الغــــزاوي ومشـــاركـــوه
AlGhazzawi & Partners

CYBERSECURITY IN SAUDI ARABIA:
LEGAL PERSPECTIVE

In the continuously evolving digital era, cybersecurity has become the cornerstone of Saudi national security and economic stability. The Kingdom’s rapid technological development and digital transformation across various sectors have made the country a prime target for cyber threats. Recognizing the critical importance of safeguarding its digital infrastructure, Saudi Arabia has implemented a comprehensive legal framework to address cybersecurity challenges. This article provides an overview of the Kingdom's cybersecurity landscape, focusing on highlighting essential legislation, regulatory authorities, and compliance obligations.

Saudi Arabia's commitment to cybersecurity is integral to its Vision 2030 initiative, which aims to diversify the economy and develop public service sectors.
The Kingdom has established significant legal and regulatory measures to protect its cyberspace from threats and ensure the security of its digital transformation.

Regulatory Authorities

- **National Cybersecurity Authority Saudi Arabia (NCA) :**
  TEstablished in 2017, the National Cybersecurity Authority (NCA) is the central authority responsible for cybersecurity related issues in Saudi Arabia. Directly linked to the Royal Court, the NCA's mandate includes developing policies, frameworks, and standards to enhance the Kingdom's cybersecurity posture.
- **Data Protection Authority (DPA):**
  The DPA is responsible for overseeing the implementation of the Saudi Data Protection Law. It has the power to investigate data breaches, impose fines on organizations that violate the law, and issue guidance on data protection best practices.

Key Cybersecurity Legislation

Anti-Cybercrime Law

Promulgated under Royal Decree No. M/17 in 2007, the Anti-Cybercrime Law aims to combat cyber offenses by defining various cybercrimes and prescribing corresponding penalties and punishments. Offenses under this law include unauthorized access to computer systems, data breaches, cyber fraud, and the creation or dissemination of materials that threaten public order or religious values. Penalties range from fines to imprisonment, depending on the severity of the offense.

Cybersecurity Law (Royal Decree No. M/33 dated 2020)

This comprehensive law establishes the Saudi Arabia cybersecurity legal frameworks and regulations. It outlines the responsibilities of government entities, private sector organizations, and individuals in protecting critical infrastructure, national security, and personal data. The law mandates the implementation of robust cybersecurity measures, **such as:**

- Conducting regular risk assessments to identify and mitigate cybersecurity risks.
- Developing and implementing incident response plans to effectively respond to and recover from cyberattacks.
- Implementing appropriate technical and organizational measures to protect personal data.
- Cooperating with the National Cybersecurity Authority (NCA) in cybersecurity investigations and incident response.

Personal Data Protection Law (PDPL)

Promulgated under Royal Decree No. M/17 in 2007, the Anti-Cybercrime Law aims to combat cyber offenses by defining various cybercrimes and prescribing corresponding penalties and punishments. Offenses under this law include unauthorized access to computer systems, data breaches, cyber fraud, and the creation or dissemination of materials that threaten public order or religious values. Penalties range from fines to imprisonment, depending on the severity of the offense.

Essential Cybersecurity Controls (ECC)

The NCA has issued the Essential Cybersecurity Controls (ECC) to establish minimum cybersecurity requirements for organizations operating in the Kingdom. The ECC framework comprises five main domains, 29 sub-domains, and 114 cybersecurity controls, covering aspects such as governance, risk management, and incident response. Compliance with ECC is mandatory for government entities and critical national infrastructure operators.

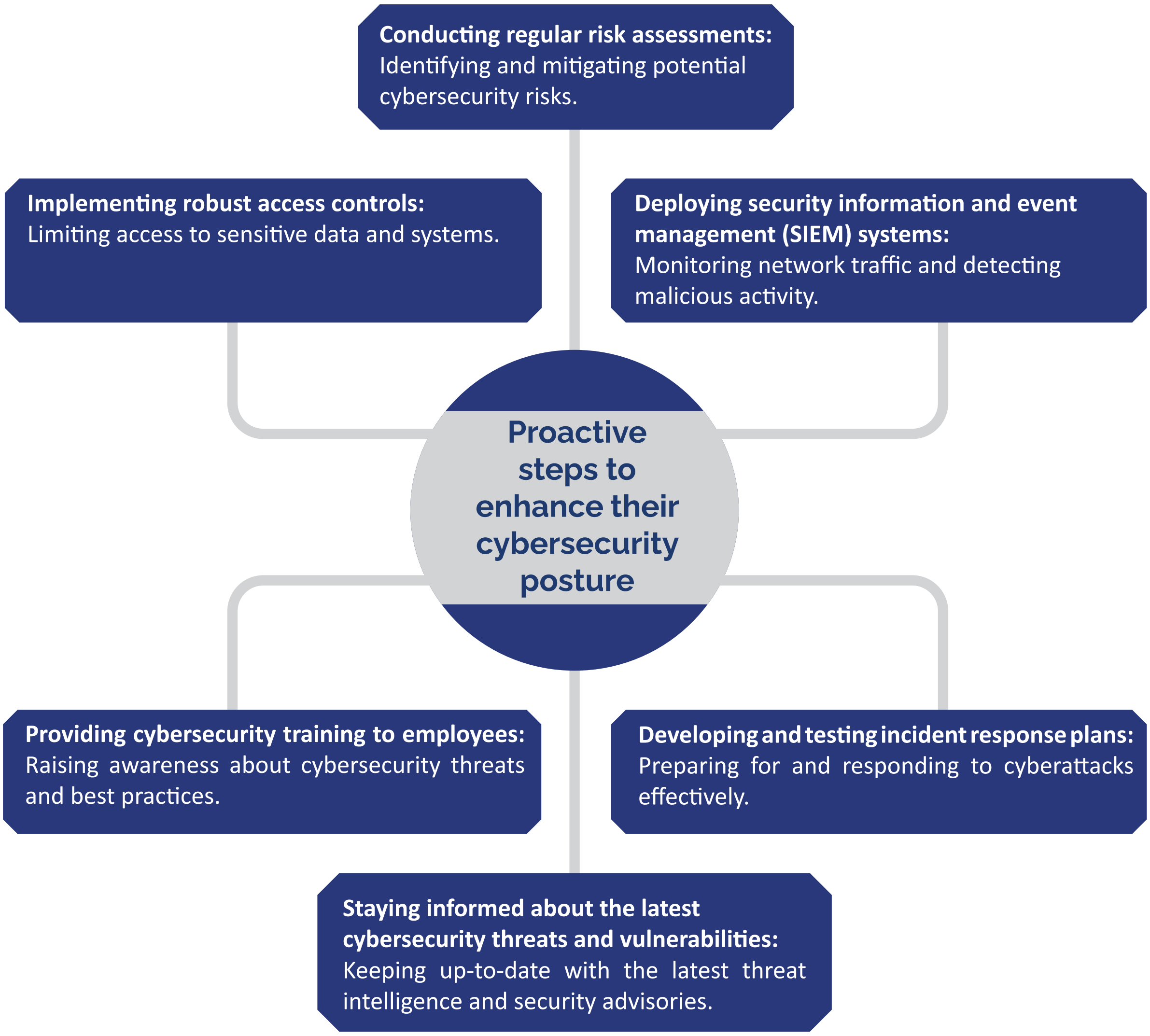
Regulatory Frameworks for Specific Sectors

- **Information and Communications Technology (ICT) and Postal Sectors:**
  The Communications, Space & Technology Commission (CSTC) has developed a Cybersecurity Regulatory Framework (CRF) tailored for service providers in the ICT and postal sectors. This framework outlines cybersecurity requirements to enhance the overall security maturity of these sectors, including guidelines for incident reporting, risk management, and compliance assessments.
- **Operational Technology (OT) Security:**
  Recognizing the convergence of IT and OT systems, Saudi Arabia has issued specific regulations to address cybersecurity in industrial control systems. These regulations mandate organizations to implement security measures that protect OT environments from cyber threats, ensuring the safety and reliability of critical infrastructure.
- **Cloud Computing Regulatory Framework:**
  Issued by the Communications and Information Technology Commission (CITC), this framework sets the standards and requirements for cloud service providers operating in Saudi Arabia. It ensures the security and confidentiality of data stored and processed in the cloud.
- **Electronic Transactions Law:**
  This law governs electronic transactions and signatures, providing a legal framework for the use of electronic documents and records. It aims to facilitate secure and reliable electronic commerce in the Kingdom.

Compliance and Enforcement

Organizations operating in the Kingdom are required to comply with the above-mentioned cybersecurity regulations for businesses in Saudi Arabia to the extent their activities fall in the relevant sectors.

Non-compliance can lead to legal penalties, including fines, imprisonment, and restrictions on business operations. The NCA conducts regular audits and assessments to ensure adherence to cybersecurity standards and may issue directives to address identified vulnerabilities.



Proactive steps to enhance their cybersecurity posture

Conducting regular risk assessments: Identifying and mitigating potential cybersecurity risks.

Implementing robust access controls: Limiting access to sensitive data and systems.

Deploying security information and event management (SIEM) systems: Monitoring network traffic and detecting malicious activity.

Providing cybersecurity training to employees: Raising awareness about cybersecurity threats and best practices.

Developing and testing incident response plans: Preparing for and responding to cyberattacks effectively.

Staying informed about the latest cybersecurity threats and vulnerabilities: Keeping up-to-date with the latest threat intelligence and security advisories.

Recent Developments

In 2024, the NCA issued new regulations and guidelines to address emerging cybersecurity threats and challenges and enhance its readiness across various sectors. For example, the NCA has updated the Basic Cybersecurity Controls (ECC-2:2024) to incorporate international standards and best practices. This update includes four main domains of cybersecurity controls, 28 subdomains, 110 cybersecurity officers, and 90 sub controls.These regulations emphasize the need for qualified cybersecurity professionals, mandating that all cybersecurity positions be filled with full-time, qualified Saudi nationals. This initiative aims to build local expertise and reduce reliance on foreign professionals.

In addition, on December 21, 2024, Saudi Arabia hosted the inaugural meeting of the Arab Cybersecurity Ministers Council, which aims to enhance regional cooperation in cybersecurity. The Kingdom has also signed a headquarters agreement with the Council, designating Riyadh as its permanent headquarters. These initiatives reflect Saudi Arabia's commitment to leading regional cybersecurity efforts.

Challenges and Considerations

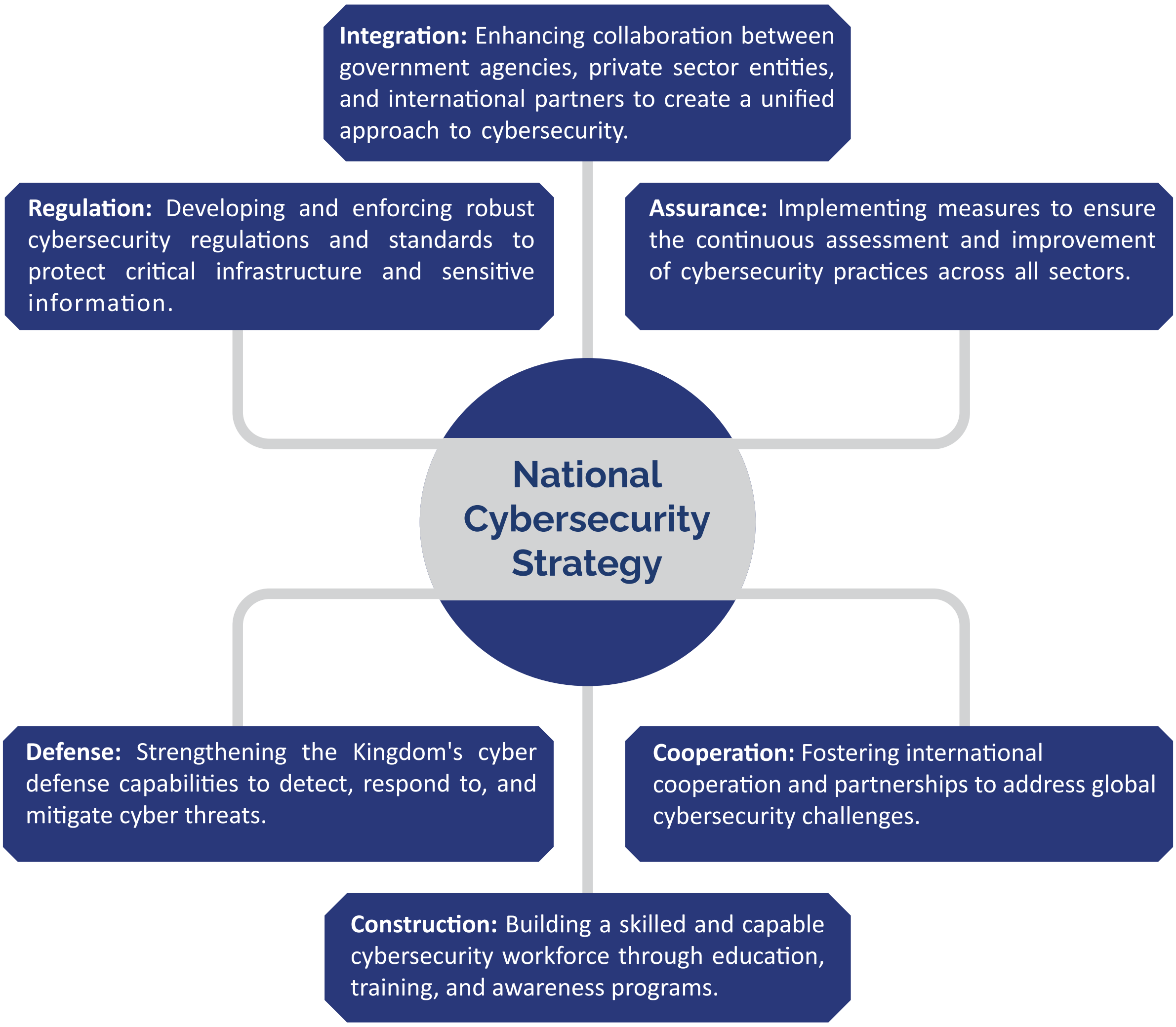
While Saudi Arabia has made significant strides in establishing a robust cybersecurity framework, challenges remain as they remain in other jurisdictions. These include keeping pace with rapidly evolving cyber threats, ensuring continuous compliance across diverse sectors, and fostering a culture of cybersecurity awareness among corporations and individuals.

Organizations must stay informed about regulatory updates and invest in ongoing training and technological advancements to effectively mitigate cyber risks.

National Cybersecurity Strategy

The Kingdom's National Cybersecurity Strategy focuses on creating a secure and reliable cyberspace that enables growth and prosperity. The strategy is built around six main concepts: Integration, Regulation, Assurance, Defense, Cooperation, and Construction.

These concepts aim to enhance cybersecurity governance, develop robust frameworks, and foster international cooperation.



National Cybersecurity Strategy

Integration: Enhancing collaboration between government agencies, private sector entities, and international partners to create a unified approach to cybersecurity.

Regulation: Developing and enforcing robust cybersecurity regulations and standards to protect critical infrastructure and sensitive information.

Assurance: Implementing measures to ensure the continuous assessment and improvement of cybersecurity practices across all sectors.

Defense: Strengthening the Kingdom's cyber defense capabilities to detect, respond to, and mitigate cyber threats.

Cooperation: Fostering international cooperation and partnerships to address global cybersecurity challenges.

Construction: Building a skilled and capable cybersecurity workforce through education, training, and awareness programs.

Strategic Initiatives

The NCA has launched several strategic initiatives to bolster cybersecurity capabilities:

- **CyberIC Program :**
  This initiative aims to cultivate specialized national expertise in cybersecurity through training, certification, and development programs. The program focuses on building a skilled cybersecurity workforce that can address the Kingdom's cybersecurity needs.
- **Managed Security Operations Center (MSOC) Services:**
  The NCA provides advanced threat detection and response capabilities through its MSOC services. These services help organizations monitor, detect, and respond to cyber threats in real-time, ensuring the security of their digital assets.
- **Cybersecurity Research and Innovation Pioneers Grants Initiative:**
  Launched in July 2024, this initiative aims to accelerate cybersecurity skills development across eight key areas, including next-generation cyber defense, cyber resilience, cyber-physical technologies and the Internet of Things (IoT), AI and cyber, cryptography and quantum security, behavioral cyber, future of cyber threats and attacks, and cyber order.
- **Cybersecurity Awareness Campaigns:**
  The NCA conducts regular awareness campaigns to educate the public and organizations about cybersecurity best practices. These campaigns aim to raise awareness about common cyber threats and how to protect against them.
- **Public-Private Partnerships:**
  The NCA collaborates with private sector entities to enhance cybersecurity capabilities and share threat intelligence. These partnerships help create a more resilient cybersecurity ecosystem in the Kingdom.
- **International Collaborations:**
  Saudi Arabia actively participates in international cybersecurity forums and collaborates with other countries to address global cyber threats. The Kingdom has signed several Memoranda of Understanding (MoUs) with other nations to enhance cooperation in cybersecurity.

Conclusion

Saudi Arabia's proactive approach to cybersecurity, backed by a robust legal framework and strategic initiatives, positions it as a leader in the region. The Kingdom's efforts to enhance cybersecurity governance, foster international cooperation, and develop a skilled workforce are crucial for safeguarding its digital future. As cyber threats continue to evolve, Saudi Arabia remains committed to strengthening its cybersecurity capabilities and protecting its digital infrastructure.

The Kingdom's journey towards a secure cyberspace is marked by continuous improvements in its legal and regulatory framework, strategic initiatives, and international collaborations. By prioritizing cybersecurity and embracing innovation, Saudi Arabia is well-positioned to navigate the challenges of the digital age and ensure a safe and secure online environment for its citizens and businesses.