الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

Report on

Key Economic Indicators in the Cybersecurity Sector 2025

TLP: White
Document Classification: General

In Collaboration with

BCG | IDC

In the Name of Allah,
The Most Gracious,
The Most Merciful

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has 4 colors (traffic lights):

🔴 Red – Personal, Confidential and for Intended Recipient Only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients either inside or outside the organization.

🟠 Amber – Restricted Sharing

The recipient may share information classified in orange only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

🟢 Green – Sharing within The Same Community

The recipient may share information classified in green with other recipients inside the organization or outside it within the same sector or related to the organization. However, it is not allowed to exchange or publish this information on public channels.

⚪ White – No Restriction

CONTENT

Executive Summary 6

Introduction 7

Foreword by Report Development Partners 8

1. Methodology 10

1.1. Classification of Products and Services in the Cybersecurity Sector 10

1.2. Data Collection 11

1.3. Quality Assurance 11

1.4. Data Analysis 12

1.5. Outputs Development 12

Key Findings 13

2. Key Economic Indicators in the Cybersecurity Sector 16

2.1. Cybersecurity Market in the Kingdom 16

2.1.1. Market Size 16

2.1.2. Expenditure by Entity Size 16

2.1.3. Market Size by Classification of Cybersecurity Products and Services 17

2.1.4. Geographic Distribution of the Demand Side 17

2.1.5. Geographic Distribution of the Supply Side 18

2.1.6. Classification of Cybersecurity Product and Service Providers by Organizational Size 18

2.2. Sector Contribution to GDP 19

3. Key Cybersecurity Workforce Indicators 20

3.1 Cybersecurity Workforce Size 20

3.2. Women Participation 20

3.3. Geographical Distribution 21

3.4. Experience Levels 21

3.5. Cybersecurity Education 21

Appendix A 22

The Taxonomy for Cybersecurity Products and Services 22

Executive Summary

Following Royal Decree No. 6801, issued on 11/2/1439H, the National Cybersecurity Authority (NCA) has been established as the sole authority in the Kingdom of Saudi Arabia for cybersecurity and serves as the National Reference in its affairs. NCA aims at strengthening cybersecurity to safeguard the State's vital interests, national security, critical infrastructures, priority sectors, and government services and activities. NCA's powers and duties provided for in its statute include stimulating the growth of the cybersecurity sector in the Kingdom, encouraging innovation and investment, conducting research studies, and development, and manufacturing processes.

To assess the current state of the cybersecurity ecosystem in the Kingdom, this second annual report by NCA in cooperation with BCG and IDC, covers data gathered for 2024 and compares results against 2023 statistics from the prior report. It offers an in-depth and forward-looking analysis of the cybersecurity sector and defines key drivers that will inform future initiatives and programs to further boost growth and help maintain the Kingdom's position as a world leader in cybersecurity.

The report is divided into three main sections:

1. Methodology – details the framework for the market study, the data collection methods and accuracy verification and validation procedures, and analytical tools employed to derive the outputs.

2. Key Economic Indicators – provides a granular view of the cybersecurity sector in the Kingdom. Significant findings include the market size of SAR (15.2) billions; spending split by sector, where (68%) is spent by private sector entities and (32%) by public sector entities; geographic distribution of demand and supply; number of registered cybersecurity providers, which reached (420) providers; and cybersecurity contributing SAR (18.5) billion to the GDP, which represents (0.40%) of GDP and (0.71%) of non-oil activities.

3. Key Workforce Indicators in the Cybersecurity Sector – examines cybersecurity workforce size and trends. The study showed the continued expansion of the national cyber talent base, which reached over (21) thousand professionals, of which (32%) are females, underscoring the Kingdom's commitment to building robust and inclusive local expertise.

Introduction

The cybersecurity sector in the Kingdom has experienced remarkable growth and transformation, leading to international recognition; as the Kingdom maintained the first position in the cybersecurity indicator in the World Competitiveness Yearbook's for 2025 released by the World Competitiveness Center of the International Institute for Management Development (IMD). This positioning acknowledges the Kingdom's leadership position in this vibrant and promising sector. This has also been confirmed by achieving leading positions, year after year, as the Kingdom is classified Tier 1 – "Role-modelling" in the Global Cybersecurity Index 2024, published by the United Nations specialized agency, the International Telecommunication Union (ITU).

The Saudi model has emerged as one of the benchmarks for excellence, resulting in both economic and security improvements and inspiring international attention and collaboration. As the model is comprehensive in addressing cybersecurity across all aspects, whether legislative, security, or economic. The Saudi model is based on the centralization of cybersecurity governance at the national level, including policies and regulations, cyber operations, cybersecurity assessments, incident response, and capacity building, while allowing for the decentralization of on-premises operations, which remain the responsibility of national entities.

This model contributes to efficient and effective management and control of the entire national cybersecurity ecosystem, maximizing the Kingdom's national gains and international standing while enabling individual national entities to carry out their cybersecurity roles and responsibilities and raise their operational readiness.

Building on last year's baseline study, NCA, in partnership with BCG and IDC, reapplied its evidence-based research framework to produce the Kingdom's second annual economic analysis of the sector. The 2025 study follows global best practices in sampling, validation and econometric modelling; achieving over (98%) confidence level with a (3.5%) margin of error. The resulting dataset illuminates market structure, GDP contribution, and workforce dynamics with granularity and precision.

Foreword by Report Development Partners

Saudi Arabia's cybersecurity sector continues to evolve at a rapid pace. It has become not only a vital enabler of national security but also a central pillar of economic diversification and long-term resilience. The sector today is characterized by its expanded providers' capabilities base, and the steady development of national talent, together forming an ecosystem that underpins trust in services and infrastructures across the Kingdom.

This report represents the second annual study produced by the National Cybersecurity Authority (NCA) in collaboration with Boston Consulting Group (BCG) and International Data Corporation (IDC). The methodology underpinning this study is rigorous and comprehensive, combining survey data, interviews, and engagements with government entities, private sector organizations, and providers of cybersecurity products and services. This report aims to provide a clear and structured view of the Kingdom's cybersecurity sector, organized around three core pillars: the market, the contribution to the economy, and the workforce.

On the market side, the study distinguishes between government entities, private sector entities owning, operating or hosting Critical National Infrastructures, and the remaining private sector entities with diverse activities and sizes. It further classifies demand and supply into products and services; enabling a comprehensive understanding of market size across all segments.

The report also examines the broader economic role of cybersecurity by assessing its direct and indirect contributions to the national economy. This analysis follows internationally recognized standards and draws on official statistical frameworks to ensure comparability and reliability. Equally important is the review of the workforce, which highlights the growth of national talent, the strengthening of education programs, and the emergence of research and development capabilities that will sustain the sector in the years ahead.

By presenting a coherent picture of the sector's size, structure, and economic impact, this report aims to provide decision-makers with the insights needed to shape policy, guide investment, and advance the Kingdom's leadership in cybersecurity. The work reflects the continued commitment of the National Cybersecurity Authority, in supporting the Kingdom to build a resilient, competitive, and sustainable cybersecurity ecosystem.

Report
Development
Partners

BCG IDC

1. Methodology

The National Cybersecurity Authority (NCA) utilized its previously established research framework to deliver the Kingdom's most comprehensive view of the cybersecurity sector. The study began by mapping the entire value chain with NCA's three-tier classification of (5) overarching categories, (26) activity clusters and (102) discrete product and service lines; so that every datapoint could be rigorously tagged and studied.

Leveraging this classification, the team assembled a primary dataset on the Kingdom's cybersecurity sector with validated responses drawn from stakeholders, spanning government entities, private sector entities owning, operating or hosting Critical National Infrastructures (private CNIs), the remaining private sector entities with diverse activities and sizes, the providers of cybersecurity products and services, academic institutions, and cybersecurity professionals. Each input underwent multi-layer quality controls that included sampling checks, outlier tests, and reconciliation against official statistics; which yielded a confidence level of over (98%) with a margin of error of (3.5%), materially above typical industry standards.

Clean data were then fed into a suite of econometric and operational models (revenue sizing, demand sizing, workforce sizing, and GDP-contribution models) calibrated inline with the General Authority for Statistics (GASTAT) methodology and leading international research partners. These models translated raw inputs into the key market, workforce and macro-economic indicators featured in this report, ensuring that every figure is both statistically robust and directly comparable year on year.

1.1. Classification of Products and Services in the Cybersecurity Sector

A comprehensive classification of cybersecurity products and services was developed in cooperation with several leading think tanks and cybersecurity analyst firms (Appendix 1). Various global companies and providers of cybersecurity products and services were evaluated to cover the details of the cybersecurity sector comprehensively. The latest classification of cybersecurity products and services, designed to be updated as needed to reflect evolving technologies and market developments, includes (102) discrete products and services, organized into three levels.

Cybersecurity Products and Services Classification Levels

Level 1

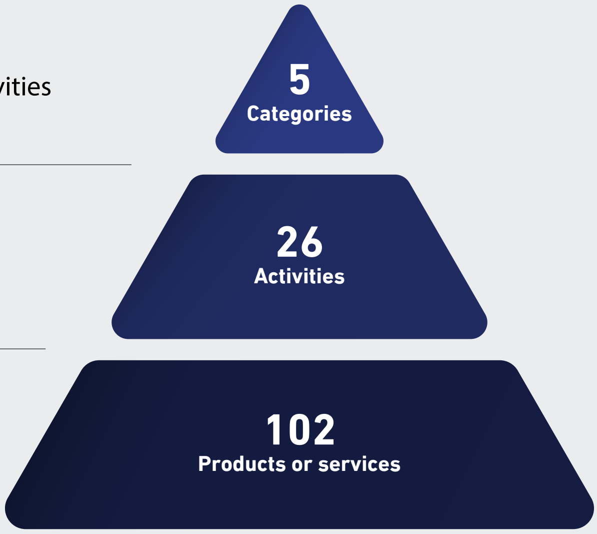
This level provides the basic classification for cybersecurity sector activities as products or services based on the business and delivery models.

Level 2

Each category from Level 1 is divided into a group of detailed activities.

Level 3

This level specifies the cybersecurity products and services within each activity from Level 2.



5 Categories

26 Activities

102 Products or services

1.2. Data Collection

The study started by capturing a complete view of the Kingdom's cybersecurity landscape through engaging all ecosystem segments. The study team deployed a nationwide survey, supplemented by targeted focus groups and individual interviews after classifying the ecosystem into government entities, private sector entities owning, operating or hosting Critical National Infrastructures (private CNIs), the remaining private sector entities with diverse activities and sizes, the providers of cybersecurity products and services, academic institutions and cybersecurity professionals.

This led to the development of a large primary dataset with validated responses, covering demand-side organizations, supply-side firms registered with NCA, academic institutions, and cybersecurity professionals. The breadth of participation produced a statistical confidence level of over (98%) with a margin of error of (3.5%), well above accepted research standards for similar reports.

1.3. Quality Assurance

Quality assurance was enforced through a multilayer verification process, in line with international standards, and the controls that are published by the National Data Management Office (NDMO), applied from collection to modelling. This process includes automated consistency checks, and manual reviews; to screen for outliers, and apply other controls. Additionally, follow-up sessions with respondents and interviews with experts across the ecosystem were conducted to validate key findings and pressure-test insights. These measures provide a robust foundation for the study outputs; giving decision makers, investors, and entrepreneurs confidence.

98% Statistical confidence

3.5% Margin of error

The methodology guaranteed breadth of participation produced high statistical confidence level and limited margin of error.

1.4. Data Analysis

Clean data were channeled into a set of statistical and econometric models that quantified every major indicator of the Kingdom's cybersecurity ecosystem. Built jointly with local and international specialists, the models measured spending on cybersecurity products and services across the different demand segments to size the demand, namely government entities, private sector entities owning, operating or hosting Critical National Infrastructures (private CNIs), and the remaining private sector entities with diverse activities and sizes. On the supply side, revenues reported by providers registered with NCA were consolidated to size the supply. Model inputs drew on expert testimony and official datasets from the Ministry of Human Resources and Social Development, the General Authority for Statistics (GASTAT), and the Small and Medium Enterprises General Authority (Monsha'at); and were stress-tested against international benchmarks to ensure coherence.

To determine the sector's impact on the wider economy, the team followed the General Authority for Statistics (GASTAT) methodology for GDP calculations. Provider revenues, labor income, and corporate taxes and subsidies were fed into an input–output framework that produced both direct and indirect GDP contributions, yielding a transparent and repeatable measure of cybersecurity's economic indicators.

1.5. Outputs Development

The findings of this study, taken from the statistical and econometric models, provide valuable insights about the cybersecurity market in the Kingdom and its economic contribution along three dimensions:

1. Cybersecurity Market Size

2. Cybersecurity Sector GDP Contribution

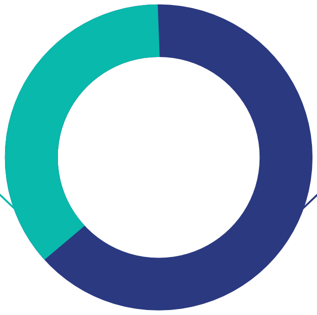
3. Cybersecurity Workforce

Due to rounding, some totals and percentages presented in the report may not add up precisely.

Key Findings

Cybersecurity Market Size in the Kingdom:

32%
Public Sector Expenditure
⃁ **4.8** Billion

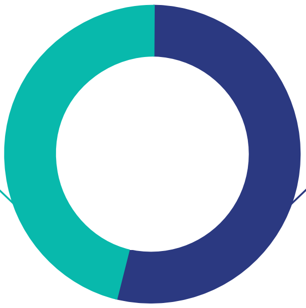


68%
Private Sector Expenditure
⃁ **10.3** Billion

⃁ **15.2** Billion

Contribution to Gross Domestic Product (GDP) at Current Prices:

49%
Direct Contribution
⃁ **9** Billion



51%
Indirect Contribution
⃁ **9.5** Billion

⃁ **18.5** Billion

0.40%
Sector Contribution to GDP

0.71%
Sector Contribution to Non-Oil Activities

Registered Cybersecurity Product and Service Providers with NCA:

420
Cybersecurity Product and Service Providers

17
Large Providers

74
Medium Providers

166
Small Providers

163
Micro Providers

Market Revenue Contribution by Provider Size

Smaller CS providers		Larger CS providers	
Micro	Small	Medium	Large
1.0%	13.0%	43.3%	42.7%

Key Cybersecurity Products and Services in the Kingdom:

- Network Security
- Endpoint Security and Management
- Cybersecurity Operations Solutions
- Cybersecurity Management Consulting
- Data Security

Cybersecurity Workforce in the Kingdom:

21.3K
Cybersecurity Specialists

32%
Women Participation

5K
Cybersecurity Graduates

3967945
352575
3852575
45
2126548
4567356
4395792
4395792
4395792
4637457
424
4637457

2. Key Economic Indicators in the Cybersecurity Sector

2.1. Cybersecurity Market in the Kingdom

2.1.1. Market Size

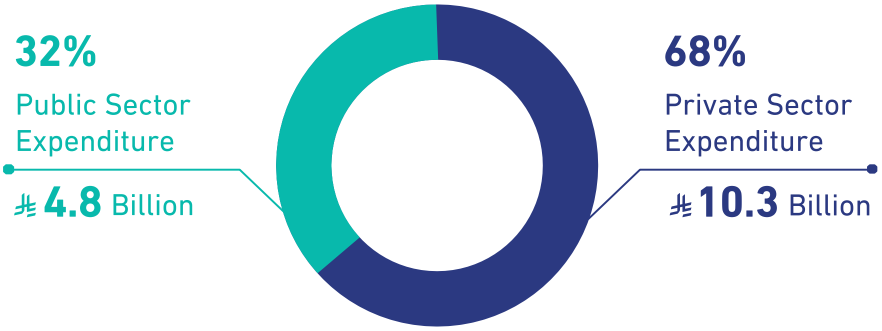
Spending on cybersecurity products and services continued its upward trajectory in 2024, reaching SAR (15.2) billion, an increase of (14%) over the previous year. This sustained growth is driven in part by NCA's ongoing initiatives to enhance the security and resilience of the Saudi cyberspace, which have elevated awareness, regulatory compliance, and investment across the various demand segments. Government entities, a smaller but strategically vital group of purchasers, spent around SAR (4.8) billion, representing (32%) of total demand. Private sector organizations remained the principal buyers, accounting for roughly (68%) of total expenditure, or about SAR (10.3) billion. Within that figure, private sector entities owning, operating or hosting Critical National Infrastructures (private CNIs) directed about SAR (3.0) billion to safeguard operations that underpin the national economy. Relative shares among the buyer segments were broadly unchanged from 2023, suggesting a maturing market with balanced growth across the public and private domains.

2.1.2. Expenditure by Entity Size

When spending is viewed through the lens of organizational size according to the Small and Medium Enterprises General Authority's (Monsha'at) classification, large entities in government and large entities in private sector owning, operating or hosting Critical National Infrastructures (private CNIs) each accounted for (94%) of total cybersecurity expenditure of their segment, a pattern shaped mainly by their regulatory roles and operational needs.

Among the remaining private sector entities with diverse activities and sizes, small entities make (39%) of total spending in their segment, followed by medium entities (34%). This is due to their numerical dominance.

⃁15.2 Billion

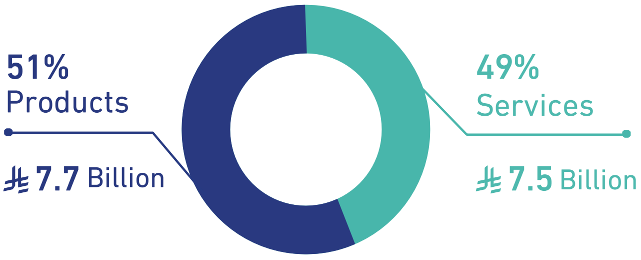


	Total Expenditure (Billion SAR)	Large Entities	Medium Entities	Small Entities	Micro Entities
Public sector entities	4.8	94%	6%	0.2%	-
Private sector entities owning, operating or hosting critical national infrastructures	3.0	94%	6%	0.3%	-
The remaining of the private sector entities	7.3	18%	34%	39%	9%

2.1.3. Market Size by Classification of Cybersecurity Products and Services

Spending on cybersecurity products reached SAR (7.7) billion, representing (51%) of the total market size, while cybersecurity services accounted for SAR (7.5) billion, or (49%).

Based on spending, the key cybersecurity products and services in the Kingdom include Network Security, Endpoint Security and Management, Security Operations Solutions, Cybersecurity Management Consulting, and Data Security. This confirms that organizations continue to prioritize perimeter defence, device resilience, and threat response.



Key Cybersecurity Products and Services in the Kingdom

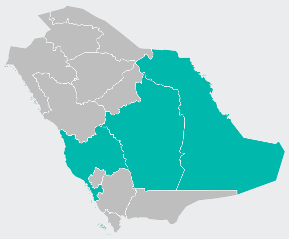
- Network Security
- Endpoint Security and Management
- Cybersecurity Operations Solutions
- Cybersecurity Management Consulting
- Data Security

2.1.4 Geographic Distribution of the Demand Side

Cybersecurity demand is concentrated, as (73%) of entities purchasing cybersecurity products and services are based in Riyadh, Makkah, or the Eastern Region; reflecting the broader economic weight of these regions in the Kingdom's economy.

73%

Of demand entities are based in Riyadh, Makkah, or the Eastern Region.



2.1.5. Geographic Distribution of the Supply Side

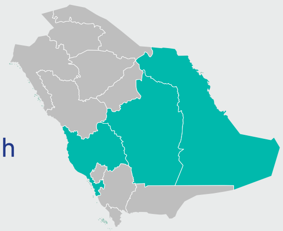
The supply landscape mirrors demand concentration, as (98%) of registered cybersecurity providers are headquartered in Riyadh, Makkah, or the Eastern Region. Riyadh alone hosts (77%) of providers, while Makkah and the Eastern Region account for (11%) and (10%), respectively. This clustering underscores the gravitational pull of the Kingdom's principal commercial centers and their growing cybersecurity ecosystems.

2.1.6. Classification of Cybersecurity Product and Service Providers by Organizational Size

The classification of the size of entities that provide cybersecurity products and services in the Kingdom is based on the definition provided by the Small and Medium Enterprises General Authority (Monsha'at). Given overlapping operational characteristics, medium and large providers were consolidated into a single category (larger providers) and small and micro providers were placed in a separate category (smaller providers). This categorization allows for clearer and more insightful comparisons and more accurate visualization of market structure.

98%

Of cybersecurity providers are based in Riyadh, Makkah or the Eastern Region



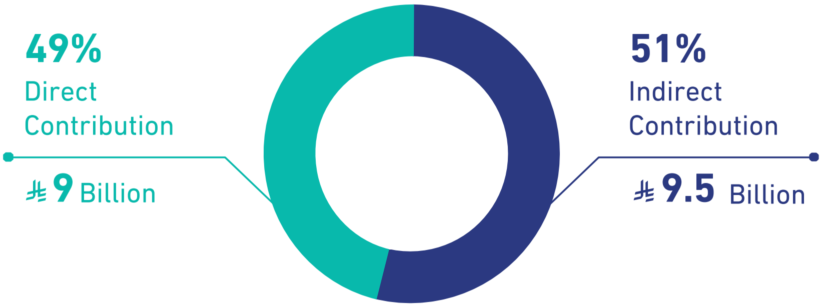
As shown in the table, smaller providers represent (78%) of all providers, demonstrating the Kingdom's vibrant and diverse cybersecurity ecosystem that encourages entrepreneurship, innovation, and broad participation across the sector. While larger providers constitute a smaller portion of the total number of providers, their contribution is pivotal to the sector's advancement, particularly in delivering specialized capabilities and to support national entities. This balanced mix between agile, fast-growing smaller providers and more established larger providers allows for resilience and depth across the cybersecurity landscape.

	(Monsha'at) Classification	Count of Cybersecurity Product and Service Providers	Percentage of Total Cybersecurity Product and Service Providers
Larger CS providers	Large Medium	91	22%
Smaller CS providers	Small Micro	329	78%

2.2. Sector Contribution to GDP

The growth rate of the cybersecurity sector’s contribution to GDP at current prices for 2024 reached (19%) compared to the previous year, with the size of the sector’s contribution estimated at around SAR (18.5) billion. This contribution represents (0.40%) of the Kingdom’s GDP, of which SAR (9.0) billion comes from the direct activities of providers of cybersecurity products and services, and SAR (9.5) billion from indirect activities.

With respect to non-oil activities, the contribution of the cybersecurity sector reached about (0.71%), an increase of (11%) compared with last year, according to the latest figures published by GASTAT.



⃁ 18.5 Billion

0.40%
Sector Contribution to GDP

0.71%
Sector Contribution to Non-Oil Activities

3. Key Cybersecurity Workforce Indicators

3.1. Cybersecurity Workforce Size

The total number of cybersecurity specialists in the Kingdom exceeded (21) thousands specialists during 2024, recording an annual growth of (9%). Approximately (2) thousands specialists work at public-sector entities, while more than (18) thousands specialists work at private-sector establishments, including private entities with critical infrastructure, and cybersecurity product and service providers. This distribution highlights the pivotal role of the private sector in developing national cybersecurity capabilities and expanding their scope.

3.2. Women Participation

At a time when women globally represent only (24%)[1] of the cybersecurity workforce, women participation in the Kingdom's cybersecurity sector reached (32%). This presence reflects the Kingdom's commitment to strengthening inclusivity and expanding the pool of skilled professionals, supported by sustained national efforts to develop the cybersecurity sector.

21.3K

Cybersecurity Specialists

32%

Women Participation

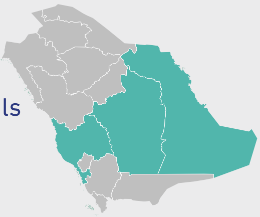
[1] Global average based on: "2024 Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap," Global Cybersecurity Forum & BCG, 2024.

3.3. Geographical Distribution

The geographical distribution of cybersecurity specialists in the Kingdom shows that (92%) are concentrated in the Riyadh, Makkah, and Eastern Regions, reflecting the economic distribution of establishments across the country.

92%

Of cybersecurity professionals are based in Riyadh, Makkah or the Eastern Region.



3.4. Experience Levels

Approximately (57%) of cybersecurity specialists in the Kingdom have fewer than (7) years of professional experience, which reflects the large inflow of promising talent driven by the increase in the number of cybersecurity graduates and the workforce-development initiatives led by NCA with support from cybersecurity-ecosystem partners in educational institutions. In the near term, this composition is expected to change as more specialists gain higher levels of experience through professional development programs and professional certifications, thereby contributing to the sector's continued growth and long-term sustainability.

3.5. Cybersecurity Education

Over the past six years, the number of academic programs and tracks specializing in cybersecurity has tripled, supported by NCA's initiatives and ongoing investments from educational institutions, driven by growing demand for qualified specialists and the attractiveness of cybersecurity as a promising career path. In 2024, the number of graduates from cybersecurity programs and tracks reached more than (5) thousands, more than double the number of graduates in the previous year. This increase reflects the growing ability of educational institutions to produce qualified graduates who are ready to enter the labor market and contribute to the future economic value of the cybersecurity sector.

5K

Number of graduates from cybersecurity programs and tracks in the Kingdom.

Appendix A

The Taxonomy for Cybersecurity Products and Services

Level I

Identifies the different business and delivery models for cybersecurity products and services.

- 1 | Cybersecurity products
- 2 | Cybersecurity professional services
- 3 | Cybersecurity technical implementation services
- 4 | Cybersecurity managed services
- 5 | Cybersecurity training & capability building services

Level II

Divides each business and delivery model identified in Level I into various activities in the cybersecurity market.

1	**Cybersecurity products**
1-1	Endpoint security & management
1-2	Network security
1-3	Data security
1-4	Application security
1-5	Identity security & management
1-6	Governance, risk & compliance
1-7	Physical security
1-8	Cybersecurity operations solutions
1-9	Cloud security
1-10	Critical systems security
2	**Cybersecurity professional services**
2-1	Cybersecurity management consulting
2-2	Cybersecurity compliance assessment
2-3	Cybersecurity risk assessment

2-4	Cybersecurity technical assessment
2-5	Cybersecurity technical consulting
2-6	Cybersecurity incident response & investigation
2-7	Bug Bounty
3	**Cybersecurity technical implementation services**
3-1	Cybersecurity product/solution development
3-2	Cybersecurity system integration
4	**Cybersecurity managed services**
4-1	Managed SOC
4-2	Cybersecurity solutions as a service
4-3	Cybersecurity manpower outsourcing
5	**Cybersecurity training & capability building services**
5-1	Cybersecurity training
5-2	Cybersecurity awareness
5-3	Cybersecurity examination & certification
5-4	Cybersecurity events & competitions

Level III

Details each activity identified in Level II into specific areas of specialization.

1	**Cybersecurity products**	
1-1	**Endpoint security & management**	
Cybersecurity solutions to protect endpoints, covering servers, workstations and mobile devices.		
1-1-1	Browser security solutions	Endpoint security solutions to secure web browsers, hardened local browsers, and browser add-ons.
1-1-2	Endpoint protection solutions	Endpoint security solutions to secure PCs, servers, etc., by detecting and preventing malware, viruses, trojans, ransomware, etc.
1-1-3	Endpoint threat detection and response (EDR) solutions	Endpoint security solutions to do live analysis of threats, containment, investigation, and response.
1-1-4	Mobile device protection solutions	Endpoint security solutions and apps that protect mobile devices and their applications/data.

1-1-5	Mobile device management (MDM) solutions	Endpoint security solutions that manage and enforce policy on corporate and employee-owned (BYOD) mobile devices.
1-1-6	Host based firewall solutions	Endpoint security solutions that create software firewalls to protect endpoints against malicious connections.
1-1-7	Security configuration management solutions	Endpoint security solutions to manage and control configurations across enterprise endpoints.
1-1-8	Asset management solutions	Endpoint security solutions used to manage all assets across an organization, including asset discovery and maintaining an asset configuration management database.
1-1-9	Patch configuration and management solutions	Endpoint security solutions to identify, prioritize, test and, install patches across an organization.
1-2	**Network security**	
Cybersecurity solutions to protect the IT environment starting from the network perimeter to endpoints.		
1-2-1	Intrusion detection/ prevention systems (IDPS)	Network security solutions that inspect network traffic, detects malicious content, sends alert (detection-only) or takes action like blocking (detection and prevention).
1-2-2	Network access control solutions	Network security solutions that allow organizations to control access to corporate networks through authentication, configuration, role-based, and other policies.
1-2-3	Network firewall solutions	Network security solutions that use rules to monitor and block malicious incoming and outgoing network traffic, including next generation firewalls (NGFW), which have more advanced features like deep packet inspection.
1-2-4	Secure web gateway (SWG) solutions	Network security solutions that filter users› web traffic and blocks malicious or unwanted (e.g., against corporate policy) content.
1-2-5	Network APT protection and sandboxing solutions	Network security solutions, either automated or manual, that allows suspicious content to be analyzed in a segregated environment.
1-2-6	Proxy solutions	Network security solutions that act as an intermediary between a user and the Internet, offering efficiency, security, and/or privacy advantages.
1-2-7	Honeynets/honeypots solutions	Network security solutions that is set-up as a decoy to lure attackers away from valuable assets and give security teams opportunity to investigate and remediate attacks.
1-2-8	Unified threat management (UTM) solutions	Network security solutions for small and medium sized organizations that serves multiple functions, e.g., firewall, content filtering, antivirus, etc.
1-2-9	DDoS protection solutions	Network security solutions to detect and protect against dedicated denial of service (DDoS) attacks that attempt to flood a corporate network and limits its availability to legitimate requests.

1-3 Data security

Cybersecurity solutions to provide protection for data covering data at rest and in transit.

1-3-1	Data discovery and classification solutions	Data security solutions that identify sensitive data and apply appropriate classification tags.
1-3-2	Data loss prevention (DLP) solutions	Data security solutions installed on endpoints and networks that prevent the loss or leakage of sensitive data.
1-3-3	Data masking & tokenization solutions	Data security solutions that facilitate protecting sensitive information inside data, either by replacing it with a token (tokenization) or obscuring/ removing (masking) sensitive data.
1-3-4	Endpoint encryption solutions and key management systems (KMS)	Data security solutions that protect data-at-rest, (e.g., files, folders, etc), by using cryptography to prevent unauthorized access; also includes systems that manage (e.g. generate, distribute, destroy, etc.) cryptographic keys.
1-3-5	Network encryption	Data security solutions that protect data-in-transit, and secure protocols like SSL/TLS.
1-3-6	Database/storage security solutions	Data security solutions that protect databases and other storage containers, including monitoring, access control, encryption, auditing, etc.
1-3-7	Secure file transfer solutions	Data security solutions for sharing data in a secure manner.
1-3-8	Secure email gateway (SEG)	Data security solutions that scans for and blocks spam and malicious inbound email (email APT protection and sandboxing).
1-3-9	Privacy enhancing technology (PET) solutions	Data security solutions for managing and protecting personal data throughout its lifecycle, including compliance, consent, control, audit, etc.
1-3-10	Digital rights management (DRM) solutions	Data security solutions use to restrict and manage access to protected content.
1-3-11	Ransomware protection solutions	Data security solutions specifically designed and packaged for preventing, detecting, and responding to ransomware threats.

1-4 Application security

Cybersecurity solutions to provide protection at the application level.

1-4-1	Application security testing (AST) solutions	Application security solutions for analyzing and testing applications for security vulnerabilities, includes static application security testing (SAST), dynamic application security testing (DAST), interactive application security testing (IAST), and run-time application security protection (RASP).
1-4-2	Web application firewall (WAF) solutions	Application security solutions that protect web applications by filtering and monitoring HTTP/S requests for malicious activity.
1-4-3	Application control solutions	Application security solutions to define the list of authorized applications for use in an organization and restrict the execution of unauthorized applications (covers application whitelisting and blacklisting).

1-4-4	Web API security solutions	Application security solutions to protect web application programming interfaces (APIs), in order to security data transfer through APIs and prevent malicious attacks on, or misuse of, web APIs.

1-5 Identity security & management

Cybersecurity solutions to provide identity governance and management of digital identities for applications and solutions within the IT environment.

1-5-1	Password manager solutions	Identity security & management solutions used to securely store and manage users' credentials.
1-5-2	Identity governance solutions	Identity security & management solutions to manage user identities across an organization or ecosystem, including identity federation.
1-5-3	Access management solutions	Identity security & management solutions that provide access control through centralized authentication, single sign on (SSO), remote access, session management, etc.
1-5-4	Privileged access management (PAM) solutions	Identity security & management solutions for securing and managing elevated access to critical assets.
1-5-5	Authentication solutions	Identity security & management solutions that verify an individual's digital identity and provide access to solutions.
1-5-6	Digital certificate management solutions	Identity security & management solutions that stores, signs, and issues digital certificates that certify the identities of trusted parties.
1-5-7	High trust computing solutions	Identity security & management solutions enabling higher levels of trust, e.g. trusted computing (TC), cross-domain security (CDS) and multilevel security solutions.
1-5-8	Multi-factor authentication solutions	Identity security & management solutions that provide additional authentication factors, e.g. tokens, biometrics, etc.

1-6 Governance, risk & compliance

Cybersecurity solutions to provide governance planning, risk management, and compliance management for the IT environment.

1-6-1	Governance, risk, and compliance (GRC) solutions	Governance, risk & compliance solutions to track and manage enterprise cyber risk and compliance programs and responsibilities.
1-6-2	Third party risk management (TPRM) solutions	Governance, risk & compliance solutions that protect against supply chain risks, including vendor risk rating and vendor management security solutions.

1-7 Physical security

Cybersecurity solutions to provide physical access security and environmental security.

1-7-1	Physical access authentication and access management solutions	Physical security solutions such as turnstile, badge readers, and physical locks that restrict access to physical locations.

1-7-2	Physical & environmental monitoring solutions	Physical security solutions used to monitor physical environments, including CCTV, water/smoke/motions sensors, etc.
1-8	**Cybersecurity operations solutions**	
Cybersecurity solutions that are used in order to execute day-to-day cybersecurity activities and tasks.		
1-8-1	Network detection and response (NDR) solutions	Cybersecurity operations solutions to use of security analytics to detect and mitigate known and unknown network threats
1-8-2	Cyber threat hunting solutions	Cybersecurity operations solutions that supports proactively uncovering previously unknown active threats and threat actors.
1-8-3	Digital forensic investigation solutions	Cybersecurity operations solutions for identifying, acquiring, and analyzing electronic evidence and completing computer investigations.
1-8-4	Behavior analysis and anomaly detection solutions	Cybersecurity operations solutions used to detect suspicious actions based on standard behaviors, including fraud detection and prevention.
1-8-5	Vulnerability assessment/scanning solutions	Cybersecurity operations solutions that identify, categorize, and manage vulnerabilities.
1-8-6	Penetration testing solutions	Cybersecurity operations solutions to detect, test, and flag exploitable security posture weaknesses, e.g. privilege escalation.
1-8-7	Incident management and security orchestration, automation and response (SOAR) solutions	Cybersecurity operations solutions that coordinate, automate, and manage security incident response.
1-8-8	Security information and event management (SIEM) solutions	Cybersecurity operations solutions for event collection/aggregation, log management and log correlation.
1-8-9	Threat intelligence solutions	Cybersecurity operations solutions to ingest, analyze, and examine the intentions, objectives, and attack techniques of threat actors, including both machine-readable and human-readable intelligence such as indicators of compromise (IoC).
1-8-10	Cybersecurity training & awareness tools	Cybersecurity operations solutions to upskill users and cyber professionals, e.g., anti-phishing campaigns, cyber-ranges, etc.
1-9	**Cloud security**	
Cybersecurity solutions to provide protection for cloud-based applications.		
1-9-1	Cloud access security broker (CASB) solutions	Cloud security solutions to add security controls to cloud services and ensure users are complying with cloud use policies

1-9-2	Cloud workload security	Cloud security solutions that protect workloads as they move through different cloud environments
1-10	**Critical systems security**	
Cybersecurity solutions to provide protection for critical systems and systems of special nature, such as operational technology (OT).		
1-10-1	Industrial security solutions	Critical systems security solutions to protect industrial control systems (ICS) and operational technology (OT), including HMI, SCADA, and DCS cybersecurity
1-10-2	Embedded & IoT security solutions	Critical systems security solutions that protect non-traditional and single- purpose Internet-connected devices from threats
2	Cybersecurity professional services	
2-1	**Cybersecurity management consulting**	
Cybersecurity professional services that are conducted in order to identify strategic areas of improvement and provide recommendations.		
2-1-1	Cybersecurity strategy & roadmap development	Cybersecurity consulting services to create a cybersecurity strategy (e.g., vision, mission, etc.) and an implementation roadmap.
2-1-2	Cybersecurity policy, process, procedure and framework development	Cybersecurity consulting services to develop cybersecurity policies, processes, procedures and frameworks inline with an organization's cybersecurity strategy and internal/external standards.
2-1-3	Cybersecurity capability model development	Cybersecurity consulting services to develop an organization's cybersecurity capabilities including organization structure, roles & responsibilities, governance, etc.
2-1-4	Cybersecurity certification & accreditation of organizations	Cybersecurity consulting services accredit/certify an organization against an externally recognized accreditation/certification standard and based on a cybersecurity assessment.
2-1-5	Cybersecurity change and project management	Cybersecurity consulting services to provide CS change management and CS project management as part of product/ solution implementation and upgrade/update and as part of cybersecurity transformation.
2-2	**Cybersecurity compliance assessment**	
Cybersecurity professional services to conduct Cybersecurity assessments at the governance level of an organization.		
2-2-1	Cybersecurity policy, process, procedure and framework assessment	Cybersecurity organization assessment services to analyze an organization›s cybersecurity policies, processes, procedures and frameworks and identify gaps and improvements
2-2-2	Cybersecurity capability model assessment	Cybersecurity organization assessment services to evaluate an organization's cybersecurity capabilities including organization structure, roles & responsibilities, governance, etc.

2-2-3	Cybersecurity maturity assessment	Cybersecurity organization assessment services to evaluate a organization’s cybersecurity maturity against a defined standard and using a maturity assessment model, e.g. NCA ECC maturity assessment
2-2-4	Cybersecurity audit/ compliance assessment	Cybersecurity organization assessment services to audit compliance with regulations or other national/international standards
2-3	**Cybersecurity Risk Assessment**	
Professional services in risk assessment conducted to identify cybersecurity risks and determine actions to address threats and security threat factors.		
2-3-1	Cybersecurity Risk Assessment Exercise	Risk assessment services to identify, assess, and prioritize cybersecurity risks in the organization.
2-3-2	Development of a Cybersecurity Risk Register	Risk assessment services to document cybersecurity risks and risk management actions in a risk management repository.
2-4	**Cybersecurity technical assessment**	
Cybersecurity professional services that assess the technical aspects for an environment.		
2-4-1	Vulnerability assessment	Cybersecurity technical services to broadly identify, classify, and prioritize vulnerabilities in specific solution or an organization
2-4-2	Penetration testing	Cybersecurity technical services to deliberately find and demonstrate exploitable vulnerabilities in specific solutions or organizations.
2-4-3	Cybersecurity architecture review	Cybersecurity technical services to assess the completeness and suitability of solutions› or organizations› cybersecurity architecture.
2-4-4	Compromise assessment/ threat hunting services	Cybersecurity technical services to identify undetected threats either proactively (threat hunting) or reactively (compromise assessment) in response to finding indicators of compromise (IoCs).
2-4-5	Red teaming exercise	Cybersecurity technical services where ethical hackers (red team) attack an organization›s systems, while the organization›s defenders (blue team) try to defend the network.
2-4-6	Application security assessment	Cybersecurity technical services to identify flaws and vulnerability in an application, e.g. source code review, application security testing, etc.
2-4-7	Cybersecurity configuration review	Cybersecurity technical services to review the security configuration of devices and identify misconfiguration and opportunities to harden.
2-4-8	Cybersecurity assessment & certification of a solution	Cybersecurity technical services to assess and certify a solution against an externally recognized certification standard.

2-5 Cybersecurity technical consulting

Cybersecurity professional services that are conducted to provide technical recommendations and technical consulting activities.

2-5-1	Cybersecurity architecture design	Cybersecurity technical services to design the security architecture of the organization using best practices and secure design principles.
2-5-2	Cybersecurity technical standards development	Cybersecurity technical services to develop and make actionable industry- standard and custom cybersecurity standards, including development of minimum baseline security standards (MBSS).
2-5-3	Cybersecurity technical plan development	Cybersecurity technical services to develop plans and detailed processes, e.g. disaster recovery and business continuity plan, vulnerability/risk mitigation plan, incident response plan, etc.
2-5-4	Cybersecurity threat intelligence services	Cybersecurity technical services to provide information and reports to ingest, analyze, and examine the intentions, objectives, and attack techniques of threat actors and threat vectors (including dark web, brand, and cyber threat monitoring).

2-6 Cybersecurity incident response & investigation

Cybersecurity professional services to analyze and/or handle cybersecurity incidents and breaches.

2-6-1	Cybersecurity incident response	Cybersecurity incident response services to help organizations manage, analyze, contain, remediate, and learn from cybersecurity incidents.
2-6-2	Cybersecurity forensics investigation	Cybersecurity incident investigation services to preserve evidence and analyze threat actor and threat vector techniques (e.g. malware analysis).

2-7 Bug bounty

Cybersecurity services provided for bug bounty programs.

2-7-1	Bug bounty program services	Cybersecurity technical services to run a program that incentivizes crowd sourced ethical hackers to conduct independent assessments and responsible disclosures.

3 Cybersecurity technical implementation services

3-1 Cybersecurity product development

Cybersecurity services to develop cybersecurity products.

3-1-1	Cybersecurity product development	Cybersecurity technical services to develop custom cybersecurity products for technology vendors (e.g. white labeled products), governments, and other advanced users.

3-2 Cybersecurity system integration

Cybersecurity services that are offered by cybersecurity vendors, IT vendors and system integrators in order to implement and/or configure a cybersecurity solution.

3-2-1	Cybersecurity implementation requirements	Cybersecurity technical services to define cybersecurity requirements for new CS products and for CS product/solution implementation.
3-2-2	Cybersecurity solution design and architecture	Cybersecurity technical services to design the cybersecurity architecture of a solution before the solution implementation using best practices and secure design principles (covering high-level and low-level design).
3-2-3	Cybersecurity implementation, solutions configuration and integration	Cybersecurity technical services to implement, configure, and integrate cybersecurity solutions into an organization's environment. In addition, this service includes maintenance and support contracts for a product/solution.
4	**Cybersecurity managed services**	
4-1	**Managed SOC**	
Cybersecurity monitoring, threat identification, and incident escalation.		
4-1-1	Cybersecurity monitoring	Managed SOC services that focus on the remote cybersecurity monitoring of alerts from cybersecurity solutions
4-1-2	Managed detection and response (MDR) services	Managed SOC services that to detect, triage, and investigate cybersecurity incidents as they occur, as well as respond and mitigate simple incidents
4-2	**Cybersecurity solutions as a service**	
Cybersecurity services related to outsourcing of cybersecurity solutions to an organization, including solution management and operations.		
4-2-1	Cybersecurity solutions as a service	Cybersecurity outsourcing services that provide day-to-day operational control and execution of cybersecurity solutions covering solution administration and operations, excluding managed SOC, and incident response.
4-3	**Cybersecurity manpower outsourcing**	
Cybersecurity services related to outsourcing of cybersecurity manpower to an organization.		
4-3-1	Cybersecurity manpower outsourcing	Cybersecurity outsourcing services that provide contractors (i.e., body leasing) to fill staffing gaps in a cybersecurity organization, excluding incident response activities.
5	**Cybersecurity training & capability building services**	
5-1	**Cybersecurity training**	
Delivery of cybersecurity training courses and workshops for cybersecurity and non-cybersecurity employees.		
5-1-1	Cybersecurity academic training	Cybersecurity training services focused on cybersecurity concepts, theory, and management.
5-1-2	Cybersecurity technical training	Cybersecurity training services focused on cybersecurity hand-on experience with tools and applied techniques.

5-1-3	Cybersecurity simulations and drills	Cybersecurity training services focused on practicing approaches to detecting, responding, and recovering from cyber incidents.
5-2	**Cybersecurity awareness**	
Delivery of cybersecurity training courses and workshops for cybersecurity and non-cybersecurity employees.		
5-2-1	Cybersecurity awareness content development	Cybersecurity awareness services focused on creating customized con- tent to improve employee/customer/etc. cybersecurity consciousness and understanding.
5-2-2	Cybersecurity awareness sessions/ workshops	Cybersecurity awareness services focused on delivering live/ remote cyber- security awareness sessions for employees/ customers/etc.
5-3	**Cybersecurity examination & certification**	
Delivery of cybersecurity exams and certificates to individuals.		
5-3-1	Cybersecurity examination for individuals	Cybersecurity examination services to test the knowledge, skills, and competency of cybersecurity students and professionals.
5-3-2	Cybersecurity certification for individuals	Cybersecurity certification services to verify training/experience and accredit/certify induvial with recognized cybersecurity certifications (includes certification by equivalency).
5-4	**Cybersecurity events & competitions**	
Delivery of cybersecurity exams and certificates to individuals.		
5-4-1	Cybersecurity events	Cybersecurity services to plan, organize and conduct cybersecurity events, conferences and forums.
5-4-2	Cybersecurity competitions	Cybersecurity services to plan, organize and conduct cybersecurity competitions such as hackathons and capture the flag (CTF).

Disclaimer

The National Cybersecurity Authority (NCA), Boston Consulting Group (BCG) and International Data Corporation (IDC), have developed this report, and the information included in it is general and for guidance purposes only. NCA, BCG, and IDC do not provide any explicit or implicit warranties or commitments of any kind related to the report, which contents can change without prior notice.

Ownership Rights

الهيئة الوطنية
للأمن السيبراني

National Cybersecurity Authority

الهيئـــة الوطنيـــة
للأمـــن السيبـــراني
National Cybersecurity Authority