Apr 2021

Pakistan: Government forges ahead with enhancing cybersecurity and digitalisation

In developing its National Cybersecurity Policy 2021 ('the Cybersecurity Policy'), the Ministry of Information Technology & Telecommunication ('MOITT') recently issued a consultation draft of the same. The Cybersecurity Policy is aimed at realising the full potential of information and communication technologies for socio-economic development by assuring availability, confidentially, and integrity of critical infrastructure and information systems, while also providing reliable, secured, and resilient cyberspace for all. Saeed Hasan Khan and Saifullah Khan, from S.U.Khan Associates Corporate & Legal Consultants, discuss the contents of the Cybersecurity Policy and how, along with other policies, it aims to progress the digitisation of governance, economy, and businesses in Pakistan.

marrio31 / Signature collection / istockphoto.com

Considering the importance of the subject matter, the Prime Minister of Pakistan constituted a Cyber Governance Policy Committee ('CGPC') comprising of all relevant ministries and organisations. The vision of the CGPC is 'to develop secure and resilient cyber systems and networks for national cyber security and response.' In turn, the scope of Cybersecurity Policy is 'to secure entire cyberspace of Pakistan including all information and communication systems used in both public and private sectors.'

The Cybersecurity Policy and the CGPC

The Cybersecurity Policy spells its objectives to augment its vision and scope. Those objectives can be summarised as follows:

- establishing a governance and institutional framework;
- creation of protection and information sharing mechanism;
- protection of national critical information infrastructure;
- enhancing security of government information systems and infrastructure;
- creation of an information assurance framework of audits and compliance;
- ensuring integrity of ICT products, systems, and services by establishing a mechanism of testing, screening, forensics, and accreditation;
- developing public private partnership;
- creating a country wide culture of cybersecurity awareness;
- availability of skilled cybersecurity professionals;
- encourage and support indigenisation through research and development;
- provision of a framework on national-global cooperation and collaborations; and
- taking legislative and regulatory actions.

The CGPC is entrusted to assert national level ownership to policy initiatives related to cyber-governance and security. The CGPC is responsible for strategic oversight over national cybersecurity issues.

The core functions of the CGPC are summarised as:

- the formulation and approval of the Cybersecurity Policy and a Cyber Security Act;
- assisting in addressing requirements of organisational structures and technical, procedural, and legal measures to support the policy mandate and implementation mechanisms;
- harmonising working and operational reporting mechanisms of all departments dealing with the subject;
- carrying out consultations on aspects related to cyber governance on a regular and permanent basis;
- assigning roles to national institutions for international representation and collaboration with global and regional bodies and organisations; and
- providing guidance to align policy with emerging cyberspace requirements through updates and periodic reviews.

The Cybersecurity Policy recommendations of the CGPC will be approved by the Federal Cabinet.

The Cybersecurity Policy states that, to achieve the objectives, an implementation framework shall be developed by a designated organisation of the Federal Government. The said designated organisation shall also act as the Central Entity at the Federal level for coordinating and implementing all cybersecurity related matters. The Central Entity, as per the Cybersecurity Policy, has a three-tier scope including: (i) National Level; (ii) Sectoral Level; and (iii) Organisational Level. It is to be seen whether the Federal Government will designate an existing organisation as the Central Entity, or a new organisation will be established pursuant to the proposed Cyber Security Act.

The Central Entity Framework

The Central Entity, as per the Cybersecurity Policy, will develop a framework in relation to following specific areas:

Active defence

Blocking malware attacks; preventing email phishing and spoofing activity; promoting best security practice; working with international law enforcement channels; implementing control to secure the routing of internet traffic for government departments; and investing in capabilities enhancement of law enforcement agencies and concerned ministries.

Protecting internet-based services

Developing an internet protocol reputation service to protect government digital services; installing products on government networks to ensure software is running correctly; and expanding beyond the gov.pk domain.

Protection and resilience of the national critical information infrastructure

Operating requisite technical platforms to protect national critical information infrastructure; ensuring secure ICT environment including mobile and cloud-based systems; implementing national security standards; developing a mechanism for protection of critical information infrastructure; establishing and enforcement of risk management methodologies; mandating national, provincial, and/or organisational critical information infrastructures to hire qualified information security individuals and to appoint a Chief Information Security Officer; and enforcing accreditation of national security standards.

Protection of Government's information systems and infrastructure

Defining and enforcing a robust government authentication and data protection framework; creating vulnerability assessment and patch management process; ensuring mandatory allocation of a certain percentage of ICT project budget for information security assurance; formulating a mechanism for creation and enforcement of staff vetting and clearance scheme; and improving security in government outsourcing and procurement.

Information security assurance framework

Implementing the concept of information security by design; upgrading and establishing next generation national cybersecurity forensic and screening setups; creating an information assurance framework for cybersecurity audit and compliance; creating infrastructure and leverage existing facilities for conformity assessment and certification of compliance to cybersecurity best practices; and developing and mandating other organisations for the establishment of testing, screening, forensic, and accreditation facilities.

Public private partnership

Nurturing an environment for entrepreneurship based on cooperation among government, industry, academia, and research institutions, alongside providing government support to start-ups.

Cybersecurity research and development

Undertaking research and development programs aimed at short term, medium term, and long term; encouraging research and development to produce cost-effective and tailor-made indigenous security solutions; facilitating the commercialisation of the outputs of research and development; and setting up centers of excellence.

Capacity building

Establishing centers of excellence to educate and train human resource in cybersecurity; formulating and implementing customised human resource development program to fulfill cybersecurity needs; increasing cybersecurity research and development budget, including cybercrime-related curriculum in graduate and post-graduate law related degrees; and training prosecutors, lawyers, and judges.

Awareness for national culture of cybersecurity

Planning and to implement education programs on cybersecurity ethics and security programs customised for specific sectors of society; encouraging the corporate sector to protect cyberspace; preparing and executing a national awareness program to educate end users at home or at workplace; implementing cybersecurity awareness program for government systems; and adding cybersecurity awareness to the national education curriculum at middle and secondary levels.

Global cooperation and collaborations

Working with international partners; maintaining continuous presence and providing professional input from Pakistan to all major global and regional organisations and professional bodies; and developing a mechanism for trusted information exchange about cyberattacks, threats, and vulnerabilities with the public/inter-government and non-government bodies, locally and globally.

Cybercrime response mechanism

Assisting and enhancing the government capacity by augmenting law enforcement agencies technical capability; establishing liaison and coordination with other national and international cybercrime agencies for sharing of information and cooperation; strengthening the processes and procedures and embed cybersecurity in the public and private sector networks vulnerable to cybercrimes.

Regulations

Formulating the Cybersecurity Policy and Cyber Security Act; developing rules and regulations for a national cybersecurity framework; establishing digital certifications for authenticity of individuals and businesses; safeguarding the privacy of citizens and ensuring data protection; standardising digital and network forensics processes and infrastructure; ensuring compliance for auditing in relation to the national cybersecurity standards across Pakistan.

Digital Pakistan Policy

Separately, the MOITT has also recently updated the Digital Pakistan Policy 2018 in line with the Government of Pakistan's aim to improve citizens' quality of life and economic well-being by ensuring the availability of accessible, affordable, reliable, universal, and high-quality ICT services. The vision of the Government of Pakistan with regards to Digital Pakistan Policy is 'to become a strategic enabler for an accelerated digitisation ecosystem to expand the knowledge based economy and spur socio economic growth.'

The key objectives of the Digital Pakistan Policy are:

- to use a holistic digital strategy;
- to create sectoral digitisation;
- to develop e-Commerce;
- to empower the youth, women, and girls using IT;
- to promote innovation, entrepreneurship, and startups in the IT sector;
- to increase software exports, IT remittances, and the domestic market;
- to increase the ICT ranking of Pakistan;
- to develop digital inclusion;
- to develop e-Governance;

- to increase foreign and domestic investment;
- to aid persons with disabilities; and
- to provide standardisation.

Key components

Legislation

Promulgate necessary policy frameworks, laws, and rules to enable the creation of a sustainable IT environment. **The laws/rules to be enacted are: the Personal Data Protection Bill 2020 ('the Bill'), a framework for cloud-based service and its regulations, including data classification mechanism/standards for access/data transparency, an e-Commerce policy framework, an on-line dispute resolution, and consumer protection, etc.**

Infrastructure development

Establish state-of-the-art software technology parks at federal and provincial capitals and establish national technology incubation centers across the country, promoting an open digitisation infrastructure for shared services including cloud technologies. As well as this, provide access to subsidised workspaces, shared services, funding, promotional and accreditation agencies, research and development facilities, and professional training, in addition to interoperability to enable any-to-any settlement amongst various existing mobile banking systems specifically with respect to Pakistan's e-Payment gateway. Finally, establish 'tele-centers' across Pakistan, facilitate IT related innovation through developing smart cities, and help to solve local problems through the use of technology.

Human resource development, entrepreneurship, research and development, and freelancing in IT

Utilise the power of IT to enhance the outreach and quality of education, at all levels, across the country through programs to enhance the requisite digital skillset of individuals that are of relevance and value to the IT industry. Initiate programs to train young graduates, freelancers, and professionals on market intensive skills through both classroom and virtual training sessions.

Software exports

Pursue all measures including legislative, policy, administrative, and international marketing measures to augment software exports, create jobs, and contribute towards the government's efforts to increase overall IT exports and remittances.

ICT for girls

Promote the use of ICT technology among women and girls for their empowerment and to bridge the digital divide.

Local languages content development

Support the creation and sharing of content in national and regional/local languages.

Persons with disabilities

Involve civil society, private sector organisations, and other relevant stakeholders for developing and instituting a holistic ecosystem to promote ICT accessibility for persons with disabilities.

Open source

Enhance the skills and capabilities within government to evaluate open source ICT products and services as an option.

Local manufacturing of hardware

Promote the local manufacturing of IT hardware (desktop PCs, laptops, mobile handsets, network equipment, LEDs, microprocessors, etc.) to augment measures already in place to incentivize local manufacturing of handsets, if so required.

e-Governance

Enable delivery of public services to citizens through innovative use of ICT, and assist relevant departments in developing technology solutions and platforms for greater productivity and effectiveness in service delivery and its standardisation.

Enabling the digitisation of key socio-economic sectors

The MOITT will play the role of an enabler and facilitator for digitisation, providing necessary guidance where required, while relevant federal ministries, divisions, and departments will take the lead role for the implementation of policy strategy falling within their domain.

Through the Digital Pakistan Policy, the Federal Government mandates the MOITT to develop an 'Action Plan,' along with relevant ministries and departments detailing the time frame and outputs. The key initiatives for ICT enablement and sectorial digitisation are listed below:

- e-Agriculture;
- e-Health;
- e-Commerce;
- e-Justice;
- ICT education;
- Internet of Things, FinTech, artificial intelligence, and robotics; and
- cloud computing and Big Data.

The Digital Pakistan Policy also lists various fiscal and non-fiscal incentives for the IT sector as follows:

Fiscal incentives

- extension of income tax holiday;
- 5% cash reward on export remittances;

- reduced rate of sales tax on domestic services;
- provision of bank loans;
- technology special economic zones; and
- proliferation of new IT parks.

Non-fiscal incentives

- reinforcement the industry status of IT sector;
- ratification of World Trade Organization's Information Technology Agreement;
- an increase of the timeframe of initial registration and renewal of call centers to five years (the registration and subsequent renewal will be valid for a period of five years in contrast to present one year);
- call centre certifications to individuals and sole propitiators will be allowed;
- Pakistan Software Export Board/Pakistan Telecommunication Authority to enable telecommuting/work from home facility for the call centers to expand business process outsourcing; and
- Government of Pakistan to encourage trade delegations comprising IT to the major international market.

Reflections

Both the policies (the Cybersecurity Policy and the Digital Pakistan Policy) complement each other and reflect the Government of Pakistan's vision towards the digitisation of governance, economy, and businesses.

In the perspective of these two policies, promulgation and enforcement of the Bill (the draft of which has passed the consultation stage) seems all the more necessary. In addition, the development of a law on cybersecurity under the Cybersecurity Policy would provide conducive legal framework in regard to the cybersecurity ecosystem in Pakistan.

These policies are a starting point for developing a new era wherein e-Governance, e-Commerce, and the digitisation of public and private services will flourish and begin to match the pace of global trends. This will enable public and private sectors to confidently engage in e-transactions while ensuring the safety of the information and systems they use, which would in turn enhance public trust in those systems.

The Bill will ensure the privacy and protection of the personal data of natural persons, whereas the Cybersecurity Act would aim to provide for the security of information systems and information/data exchanges beyond the personal data. In this way, both laws will jointly provide a complete framework of protection and security to personal data and all other data/information systems.

Businesses and organisations need to have cybersecurity governance and risk management programs which are appropriate for the size of the organisation. Cybersecurity risk needs to be considered as a significant business risk by the stakeholders.

Organisations need to implement a formal risk assessment process and develop policies to ensure that systems are not misused and ensure that applicable policies are continually reviewed and updated to reflect the most current risks. This governance and risk assessment further needs to be aligned with the relevant regulatory framework (to be framed under these policies) and are to be complied with proposed national security standards.

Saeed Hasan Khan Partner
Saeed.Hasan@sukhan.com.pk
Saifullah Khan Managing Partner
Saifullah.Khan@sukhan.com.pk
S.U.Khan Associates Corporate & Legal Consultants, Islamabad