الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

REPORT ON KEY ECONOMIC INDICATORS IN THE CYBERSECURITY SECTOR

2024

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 four 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

Contents

Executive Summary

Under the Royal Decree No. 6801, dated 11/2/1439H, the National Cybersecurity Authority (NCA) has become the sole authority in the Kingdom of Saudi Arabia for cybersecurity, and the National Reference in its affairs. The NCA aims at strengthening cybersecurity to safeguard the State's vital interests, national security, critical infrastructures, priority sectors, and government services and activities. The 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, as well as technology transfer and development in cybersecurity and related fields.

From this national perspective towards enhancing understanding of the cybersecurity sector from the economic perspective, this report has been developed into two key sections: (1) Methodology, in which the cybersecurity market is divided into products, solutions and services. The target categories were identified, the data collection method and analysis were determined, and output accuracy verification and validation were also set; (2) Key Economic Indicators in the Cybersecurity Sector, including market size, spending by entity size, geographic distribution of the supply and demand, categorization of cybersecurity product, solution and service providers, and contribution of the cybersecurity sector to the Kingdom's Gross Domestic Product (GDP).

Introduction

The cybersecurity sector in the Kingdom has seen significant growth and development since its inception. This development encompasses both economic and security aspects, with a focus on both domestic and international dimensions. The Saudi model has become a pioneer in the field, attracting international emulation.

The Saudi cybersecurity model is uniquely comprehensive in addressing cybersecurity across various sectors, whether legislative, security, or economic development. The Saudi model of cybersecurity is based on decentralization of national entities' on-premises operations under the responsibility of national entities, and centralization of cybersecurity governance at the national level through centralization of organization, centralization of cyber operations, and specifically centralization of cybersecurity assessment work, cyber incident response work, capacity building, and competencies at the national level. The Saudi cybersecurity model contributes to enhancing understanding of the entire national cybersecurity scene in such a manner that maximizes the Kingdom's gains and international standing, and at the same time enables national entities to carry out their roles and responsibilities and raise their operational readiness.

Building on these achievements, a research study was conducted to highlight key economic indicators related to the cybersecurity sector in Saudi Arabia for the years 2023 and 2024. The research study adopted the best practices used globally, contributing to the development of the cybersecurity sector in the Kingdom and empowering entrepreneurs and investors. This report presents the key findings revealed by the research study.

Foreword by Report Development Partners

In light of the continued development across the cybersecurity sector in the Kingdom, it has become crucial to understand the current cybersecurity market and its future prospects in detail. This involves examining and analyzing the market size and the products, solutions, and services provided by the government entities, private sector entities owning, operating or hosting Critical National Infrastructures, and the remaining of the private sector entities. This study aims to give a detailed view of the forces influencing the cybersecurity market in the Kingdom, including supply and demand trends. Additionally, the study provides a detailed analysis of the current cybersecurity workforce in the Kingdom, which is an integral component for the growth of the cybersecurity sector. This includes the development of strategies to enhance cybersecurity protections.

Through the joint collaboration between the Boston Consulting Group (BCG), the International Data Corporation (IDC), and The National Cybersecurity Authority (NCA), a comprehensive research study was developed to provide a global perspective on the cybersecurity market. This collaboration brought together the in-depth subject-matter expertise of international specialists in cybersecurity, with a deep understanding of the local cybersecurity sector in the Kingdom. The study utilizes advanced analytical models to extract insights, offering a detailed and integrated view of the cybersecurity market in the Kingdom. This approach ensures the inclusion of all relevant economic indicators and classification of cybersecurity products, solutions, and services within the sector, providing a thorough and precise understanding of the cybersecurity market.

This research study stands out in its comprehensive approach to data collection and analysis, covering a two-year span across 2023 and 2024. It involved gathering data from various sources that represent all components of the cybersecurity sector, significantly enhancing the accuracy and reliability of the findings. The research study adheres to best global practices in data analysis, ensuring that the findings are statistically robust and reliable, achieving 98% statistical confidence and a margin of error of only 4%, ensuring high-quality study outputs.

This study was enhanced through extensive collaboration with relevant stakeholders, which included discussions with experts in the field, inputs from the government entities, private sector entities owning, operating or hosting Critical National Infrastructures, and the remaining of the private sector entities. Furthermore, inputs from cybersecurity vendors, as well as educational institutions in the Kingdom, were included. These diverse sources have significantly contributed to the comprehensiveness and accuracy of the study, ensuring that the findings are statistically sound, robust, and relevant to the Kingdom's context.

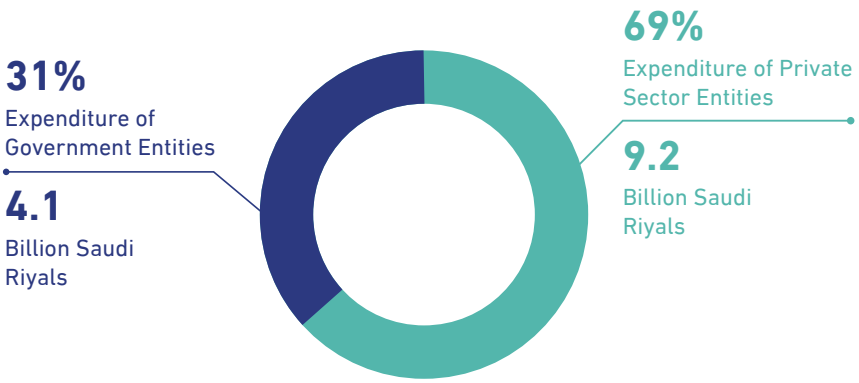
The study's findings focus on various strategic aspects of the cybersecurity market in the Kingdom, serving as a strategic tool for decision-makers and local cybersecurity entities. The research study provides a comprehensive understanding of the cybersecurity sector in the Kingdom, highlighting the current trends and future directions, ensuring informed decision-making and strategic planning for future developments in the sector.

Report Development Partners:

Key Findings

Cybersecurity Market Size in the Kingdom

13.3
Billion Saudi Riyals



Contribution to Gross Domestic Product (GDP) at Current Prices

15.6
Billion Saudi Riyals

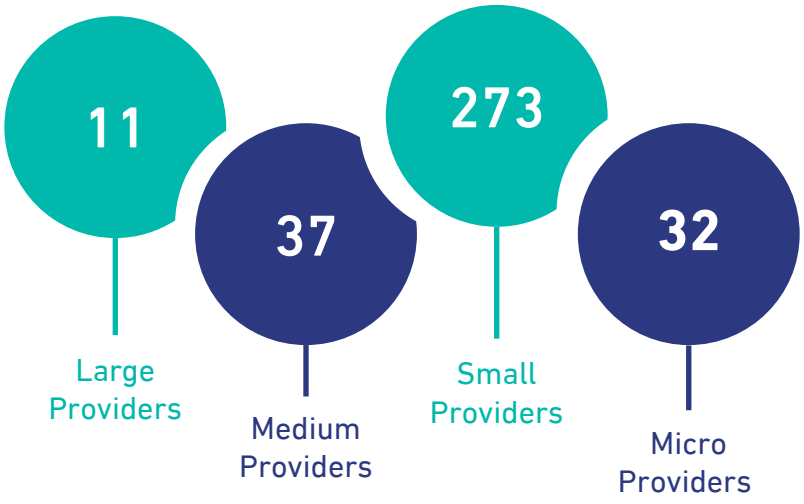
0.39%
Sector's Contribution to Overall GDP

0.81%
Sector's Contribution to Non-Oil GDP

Number of Registered Cybersecurity Product, Solution, and Service Providers with the NCA

353

Cybersecurity Product, Solution, and Service Providers



Cybersecurity Key Products, Solutions, and Services in the Kingdom

Network Security

Cybersecurity System Integration

Endpoint Security and Management

Managed Security Operations Center

Cloud Security

Cybersecurity Workforce in the Kingdom

19.6

Thousand Cybersecurity Specialists

32%

Women's Participation

1 Methodology

1.1 Classification of Products, Solutions, and Services in the Cybersecurity Sector

The work on this step was carried out in cooperation with several leading thinks tanks and firms to establish a comprehensive classification of cybersecurity products, solutions, and services (Appendix 1). Various global companies and providers of cybersecurity products, solutions, and services were evaluated to cover the details of the cybersecurity sector comprehensively. The classification of cybersecurity products and services included more than 100 categories, organized into three levels:

Level 1

This level provides the basic classification for cybersecurity sector activities as products, solutions, or services based on the models presented.

Level 2

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

Level 3

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

1.2 Data Collection

This step involved identifying the target categories, the data to be collected, and the mechanism for collecting data and creating a representative sample for each category. The data collection mechanism included surveys, workgroups, and personal interviews with cybersecurity experts to gather their insights. The demand side in the market was also identified, including the government entities, private sector entities owning, operating or hosting Critical National Infrastructures, and the remaining of the private sector entities with diverse activities and sizes. The supply side was identified through the registration of cybersecurity products, solutions, and service providers with the NCA, thereby defining the data collection level in the Kingdom.

The statistical confidence in the research study's results is 98%, with a margin of error of 4%. Data collection for the research study was conducted in the first quarter of 2023 and 2024.

1.3 Quality Assurance

This step included verification of accuracy and validity of the data across different stages of the study. It aimed to ensure the precision and pinpoint accuracy of statistics and findings according to the best standards observed in similar studies, proposed by various international organizations such as the United Nations. The process included applying various technical standards to filter out data that fell outside the research study's scope or was deemed inaccurate.

98%

Statistical Confidence Level
of the research study's results

1.4 Data Analysis

Statistical and economic models were developed to extract specific indicators related to the cybersecurity sector in the Kingdom. Based on these statistical models, the revenues of cybersecurity products, solutions, and services providers in the Kingdom were analyzed, and the expenditure of the government entities, private sector entities owning, operating or hosting Critical National Infrastructures, and the remaining of the private sector entities. The economic model was used to estimate the total contribution of the sector to the GDP.

Our modeling leveraged inputs from both local and international professionals, as well as subject matter experts. In addition, the models were validated using contextual evidence derived from international benchmarking and government databases. These data sources included datasets from the Ministry of Human Resources and Social Development, the General Authority for Statistics, and the Zakat, Tax, and Customs Authority.

The contribution of the cybersecurity sector to the GDP was estimated in alignment with the methodology used by the General Authority for Statistics. The study included estimating the revenues of cybersecurity products, solutions, and service providers in the Kingdom based on the data and results from the research study, the taxes and support provided to companies, and the economic input-output tables were utilized to gauge both the direct and indirect financial impacts of the cybersecurity market in the Kingdom.

1.5 Outputs Development

Based on the results of the statistical and economic models, valuable insights were drawn to describe the cybersecurity market in the Kingdom and its economic contribution.

Demand Side

Market Size

Supply Side

Contribution to GDP

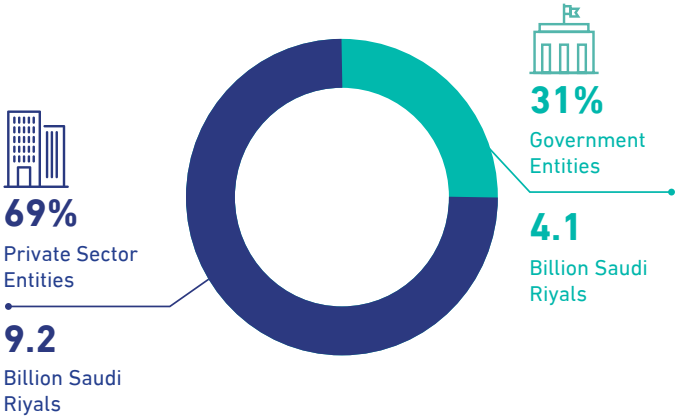
2 Key Economic Indicators in the Cybersecurity Sector

2.1 Cybersecurity Market

2.1.1 Market Size

The total expenditure by entities operating in the Kingdom on cybersecurity products, solutions, and services account for 13.3 Billion Saudi Riyals. This expenditure is divided between the public and private sectors, with the total expenditure by the government entities reaching at 4.1 Billion Saudi Riyals, accounting for 31% of the market size. Meanwhile, the private sector entities have spent approximately 9.3 Billion Saudi Riyals, accounting for 69% of the market size, including 2.8 Billion Saudi Riyals spent by private sector entities owning, operating or hosting Critical National Infrastructures.

13.3
Billion Saudi Riyals



2.1.2 Expenditure by Entity Size in the Kingdom

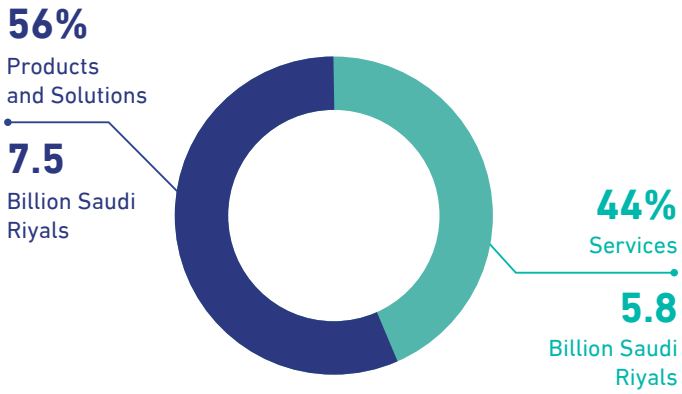
When examining the expenditure by the entities in the Kingdom on cybersecurity products, solutions, and services, it becomes clear that most of the expenditure by the government entities and private sector entities owning, operating or hosting Critical National Infrastructures is made by large and very large entities. This is due to these entities overseeing other dependent entities.

In contrast, the remaining of the private sector entities, medium-sized enterprises represent the largest number of entities requiring cybersecurity products, solutions, and services. These medium-sized entities are the most substantial spenders within the private sector on cybersecurity products, solutions, and services.

		Very Large	Large	Medium	Small	Micro
Government Entities	**4.1 Billion Saudi Riyals**	**38%**	**50%**	**11%**	**1%**	**-**
Private sector entities owning, operating or hosting Critical National Infrastructures	**2.8 Billion Saudi Riyals**	**33%**	**62%**	**4%**	**1%**	**-**
The remaining of the private sector entities	**6.4 Billion Saudi Riyals**	**14%**	**26%**	**41%**	**16%**	**3%**

2.1.3 Market Size by Classification of Cybersecurity Products, Solutions, and Services

The cybersecurity market in the Kingdom is divided according to the classification into cybersecurity products, solutions, and services. The cybersecurity products and solutions contributed to 56% of the market size at 7.5 Billion Saudi Riyals. While the market size share of cybersecurity services accounts for 44%, valued at 5.8 Billion Saudi Riyals.



Key Cybersecurity Products, Solutions, and Services

- Endpoint Security and Management
- Cybersecurity System Integration
- Network Security
- Cloud Security
- Managed Security Operations Center

2.1.4 Geographic Distribution on the Demand Side

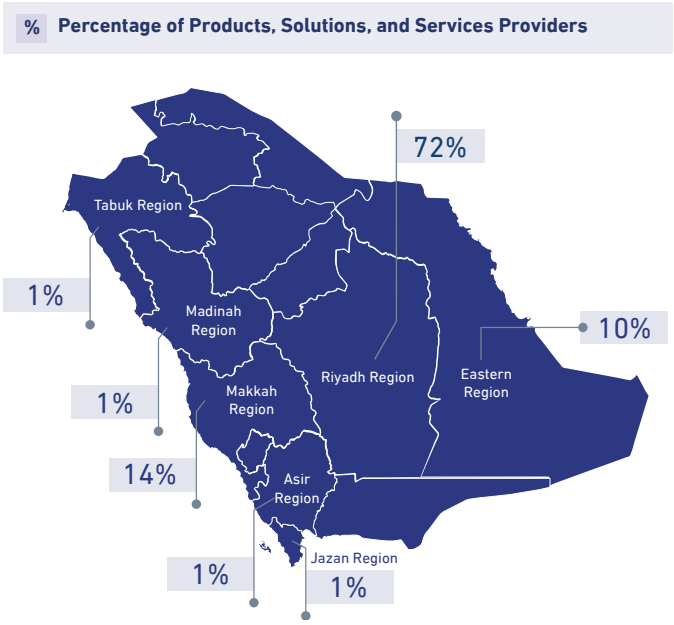
The geographic distribution is based on the administrative regions of the main entities operating in the Kingdom on the demand side. Of note, 83% of these entities are concentrated in Riyadh, Makkah, and the Eastern Region, as reported by the General Authority for Statistics in accordance with the reports issued by the Small and Medium Enterprises General Authority.

83%

of entities are concentrated in Riyadh, Makkah and the Eastern Region

2.1.5 Geographic Distribution on the Supply Side

The geographic distribution of cybersecurity products, solutions and services providers relies on the regions of their main administrative headquarters in the Kingdom. Riyadh takes the lead at 72% of the providers, followed by Makkah at 14%, and the Eastern Region at 10%. This distribution aligns with the regions of highest economic concentration in the Kingdom, while 4% of the providers of cybersecurity products, solutions, and services are spread across the remaining administrative regions.



2.1.6 Classification of Cybersecurity Product, Solution, and Service Providers

The classification of the size of entities that provide cybersecurity products, solutions and services in the Kingdom is based on the definition of the Small and Medium Enterprises General Authority. Given the similar characteristics between enterprises categories in the Kingdom and for the purpose of drawing clearer conclusions from this study, the medium and large cybersecurity product, solution, and service providers have been grouped into one category (large category) and the small and micro cybersecurity product, solution, and service providers into another category (small category).

Classification by the Small and Medium Enterprises General Authority	Number of Cybersecurity Product, Solution, and Service Providers	Percentage of Total
Large	11	3%
Medium	37	11%
Small	273	77%
Micro	32	9%
Total	**353**	**100%**

2.2 Contribution of the Cybersecurity Sector to GDP

Based on the findings of the cybersecurity market study in the Kingdom and the numbers provided by the General Authority for Statistics for the year 2023, the contribution of the cybersecurity sector to the GDP at current prices is estimated to be around 15.6 Billion Saudi Riyals. Of which, 8.6 Billion Saudi Riyals represent direct contribution, and 7 Billion Saudi Riyals represent indirect and induced contribution.

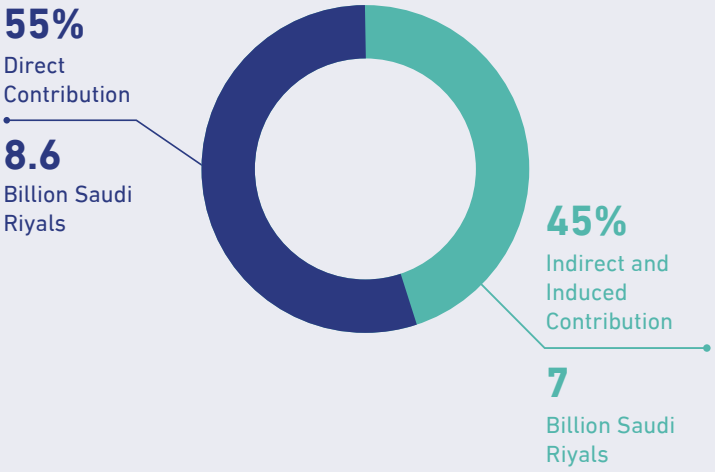
The contribution of the cybersecurity sector in the Kingdom represents 0.39% of the total GDP and 0.81% of the non-oil GDP.

Size of Contribution to GDP at Current Prices

15.6
Billion Saudi Riyals

0.39%
Sector's Contribution to Total GDP

0.81%
Sector's Contribution to Non-Oil GDP



Appendix A

The Taxonomy for Cybersecurity Solutions, Products and Services

Level I

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

1	2	3	4	5
Cybersecurity products/ solutions	Cybersecurity professional services	Cybersecurity technical implementation services	Cybersecurity managed services	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/solutions
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
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/solutions**	
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 authenti- cation 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	Bug bounty program services	Cybersecurity technical services to run a program that incentivizes crowd- sourced ethical hackers to conduct independent assessments and responsible disclosures.
2-4-8	Cybersecurity configuration review	Cybersecurity technical services to review the security configuration of devices and identify misconfiguration and opportunities to harden.
2-4-9	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 icident 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).
3	**Cybersecurity technical implementation services**	
3-1	**Cybersecurity product/solution development**	
Cybersecurity services to develop cybersecurity products and solutions.		
3-1-1	Cybersecurity product/ solution development	Cybersecurity technical services to develop custom cybersecurity solutions and 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/solutions 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.

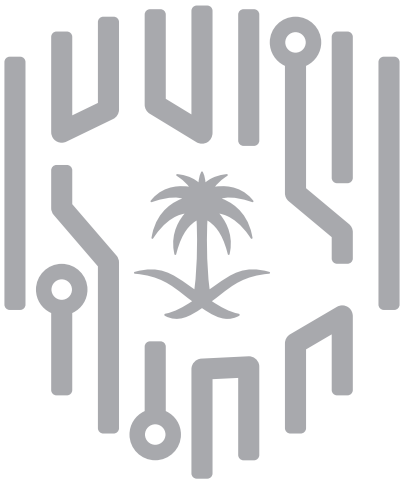
4-3	**Cybersecurity manpower outsourcing**	
Cybersecurity services related to outsourcing of cybersecurity manpower to an organization.		
4-3-1	Cybersecurity manpower outsourcing	Cybersecurity outsourcing services that provide contractors (i.e., body leasing) to fill staffing gaps in a cybersecurity 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 awareness sessions and workshops for cybersecurity and non- cybersecurity employees.		
5-2-1	Cybersecurity awareness content development	Cybersecurity awareness services focused on creating customized content 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 events and competitions for organizations.		
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 hackthons and capture the flag (CTF).

Disclaimer

The National Cybersecurity Authority (NCA), Boston Consulting Group (BCG) and International Data Corporation (IDC), have developed a specialized methodology to analyze and study the cybersecurity market in the Kingdom. This report is prepared based on this mentioned methodology, and the information included in it is general and for guidance purposes only. NCA, BCG and IDC, ensure the accuracy and correctness of the report's content. However, they do not provide any explicit or implicit warranties or commitments of any kind regarding the completeness, accuracy, or credibility of the report's content, whether it was in text form, analysis, charts, or any other format.

They are not responsible for any errors or omissions in the report's content. Moreover, they are not liable for any consequences related to its content, which is subject to change at any time without prior notice.

Ownership Rights



الهيئة الوطنية
للأمن السيبراني

National Cybersecurity Authority


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority