PKCERT

National Computer Emergency Response Team

Current Status & Future Roadmap

Dr. Haider Abbas, Tamgha-e-Imtiaz 🥇

PhD (KTH-Sweden), Post-Doc, ACS (MIT,USA)

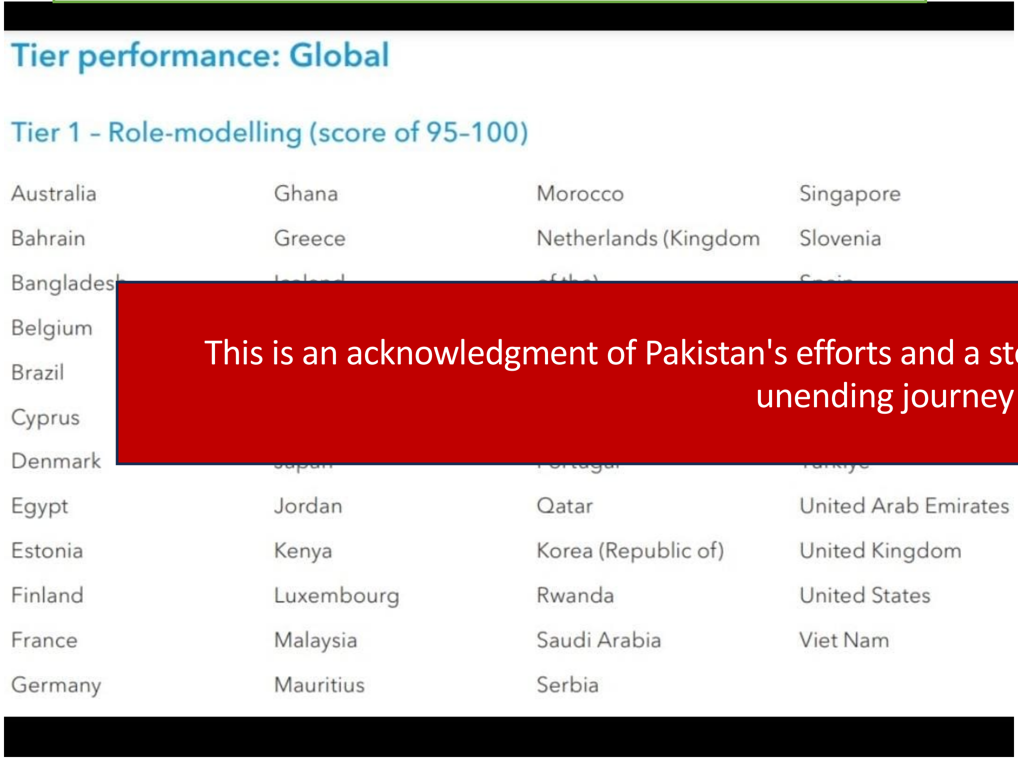
Certified Ethical Hacker, ACM Distinguished Speaker (USA)

Fellow of the IET (UK), Fellow of The British Computer Society (UK)

-Director General, National Cyber Emergency Response Team
Government of Pakistan

Safeguarding Pakistan’s Cyberspace

Global Cybersecurity Index 2024 by The ITU



Tier performance: Global

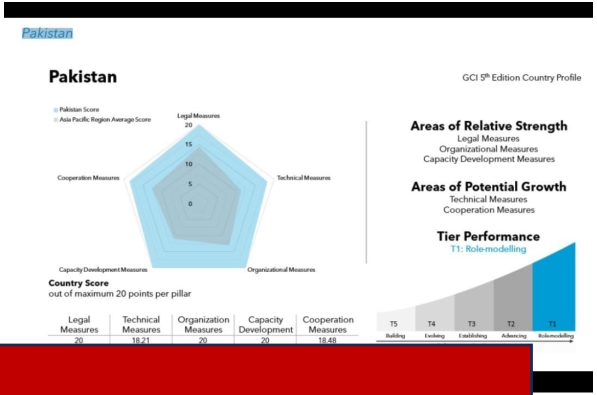
Tier 1 – Role-modelling (score of 95–100)

- Australia
- Bahrain
- Bangladesh
- Belgium
- Brazil
- Cyprus
- Denmark
- Egypt
- Estonia
- Finland
- France
- Germany

- Ghana
- Greece
- Iceland
- Japan
- Jordan
- Kenya
- Luxembourg
- Malaysia
- Mauritius

- Morocco
- Netherlands (Kingdom of the)
- Portugal
- Qatar
- Korea (Republic of)
- Rwanda
- Saudi Arabia
- Serbia

- Singapore
- Slovenia
- Spain
- Türkiye
- United Arab Emirates
- United Kingdom
- United States
- Viet Nam



Pakistan

Pakistan

GCI 5th Edition Country Profile

Country Score
out of maximum 20 points per pillar

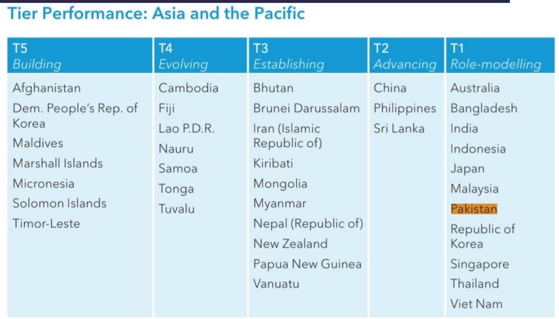
Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures
20	18.21	20	20	18.48

Areas of Relative Strength
Legal Measures
Organizational Measures
Capacity Development Measures

Areas of Potential Growth
Technical Measures
Cooperation Measures

Tier Performance
T1: Role-modelling

This is an acknowledgment of Pakistan's efforts and a step in the right direction on a long and unending journey



Tier Performance: Asia and the Pacific

T5 *Building*	T4 *Evolving*	T3 *Establishing*	T2 *Advancing*	T1 *Role-modelling*
Afghanistan	Cambodia	Bhutan	China	Australia
Dem. People's Rep. of Korea	Fiji	Brunei Darussalam	Philippines	Bangladesh
Maldives	Lao P.D.R.	Iran (Islamic Republic of)	Sri Lanka	India
Marshall Islands	Nauru	Kiribati		Indonesia
Micronesia	Samoa	Mongolia		Japan
Solomon Islands	Tonga	Myanmar		Malaysia
Timor-Leste	Tuvalu	Nepal (Republic of)		Pakistan
		New Zealand		Republic of Korea
		Papua New Guinea		Singapore
		Vanuatu		Thailand
				Viet Nam

National Cyber Security Policy 2021

Course of action outlined in the National Cybersecurity Policy

The National Cybersecurity Policy aims to establish a holistic digital ecosystem, enhance local IT industry capabilities, and promote online businesses. It focuses on strengthening national Cyber Security capabilities through governance frameworks, security standards, and regulatory mechanisms. Cyber threats have reached unprecedented levels, affecting individuals, businesses, and nations globally. The interconnected nature of our digital world exposes us to various forms of cyber attacks.

Vision

The vision is for Pakistan to have a secure, robust, and continually improving nationwide digital ecosystem ensuring confidentiality, integrity, and availability of digital assets, leading to socio-economic development and national security.

Scope

The policy aims to secure the entire cyberspace of Pakistan, including all digital assets, data, and information systems used by citizens, in both public and private sectors.

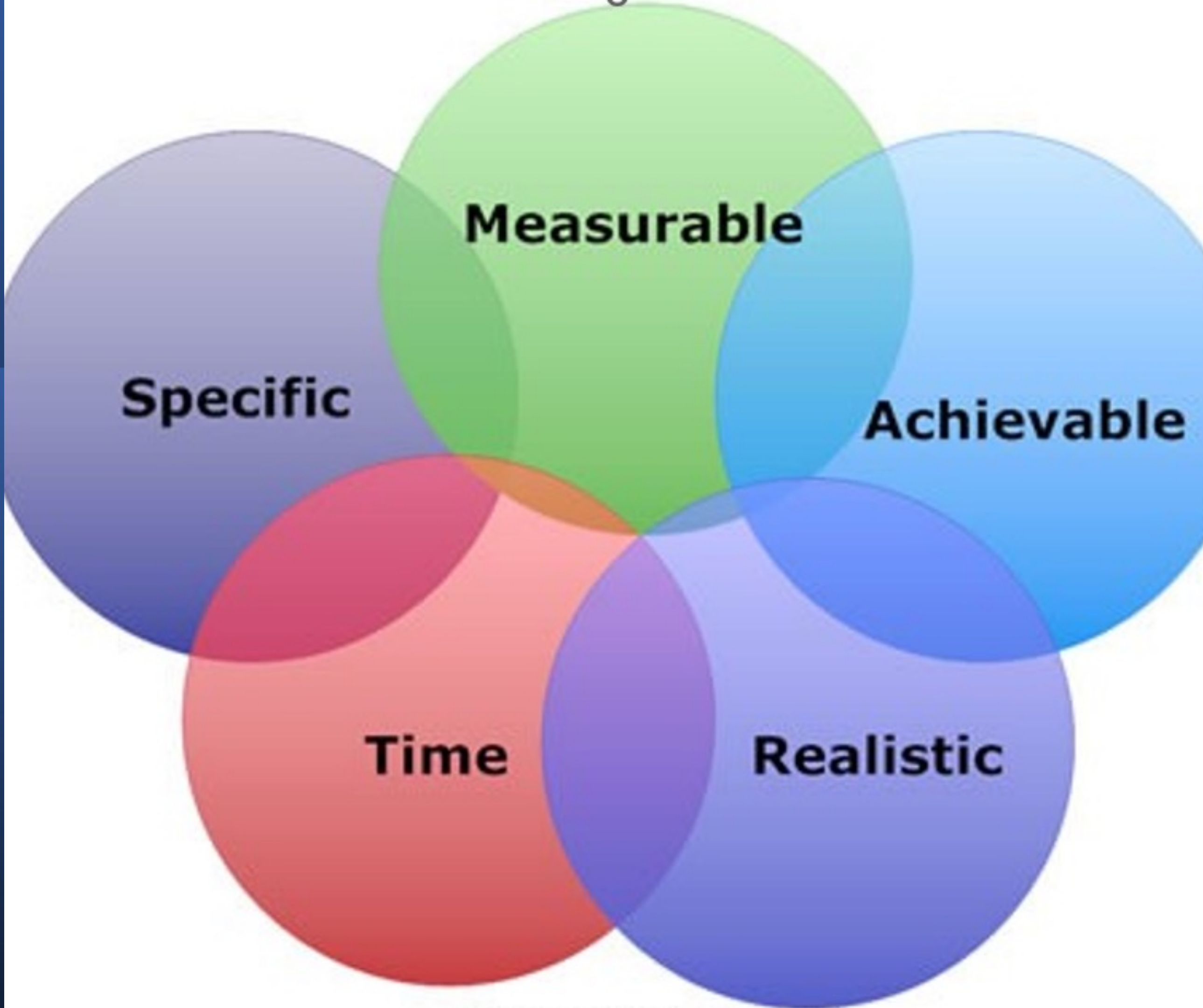
Objectives

- Establish governance and institutional framework for a secure cyber ecosystem.
- Enhance the security of national information systems and infrastructure.
- Create protection and information-sharing mechanisms against threats.
- Protect National Critical Information Infrastructure by mandating security standards.
- Develop an information assurance framework and ensure the integrity of ICT products and services.
- Protect the online privacy of citizens and promote Cyber Security awareness.
- Train skilled cybersecurity professionals and encourage the indigenization of solutions.
- Foster public-private partnerships and global cooperation on Cyber Security.
- Manage risks related to cybersecurity continuously through a risk-based approach.

Cyber Security Policy to a Coordinated Strategy

Define Strategic Objectives

Break down policy goals into specific, actionable objectives for each sector.



National Cyber Emergency Response Team of Pakistan (PKCERT)

Main Components of National CERT

Governance Risk & Compliance

Incident Response & Management

National /International Collaborations

Forensic & Screening Labs

Technical Development

Capacity Building

Central Coordination

National Center for Cybersecurity

PTA

Cybersecurity Initiatives

Academia

NUST / Air Uni / LUMS etc

Coordination Through National CERT

FIA

NRC3/Cyber crimes

State Bank

Cybersecurity Initiatives

- SPD
- Private Sector

PISA / SECP etc

Army Cyber Command

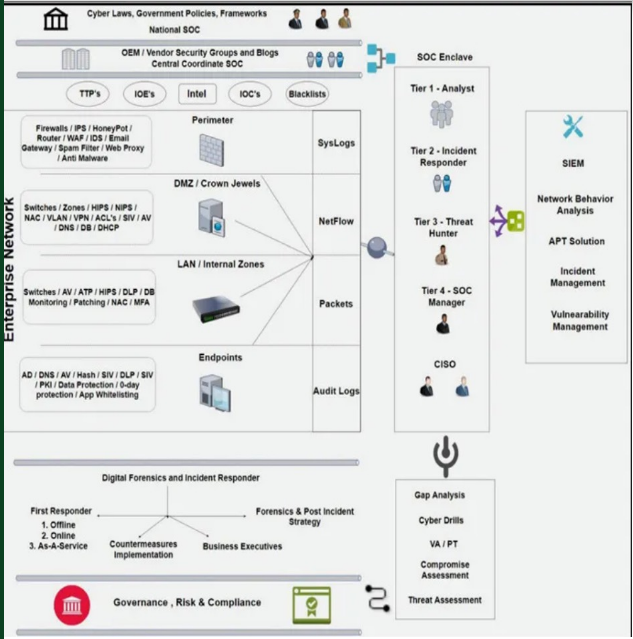
Pakistan Airforce

NASTP/ Cybercommand/Academy

Cyber laws /Regulations

PECA /

3 Tier CERT Structure

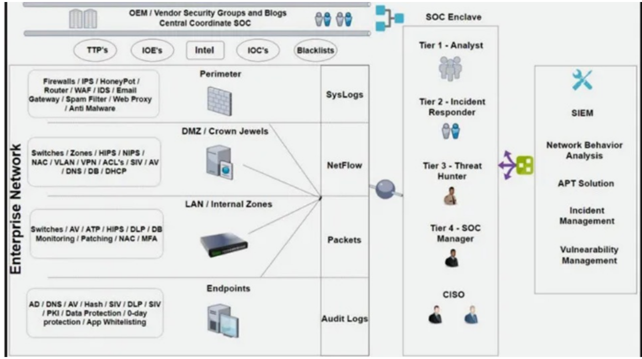

Cyber Laws, Government Policies, Frameworks
National SOC
OEM / Vendor Security Groups and Blogs
Central Coordinate SOC
TTP's
IOE's
Intel
IOC's
Blacklists
Enterprise Network
Perimeter
Firewalls / IPS / HoneyPot / Router / WAF / IDS / Email Gateway / Spam Filter / Web Proxy / Anti Malware
SysLogs
DMZ / Crown Jewels
Switches / Zones / HIPS / NIPS / NAC / VLAN / VPN / ACL's / SIV / AV / DNS / DB / DHCP
NetFlow
LAN / Internal Zones
Switches / AV / ATP / HIPS / DLP / DB Monitoring / Patching / NAC / MFA
Packets
Endpoints
AD / DNS / AV / Hash / SIV / DLP / SIV / PKI / Data Protection / 0-day protection / App Whitelisting
Audit Logs
SOC Enclave
Tier 1 - Analyst
Tier 2 - Incident Responder
Tier 3 - Threat Hunter
Tier 4 - SOC Manager
CISO
SIEM
Network Behavior Analysis
APT Solution
Incident Management
Vulnerability Management
Digital Forensics and Incident Responder
First Responder
1. Offline
2. Online
3. As-A-Service
Forensics & Post Incident Strategy
Countermeasures Implementation
Business Executives
Gap Analysis
Cyber Drills
VA / PT
Compromise Assessment
Threat Assessment
Governance , Risk & Compliance

National CERT

PKCERT/NCERT

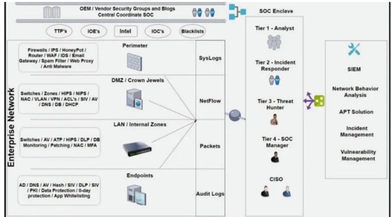
Sectoral CERTs

PTA, State bank, NEPRA SECP etc


OEM / Vendor Security Groups and Blogs
Central Coordinate SOC
TTP's
IOE's
Intel
IOC's
Blacklists
Enterprise Network
Perimeter
Firewalls / IPS / HoneyPot / Router / WAF / IDS / Email Gateway / Spam Filter / Web Proxy / Anti Malware
SysLogs
DMZ / Crown Jewels
Switches / Zones / HIPS / NIPS / NAC / VLAN / VPN / ACL's / SIV / AV / DNS / DB / DHCP
NetFlow
LAN / Internal Zones
Switches / AV / ATP / HIPS / DLP / DB Monitoring / Patching / NAC / MFA
Packets
Endpoints
AD / DNS / AV / Hash / SIV / DLP / SIV / PKI / Data Protection / 0-day protection / App Whitelisting
Audit Logs
SOC Enclave
Tier 1 - Analyst
Tier 2 - Incident Responder
Tier 3 - Threat Hunter
Tier 4 - SOC Manager
CISO
SIEM
Network Behavior Analysis
APT Solution
Incident Management
Vulnerability Management

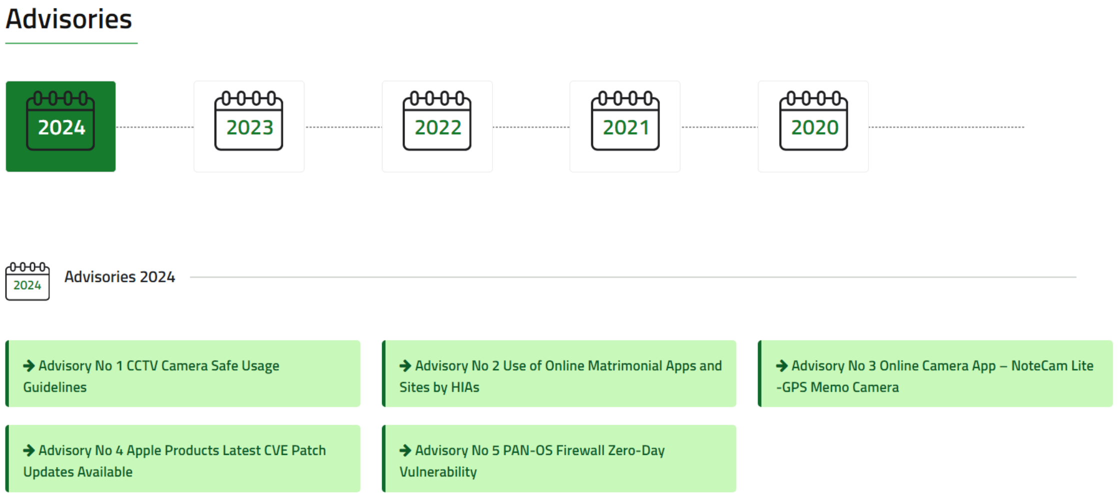
Organizational CERTs

Mobilink, Bank Alfalah. etc



Advisory Services (Web & SMS Alert Service)

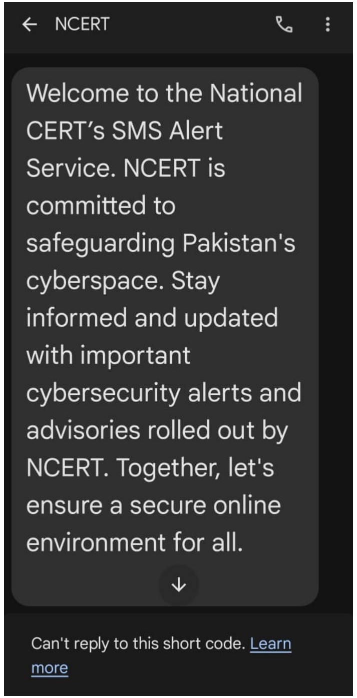
NCERT has initiated a proactive approach to disseminate advisories and alerts via its web platform and SMS Alert Service, enhancing accessibility and outreach to stakeholders. This strategic move ensures timely communication of crucial information, fostering a more informed and prepared educational community.



Advisories

Advisories 2024

- Advisory No 1 CCTV Camera Safe Usage Guidelines
- Advisory No 2 Use of Online Matrimonial Apps and Sites by HIAs
- Advisory No 3 Online Camera App – NoteCam Lite -GPS Memo Camera
- Advisory No 4 Apple Products Latest CVE Patch Updates Available
- Advisory No 5 PAN-OS Firewall Zero-Day Vulnerability



Welcome to the National CERT’s SMS Alert Service. NCERT is committed to safeguarding Pakistan's cyberspace. Stay informed and updated with important cybersecurity alerts and advisories rolled out by NCERT. Together, let's ensure a secure online environment for all.

Can't reply to this short code. Learn more

CyberWatch – Webinar Series

Webinar 1: From Bruteforce to Biometrics: Evolution of Password Attacks and Defenses
Dr. Asad Raza, New Jersey Institute of Technology, USA

Webinar 2: Behavior Analytics and Insider Threat
Dr. Fatima Hussain, Principal SaaS Security Architect, Royal Bank of Canada

Webinar 3: Global CERT/CSIRT Collaborations
Mr. Adli Bin Abd Wahid, Senior Internet Security Specialist, APNIC, Australia

Webinar 4:Resilient Phishing Tactics of Adversary Groups and Defensive Strategies
Mr. Nadeem Ashraf, Group Director of MSSP Operations at (PTCL)

Webinar repository maintained on the National CERT YouTube channel

The videos of the webinars are uploaded on National CERT's YouTube Channel.

PKCERT

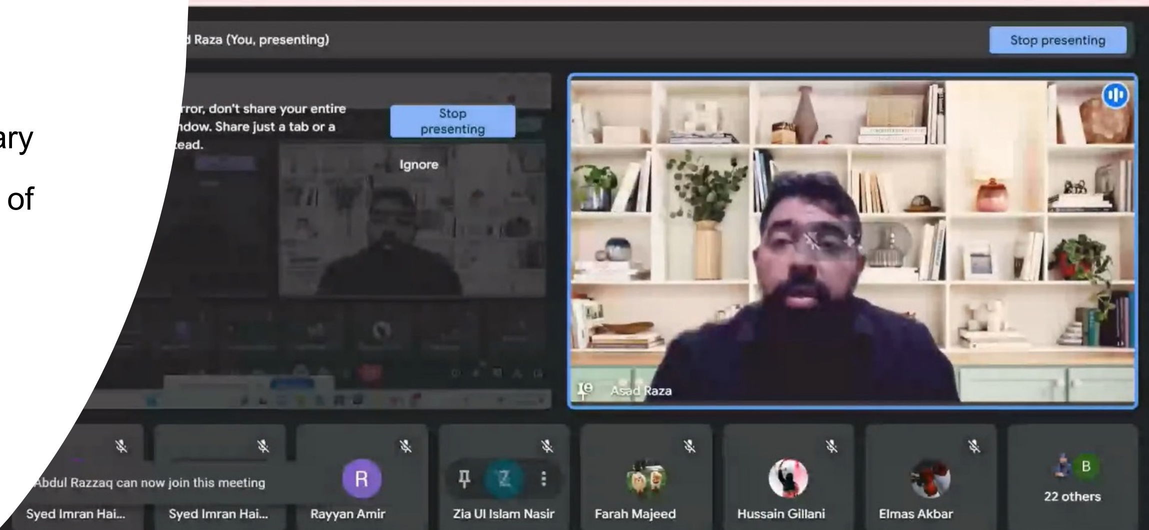
CyberWatch - Webinar Series

Topic:

Behaviour Analytics and Insider Threat

WHEN:
Thursday, May 16th 2024
TIME:
06:30 pm PKT

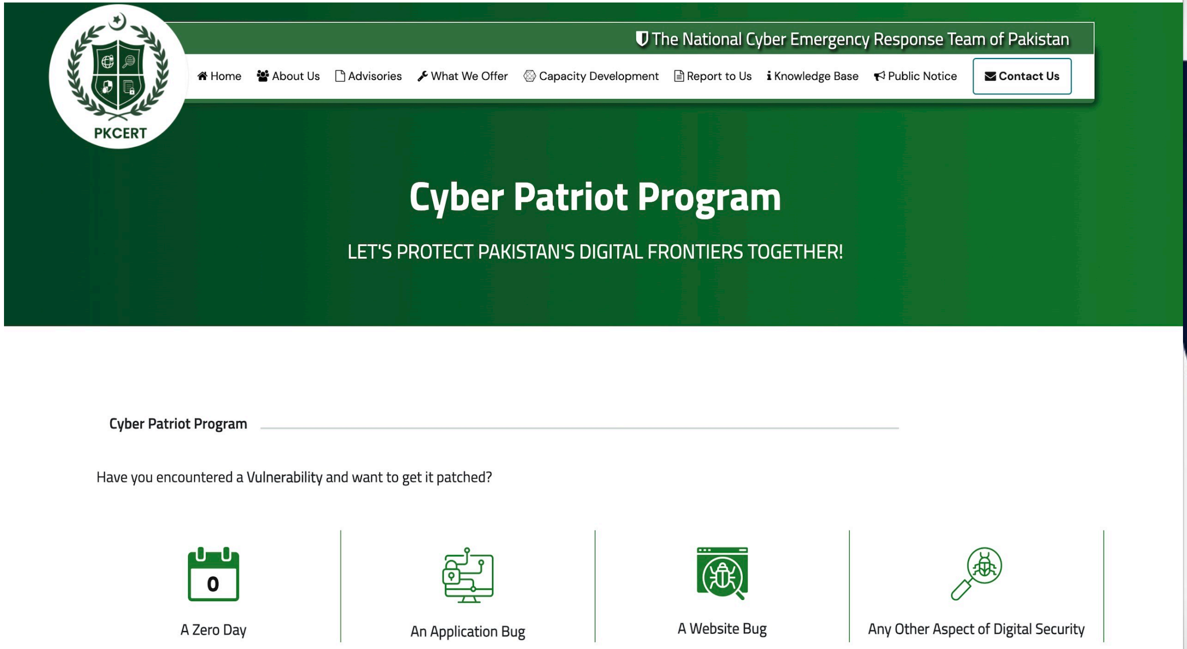
er: Dr. Fatima Hussain



rror, don't share your entire ndow. Share just a tab or a ead.

Abdul Razzaq can now join this meeting

National CERT CyberPatriot Program



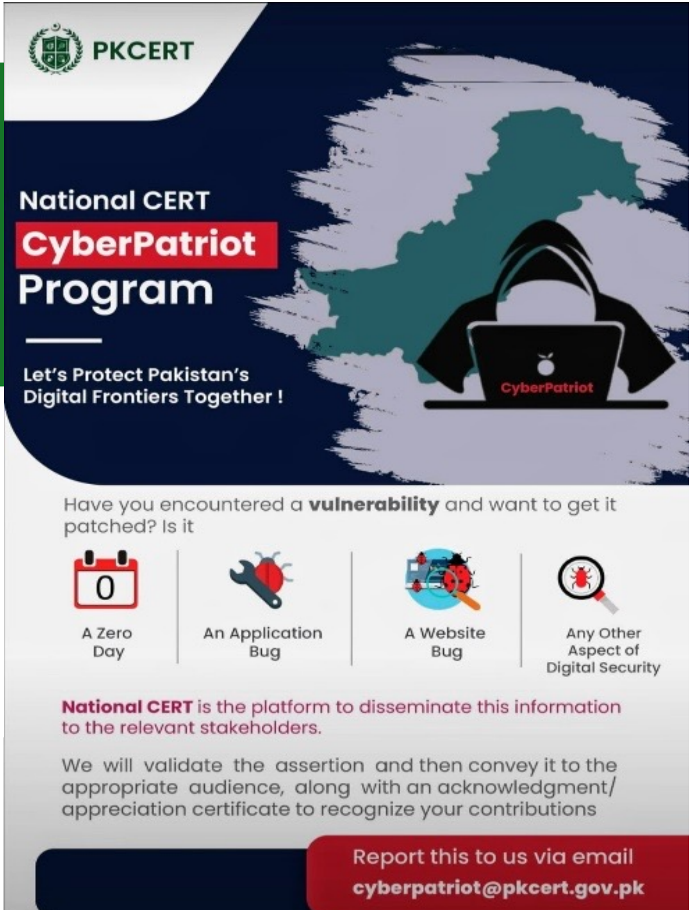
Cyber Patriot Program

LET'S PROTECT PAKISTAN'S DIGITAL FRONTIERS TOGETHER!

Cyber Patriot Program

Have you encountered a Vulnerability and want to get it patched?

- A Zero Day
- An Application Bug
- A Website Bug
- Any Other Aspect of Digital Security



National CERT **CyberPatriot** Program

Let's Protect Pakistan's Digital Frontiers Together !

Have you encountered a **vulnerability** and want to get it patched? Is it

- A Zero Day
- An Application Bug
- A Website Bug
- Any Other Aspect of Digital Security

National CERT is the platform to disseminate this information to the relevant stakeholders.

We will validate the assertion and then convey it to the appropriate audience, along with an acknowledgment/ appreciation certificate to recognize your contributions

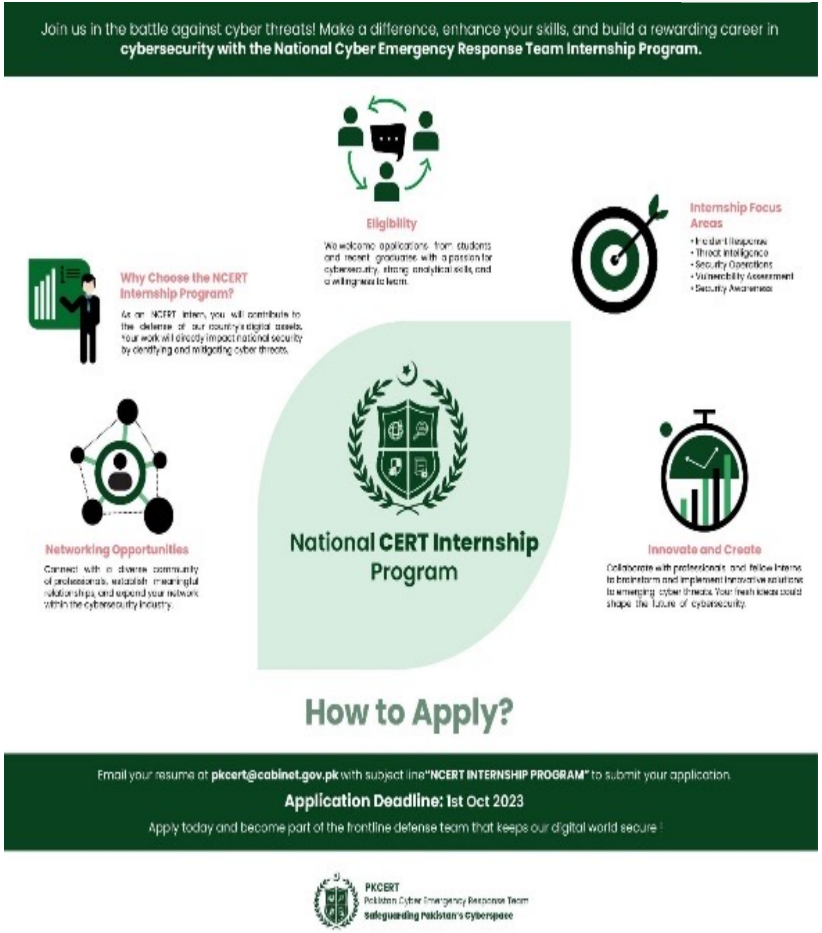
Report this to us via email **cyberpatriot@pkcert.gov.pk**

National-CERT Internship Program

PKCERT

Industry Driven Problems

- **Real-World Case Studies:** Partner with cybersecurity firms to provide real-world problems for interns to solve.
- **Problem-Specific Teams:** Create multi-disciplinary teams to address a specific industry problem, allowing cross-functional learning.
- **Collaborative Projects :** Collaborate with cybersecurity startups to create projects focused on niche areas like IoT security, AI security, etc.
- **Problem Briefing Sessions:** Weekly sessions where industry experts explain ongoing security challenges and the approaches taken to solve them.
- **Industry Mentorship :** Assign each intern a mentor from a relevant industry organization to guide them throughout their project.
- **Virtual Labs & Challenges:** Setting up virtual labs where students can work on penetration testing, malware analysis, and other security tasks.
- **Hands-on Experience with Industry Tools:** Ensure regular internships focus on giving interns access to industry tools such as SIEM systems, IDS/IPS tools, etc.
- **Remote Internship Opportunities:** Given the global nature of cybersecurity, provide remote internships, allowing students to work remotely.
- **Real-Time Threat Monitoring:** Allow interns to be part of the Security Operations Center (SOC) to monitor and analyze real-time cyber threats.
- **Involvement in Incident Response:** Interns can be involved in real-world incident response exercises or simulations with industry partners.



Join us in the battle against cyber threats! Make a difference, enhance your skills, and build a rewarding career in **cybersecurity with the National Cyber Emergency Response Team Internship Program.**

Eligibility

We welcome applications from students and recent graduates with a passion for cybersecurity, strong analytical skills, and a willingness to learn.

Why Choose the NCERT Internship Program?

As an NCERT intern, you will contribute to the defense of our country's digital assets. Your work will directly impact national security by identifying and mitigating cyber threats.

Internship Focus Areas

- Incident Response
- Threat Intelligence
- Security Operations
- Vulnerability Assessment
- Security Awareness

National CERT Internship Program

Networking Opportunities

Connect with a diverse community of professionals, establish meaningful relationships, and expand your network within the cybersecurity industry.

Innovate and Create

Collaborate with professionals and fellow interns to brainstorm and implement innovative solutions to emerging cyber threats. Your fresh ideas could shape the future of cybersecurity.

How to Apply?

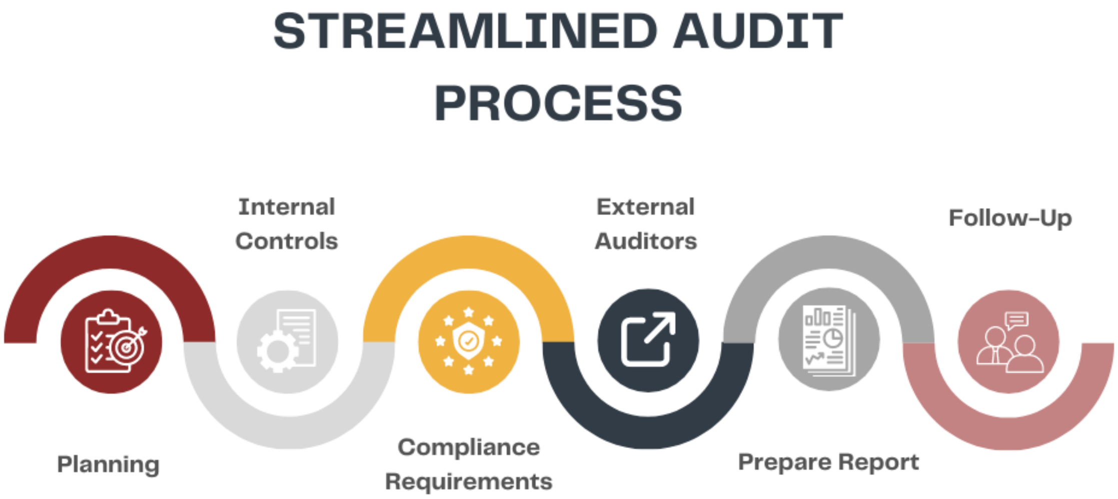
Email your resume at **pkcert@cabinet.gov.pk** with subject line **"NCERT INTERNSHIP PROGRAM"** to submit your application.

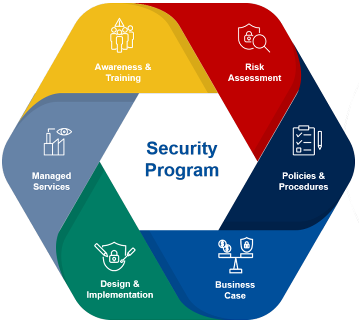
Application Deadline: 1st Oct 2023

Apply today and become part of the frontline defense team that keeps our digital world secure !

PKCERT
Pakistan Cyber Emergency Response Team
Safeguarding Pakistan's Cyberspace

PKCERT



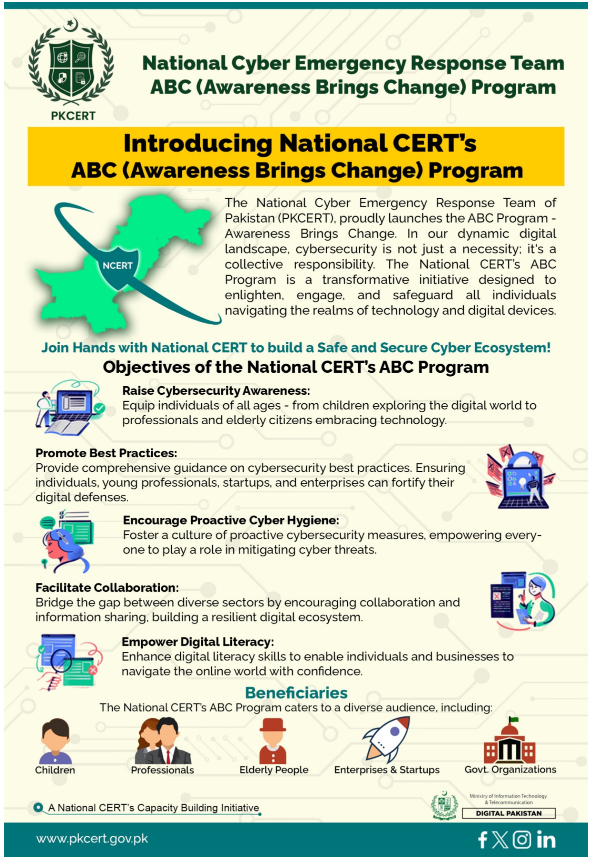


Cybersecurity Program Establishment

Strategies , Procedures , Audit Criteria , Guidelines

National CERT's Initiatives

Awareness Programs



PKCERT

National Cyber Emergency Response Team
ABC (Awareness Brings Change) Program

Introducing National CERT's ABC (Awareness Brings Change) Program

The National Cyber Emergency Response Team of Pakistan (PKCERT), proudly launches the ABC Program - Awareness Brings Change. In our dynamic digital landscape, cybersecurity is not just a necessity; it's a collective responsibility. The National CERT's ABC Program is a transformative initiative designed to enlighten, engage, and safeguard all individuals navigating the realms of technology and digital devices.

Join Hands with National CERT to build a Safe and Secure Cyber Ecosystem!

Objectives of the National CERT's ABC Program

Raise Cybersecurity Awareness:
Equip individuals of all ages - from children exploring the digital world to professionals and elderly citizens embracing technology.

Promote Best Practices:
Provide comprehensive guidance on cybersecurity best practices. Ensuring individuals, young professionals, startups, and enterprises can fortify their digital defenses.

Encourage Proactive Cyber Hygiene:
Foster a culture of proactive cybersecurity measures, empowering everyone to play a role in mitigating cyber threats.

Facilitate Collaboration:
Bridge the gap between diverse sectors by encouraging collaboration and information sharing, building a resilient digital ecosystem.

Empower Digital Literacy:
Enhance digital literacy skills to enable individuals and businesses to navigate the online world with confidence.

Beneficiaries

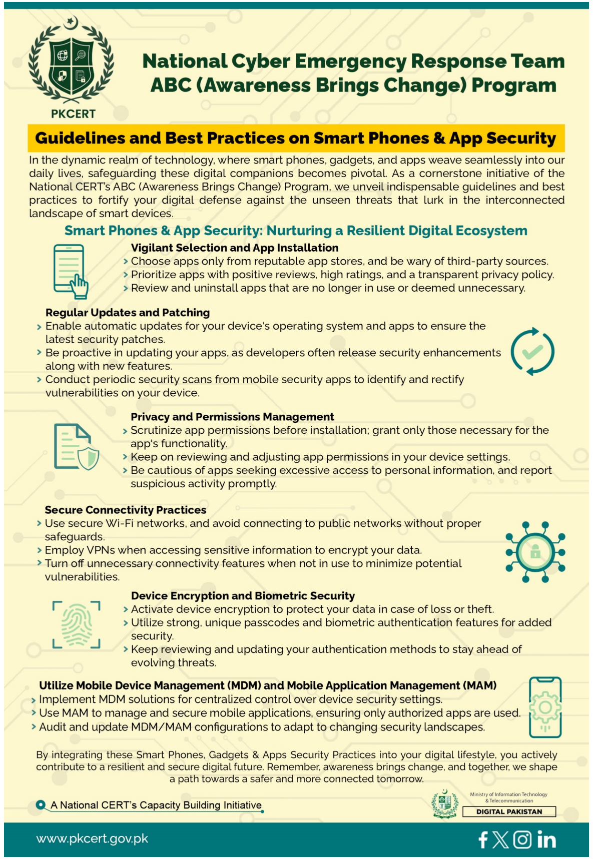
The National CERT's ABC Program caters to a diverse audience, including:

Children | Professionals | Elderly People | Enterprises & Startups | Govt. Organizations

A National CERT's Capacity Building Initiative

Ministry of Information Technology & Telecommunication
DIGITAL PAKISTAN

www.pkcert.gov.pk



PKCERT

National Cyber Emergency Response Team
ABC (Awareness Brings Change) Program

Guidelines and Best Practices on Smart Phones & App Security

In the dynamic realm of technology, where smart phones, gadgets, and apps weave seamlessly into our daily lives, safeguarding these digital companions becomes pivotal. As a cornerstone initiative of the National CERT's ABC (Awareness Brings Change) Program, we unveil indispensable guidelines and best practices to fortify your digital defense against the unseen threats that lurk in the interconnected landscape of smart devices.

Smart Phones & App Security: Nurturing a Resilient Digital Ecosystem

Vigilant Selection and App Installation
- Choose apps only from reputable app stores, and be wary of third-party sources.
- Prioritize apps with positive reviews, high ratings, and a transparent privacy policy.
- Review and uninstall apps that are no longer in use or deemed unnecessary.

Regular Updates and Patching
- Enable automatic updates for your device's operating system and apps to ensure the latest security patches.
- Be proactive in updating your apps, as developers often release security enhancements along with new features.
- Conduct periodic security scans from mobile security apps to identify and rectify vulnerabilities on your device.

Privacy and Permissions Management
- Scrutinize app permissions before installation; grant only those necessary for the app's functionality.
- Keep on reviewing and adjusting app permissions in your device settings.
- Be cautious of apps seeking excessive access to personal information, and report suspicious activity promptly.

Secure Connectivity Practices
- Use secure Wi-Fi networks, and avoid connecting to public networks without proper safeguards.
- Employ VPNs when accessing sensitive information to encrypt your data.
- Turn off unnecessary connectivity features when not in use to minimize potential vulnerabilities.

Device Encryption and Biometric Security
- Activate device encryption to protect your data in case of loss or theft.
- Utilize strong, unique passcodes and biometric authentication features for added security.
- Keep reviewing and updating your authentication methods to stay ahead of evolving threats.

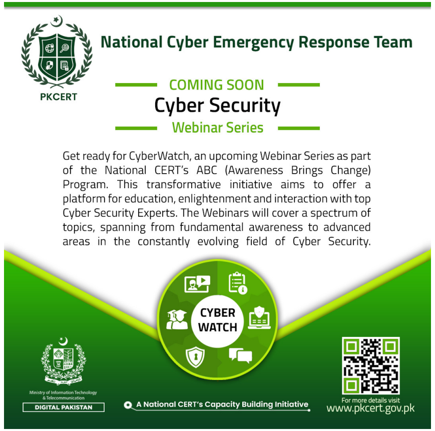
Utilize Mobile Device Management (MDM) and Mobile Application Management (MAM)
- Implement MDM solutions for centralized control over device security settings.
- Use MAM to manage and secure mobile applications, ensuring only authorized apps are used.
- Audit and update MDM/MAM configurations to adapt to changing security landscapes.

By integrating these Smart Phones, Gadgets & Apps Security Practices into your digital lifestyle, you actively contribute to a resilient and secure digital future. Remember, awareness brings change, and together, we shape a path towards a safer and more connected tomorrow.

A National CERT's Capacity Building Initiative

Ministry of Information Technology & Telecommunication
DIGITAL PAKISTAN

www.pkcert.gov.pk



PKCERT

National Cyber Emergency Response Team

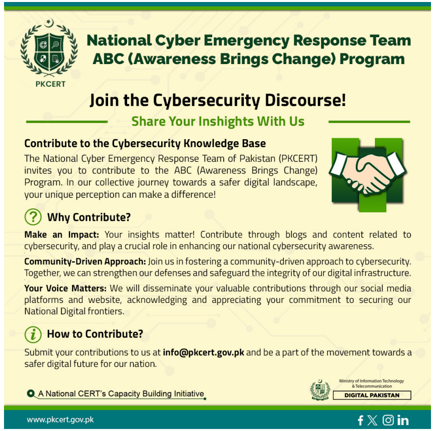
COMING SOON
Cyber Security
Webinar Series

Get ready for CyberWatch, an upcoming Webinar Series as part of the National CERT's ABC (Awareness Brings Change) Program. This transformative initiative aims to offer a platform for education, enlightenment and interaction with top Cyber Security Experts. The Webinars will cover a spectrum of topics, spanning from fundamental awareness to advanced areas in the constantly evolving field of Cyber Security.

Ministry of Information Technology & Telecommunication
DIGITAL PAKISTAN

A National CERT's Capacity Building Initiative

For more details visit
www.pkcert.gov.pk



PKCERT

National Cyber Emergency Response Team
ABC (Awareness Brings Change) Program

Join the Cybersecurity Discourse!

Share Your Inshights With Us

Contribute to the Cybersecurity Knowledge Base

The National Cyber Emergency Response Team of Pakistan (PKCERT) invites you to contribute to the ABC (Awareness Brings Change) Program. In our collective journey towards a safer digital landscape, your unique perception can make a difference!

Why Contribute?

Make an Impact: Your insights matter! Contribute through blogs and content related to cybersecurity, and play a crucial role in enhancing our national cybersecurity awareness.

Community-Driven Approach: Join us in fostering a community-driven approach to cybersecurity. Together, we can strengthen our defenses and safeguard the integrity of our digital infrastructure.

Your Voice Matters: We will disseminate your valuable contributions through our social media platforms and website, acknowledging and appreciating your commitment to securing our National Digital frontiers.

How to Contribute?

Submit your contributions to us at **info@pkcert.gov.pk** and be a part of the movement towards a safer digital future for our nation.

A National CERT's Capacity Building Initiative

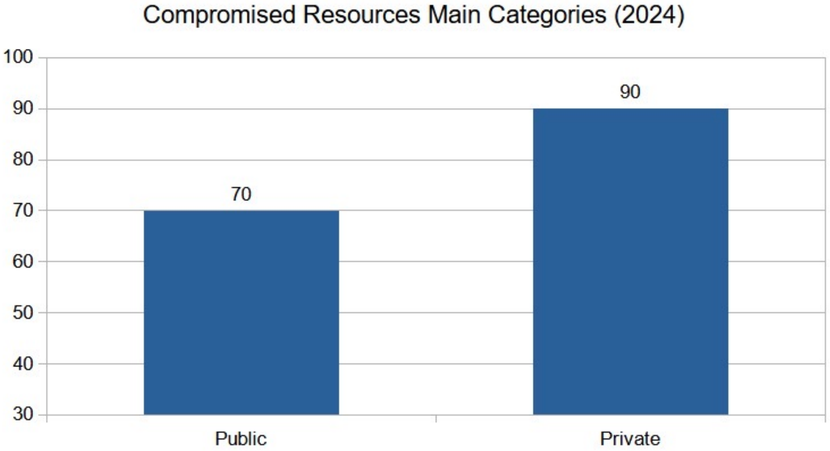
Ministry of Information Technology & Telecommunication
DIGITAL PAKISTAN

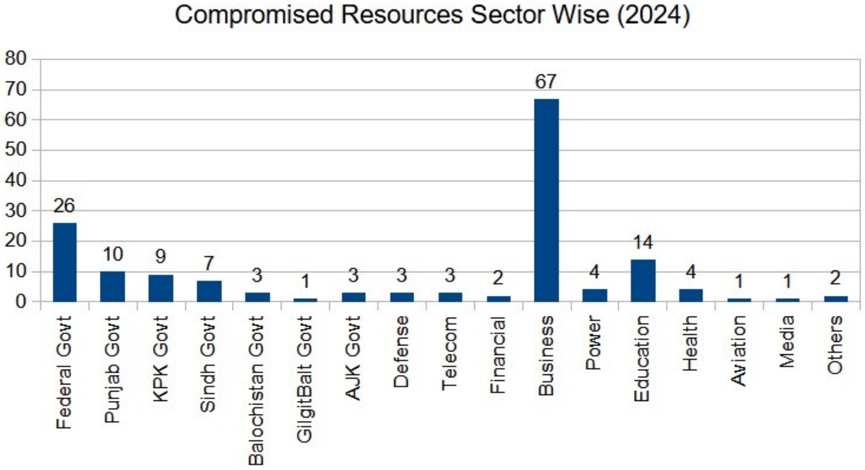
www.pkcert.gov.pk

Incident Management

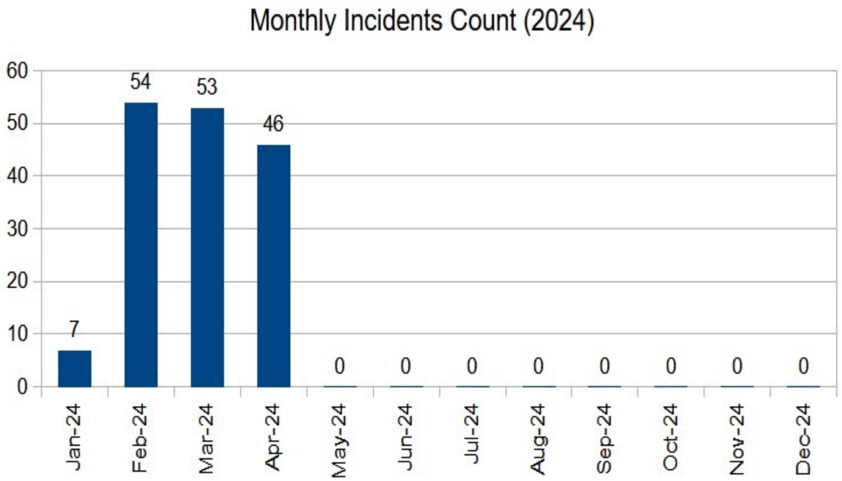
Cyber Incidents being monitored and managed since Jan. 2024

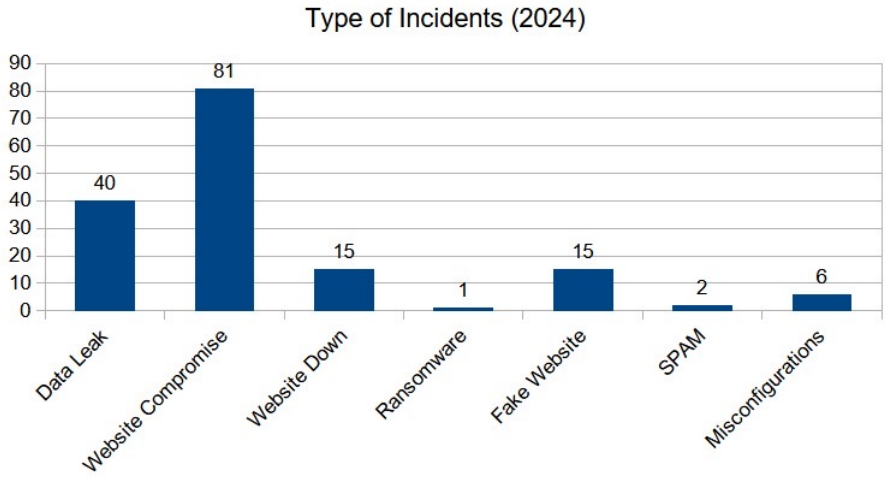
- 29/80 incidents affected public sector assets
- 51/80 incidents affected private sector assets
- Notable assets include various Govt. and private organizations in Islamabad, Punjab, Sindh and Baluchistan





Incident Management





Training Delivered by National CERT

1. Five Day Technical Training of ISMS ISO 27001-Lead Auditor for Government and strategic organizations *(June 2024)*
2. International Diplomatic Capacity Building training on New & Emerging Threats, Cyber Tools of Terrorism, Dark Web, and Transnational Crime delivered to a group of 27 United Nations (UN) New York based foreign diplomats of Small Island Developing States (SIDs) and Least Developed Countries (LDCs) at Foreign Service Academy, Ministry of Foreign Affairs *(May 2024)*
3. 3-day Cyber Security Compliance and Auditing training for Government Sector held at Military College of Signals *(May-June 2024)*
4. Cyber Security Capacity Building training for all Ministries, Divisions and attached departments conducted in collaboration with NCCS *(May 2024)*
5. Training session for the Intelligence Bureau Officers on National Cyber Security Policy and Cyber Crime laws at the National IB Academy *(February 2024)*
6. Specialized Training session at National IT Board on enhancing Cyber Security Preparedness with over 100 participants from NITB and various Ministries *(January 2024)*
7. Cyber Security training on Cybersecurity Awareness – Identifying and Mitigating Human Based Threats conducted at National Intelligence Bureau Academy *(January 2024)*
8. Technical session on Supply Chain Cyber Security Landscape under the Digital Pakistan Cyber Security Hackathon training program for Government Officials *(December 2023)*
9. Training session on Collaboration Efforts on Cybersecurity with Foreign Diplomats from Brotherly Countries involving foreign diplomats from over 12 friendly countries at Foreign Services Academy *(December 2023)*
10. Training for Ministry of Foreign Affairs officials and 40 Pakistan Embassies on Safe and Secure Use of Technology – Cyber Security Threat Landscape at Ministry of Foreign Affairs *(August 2023)*

Keynote Addresses/ Talks and Panel Discussions (Seminars and Conferences)

1. Keynote Address at the PAF Air War College Institute on Next Generation Warfare (October 2024).
2. Participation in a high-level roundtable discussion hosted by the Centre for Aerospace & Security Studies (CASS), Islamabad. The event, titled “*Lebanon Explosions: Weaponizing Consumer Technologies*”. (October, 2024)
3. Lecture on National Cybersecurity Threats and Countermeasures for Pakistan Administrative Service (PAS) officers from federal and provincial governments at the National Institute of Management (NIM), Lahore. (Sep, 2024)
4. Participation and Keynote Address for delineating comprehensive vision for the online protection of children in the four-day Child Online Protection (COP) training organized by UNICEF Pakistan. (Sep, 2024)
5. Participation in Expert Panel Discussuin on AI, Cybersecurity and the Future of Work at FC College, Lahore. (Aug, 2024)
6. Technical Talk at The Challenges and Opportunities of Artificial Intelligence (AI) & Cybersecurity in Pakistan Seminar organized by Sustainable Development Policy Institute *(March 2024)*
7. Keynote at EDI Policy Dialogue held at National School of Public Policy on Digital Ethics and Cybersecurity *(March 2024)*
8. Keynote at Fortinet Cyber Security Day at Karachi *(March 2024)*
9. Roundtable discussion in NDU over Cyber Security in Pakistan: Challenges and Opportunities *(Feb 2024)*
10. Keynote Address at the Beijing Cybersecurity Conference *(June 2024)*
11. Keynote addresses at ReCypher International Cyber Security Conference (IBA Karachi) *(Jan 2024)*
12. Keynote at International Conference on Open-Source Systems and Technology (UET, Lahore) *(Dec 2023)*
13. Technical Talk at AI for sustainable Future: Its role in Ethical Policies and Climate Resilience conference, jointly organized by Institute of Regional Studies (IRS) and the Centre of Pakistan and International Relations (COPAIR) *(Dec 2023)*
14. Keynote address at AI-Driven hackathon and International Colloquium on AI-based interdisciplinary research *(Aug 2023)*

PANEL DISCUSSION: CYBERWARFARE AND NEED FOR CRITICAL INFRASTRUCTURE PROTECTION - ROLE OF CERT & CTI
MODERATOR
KHAWAJA MOHAMMAD ALI
ZAKIR SYED
BRIG. RANA FARRUKH
DR. HAIDER ABBAS
AMMAR JAFFRI
CYBER THREAT INTELLIGENCE [2023]

National CERT’s Initiatives

National Competitions / Hackathons /Skill Development

Ignite
Ministry of IT & Telecom
DIGITAL PAKISTAN
DIGITAL PAKISTAN CYBERSECURITY HACKATHON 2023
SHOW YOUR SKILLS GET REWARDED

INSTITUTE FOR STRATEGIC STUDIES, RESEARCH AND ANALYSIS
NATIONAL DEFENCE UNIVERSITY
Home
Programmes
Events Gallery
Research Archives
Library
About Us
25th National Security Workshop
09 Oct - 10 Nov, 2023

AI-Driven Interdisciplinary Hackathon
2nd August, 2023
GOING GLOBAL PAK-UK EDUCATION GATEWAY MOBILITY PARTNERSHIP FOR FACULTY
AI-Driven Hackathon

National CERT’s Initiatives

Sectoral-Stakeholder Engagement

Stakeholder engagements for current state assessment and Capacity Development needs under the National CERT's Guidelines

MEMORANDUM OF UNDERSTANDING
BETWEEN
NADRA
NATIONAL DATABASE AND REGISTRATION AUTHORITY
&
PKCERT
NATIONAL CYBER EMERGENCY RESPONSE TEAM OF PAKISTAN

National CERT's Collaborations

Government & Private Organizations

- MoU with the Center of Pakistan and International Relations (COPAIR).
- MoU with SNSKIES.
- MoU with NADRA and NTL.
- (MoU) with the Institute of Business Administration's Center for Information and Communication Technology (IBA - CICT). This collaboration aims to enhance research and development, promote cybersecurity awareness programs, and provide customized cybersecurity training for industry professionals.
- Initial collaborative meetings held with Asia Pacific Network Information Center for joint capacity building program to be launched in collaboration with APNIC
- Inceptive meetings with NRD CS Lithuania, for collective capacity development collaborations and interaction with peer CERTs from Baltic states
- Initial Collaboration meetings with CISCO and SANS for capacity development programs and collective initiatives
- Collaboration with NCCS for joint Cyber Security Activities and Events including Trainings, Awareness sessions, Hackathons and Conference/Seminars

MEMORANDUM OF UNDERSTANDING
BETWEEN
NADRA
NATIONAL DATABASE AND REGISTRATION AUTHORITY
&
PKCERT
NATIONAL CYBER EMERGENCY RESPONSE TEAM OF PAKISTAN

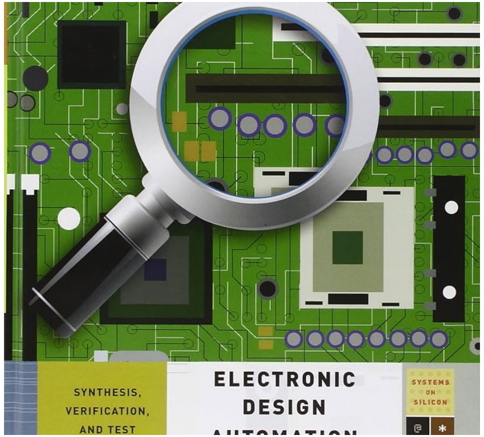
NCERT Cyber Campus

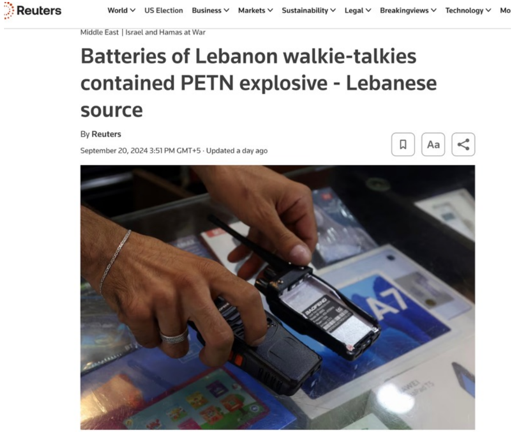
Impactful Research Efforts

GOVERNMENT
INDUSTRY
ACADEMIA

policy
What needs to be Audited ?
OLD- ISO 27001: 2005
Annex A: Control Objectives and Controls
11 Key Domains of Information Security
Governing Policy
(Single Document)

Fellowship
PROGRAMME



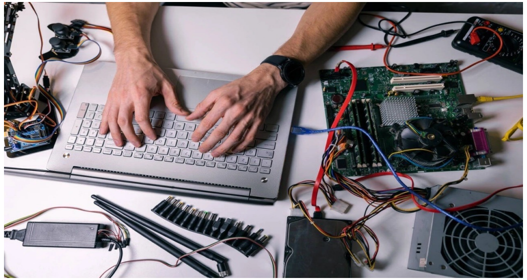


Middle East | Israel and Hamas at War

Batteries of Lebanon walkie-talkies contained PETN explosive - Lebanese source

By Reuters

September 20, 2024 3:51 PM GMT+5 · Updated a day ago



Hardware & Software Sceerning

Consolidated Future Roadmap

At Government Level

- National Cybersecurity Gap Analysis
- Establishment National Vulnerability Assessment Centre
- Conducting independent audits of Government agencies
- Supporting research, indigenous product development and cyber awareness centers
- Collaborate with the private sector and international cybersecurity research organizations
- Ensure capacity building of LEAs to combat cybercrimes

At Organizational Level

- Help to Evaluate the cyber health of the organizations
- Help to build a system for Incident Response, Regular Audits & Risk Mgmt
- Regular Security Updates, Backups
- Supporting to Focus on indigenous development
- Hunting/discouraging pirated software
- Employees Training on cyber attack prevention
- MDM and Security Culture

At Individual Level

- Advisory about the latest cybersecurity threats and best practices
- Awareness about pirated softwares
- Provision of Basic Protection: Firewalls and Anti-Virus
- Strengthen First line of Defense
- Anti Phishing: Responding to unknown requests/emails
- Safe Ecommerce Usage/Use multi-factor authentication
- Secure Social Media Usage
- Cybersecurity for Children Awareness Programs

THANK YOU

Happy to take your suggestions /feedback
Email: dg@pkcert.gov.pk
https://www.linkedin.com/company/national-cert-pakistan/
https://www.facebook.com/profile.php?id=100095346962455
https://twitter.com/PKCERT_official