Amman
Tel. 962 6 568 1608
Fax. 962 6 568 1530
PO Box 2374, Amman 11821
Jordan

Governmental Cybersecurity Efforts in the GCC and Yemen Series: Summary and Findings

Arab Advisors Group
Strategic Research Service

This summary report provides findings from Arab Advisors Group's new published report series: Regulatory Authorities, National Cybersecurity Strategies, and Legislations and Regulations. These reports answer the below questions

- *Do the GCC countries and Yemen have established governmental cybersecurity regulatory authorities?*
- *What are the roles of the each of the cybersecurity regulatory authorities in the GCC and Yemen?*
- *How active is each cybersecurity regulatory authority in terms of initiatives to advance the cybersecurity sector in the GCC and Yemen?*
- *What international and local partnerships did cybersecurity regulatory authorities develop to advance the cybersecurity sector?*
- *Which countries in the GCC and Yemen have established a national cybersecurity strategy?*
- *Who are the designated cybersecurity regulatory authorities responsible for implementing and overseeing the national cybersecurity strategy in the GCC and Yemen?*
- *What are the key pillars, strategic objectives, and sub-goals outlined in each national cybersecurity strategy?*
- *What common themes and priorities emerge across the national cybersecurity strategies in the region?*
- *Which sectors are identified as critical national infrastructure in the GCC and Yemen?*
- *Which countries within the GCC and Yemen have enacted cybersecurity legislation and regulatory frameworks?*
- *What specific cybersecurity laws and regulations are currently in place in each country under study?*
- *What penalties and enforcement measures are associated with each of these cybersecurity legislations?*
- *Which regulatory bodies or authorities are responsible for monitoring and ensuring compliance with cybersecurity laws in each country?*
- *What is the broader legal and strategic context surrounding the development of cybersecurity legislation across the GCC and Yemen?*

Feedback: Our clients' satisfaction is of our utmost concern. We welcome all feedback regarding our research and products. Please send us your notes on this report, what you found useful in it and future research directions that would help you in your business. Send feedback emails to: arabadvisors@arabadvisors.com

Table of Contents

List of Exhibits

Section I: Executive Summary

The Gulf Cooperation Council ("GCC") states and Yemen are a prominent bloc within the MENA region. The GCC countries are politically and economically influential, known for their leadership in driving economic development and technological advancement. In contrast, Yemen stands as a focal point of instability in the region. Despite these differences, all these nations face pressing and critical cybersecurity challenges that require focused attention and action.

The GCC countries are home to some of the world's largest oil and gas reserves, positioning their energy infrastructure as a high-value target for cyberattacks. Any disruption to these critical sectors could trigger far-reaching consequences, not only for the regional economy but also for global markets that heavily rely on the steady flow of energy resources. For Yemen, the ongoing political instability and conflict have created a unique cybersecurity landscape. Ensuring the protection of its digital infrastructure has become increasingly vital, not just for the security of the state's operations, but also for safeguarding the safety and well-being of its citizens in a turbulent environment. Both regions face urgent cybersecurity challenges, each shaped by their own geopolitical context, yet crucial for their stability and prosperity.

The GCC countries have also emerged as leaders in the digital transformation of the MENA region, with early and advanced adoption of cutting-edge technologies such as 5G, artificial intelligence, and the Internet of Things ("IoT"). As key players in the global race towards technological innovation, these nations are at the forefront of implementing 5G networks, driving connectivity, and revolutionizing industries; however, this rapid digital advancement also exposes them to an escalating range of cyber threats. The interconnectedness enabled by new technologies, while offering immense economic and technological benefits, also creates new vulnerabilities that demand robust and adaptive cybersecurity measures. In this context, securing digital infrastructures and data has become a critical priority for the GCC to ensure the continued safety and resilience of their economies and societies.

Governments play a pivotal role in addressing the growing significance of cybersecurity within their borders. As the digital landscape evolves, they are tasked with designating the regulatory authorities responsible for overseeing national cybersecurity efforts. These authorities are crucial in shaping and enforcing the regulatory and legal frameworks that ensure the protection of digital infrastructures and assets. In the context of the GCC, where rapid technological advancements such as 5G, AI, and IoT are transforming industries, governments are not only responding to emerging cyber threats but also actively creating policies that foster resilience and security. These regulatory authorities work alongside key national cybersecurity frameworks, initiatives, and legislative efforts to safeguard their countries' digital futures. By establishing clear strategies, objectives, and partnerships, governments are reinforcing their commitment to protecting citizens, businesses, and critical sectors from

the evolving risks of cyber threats. This interconnected role of governance and regulation forms the backbone of any nation's cybersecurity strategy, ensuring that digital security aligns with broader national and regional goals.

Arab Advisors Group released a new report series that provide in-depth insights into government-led efforts aimed at strengthening the cybersecurity landscape in the GCC and Yemen. This three-part series comprehensively examines the cybersecurity initiatives across all seven countries, focusing on the roles of relevant governmental regulatory authorities, their key partnerships and initiatives, as well as national cybersecurity frameworks and plans. Additionally, the series delve into the region's cybersecurity legislation and regulations. For countries with published national cybersecurity strategies, the series also offers an analysis of the core objectives and goals of each strategy, identifying common themes across the region.

Arab Advisors Group took a focused look at the governmental cybersecurity regulatory authorities established within the GCC region and Yemen as well as any computer-emergency response teams ("CERT"). The analysis highlighted the critical roles these authorities play in advancing their nations' cybersecurity agendas, evaluates the activeness of these authorities by examining their announced key partnerships and initiatives. Arab Advisors Group also analyzed national cybersecurity strategies in the GCC region and Yemen, highlighting the availability of a national cybersecurity strategies, which entities are the designated for implementing and overseeing the national cybersecurity strategy in the GCC and Yemen, their key pillars, strategic objectives, and sub-goals outlined in each national cybersecurity strategy. Furthermore, Arab Advisors Group examined common themes and priorities that emerge across the national cybersecurity strategies in the region, as well as the identified sector as critical national infrastructure. We looked into critical national infrastructures ("CNI") in each of the countries under study. Arab Advisors Group also provided a comprehensive overview of cybersecurity legislation and regulatory frameworks across the GCC and Yemen. The analysis for each country includes an assessment of the existence and scope of relevant laws and regulations, the specific types of cybersecurity measures in place, the presence of national policies and control mechanisms, and the identification of the competent authority responsible for enforcement and oversight.

The Global Cybersecurity Index 2024 – The GCC and Yemen

Arab Advisors Group contextualized the cybersecurity status of each country with reference to the ITU's latest Global Cybersecurity Index, published in 2024. This data was used as a starting point to determine the current strength of each country's cybersecurity based on global standards.

The Global Cybersecurity Index is measured by assessing each country's legal measures, technical measures, organizational measures, capacity development and cooperation measures. Three GCC countries had

exceptional scores (the UAE, KSA and Qatar), achieving perfect scores across all 5 scoring pillars. Bahrain and Oman slightly missed the mark, with scores of 97.94 and 97.01, respectively. Kuwait lagged behind its peers in the GCC with a score of 60.58, while Yemen scored the lowest across all MENA countries with a score of 7.19.

In the ITU Global Cybersecurity Index 2024, five GCC countries achieved perfect scores in the Organization Measures, highlighting their strong organizational frameworks in cybersecurity. Additionally, four countries attained perfect scores across the remaining four measures; however, it is important to note that three measures (Organization, Capacity, and Cooperation) registered a zero score for one country in the analysis: Yemen.

Of particular interest is Kuwait, which recorded a notably low score in the Technical Measures, falling below 6. This score is considerably lower compared to the other GCC countries, underscoring a gap in technical cybersecurity capabilities that sets Kuwait apart from its regional peers.

Exhibit 1: Global Cybersecurity Index 2024 – detailed scoring (September 2024)

Country	Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures	Total Score
	20.00	**20.00**	**20.00**	**20.00**	**20.00**	**100.00**
Qatar	20.00	20.00	20.00	20.00	20.00	**100.00**
Saudi Arabia	20.00	20.00	20.00	20.00	20.00	**100.00**
United Arab Emirates	20.00	20.00	20.00	20.00	20.00	**100.00**
Bahrain	20.00	20.00	20.00	20.00	17.94	**97.94**
Oman	19.59	18.39	20.00	19.03	20.00	**97.01**
Kuwait	16.90	5.80	11.88	12.16	13.84	**60.58**
Yemen	5.29	1.90	0.00	0.00	0.00	**7.19**

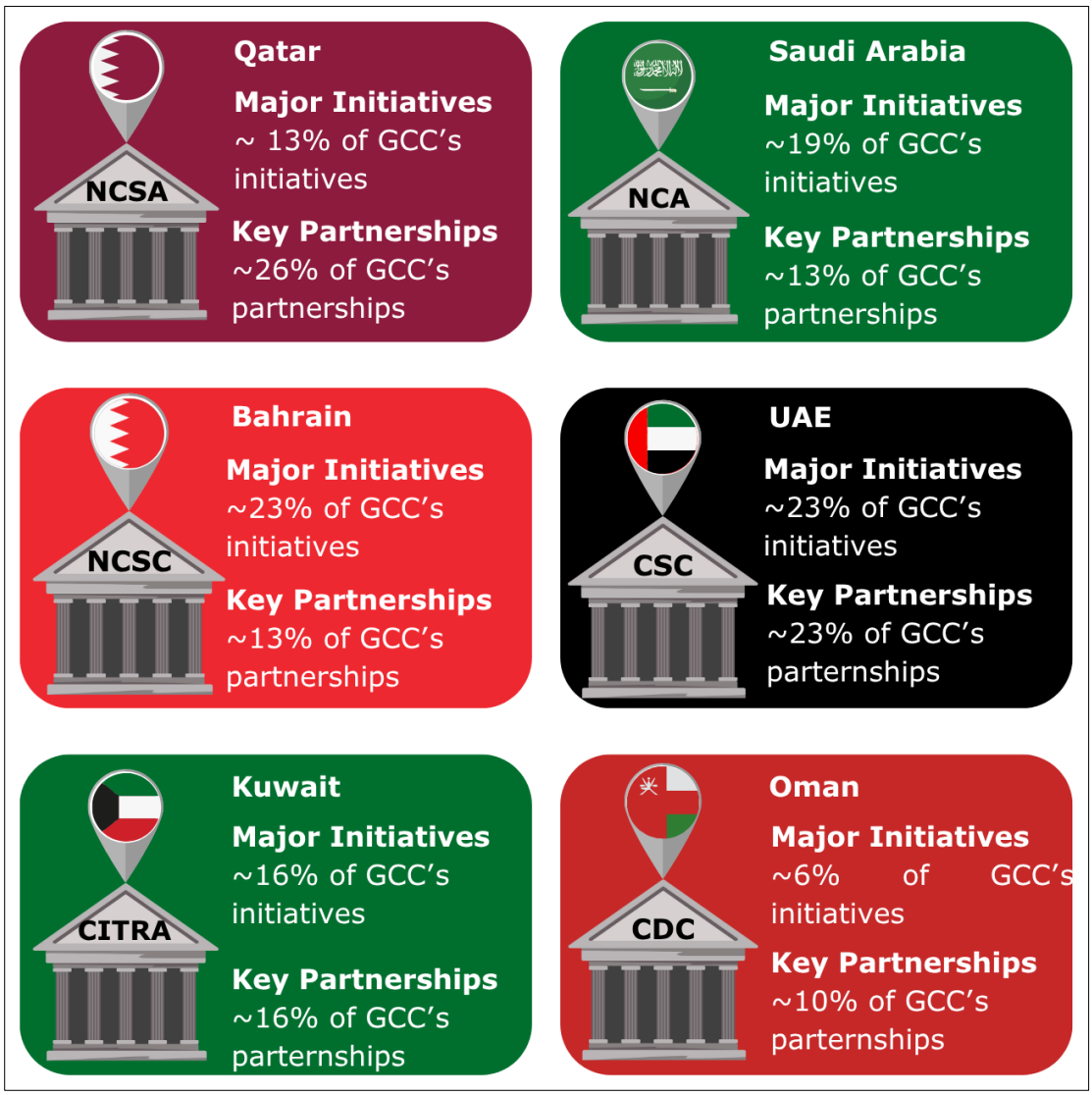
Source: ITU

Governmental Cybersecurity Entities and Authorities in the GCC and Yemen

Arab Advisors Group found that 6 out of 7 assessed countries had governmental authorities responsible for overseeing cybersecurity, with Yemen being the sole outlier. Arab Advisors Group further spotted an anomaly in the cybersecurity realm in the GCC and Yemen; Yemen was the sole country which did not have a cybersecurity emergency response team. Lastly, all of the GCC countries announced several key initiatives and partnerships aimed at strengthening cybersecurity in their countries.

Upon examining each cybersecurity regulatory authority's publicized key partnerships and initiatives, Qatar's National Cybersecurity Agency ("NCSA") topped the list with the highest number of key partnerships in the cybersecurity sector. The UAE's Cybersecurity Council ("CSC") followed.

Exhibit 2: Overview of governmental cybersecurity regulatory authorities in the GCC and Yemen

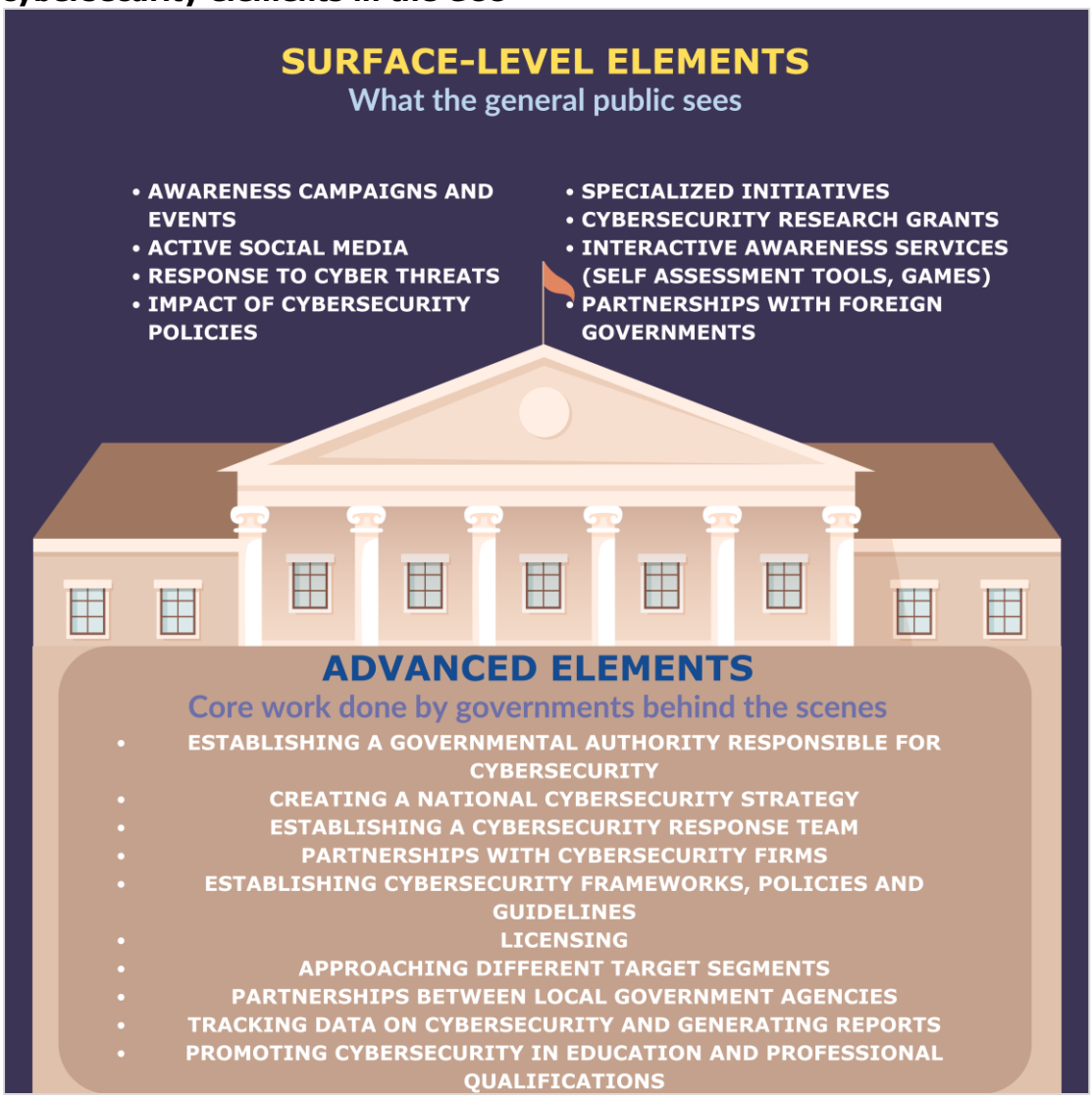


Source: Arab Advisors Group, Cybersecurity regulatory authorities

Cybersecurity Regulatory Authorities Elements

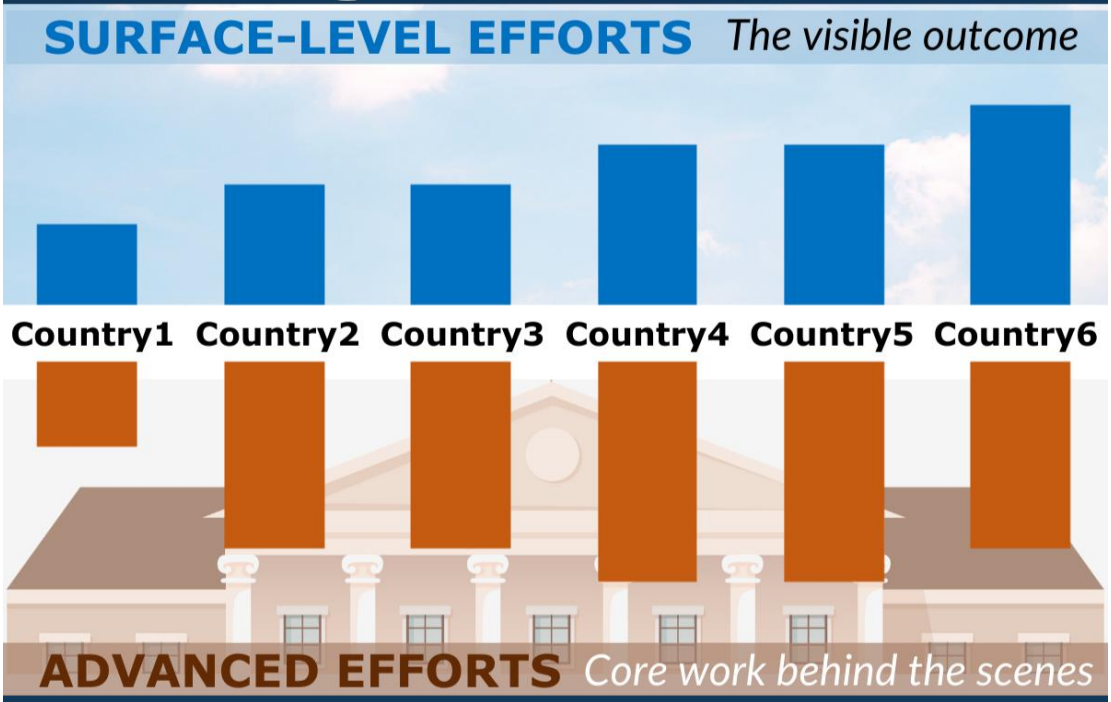
Building a robust and cohesive cybersecurity framework involves various critical components. These components can be broadly categorized into **surface-level elements**, which are visible to the public, and more **advanced elements**, which operate behind the scenes. According to Arab Advisors Group, these components are classified based on the roles of the cybersecurity regulatory authorities, key partnerships, and initiatives. Surface-level elements are: Awareness campaigns and events, active social media accounts, specialized initiatives, as well as partnerships with foreign governments. As for advanced cybersecurity elements, these are: creating national cybersecurity strategies, tracking data and reporting on cybersecurity, as well as licensing. Among the countries analyzed, the most prominent surface-level element was awareness campaigns, which was widely implemented across the GCC's authorities; Yemen has yet to achieve any of these surface-level elements. The exhibit below illustrates the combined surface-level and advanced cybersecurity elements implemented by the GCC's cybersecurity regulatory authorities.

Exhibit 3: Surface-level cybersecurity elements vs. advanced cybersecurity elements in the GCC



Source: Arab Advisors Group, Cybersecurity regulatory authorities

Efforts Vary Across the Region



- Some governments show deep, strategic activity
- Others remain limited to surface-level actions
- Disparities create regional imbalance

Common Themes Across the GCC's National Cybersecurity Strategies

When analyzing the national cybersecurity strategies of all GCC countries, Arab Advisors Group came across four common strategic themes: **cybersecurity resilience**, **cyber ecosystem development**, partnerships and collaborations and **cyber regulatory development**.

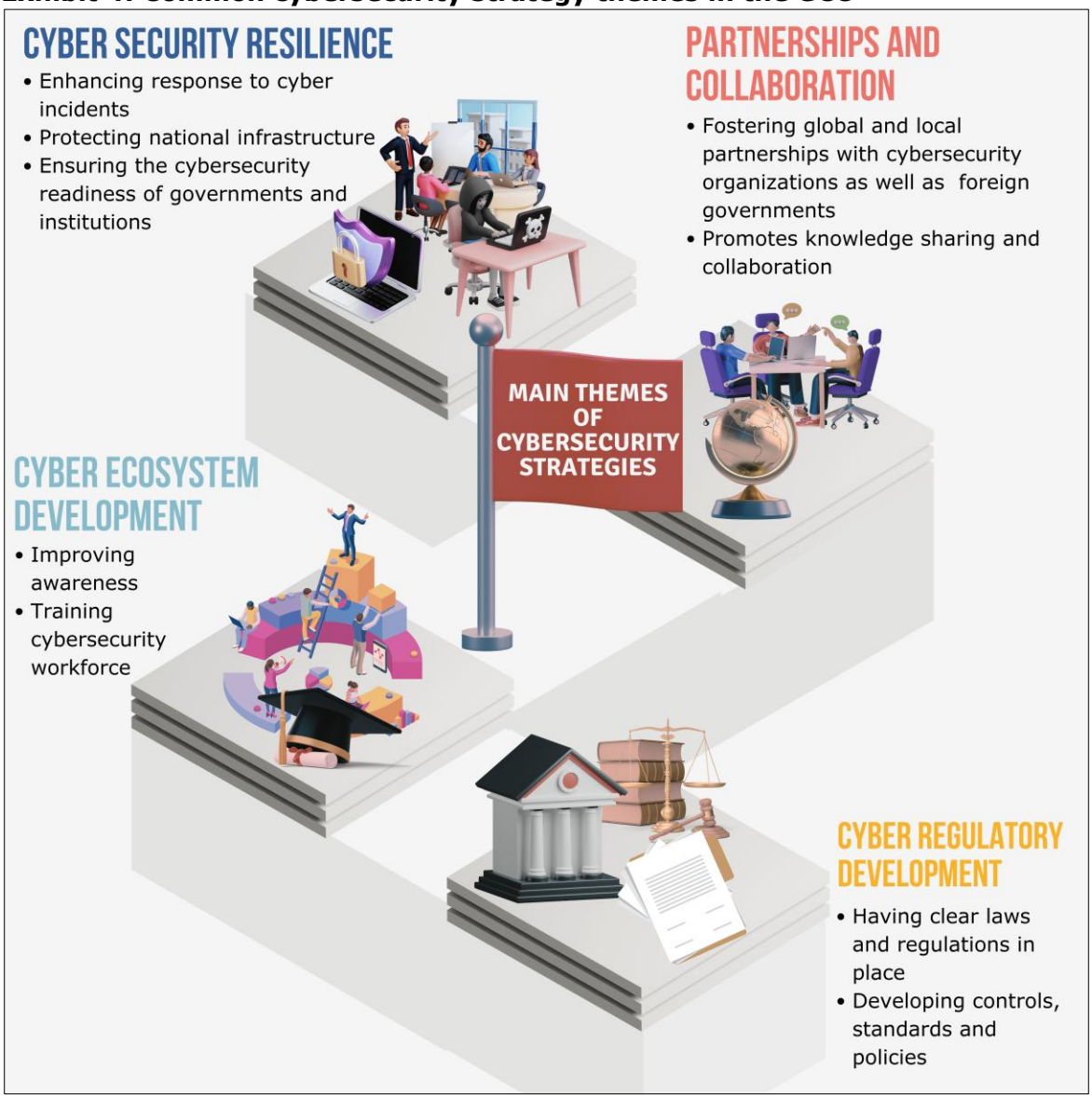
The first theme, cybersecurity resilience, focuses on enhancing response to cyber incidents, protecting national infrastructure, and ensuring the cybersecurity readiness of governments and institutions.

As a part of cybersecurity resilience, many countries in the region have chosen to improve response to cyber incidents through the establishment of computer emergency response teams ("CERT"), and cybersecurity defence centres that may fall under a different name but perform the same function. Arab Advisors Group has considered any type of cybersecurity incident response team to fall under the umbrella of a CERT.

The next common theme seen across the strategies studied was cyber ecosystem development. Partnerships and collaborations were another critical aspect of ensuring cybersecurity strength within a country.

Perhaps the most critical component is cyber regulatory development. This theme was present across all six cybersecurity strategies and has already been enacted by all six GCC countries.

Exhibit 4: Common cybersecurity strategy themes in the GCC



Source: Arab Advisors Group, Cybersecurity regulatory authorities

3 Shared Goals Across All National Cyber Strategies

✅ Strengthen resilience
🤝 Foster collaboration
👩‍💻 Build digital capabilities

Cybersecurity Governance in the GCC and Yemen

Arab Advisors Group identified the key entities responsible for overseeing cybersecurity governance across the GCC and Yemen. Cybersecurity governance in the GCC was either centralized, meaning that there was a singular responsible entity, or a network, meaning that there were multiple responsible entities.

Arab Advisors Group also identified the number of cybersecurity legislations in each of the 6 GCC states. KSA and the UAE stood out with the highest number of legislations. Two of the UAE's legislations concern the same cybersecurity matter, meanwhile all KSA's legislations tackle a different aspect of cybersecurity. Conversely, Bahrain had the fewest number of cybersecurity legislations.

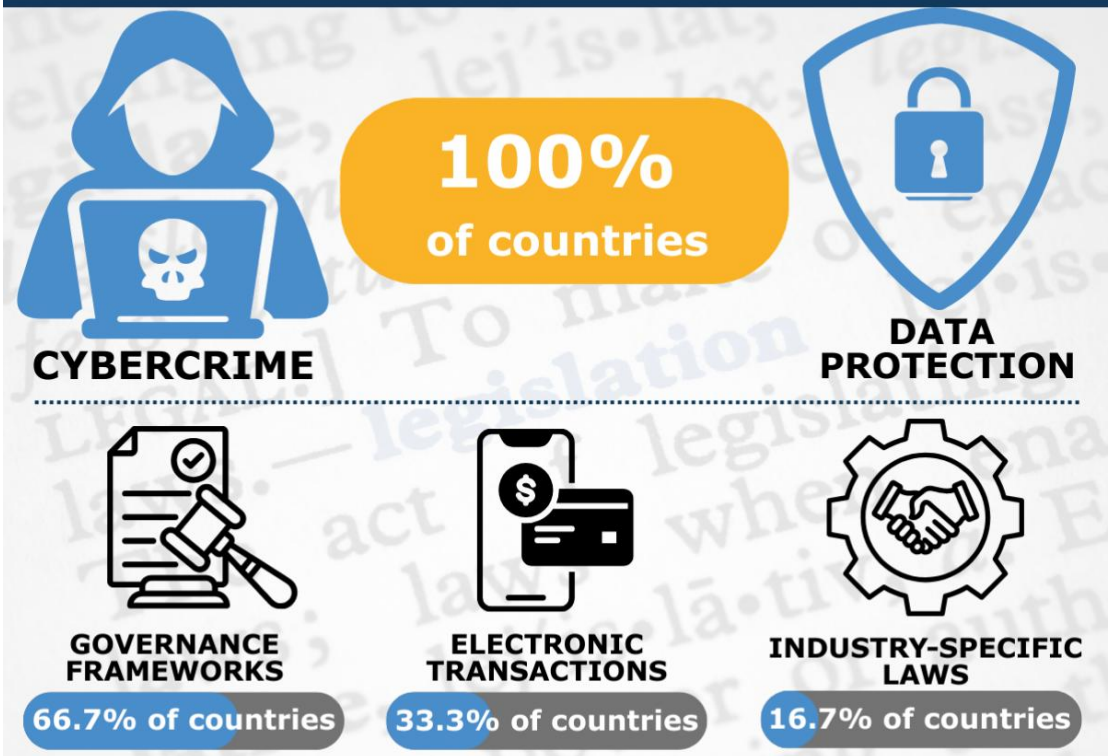
Areas of Convergences in Cybersecurity Legislations and Regulations in the GCC and Yemen

Arab Advisors Group conducted an in-depth analysis of existing legislation and regulatory frameworks across the GCC and Yemen, identifying areas of convergence. Arab Advisors Group divided the areas of convergence into five distinct categories: **Cybercrime Laws**, **Data Protection Laws**, **Governance Frameworks**, **Electronic Transactions**, and **Industry-specific Laws**.

The most commonly enacted laws across these countries pertain to cybercrime and data protection laws, both of which are foundational components of the GCC's national cybersecurity strategies. Notably, the data protection laws in the GCC are largely modeled after the internationally recognized General Data Protection Regulation ("GDPR"), reflecting a regional commitment to aligning with global best practices. Such legislation plays a critical role in safeguarding individuals' rights and ensuring the secure handling of personal data in the digital environment.

In terms of regulatory alignment, Saudi Arabia and Kuwait share identical cybersecurity laws. Meanwhile, the UAE distinguished itself, featuring industry-specific legislations.

Legislation: Present but Uneven



✅ All countries have data protection laws
⚠️ only 33% address e-transactions
🚫 Just 1 country covers industry-specific operations