policy development, protection of digital and essential services; This sounds a bit alarming and raises questions about the accuracy of the data obtained by the NCSI team as Pakistan had made a considerable progress in the area of

cybersecurity policy development. However the scores in the area of protection of personal information and education & professional development were between 89 % and 100 %; thanks to the contribution by the higher education sector and efforts of the ministry of IT and Telecom in funding initiatives focused and trainings and certifications in the area of cybersecurity.

Reflections from World Economic Forum "Global Risks Perception Report"

The world economic forum published the Global Risks Perception report in January'2023. This year's GRPS has brought together leading insights on the evolving global risks landscape from over 1,200 experts across academia, business, government, the international community and civil society. Responses for the GRPS 2022-2023 were collected from 7 September to 5 October 2022. "Global risk" is defined as the possibility of the occurrence of an event or condition which, if it occurs, would negatively impact a significant proportion of global GDP, population or natural resources.

Amongst the top 5 risks list for Pakistan. Failure of cybersecurity (including loss of privacy, data fraud or theft, cyber espionage) is amongst the top risks to the country. Pakistan is amongst the two only countries where cybersecurity is ranked amongst the top 2 risks. The other country is the eastern European country Albania. This directly impacts the potential of any foreign investment in the country.

PTA's Annual Cybersecurity Report

The Telecom regulator of Pakistan, Pakistan Telecommunication Authority (PTA) published The Critical Telecom Data and Infrastructure Security Regulations compliance report (CTDISR) for 2022.

As part of this effort the top 15 telecom providers in Pakistan were assessed regard to their cyber security resilience and readiness.

An overall Cyber Security Index (CSI) for the telecom industry was provided in the study, and telecom operators are ranked according to how well they adhere to the 104 Security Controls included in the CTDISR's 16 Security Domains. Additionally, the report identifies the telecom industry's strong and weak points and offers anonymized data that has been compiled regarding the cyber security incidents in 2022.

The Cyber Security Annual Report 2022 is based on third-party audits conducted by PTA's registered cyber security companies and the Cyber Security Framework issued by PTA in 2020.

This is a step in the right direction and will help boost credibility of the telecom sector from the cybersecurity and privacy perspective, as they have been a target of several cybersecurity incidents in the past few years

Rising tensions in the region and Current Geo political Situation

In mid 2022 Chinese state media claimed that an 'advanced persistent threat (APT) group' operating from India under the nom de guerre "Confucius" had launched fresh cyber-attacks on the Pakistani government and military institutions. Based on the investigation into this matter and determined that the group's first attacks can be dated to 2013.

The group primarily targeted the governments, military, and energy sectors of neighboring countries such as China, Pakistan, and Bangladesh to steal sensitive data.

There multiple website defacements attributed to the Indian based groups that targeted the telecom sector and key government institutions.

Way forward

Given the growth in the tech sector in Pakistan and steps being taken to build a strong digital economy in Pakistan. It is imperative that concrete steps are taken to apply and enforce the Cyber Security Policy which was passed by the parliament in 2021. The government should not shy away from making any changes where required.

It's difficult, but not impossible, to maintain deterrence in cyberspace. Even the developed countries are not prone to cyber-attacks. In order to reduce cyber-attacks and our ability to detect and respond to them in a timely manner we need an infrastructure governed by strong civil and military cooperation. Along with policy implementation and regulatory system strengthening, more investments in emerging technologies are needed.

Farooq Naiyer is a visiting fellow at Islamabad Policy Institute. He is the Chief Informationan Seucity Officer at ORION. He has vast experience in cyber-security, privacy, technology compliance and assurance.