Merak.Capital

Unlocking Saudi Arabia's Cybersecurity Potential

An Industry Report

A Letter From Our CEO

Saudi Arabia is advancing rapidly toward a sophisticated digital future, in which cybersecurity has emerged as a key enabler of national resilience and economic growth. As digital infrastructure expands, reliance on cloud technologies increases, and the use of artificial intelligence grows across sectors, the Kingdom's digital ecosystem continues to strengthen. This expansion, however, has been accompanied by a rise in the scale and complexity of cyber risks. Cybersecurity is no longer merely an operational requirement, but a strategic necessity and an integral component of national security.

The market reflects this shift, Saudi Arabia's cybersecurity sector has grown at approximately 14%, reaching SAR 15.2 billion in 2024. Behind this headline figure lies a more fundamental transition, cybersecurity has moved from an IT budget line to a boardroom priority across the government and private sector. Organizations are no longer asking whether to invest in security, but how to build capabilities that match the sophistication of emerging threats.

This transition is being driven by regulation as much as by threat exposure. The National Cybersecurity Authority and sector-specific regulators have progressively expanded compliance requirements, creating sustained demand for providers with the technical depth and operational scale to serve critical infrastructure. This combination of regulatory tailwinds, rising threat complexity, and digital acceleration across critical sectors creates a compelling environment for cybersecurity providers and the broader ecosystem supporting them.

This report offers our perspective on the forces shaping Saudi Arabia's cybersecurity future. We hope it provides clarity on the broader trends and supports leaders in making informed decisions as the Kingdom continues its transformation toward a secure and resilient digital economy.

Abdullah Altamami
Founder & CEO, Merak Capital

About Merak Capital

Merak Capital is a Saudi-based multi-strategy investment firm focused on opportunities across multiple stages and industries. Licensed by the Capital Market Authority, the firm manages over SAR 3 billion across 10 funds spanning venture capital, private equity, credit financing, and special projects. Merak is built on deep technological insight and market research, staying at the forefront of digital trends and identifying investments aligned with adoption cycles across sectors locally, regionally, and globally.

The firm partners with visionary founders and enterprises driving transformation, unlocking new markets, and enabling sustainable growth. Merak takes an active approach to value creation, supporting portfolio companies through governance enhancement, operational development, and strategic growth initiatives as they scale toward market leadership.

2017	10+	﷼3B+
INCEPTION	FUNDS	AUM

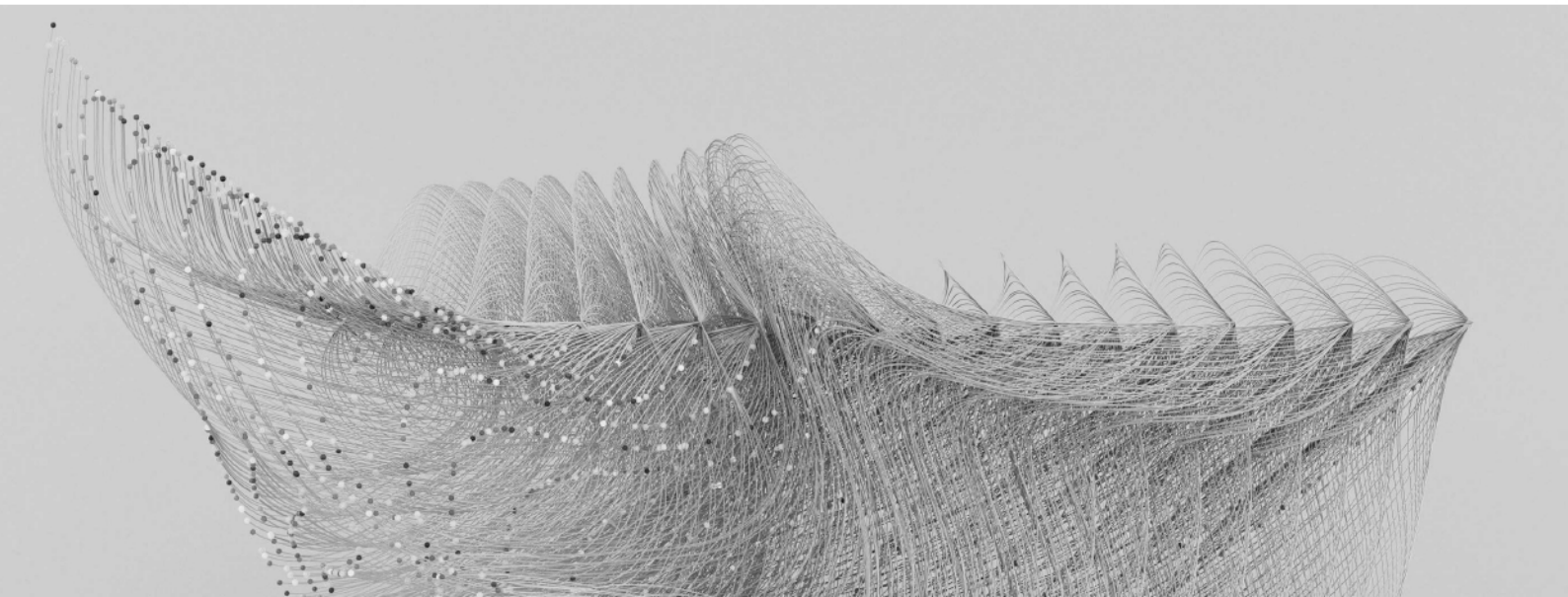
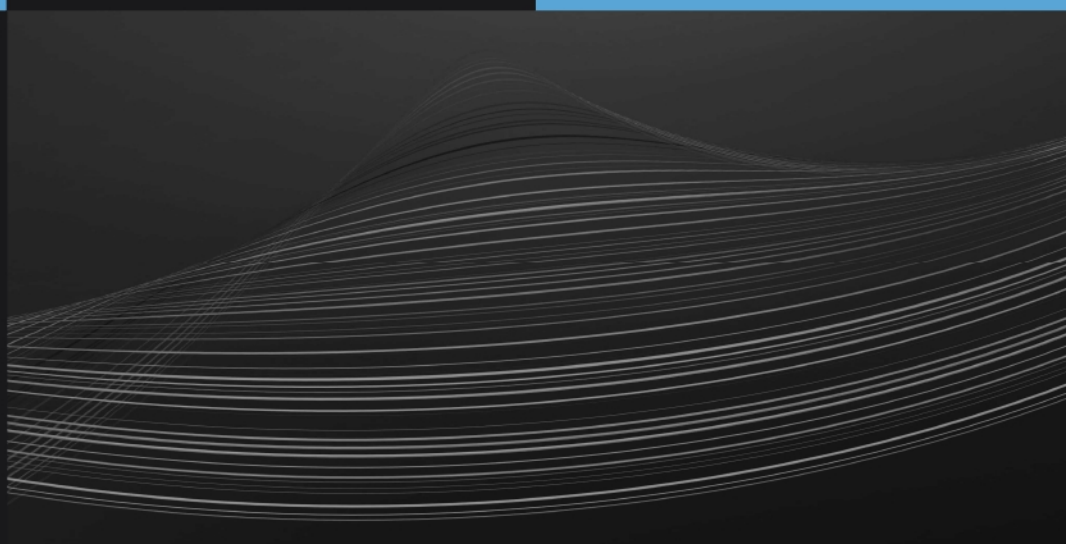
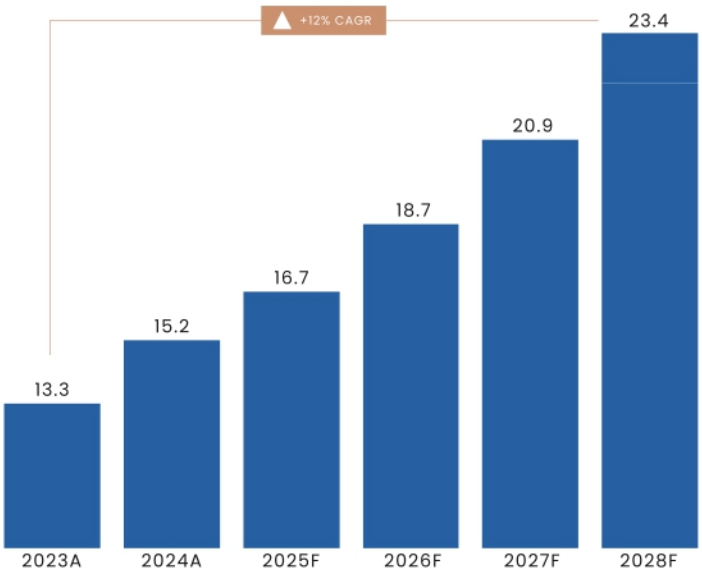


Table Of Contents



Saudi Cybersecurity Market

Market Size and Growth Potential in Cybersecurity Solutions (﷼ Billion)

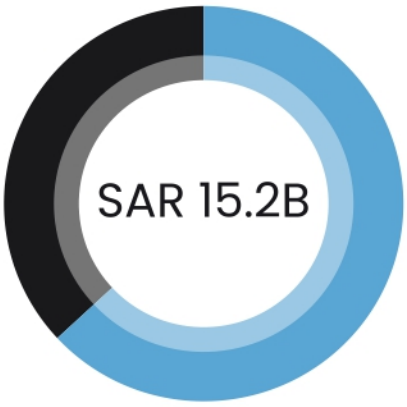


Growth drivers

- REGULATORY-DRIVEN MARKET EXPANSION
- SPENDING BY GOVERNMENT AND CRITICAL SECTORS
- CYBERSECURITY AS A NATIONAL SECURITY PRIORITY
- GROWING PRIVATE SECTOR DEMAND
- AI-DRIVEN SECURITY INNOVATION
- ADVANCED TECHNOLOGIES DRIVING SECURITY INNOVATION

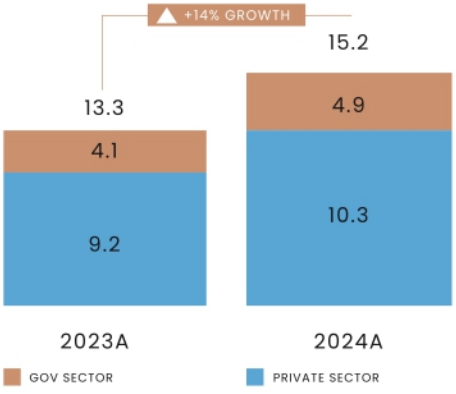
Cybersecurity Market Size in the Kingdom (2024)

32%
EXPENDITURE OF GOVERNMENT ENTITIES

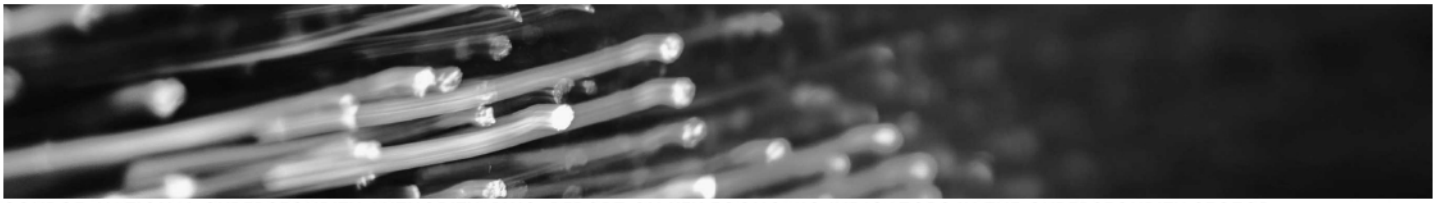


68%
EXPENDITURE OF PRIVATE SECTOR ENTITITES

Market Growth (﷼ Billion)



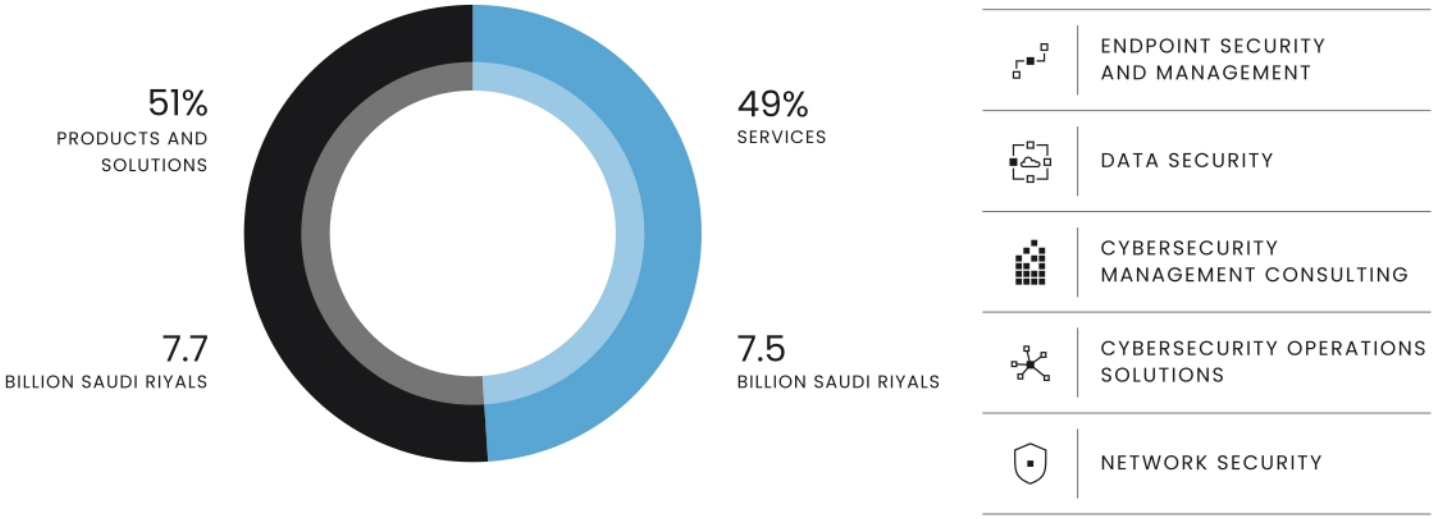
According to the National Cybersecurity Authority, the Saudi cybersecurity market reached SAR 15.2 billion in 2024, up from SAR 13.3 billion in 2023, representing approximately 14% year-on-year growth. Private sector entities account for 68% of cybersecurity spending, with government entities contributing 32%. This broad-based expansion underscores the sector's critical role in national digital resilience.



SOURCE: NATIONAL CYBERSECURITY AUTHORITY, PWC, REPORT ON KEY ECONOMIC INDICATORS IN THE CYBERSECURITY SECTOR,

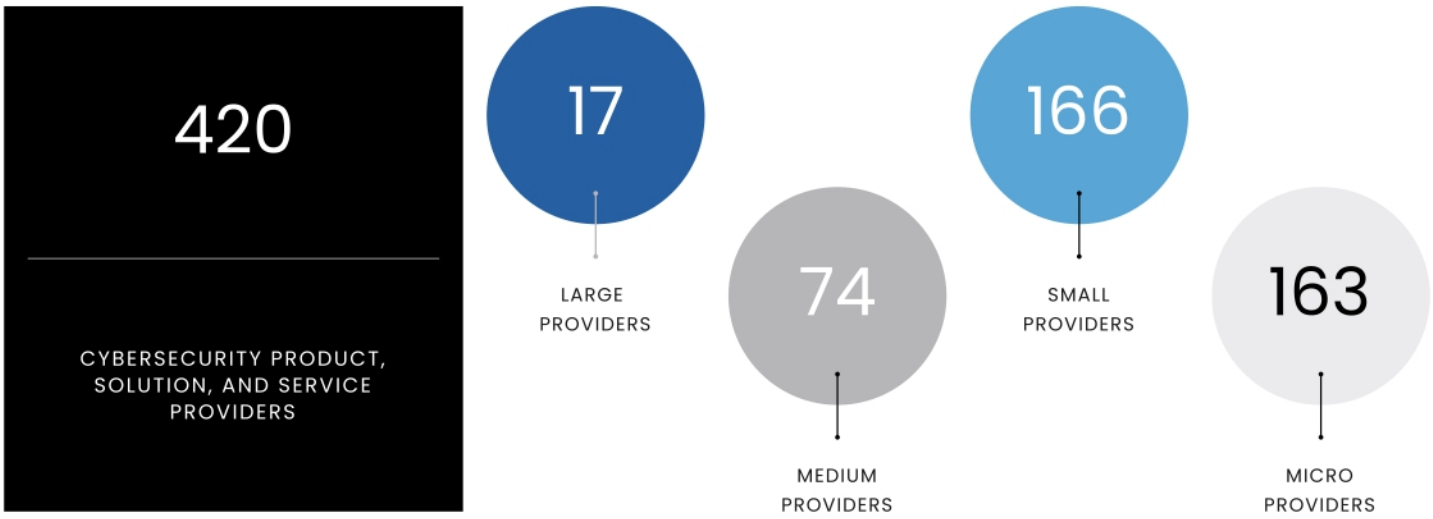
Supply Side Overview

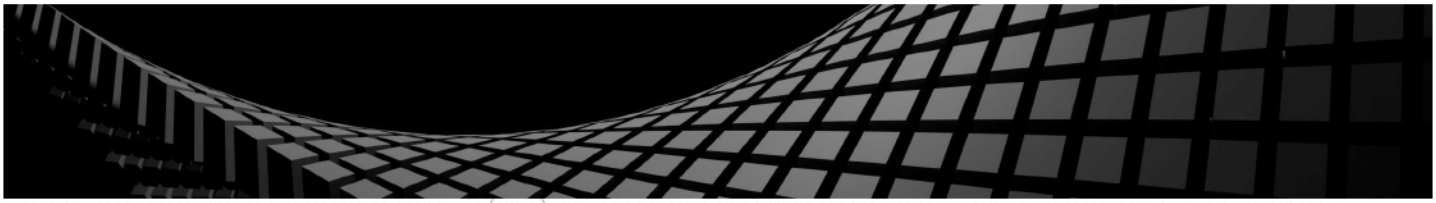
Key Cybersecurity Products, Solutions, and Services (2024)



The market is evenly split between products (51%) and services (49%). While 420 providers are registered with the National Cybersecurity Authority, the market remains fragmented. Small and micro providers represent 78% of the total, though large and medium providers capture the majority of revenue.

Number of Registered Cybersecurity Product, Solution, and Service Providers





SOURCE: NATIONAL CYBERSECURITY AUTHORITY (NCA). PROVIDER SIZE CLASSIFICATION ALIGNED WITH MONSHA'AT SME DEFINITIONS.

Rising Cyberthreats Fuel Security Demand

Cyber risk exposure creates opportunities for growth

RISING CYBERCRIME AND DIGITAL DISRUPTION

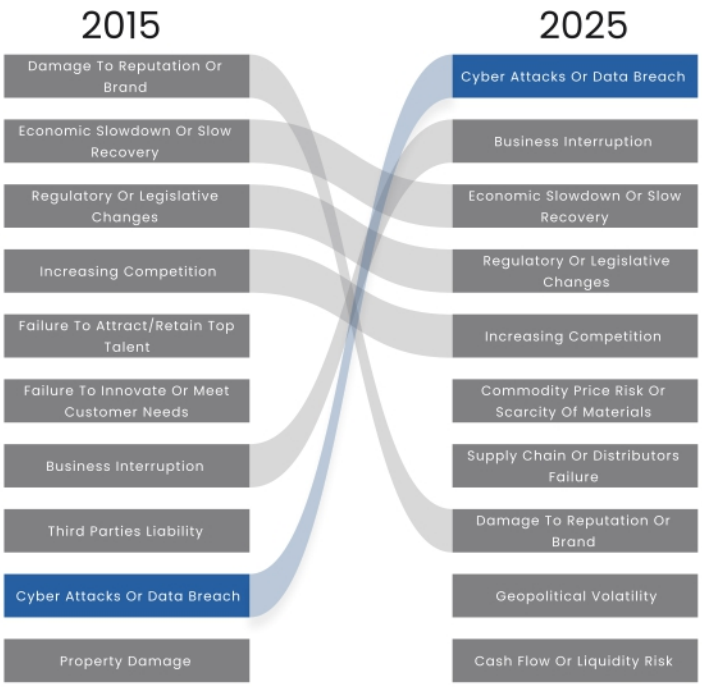
THE INCREASING SOPHISTICATION OF PHISHING METHODS POWERED BY GEN AI

UNSTRUCTURED AND NON-MONITORED USE OF GEN AI ACROSS ORGANIZATIONS

CYBERATTACKS ON NATIONAL SECURITY

FUELING DEMAND FOR ADVANCED SECURITY SOLUTIONS

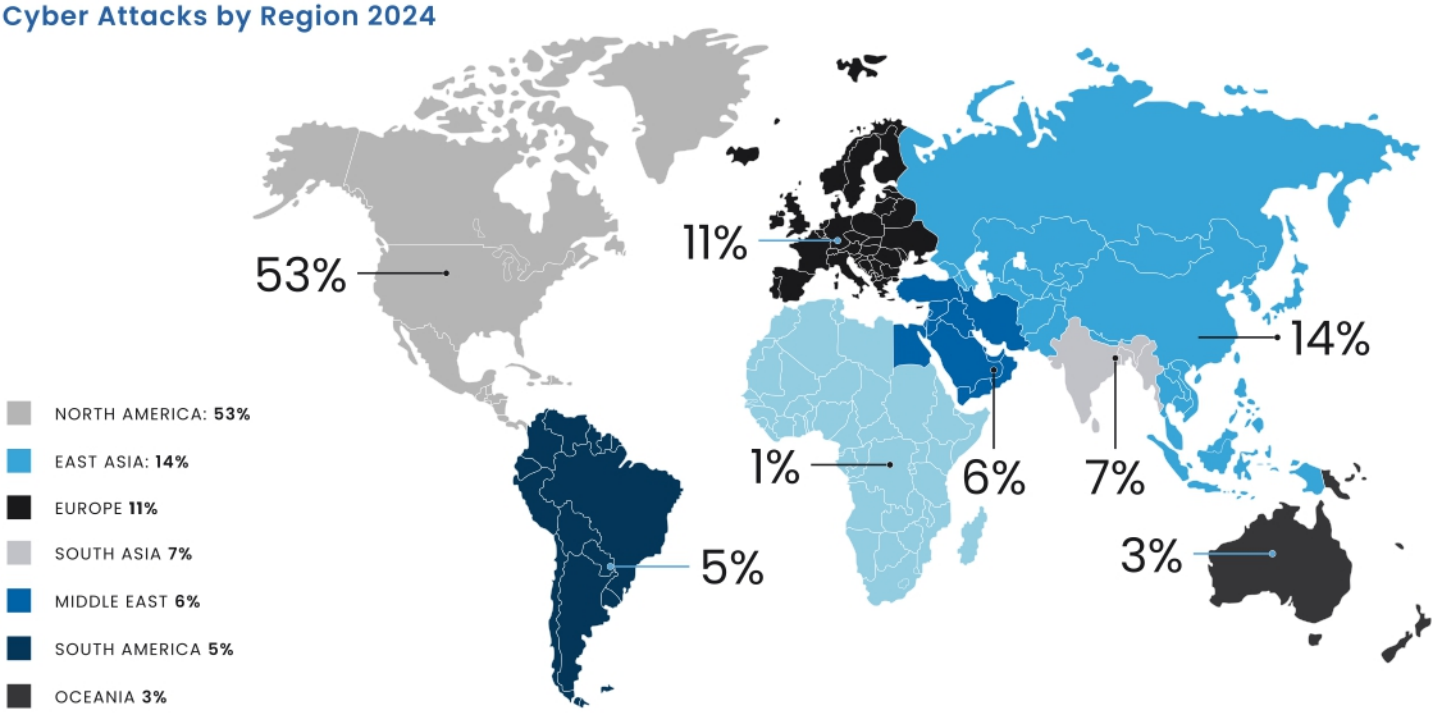
Top Threats Facing Organization



Top 10 Industries Targeted by Cyber Attacks

- TECHNOLOGY: **23%**
- CONSULTING AND PROFESSIONAL SERVICES: **15%**
- MANUFACTURING **12%**
- RETAIL **11%**
- FINANCIAL SERVICES: **10%**
- HEALTHCARE: **9%**
- TELECOMMUNICATIONS: **7%**
- GOVERNMENT **6%**
- INDUSTRIALS AND ENGINEERING: **4%**
- ACADEMIC: **3%**

Cyber Attacks by Region 2024



SOURCE: CROWDSTRIKE, IDC, MORDOR COUNTRY INDUSTRY REPORT, AON'S GLOBAL RISK FACTORS SURVEY

Market Drivers

CYBERCRIME SURGE
Rising cybercrime, digital disruption, and increased compliance demands

CLOUD ADOPTION
Growing adoption of cloud-based technology and remote work

DATA PROLIFERATION
Rapid rise in data flow considering the customer centric approach of industries

CRITICAL INFRASTRUCTURE RISK
Increasing sophistication of attacks and impact on critical infrastructure

AI-DRIVEN THREAT DETECTION
Artificial intelligence enabling predictive monitoring, analytics, and automated incident response

CUSTOMER-CENTRIC EVOLUTION
Industry shifts to real-time, customer-first data models

Securing The Nation's Most Critical And Vulnerable Industries

IT AND TELECOM
The rise of cloud computing, IoT, and 5G has escalated cybersecurity needs in IT and telecom. As cyberattack risks grow, companies are turning to managed security services to protect networks, data, and digital infrastructure.

GOVERNMENT AND DEFENSE
In recent years, the government and defense sectors have become prime targets for cyber adversaries seeking to disrupt critical functions or steal confidential data. The consequences of a breach in these sectors could be material, impacting national security and defense strategies.

BANKING, FINANCIAL SERVICES, AND INSURANCE
With increasing digitalization, BFSI institutions are major cyberattack targets. In 2023, cyber incidents on financial institutions surged by 45%, driving strong demand for advanced cybersecurity solutions.

ENERGY, OIL, AND GAS
The energy, oil, and gas industry sector is vital to the Kingdom's economy. As a result, the demand for robust security solutions has surged, particularly in the wake of increasing cyber threats and geopolitical tensions. The energy sector in Saudi Arabia, which includes some of the largest oil reserves globally, faces unique challenges regarding cybersecurity.

HEALTHCARE
Healthcare organizations are rapidly digitizing patient records, medical devices, and operational systems. This expansion of connected infrastructure creates new vulnerabilities, making cybersecurity essential for protecting sensitive patient data and ensuring continuity of care.

RETAIL AND E-COMMERCE
As more businesses in the retail and e-commerce segments adopt digital platforms, they face increasing cyber threats, making managed security services essential for maintaining consumer trust and safeguarding their operations.

SOURCE: MORDOR COUNTRY INDUSTRY REPORT

Regulations Drive Cyber Growth

Five key regulatory bodies govern cybersecurity across sectors

Saudi Arabia has established a comprehensive regulatory framework for cybersecurity, with oversight distributed across five key bodies. The National Cybersecurity Authority (NCA) sets the national agenda, while sector-specific regulators including SAMA, SDAIA, CMA, and MCIT enforce standards within their respective domains. As digital transformation accelerates across healthcare, defense, telecommunications, and financial services, regulatory requirements continue to evolve, creating sustained demand for compliant cybersecurity solutions.

Regulatory Bodies

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

The National Cybersecurity Authority (NCA), established in 2017, regulates cybersecurity standards across key areas and aims to strengthen national cybersecurity, stimulate sector investment, enhance competitiveness, and improve services for national organizations.

البنك المركزي السعودي
SAMA
Saudi Central Bank

SAMA oversees the cybersecurity of all banks, insurance, and reinsurance companies, financing firms, credit bureaus, and financial market infrastructure operating in Saudi Arabia.

SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

SDAIA oversees data governance and AI-related cybersecurity across both public and private sectors. Its regulations focus on data protection, privacy, secure data sharing, and the safe deployment of AI technologies.

هيئة السوق المالية
Capital Market Authority

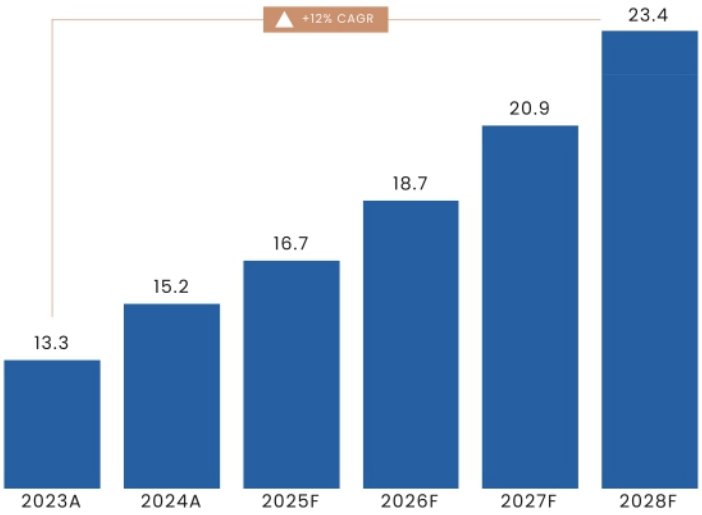
CMA oversees all capital market institutions under its jurisdiction, issuing guidelines that cover cybersecurity governance, risk management, audits, operational controls, and third-party cybersecurity practices.

وزارة الاتصالات وتقنية المعلومات
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

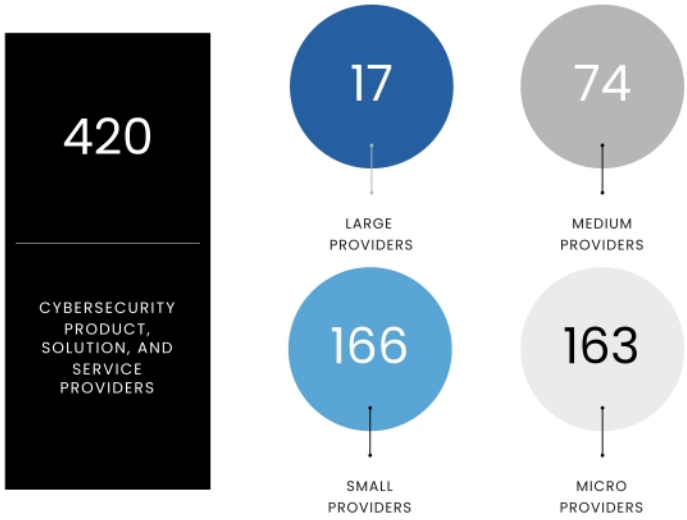
MCIT regulates cybersecurity in the ICT sector, focusing on digital infrastructure policies, secure technology adoption, and enforcing standards across telecom and digital service providers.

Key Takeaways

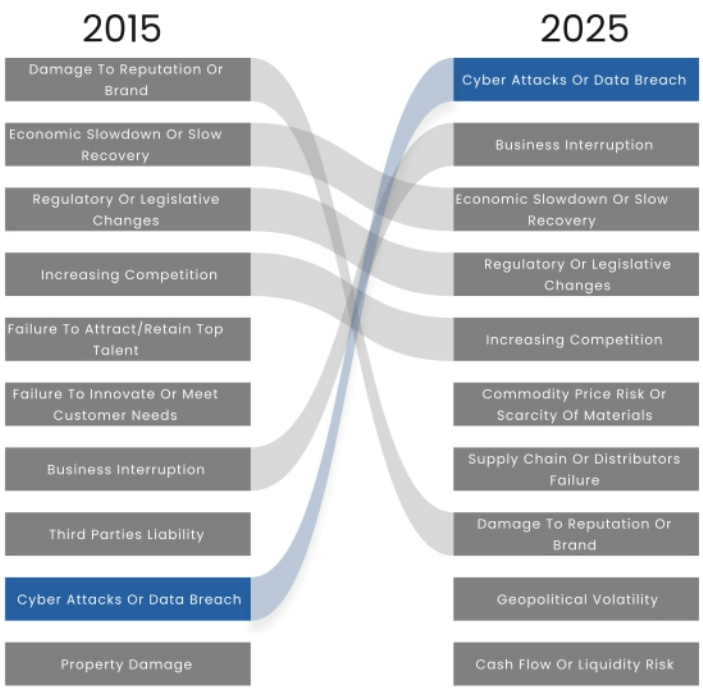
Potential in Cybersecurity Solutions (﷼B)



Number of Registered Cybersecurity Product, Solution, and Service Providers



Top Threats Facing Organization



Top 10 Industries Targeted by Cyber Attacks

- TECHNOLOGY: **23%**
- CONSULTING AND PROFESSIONAL SERVICES: **15%**
- MANUFACTURING **12%**
- RETAIL **11%**
- FINANCIAL SERVICES: **10%**
- HEALTHCARE: **9%**
- TELECOMMUNICATIONS: **7%**
- GOVERNMENT **6%**
- INDUSTRIALS AND ENGINEERING: **4%**
- ACADEMIC: **3%**

Market drivers

CYBERCRIME SURGE

Rising cybercrime, digital disruption, and increased compliance demands

CLOUD ADOPTION

Growing adoption of cloud-based technology and remote work

DATA PROLIFERATION

Rapid rise in data flow considering the customer centric approach of industries

CRITICAL INFRASTRUCTURE RISK

Increasing sophistication of attacks and impact on critical infrastructure

AI-DRIVEN THREAT DETECTION

Artificial intelligence enabling predictive monitoring, analytics, and automated incident response

CUSTOMER-CENTRIC EVOLUTION

Industry shifts to real-time, customer-first data models

Legal Disclaimer

The material in this presentation has been prepared by Merak Capital. This information is given in summary form and does not purport to be complete. Information in this presentation, including forecast financial information, should not be considered as advice or a recommendation to investors or potential investors in relation to holding, purchasing or selling securities or other financial products or instruments and does not consider your particular investment objectives, financial situation or needs.

This presentation may contain forward-looking statements including statements regarding our intent, belief or current expectations with respect to Merak Capital businesses and operations, market conditions, results of operation and financial condition, capital adequacy, specific provisions and risk management practices. Readers are cautioned not to place undue reliance on these forward-looking statements.

Merak Capital does not undertake any obligation to publicly release the result of any revisions to these forward-looking statements to reflect events or circumstances after the date hereof to reflect the occurrence of unanticipated events. While due care has been used in the preparation of forecast information, actual results may vary in a materially positive or negative manner. Forecasts and hypothetical examples are subject to uncertainty and contingencies outside Merak Capital's control. Past performance is not a reliable indication of future performance. Unless otherwise specified, all information contained herein is for Merak Capital.

Merak Capital is a licensed company by the CMA to manage private investment funds, investor portfolios, and advise on financial securities, under the license number 18194-32 issued on 11-11-2018, with a specialized focus on technology investments.