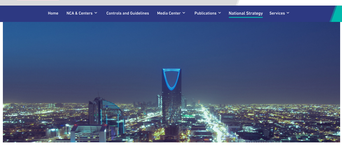


National Cybersecurity Strategy

Foreword

The existence of a secure and trusted national cyberspace is a key enabler for growth and prosperity. Additionally, the expansion in the use of technology opens new horizons for cyber threats, which requires enhancing cybersecurity to protect networks, information technology systems and Industrial Control Systems and operational technologies and their hardware and software components. Furthermore, data and services must be protected from cyber threats and risks such as disruption, amendment, illegal use or exploitation, as well as providing a secure and trusted infrastructure that enables government services and support of the digital transformation.

NCA will lead and coordinate national efforts through the interaction, participation and integration of national entities and international partners and stakeholders to achieve its ambition and goals.

Strategic Vision

NCA developed a strategic vision for cybersecurity that reflects the strategic ambition of the Kingdom in a manner that balances between security, trust and growth. The vision that NCA seeks to reach is:

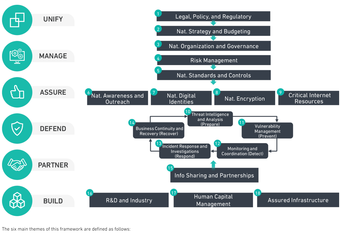
A resilient, secure, and trusted Saudi cyberspace that enables growth and prosperity

This vision is comprehensive for the entire cyberspace and it aligns the Kingdom's priorities and aspirations and emphasizes strengthening the protection and resilience of technical and operational systems and critical infrastructure. It also enhances the confidence of national entities, investors and individuals in the Saudi cyber space, and contributes to the economic and social growth of the Kingdom. Each of the vision's words captures a distinctive aspect of the Kingdom's cybersecurity aspiration:

- Resilient emphasizes the importance of recovering quickly from cyber incidents. This is critical since it is impossible to prevent all cyber-attacks.
- Secure emphasizes the protection of the confidentiality, integrity, and availability of digital or digitally connected assets, networks, and systems.
- Trusted assures investors and citizens that the Saudi cyber ecosystem is a safe place in which to do business and conduct daily life.
- Saudi provides a point of national emphasis – this is the Kingdom's cybersecurity program and it is designed for the Kingdom's needs and priorities in cyberspace.
- Cyberspace covers the entire online, digital world.
- Enables highlights that the digital world contributes to and helps facilitate the Kingdom's greater ambitions.
- Growth reflects the importance of a thriving economy within the Kingdom, as well as the opportunities cyberspace provides to facilitate a vibrant society and ambitious nation.
- Prosperity emphasizes that this program is ultimately about the social and economic well-being of Saudi citizens and guests.

Reference Model:

In order to set a practical reference for the various aspects of cybersecurity at the national level, NCA was keen to design a reference framework for cybersecurity for the Kingdom based on local and international best practices, and the most important developments and challenges facing cybersecurity, so that it is considered an advanced model that includes various aspects of cybersecurity at the country level. This framework contains six themes, including eighteen major elements of cybersecurity and helps to deepen understanding of the cyber kingdom space. This framework was used to develop cybersecurity strategy at the national level. The figure below shows the reference framework:



The six main themes of this framework are defined as follows:

Unify:

This theme is concerned with the integration of all components of the cyber security regulation and it contains three elements:

- **Legal, Policy, and Regulatory:** The frameworks and mechanisms needed to manage strategic directions as required, through the necessary authorities, policies, regulations and legislation.
- **Nat. Strategy and Budgeting:** Develop and review national strategic directions for cybersecurity by working to prepare and review: scope, objectives, initiatives, budgets and expected performance indicators to measure the extent of commitment to the implementation plan.
- **Nat. Organization and Governance**: Develop a governance framework that clarifies the roles, responsibilities and powers of the authorities and individuals concerned.

Manage:

This theme is concerned with identifying critical infrastructures and managing cyber risks, and it contains two elements:

- **Risk Management**: Reducing risks from threats and vulnerabilities by implementing risk management processes that begin with identifying critical infrastructures, identifying and assessing risks, working to reduce them, and ending with monitoring risks to contribute in enhancing cyber resilience.
- **Nat. Standards and Controls:** Providing a reference model for national standards and cyber controls, so that they work to define the scope of the essential and sub-controls, their coverage and how they work to implement them with the various sectors and related entities, and their compliance.

Assure:

This theme is concerned with assuring the protection of cyberspace, and it contains four elements:

- **National Awareness and Outreach**: Awareness in the cyberspace at the national level through awareness and training campaigns, which contributes to improving behavior and adopting and applying best practices.
- **National Digital Identities:** Enhancing cybersecurity aspects of digital identities at the national level, which contributes to raising the level of reliability of digital identities in the cyberspace.
- **National Encryption:**The national data encryption mechanism includes the development and evaluation of national encryption mechanisms, algorithms, and standards.
- **Critical Internet Resources:** Through enhancing cybersecurity aspects to protect critical internet resources and enhancing Internet resilience.

Defend:

This theme is concerned with developing the national cyber defense mechanisms to protect against risks and threats, and it contains five elements:

- **Threat Intelligence and Analysis (Prepare)**:Monitor and share cyber threats with relevant stakeholders from the public and private sectors.
- **Vulnerability Management (Prevent):** It includes working jointly with individuals and related entities to scan for any vulnerability that can be exploited and sharing recommendations with affected parties to take appropriate action.
- **Monitoring and Coordination (Detect):** Enhance the level of situational awareness, classify threats and test incident response plans for specific attacks and then contain them if they occur before they cause significant damage.
- **Incident Response and Investigations (Respond):** Mechanisms to respond to incidents and test their plans on specific attacks to create continuous improvements to adapt to cyber threats and risks, and activities are coordinated at the national level to contain and reduce cyber-attacks and reduce their damage.
- **Business Continuity and Recovery (Recover):** This element includes making sure that there are contingency plans and tests of critical infrastructures and important electronic services, as well as specific procedures to restore service after a cyber incident, and to constantly work on these tests to verify the integrity of the infrastructure.

Partner:

This theme is concerned with setting up the appropriate mechanisms for building partnerships and sharing information, and it contains:

- **Information Sharing and Partnerships:** It enables the development of policies, mechanisms, and best practices that allow information related to cyber threats to be shared with national and international partners, as well as assistance in coordination and cooperation, which contributes to raising readiness, preparedness, interruption, and the speed of the response.

Build:

This theme is concerned with ensuring the existence of a strong and secure national base, and it contains three elements as follows:

- **R&D and Industry:**Encourage research in the field of cybersecurity at the national level, and support innovation and investment in the field of cybersecurity to convert research and development outputs into products and services. It also includes motivating the cybersecurity industry to ensure that adequate capacity is built.
- **Human Capital Management:**This component includes the preparation and qualification of national capabilities specialized in cybersecurity and developing those cadres to maintain them, in order to meet the national need in this field through high-quality education and training programs.
- **Assured Infrastructure:** Work on adopting a proactive approach to ensure the security of systems, devices and services across the entire supply chain, from design to production, and then operation, to destruction, and the development of mechanisms and standards for evaluation and testing, and the services and parameters of the services and services.

Strategic Goals:

To reach a resilient, secure, and trusted Saudi cyberspace that enables growth and prosperity, NCA seeks to achieve six main goals as follows:

- **1. 'Unify :Whole-of-Nation Cybersecurity'**

In order to ensure high levels of coordination and alignment, it is important to adopt a comprehensive national approach to cybersecurity by integrating and defining the roles and responsibilities of cybersecurity-related entities at the national level in order to develop and implement regulations and policies, and to comply with national standards in all aspects of cybersecurity. In addition to the existence of unified mechanisms for planning and budgeting, and setting priorities in the field of cybersecurity effectively, which enhances the efficiency of spending.

- **2. 'Manage: Adaptive Risk Management'**

Managing cyber risks at the level of entities and sectors and at the national level, identifying the affected elements in the cyberspace and the severity of the damage, and choosing the best methods for dealing with them to limit their effects. In addition to defining protection and defense measures according to the level of risk.

- **3. 'Assure :Cyber Ecosystem Assurance'**

The existence of comprehensive controls, national standards, and a compliance-monitoring system that achieves protection for the cybersecurity ecosystem, in addition to raising the level of social awareness of cybersecurity, and continuing and enhancing communication with it through public awareness campaigns for individuals and entities, thus achieving maturity and application of cybersecurity controls at the level of individuals, sectors and national entities.

- **4. 'Defend :Dynamic Defense'**

Reinforcement and continuous development of national capabilities in defense against cyber threats, to detect and deal with cyber-attacks and threats, and to respond and recover from them if they are infected.

- **5. 'Partner :Collaborative Security'**

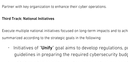
Cybersecurity requires effective local and international partnerships reinforced by advanced mechanisms for sharing information. It enables continuous development and improvement and the sharing of best practices, investigative information and necessary measures. To reach the desired level of cooperation, strengthen partnerships and build channels for sharing information inside and outside the Kingdom.

- **6. 'Build :Cyber Ecosystem Development'**

Protecting the Kingdom's cyberspace requires a strong base of qualified national capabilities in this field in addition to a thriving national cybersecurity industry, one of the main directions is building national capabilities in cybersecurity through high-quality education and training programs, programs that stimulate and support industry, research and development, innovation and investment in Cyber security to enable growth and prosperity.

Action Plan

The action plan created three main tracks to achieve measurable national impacts in both the short and long term. These three tracks, shown below, were set to achieve both the Strategy's vision and national strategic goals



First Track: High-Return Projects

Accomplish high-impact, low-effort security hygiene projects.

Second Track: Cybersecurity catalyst

Partner with key organization to enhance their cyber operations.

Third Track: National Initiatives

Execute multiple national initiatives focused on long-term impacts and to achieve the goals of the national cybersecurity strategy. Each initiative is linked with one of the six strategic goals. They can be summarized according to the strategic goals in the following:

- Initiatives of **'Unify'**: goal aims to develop regulations, policies, activating roles and responsibilities, and developing cybersecurity strategies, and develop the guidelines in preparing the required cybersecurity budgets.
- Initiatives of **'Manage'**: goal aims to establish the capacities for cyber risk management on a national level, and developing a comprehensive guide to manage risks, and complying with this guide.
- Initiatives of **'Assure'**: goal aims to raise awareness on a national scale constantly and effectively through a number of awareness programs, improve cyber resilience against attacks, and developing the national encryption mechanisms and standard.
- Initiatives of **'Defend'**: goal aims to design and develop technical capacities to detect cybersecurity threats and monitor them constantly, in addition to managing cybersecurity operations and monitoring events.
- Initiatives of **'Partner'**: goal aims to manage the national and global strategic partnerships, and govern the information sharing process with the national entities.
- Initiatives of **'Build'**: goal aims to build national capacities, and establish the national program to support cybersecurity research and innovation, and attracting local and foreign investment.

Overview

To View The National Cybersecurity Strategy Overview