DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

INDIA | CYBERSECURITY DOMESTIC MARKET 2023

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

4th Floor, nasscom Campus
Plot No. 7-10, Sector 126, Noida
Uttar Pradesh 201303, India
E-mail: research@dsci.in

Copyright ©2023

All rights reserved.

The information contained herein has been obtained from sources believed to be reliable. DSCI disclaims all warranties as to the accuracy, completeness or adequacy of such information. DSCI shall have no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof.

The material in this publication is copyrighted. No part of this report can be reproduced either on paper or electronic media without permission in writing from DSCI. Request for permission to reproduce any part of the report may be sent to DSCI.

The information contained herein should not be relied upon as a substitute for specific professional advice. Professional advice should always be sought before taking any action based on the information provided.

Usage of Information

Forwarding/copying/using in publications without approval from DSCI will be considered as infringement of intellectual property rights.

FOREWORD

The past four years have been pivotal in the global digital transformation landscape and the widespread adoption of emerging technologies. The spotlight is now on leveraging digitization as a catalyst for propelling organizations towards data-driven strategies, elevating customer experiences, extending market reach, fostering innovation, and fortifying overall agility.

Organizations are increasingly investing in emerging technologies, with Cloud and AI/ML emerging as cornerstones of strategic investment. ~97% and ~84% of the analyzed organizations have invested in AI/ML and cloud, respectively. GenAI has garnered significant attention, transforming how organizations approach automation. The accelerating innovation and proliferation of sensitive data has drawn the attention of regulatory bodies keenly focused on upholding data integrity and privacy.

The narrative surrounding cybersecurity has transformed into a central topic in boardroom discussions. The heightened focus on brand reputation and regulatory compliance has spurred the creation and implementation of robust cybersecurity and risk management policies. A noticeable shift is observed with security leaders now directly reporting to the board, underscoring cybersecurity's significance in corporate governance. This transformation reflects the evolving landscape where cybersecurity has become a pivotal and integral component of organizational leadership.

India's cybersecurity market has undergone a remarkable transformation, marked by substantial growth which underscores the escalating significance placed on fortifying digital defenses in the face of evolving threats. A pivotal driver of this expansion has been the substantial investment in cybersecurity products. Notably, these products have demonstrated extraordinary growth, growing by a CAGR of ~38% and witnessing an astonishing increase of more than 3X since CY2019.

A strong synergy in the ecosystem, led by the Government, end users, and services and product players, will propel cybersecurity spending in India, accounting for 5% of global expenditure by 2028. Market traction is growing for product and service offerings such as ZTNA, CNAPP, CASBs, XDR, MFA, VAPT, Security Audits and Assessments, and Threat Intelligence Services. Over 60% of surveyed organizations have invested or plan to invest in these solutions to enhance their cybersecurity resilience.

The impetus behind these investments lies in the ongoing digital transformation initiatives and the imperative to ensure regulatory compliance. Among the analyzed organizations, ~90% recognized email as the foremost and most critical pathway for cyberattacks and 84% acknowledged phishing as the predominant cyber threat confronting their industry.

The report unfolds the compelling narrative of the growth trajectory within the Indian cybersecurity market. It delves into various dimensions such as cybersecurity spending analysis, offerings adoption and sectoral spending analysis, talent and regulatory landscape, and advancements in technology adoption. It also showcases the practical strategies organizations employ to enhance cyber resilience and provides recommendations for improving cybersecurity practices.

We sincerely hope that this research report gives you a better understanding of the India's cybersecurity market and supports a robust and resilient cyber ecosystem to drive your digital transformation endeavors securely and confidently.

Vinayak Godse

CEO, DSCI

Pramod Bhasin

Chairman, DSCI

Digital transformation has become a catalyst for adopting data-driven strategies, uplifting customer experiences, and fostering innovation. Cybersecurity has become a fundamental pillar in supporting digital transformation and integrating emerging technologies to drive organizational growth in line with the Government of India's vision to transform the nation into a digitally empowered society, with the digital economy accounting for 10% of the total economy in 2023 and expected to take 20% share by 2026. The demand for cybersecurity products and services has increased significantly in the last three years, transforming India into a favourable destination for cybersecurity companies. Guidelines issued by regulatory bodies and ministries, such as the Ministry of Power, Ministry of New and Renewable Energy, and RBI, have spurred a surge in cybersecurity investments, particularly within regulated sectors. DPDP Act, 2023, will encourage companies to bolster data security and privacy measures. While the security industry is expanding in India, companies invest in next-gen SOC, threat intelligence services, and cloud-based security services to safeguard their network from the evolving threat landscape. A strong synergy in the ecosystem, led by the Government, end users, and cybersecurity providers, will propel cybersecurity spending in India.

Debjani Ghosh

President, nasscom

With the rapid advancement in emerging technologies, organizations worldwide, including India, are significantly scaling up efforts to digitally transform business processes at scale for higher productivity and competitive advantage. This paradigm shift underscores a commitment to innovation and the adoption of data-driven decision-making processes. However, this surge in technological advancements has also given rise to heightened security challenges.

As cybersecurity evolves into a pivotal element for fortifying the resilience of businesses, it is transcending its role from a mere operational necessity to a strategic priority—a critical success factor that forms the bedrock of effectiveness in digitization and technology transformation initiatives. Cybersecurity has moved to the forefront of business strategy management, gaining recognition from CEOs and boards who increasingly acknowledge its significance for business success.

These dynamics collectively position India as a burgeoning market for security capabilities, encompassing both products and services. The accelerated pace of digitization and technological advancements over the past three years has propelled the security market into a higher orbit of growth. Indian cybersecurity has experienced an impressive threefold growth since CY2019, surging past the USD 6 billion mark in 2023. As businesses navigate the intricacies of the digital era, cybersecurity is no longer merely a defensive measure; it has evolved into a proactive strategy that is indispensable for sustainable growth and success.

एस. कृष्णन, आई.ए.एस.
सचिव
S. Krishnan, I.A.S.
Secretary

सत्यमेव जयते

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
भारत सरकार
Ministry of Electronics &
Information Technology (MeitY)
Government of India

Message

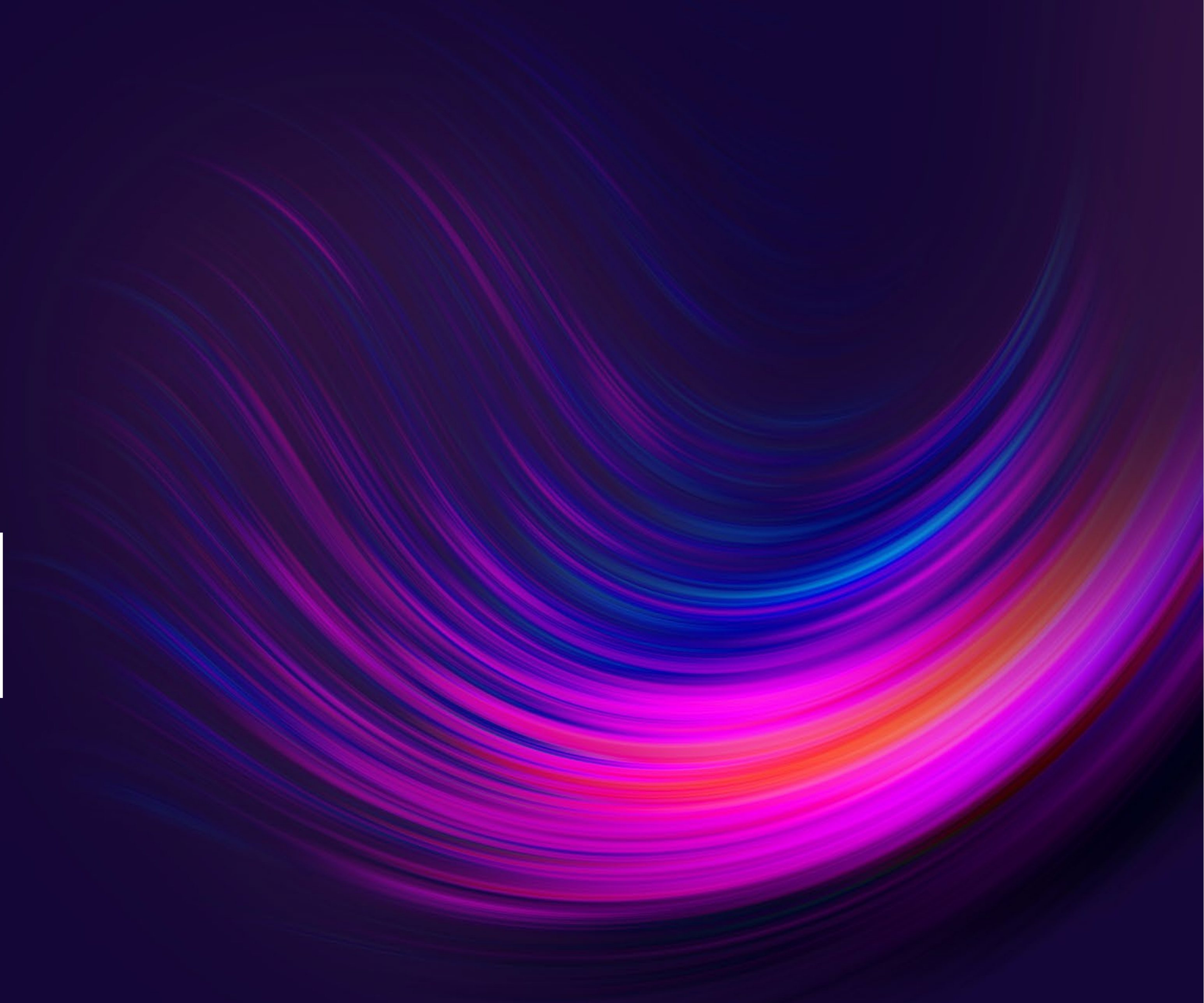
The Government of India and The Ministry of Electronics & IT (MeitY) have spearheaded the transformation of India's digital landscape. At a large scale, the comprehensive Digital India Programme, and innovative digital projects like Aadhaar, UPI, DigiLocker, GeM, UMANG, and API Setu have enabled affordable access to digital services and ensured digital inclusion. The Indian cybersecurity industry has been at the forefront, supporting the Government and other critical sectors, facilitating the adoption of emerging technologies, including AI/ML and cloud, and mitigating evolving cybersecurity risks. India is emerging as a global cybersecurity hub. The Government's commitment to digitization, supported by adequate and evolving policies, has fostered an environment conducive to a rise in cybersecurity investment in India. The 'India Cybersecurity Domestic Market 2023 Report' showcases the current cybersecurity spending and adoption trends, evolving cybersecurity priorities, preparedness, and best practices. The Ministry of Electronics and IT is committed to accelerating innovation and the technology ecosystem and ensuring the Indian Internet is Open, Safe, Trusted, and Accountable. Ministry of Electronics and IT is committed to partnering with DSCI to scale innovation in emerging areas like 5G, Hardware, and IoT security, and through our flagship ISEA and Future Skills Programmes, meet the talent demand of the industry.

(S. Krishnan)

75 आज़ादी का अमृत महोत्सव

Digital India
Power To Empower

EXECUTIVE SUMMARY



EXECUTIVE SUMMARY

REVENUE INSIGHTS

- India cybersecurity domestic market grew from USD **1.98 billion** in 2019 to **USD 6.06 billion** in 2023.
- India cybersecurity products market grew from USD **1.03 billion** in 2019 to reach USD **3.76 billion** in 2023.

SECTORAL INSIGHTS

- BFSI spending on cybersecurity grew from USD **518 million** in 2019 to USD **1,738 million** in 2023.
- IT/ITeS grew at a CAGR of **36%** during 2019-2023.

TECHNOLOGY

- **~97%** of the organizations have invested in AI/ML and **~84** have invested in Cloud.
- **~81%** organizations invested in Zero Trust to bolster their cyber resilience.

SECURITY INITIATIVES

- Organizations focused on employee training and awareness sessions, and incident response plan to improve their cybersecurity posture as indicted by **78%** and **56%** respondents.

SERVICES

- Security operations accounted for **~45%** share in the services market.
- Security implementation services grew at a CAGR of **22%** during 2019-2023.

PRODUCT INSIGHTS

- From the organizations analysed, **~73%** have either invested or plan to invest in Identity & Access Management (IAM) offerings in the next two years.

KEY INVESTMENT DRIVERS

- Digital transformation initiatives and ensuring regulatory compliance are the key factors driving investment in cybersecurity, identified by **~84%** and **~81%** of the respondents, respectively.

THREAT LANDSCAPE

- **~90%** of the organizations identified 'email' as the most critical cyberattack pathway.
- From the organizations analysed, **~84%** consider phishing as the biggest cyber threat faced by their industry.

STUDY METHODOLOGY

As part of DSCI's industry development initiative, the report titled **'India Cybersecurity Domestic Market'** was developed through a three-month comprehensive study.

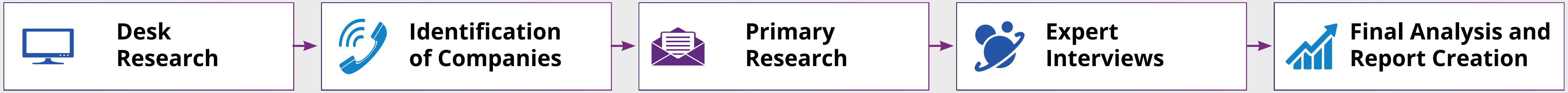
> The insights published in the report are primarily based on the survey conducted by DSCI in 2023. The report findings is based on a detailed study of 120+ organizations including end user organizations, cybersecurity products and services organizations.

Scope

The report aims to showcase the current cybersecurity spending and adoption trends, changes in cybersecurity priorities, preparedness, and best practices. It also reflects on cybersecurity drivers and trends highlights achievements, and evolutions, highlighting the cybersecurity talent scenario, and the cybersecurity offerings that organizations consider for adoption and investment. It demonstrates the increasing need and imperative for cybersecurity offerings.

Objective

To showcase the potential of India's cybersecurity market and its emergence as a global hub for innovation and cybersecurity.



Desk Research

Literature review and secondary research to gather information on cybersecurity landscape, spending and industry trends. Industry report, annual reports, government publications, and other relevant sources were reviewed.

Identification of Companies

Identification of stakeholders in cybersecurity industry. The mapping, including end-user organizations, product and services organizations.

Primary Research

Primary consultation with each stakeholder group to understand their perspective on the cybersecurity market.

Expert Interviews

Discussions with a cross section of CEOs, CISOs, founders and industry leaders to validate cumulative trends and obtain deeper insights.

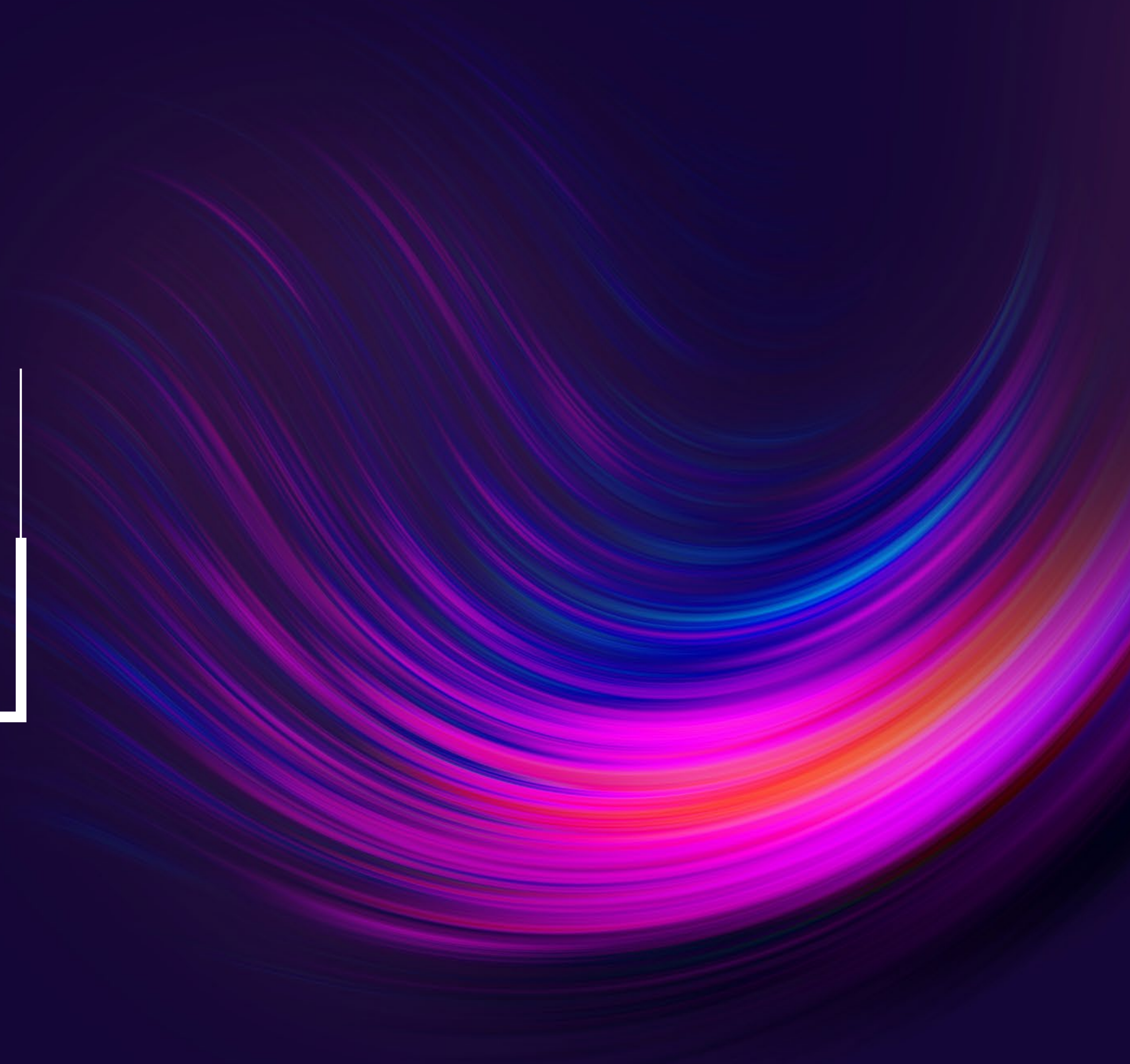
Final Analysis and Report Creation

Analysis of primary and secondary data, and creation of the report.

TABLE OF CONTENTS

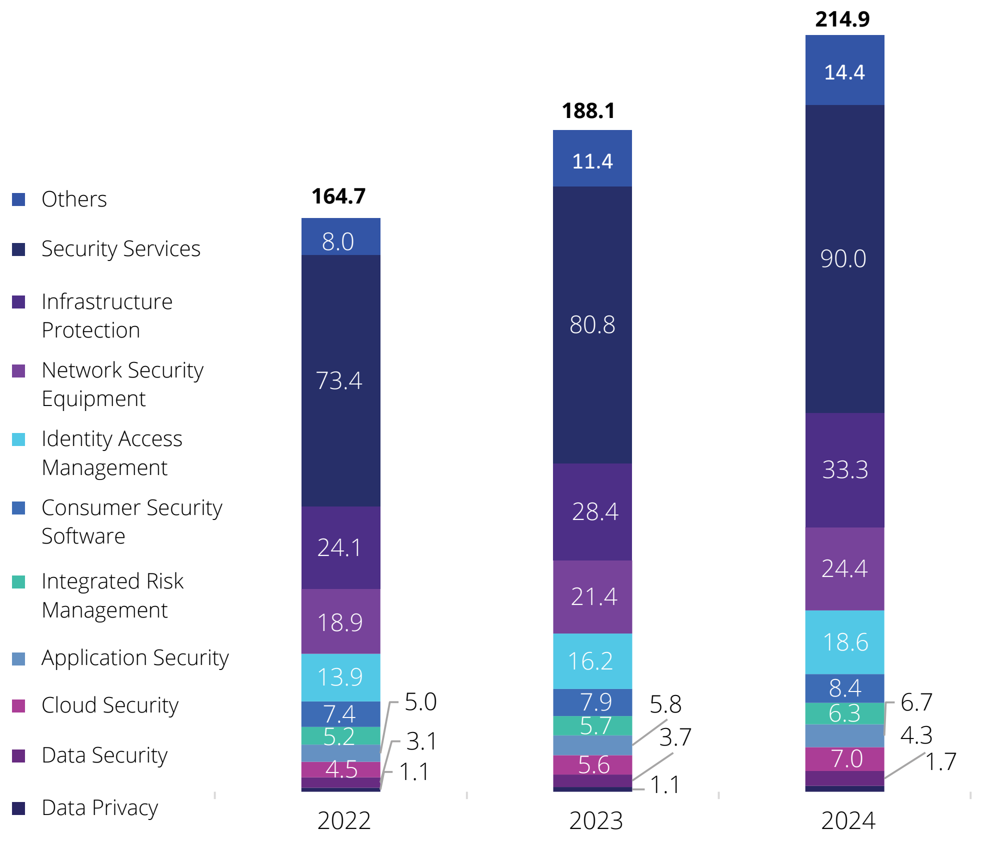
GLOBAL CYBERSECURITY

Market Overview



GLOBAL CYBERSECURITY MARKET OVERVIEW

Global Information Security and Risk Management market 2022-2024 (USD billion)



Overview

According to Gartner[1], the global spending on Information Security and Risk Management is expected to reach USD 188 billion in 2023 from USD 169 billion in 2022, growing at 11.3%. Increase in digitalization, shift towards hybrid and remote work, the growing adoption of cloud services, and IT & OT convergence have increased external attack surfaces for organizations, making them vulnerable to disruption, breaches, and data loss, thereby driving investment in cybersecurity worldwide.

Spending on digital transformation technologies is expected to reach USD 2.16 billion in 2023. Security risks from zero-day vulnerabilities, increasing data and privacy regulations worldwide, and the emergence and adoption of GenAI have further bolstered cybersecurity spending.[2]

Key Trends

Cloud security grew at a Y-o-Y growth rate of 25.2%.

- According to Gartner's forecast[3], by 2026, 75% of organizations are expected to utilize cloud as the foundational platform for their digital transformation initiatives.

Data privacy and data security grew at a Y-o-Y growth rate of 18.5% and 20.1%, respectively.

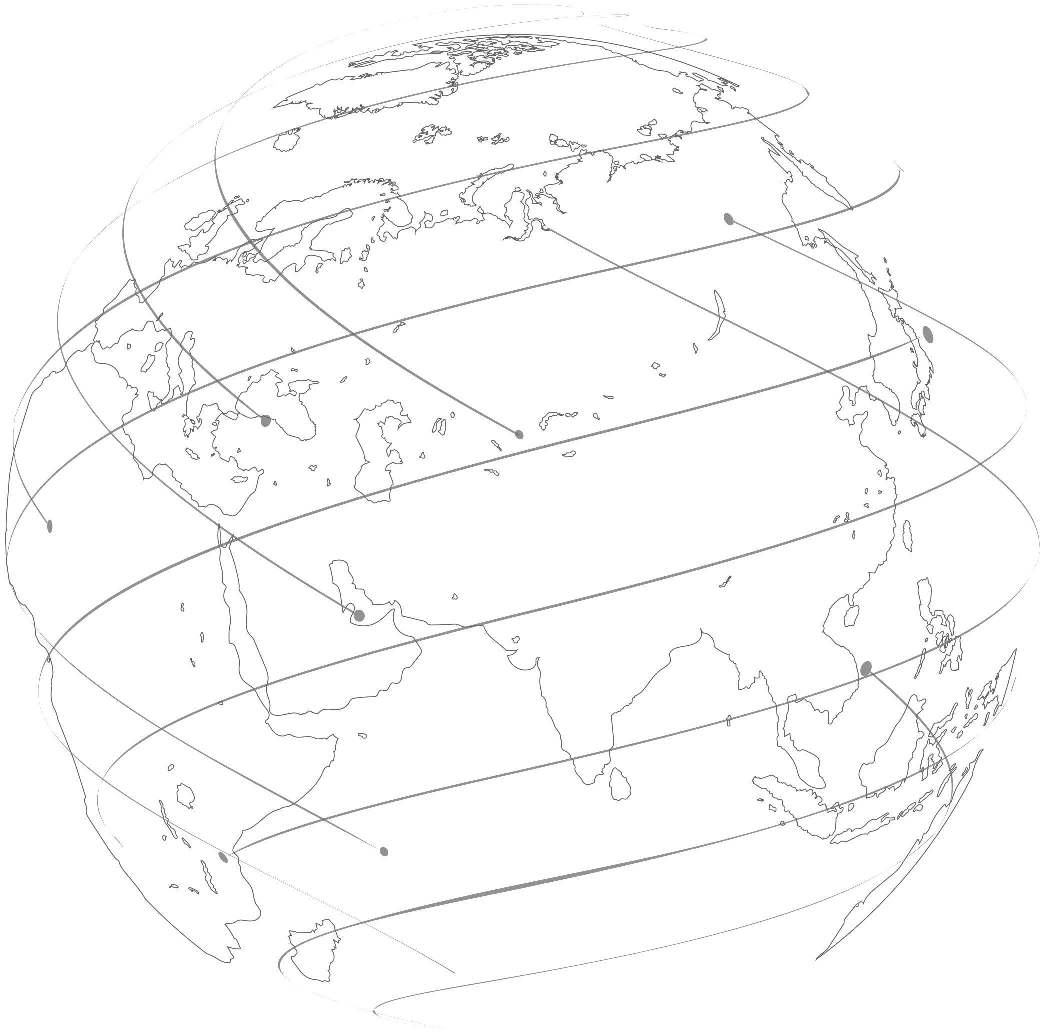
- According to Gartner[4], modern privacy regulations are anticipated to encompass the personal data of 75% of the world's population by 2025.

- There has been an increase in zero-day vulnerabilities since 2012. In 2022, 41 zero-day vulnerabilities were either disclosed or detected. Organizations need to invest in threat intelligence, attack surface management, vulnerability management, patch management, and zero-trust architecture.[5]

Key Offerings in Demand

- Security services, including consulting and IT sourcing to grow by 11% to reach ~USD 90 billion in 2024.
- Cloud security: Spending on Cloud Workload Protection Platforms (CWPP) and Cloud Access Security Brokers (CASB) is expected to grow by 24.7% Y-o-Y to USD 7 billion in 2024.
- In 2024, there is an anticipated growth in cloud-based detection and response solutions, including technologies like Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR).

The global spending on Information Security and Risk Management is expected to reach USD 188 billion in 2023 from USD 169 billion in 2022, growing at 11.3%.



GLOBAL THREAT LANDSCAPE

16,312

Security Incidents reported between 1 November 2021 to 31 October 2022[6]

USD 4.45 million

Average cost of **Data Breach** in 2023[9]
Cost of Data Breach includes detection and escalation, notification, post-breach response and lost business costs

5,199

Breaches reported during 1 November 2021 to 31 October 2022[7]

36%

Vulnerability exploited for ransomware attacks January – March 2023[10]

6,248

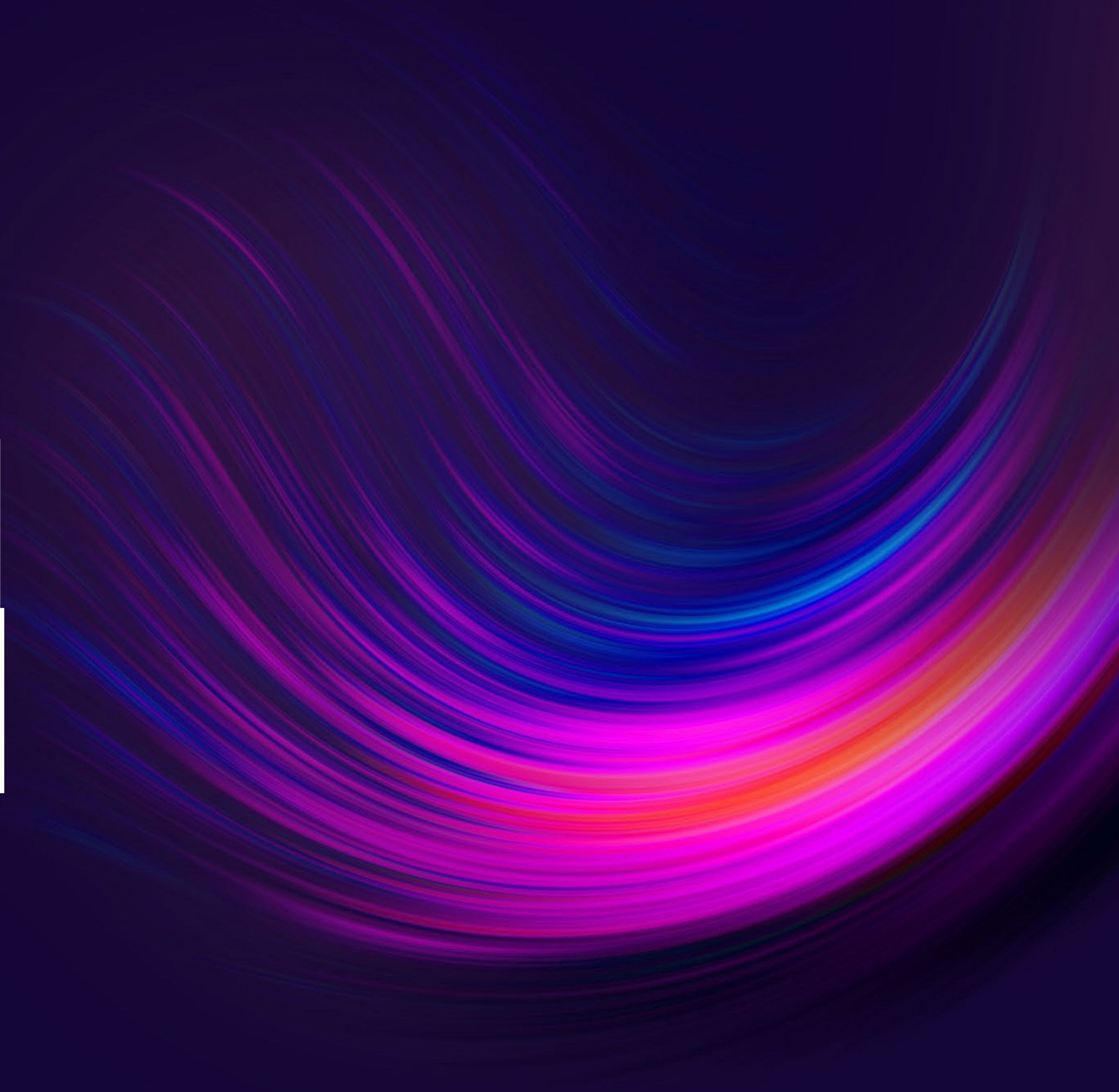
Denial of Service incidents with 4 confirmed data disclosure between 1 November 2021 to 31 October 2022[8]

742%

Rise in **open-source software attacks** since 2019[11]

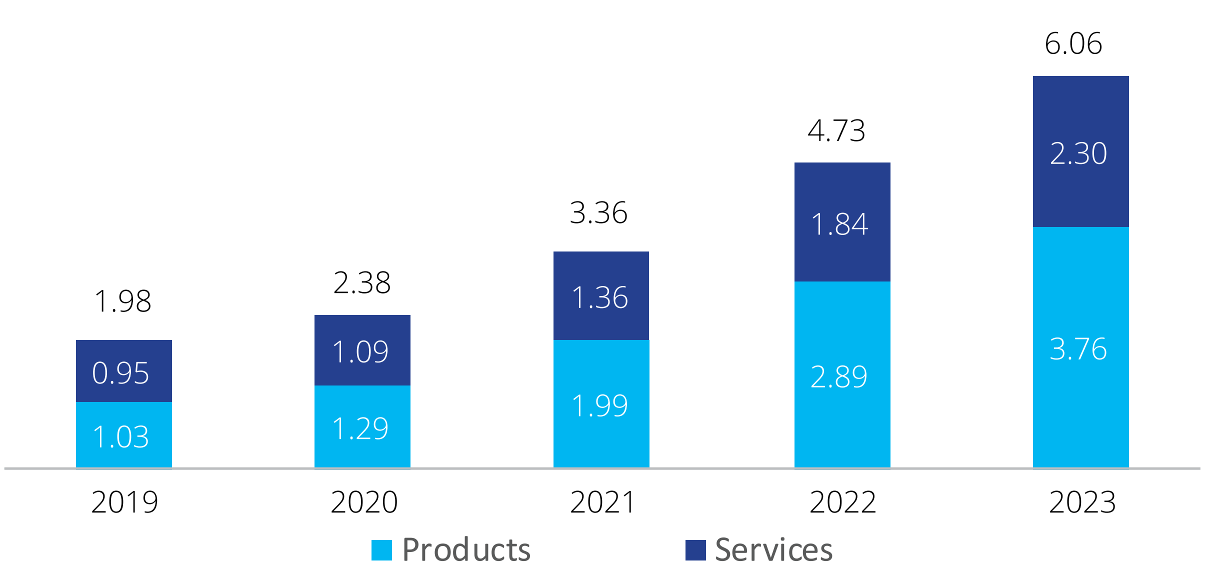
INDIA CYBERSECURITY

Domestic Market Overview



INDIA CYBERSECURITY DOMESTIC MARKET OVERVIEW

India Cybersecurity Domestic Market (USD billion)



India cybersecurity market grew at a CAGR of over ~30% during 2019-2023 to reach USD 6.06 billion in 2023. Digital transformation initiatives and ensuring regulatory compliance drove cybersecurity spending, identified by ~84% and ~81% of respondents.

Key Observations

The market witnessed significant growth during 2020 and 2022 due to heightened technology adoption due to the continued focus on digital transformation and emerging technology adoption, including AI/ML, zero trust model, cloud and edge computing, and GenAI.

- IT modernization and remote/hybrid working fueled spending on public cloud services, witnessing double-digit growth since 2019. In 2020, 2021, 2022, and 2023, the growth rates were 47.3%, 34.6%, 42.3%, and 26%, respectively. Projections suggest that the growth is expected to reach 34.4% in 2024.[12,13]
- As per PwC survey,[14] AI adoption increased in India, reflected by over 90% respondents from industrial products and manufacturing, Technology, Media and Telecom (TMT), travel and hospitality. Healthcare and pharmaceuticals and financial services also witnessed an increase in AI adoption.

Demand for security offerings including CNAPP, WAF, CIEM, CASBs, EDR, XDR, SASE, PAM, MDR, GRC, next-gen SOC and threat intelligence services is increasing in India. Regulatory requirements, digital transformation and use of emerging technologies also led to the formation and adoption of cybersecurity and risk management policies, frameworks, and security leaders directly reporting to the board.

Key Observations

India cybersecurity market accounted by ~3% of the overall global cybersecurity market. It is expected to account for 5% of the global market by 2028.

There is a significant untapped accessible market available for cybersecurity providers in the country. The technology landscape is rapidly evolving in the country with ~27,000 tech start-ups as of March 2023.[15]

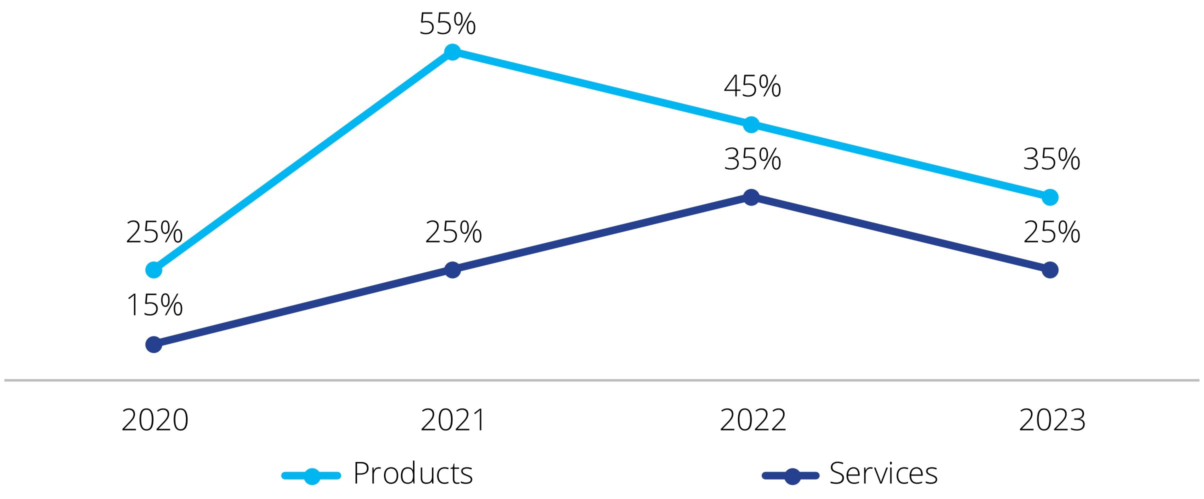
Furthermore, organizations in the country are allocating increased budgets to security, as it is closely linked with brand reputation and is considered as a crucial aspect in tabletop exercises.

The Government of India is actively fostering the growth of the cybersecurity industry, exemplified by its robust support in the FY 2023-24 Union Budget. Allocating INR 400 crore for cybersecurity projects and INR 225 crore for CERT-In, demonstrates a commitment to fortify the nation's digital defenses.[16]

Government initiatives, including Digital India Programme and Cybersecurity R&D units, National Center of Excellence (NCoE), a MeitY and DSCI joint initiative, are also driving the cybersecurity industry in India.[17]

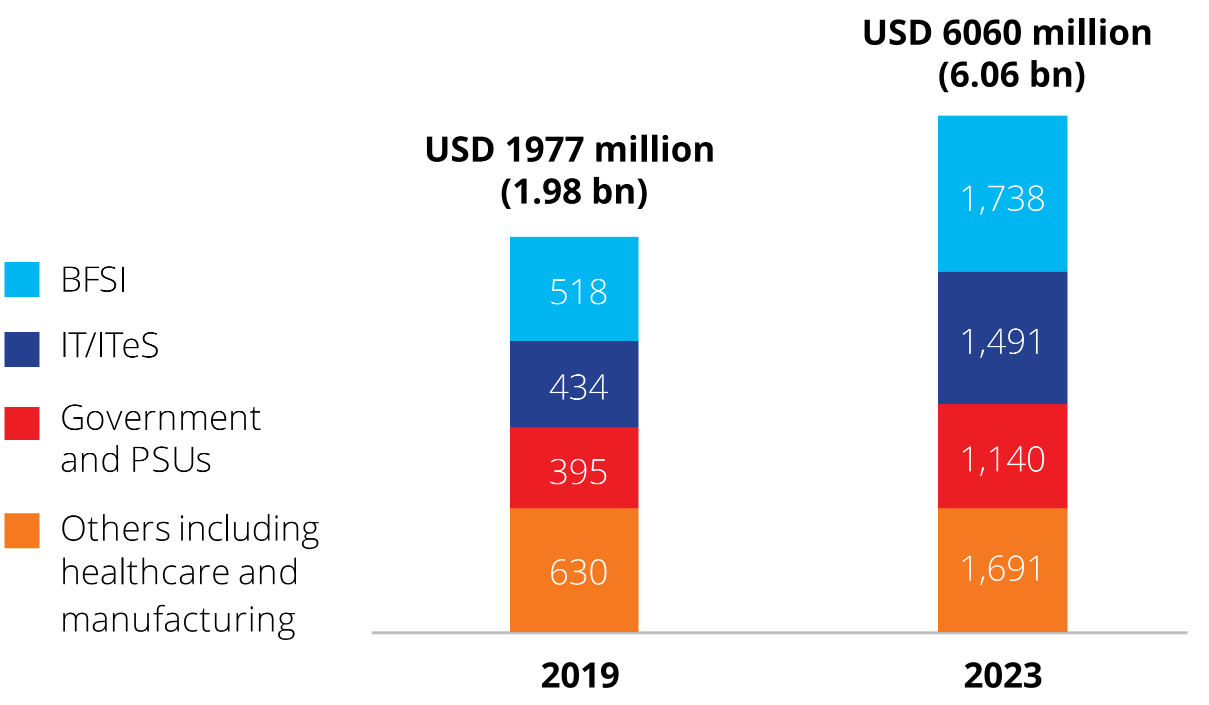
A significant milestone is the government's allocation of approximately INR 14,903 crore for the expansion of the Digital India initiative. This includes innovative strides, such as the development of cybersecurity tools and the integration of the National Cyber Coordination Centre (NCCC) with 200 sites, enhancing the nation's cybersecurity infrastructure.[18]

India Cybersecurity Domestic Market Growth - Product and Services (%Y-o-Y)



India cybersecurity market accounted by ~3% of the overall global cybersecurity market. It is expected to account for 5% of the global market by 2028.

India Cybersecurity Domestic Market - Sectoral Overview (USD million)



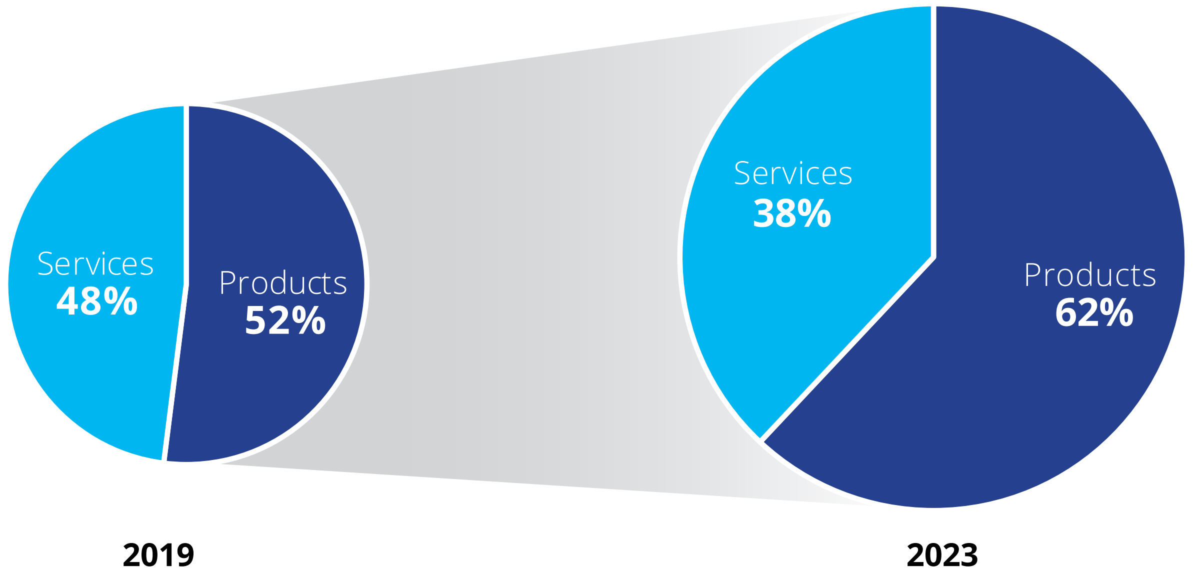
Key Trends and Drivers

- Stringent regulatory requirements, ensuring data privacy and protection, and rise in digital discoveries drive demand for data and privacy offerings, GRC, cloud security, and IAM in the BFSI sector.
- Securing customer and employee data, facilitating secure hybrid working, and deploying emerging technologies are leading to investments in tighter operations and technical controls, such as encryption, DLP, etc., in the IT and ITeS sector.
- Large conglomerates are driving cybersecurity spending through digital transformation imbibed with cybersecurity.
- Government with 5G, smart city projects, Digital India, Digital inclusion, API Setu, India Stack Global, and Global Digital Public Infrastructure Repository, is emerging as high potential market.

Healthcare is witnessing robust growth as cybersecurity has emerged as a boardroom agenda amid rising technology adoption, cloud migration and rising cyberattacks.

BFSI spending on cybersecurity grew at a CAGR of 35% from USD 518 million in 2019 to USD 1,738 million in 2023 due to stringent and granular policy requirements. IT/ITeS grew at a CAGR of 36% during 2019-2023, driven by the need for secure adoption of advanced technologies like AI/ML, edge computing, and GenAI.

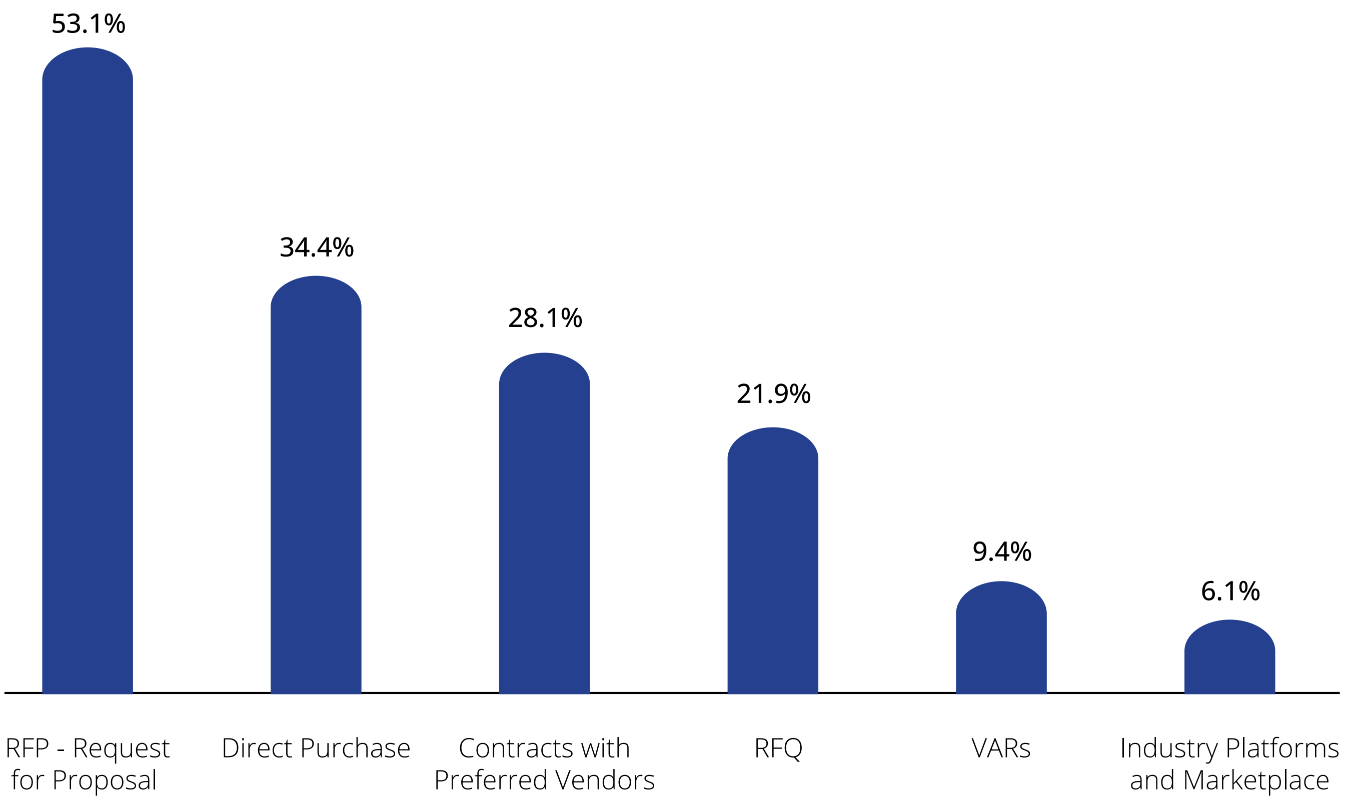
India Cybersecurity Domestic Market - Products vs Services



- Organizations focused on facilitating remote work and business continuity during the pandemic have transitioned to harnessing technology to enhance customer experience, expand market reach, and promote innovation.
- Enablement of remote workforce has led to increased product adoption, with higher investment in SaaS-based products.
- Solution automation is gaining traction, with 53% of organizations opting for it. This pattern has also contributed to the proliferation of products leveraging AI/ML to improve security processes and augment incident response capabilities.
- Industries with advanced cyber maturity and cloud-first strategies, like BFSI and IT/ITeS, and digital-first organizations prefer products. In contrast, industries such as manufacturing and energy are fortifying their basic security controls and exhibit a greater inclination toward investing in services.

From the organizations analysed, ~73% have either invested or plan to invest in Identity & Access Management (IAM) offerings in the next two years.

Cybersecurity Procurement - Preferred Mode



Source – DSCI Survey 2023

Request for Proposals (RFPs) is the most leveraged medium in India for procuring cybersecurity services. The Government and PSUs predominantly leverage RFPs for their cybersecurity requirements. The mode is also prefered by other sectors such as- healthcare, BFSI and manufacturing.

RFPs enable organizations to validate vendor capabilities thoroughly, establish a fair and standardized process, outline precise requirements, and conduct due diligence.

IT/ITeS organizations leverage direct purchases and contracts with preferred vendors for cybersecurity requirements.

Direct purchase offers more flexibility in securing cybersecurity products and services, reduces the time for completing the transactions, and provides better control over the procurement process.

Contract with Preferred Vendors help organizations achieve quality assurance operational efficiencies and acquire customized solutions.

STRENGTHENING INDIA'S CYBERSECURITY POSTURE

INDIA VISION 2026

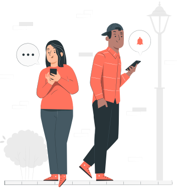
USD 1 TRILLION DIGITAL ECONOMY

1.38 billion

World's largest unique digital identity program as of 18 December 2023[19]

840 million

People with online presence as of June 2023[20]



1.01 billion

Smartphone users as of December 2023[21]

226.58 million

Digital Lockers users as of 18 December 2023[22]

876.5 million

Broadband subscribers in August 2023[23]

600,000 KM

OFC under BharatNet as of 13 July 2023[24]

INR 2,086 trillion

Digital payments value in FY 2022-23[25]

1,811

Government services available at UMANG as of 18 December 2023[26]

API Setu

>4,700

Published APIs As of 18 December 2023[27]

1,400

API publishers as of 18 December 2023[28]

AADHAAR

1.29 billion

Aadhaar based authentications in November 2023[29]

104.38 trillion

Aadhaar authentication as of 18 December 2023[30]

DigiLocker
Your documents anytime, anywhere

1,684 million

as of 18 December 2023[31]

6.28 billion

Stored documents as of 18 December 2023[32]

national health authority

498.93 million

ABHA accounts as of 18 December 2023[33]

328.40 million

Health Records linked as of 18 December 2023[34]

AADHAAR

17.37 trillion

eKYCs done as of 18 December 2023[35]

UPI
UNIFIED PAYMENTS INTERFACE

83.71 billion

UPI transactions achieved during FY 2022-23[36]

10%

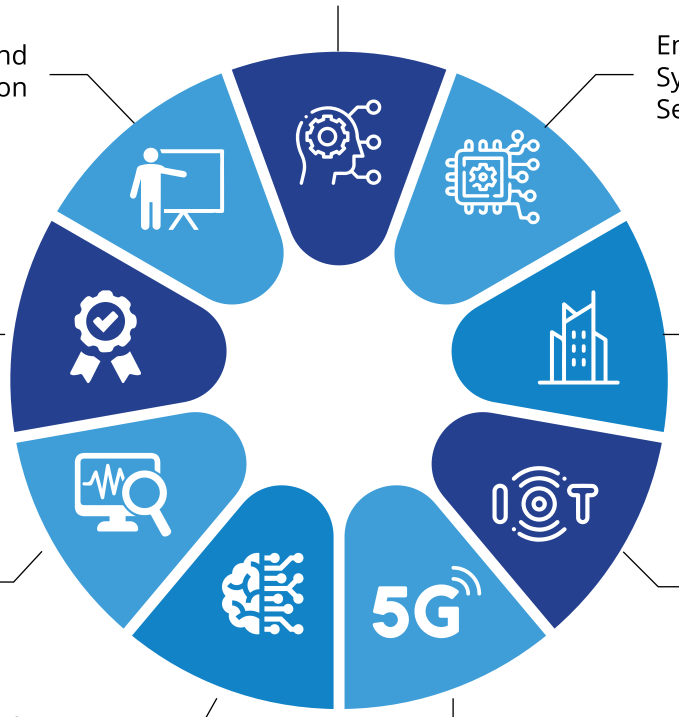
Digital economy as a % of India's economy as of June 2023[37]

46%

Share in global real-time payments in 2022[38]

CYBERSECURITY ENABLEMENT - GOVERNMENT INITIATIVES

Cybersecurity Research Areas



Critical Infrastructure Security

Embedded System Security

Zero Trust Architecture and Trusted Supply Chain

IoT and Connected Devices Security

5G Wireless Security, Cloud, Edge and Fog Computing Security

AI in Information Security including Threat Intelligence

Digital Forensics and Monitoring tools

Vulnerability prioritization, Remediation and Assurance

Capacity Building and Awareness Creation

CERT-In activities in 2022[39]	Number
Incidents Handled	1,391,457
Vulnerability Notes	488
Security Drills	5
Trainings Organized	23

Cybersecurity Budget Allocation in India, FY2021-22 to FY2023-24[40]

Budget head [28]	Budget FY2021-22 to FY 2023 -24 (in INR crore)
Cyber Security Projects (NCCC & Others)	1,010.51
CERT-In	633.69

Indian Government Cybersecurity Projects and Initiatives*

Indian Cybercrime Coordination Centre (I4C)

Cyber Security Grand Challenge

Notification for Preferential Market Access for Cyber Security Products

Cyber Security Training of officials of Government of India

Indian Common Criteria Certification Scheme

Centre for Advanced Security Technology development in Cyber Physical Systems

Cyber Swachhta Kendra

National Facility for Security Testing, Evaluation and Certification of IoT Devices and Embedded Systems leading to Security Assurance

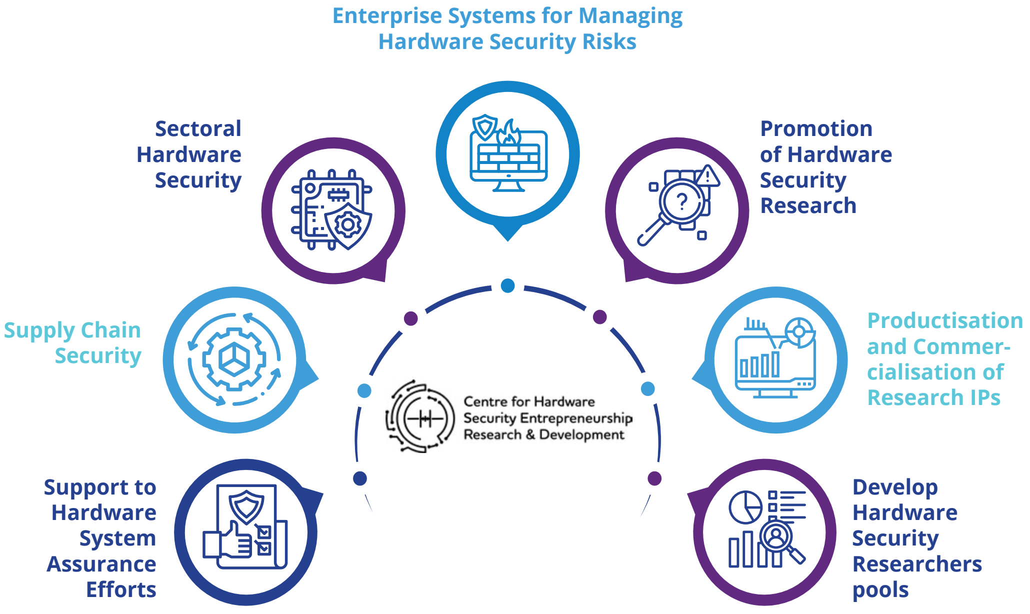
Cyber Forensics Training cum Investigation Labs in 8 North Eastern States

Cloud based Centralized Cyber Forensics Lab Infrastructure

National Cyber Security Exercice (NCX)

Cyber Surakshit Bharat

Please note that this is not an exhaustive list



Enterprise Systems for Managing Hardware Security Risks

Promotion of Hardware Security Research

Productisation and Commercialisation of Research IPs

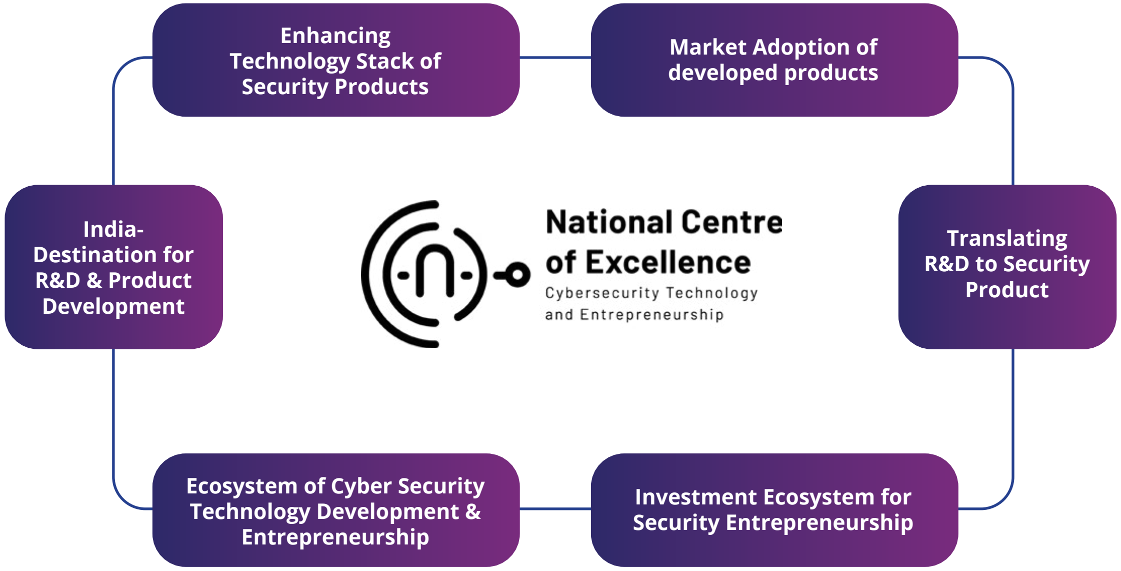
Develop Hardware Security Researchers pools

Support to Hardware System Assurance Efforts

Supply Chain Security

Sectoral Hardware Security

Centre for Hardware Security Entrepreneurship Research & Development



National Centre of Excellence
Cybersecurity Technology and Entrepreneurship

Enhancing Technology Stack of Security Products

Market Adoption of developed products

Translating R&D to Security Product

Investment Ecosystem for Security Entrepreneurship

Ecosystem of Cyber Security Technology Development & Entrepreneurship

India- Destination for R&D & Product Development

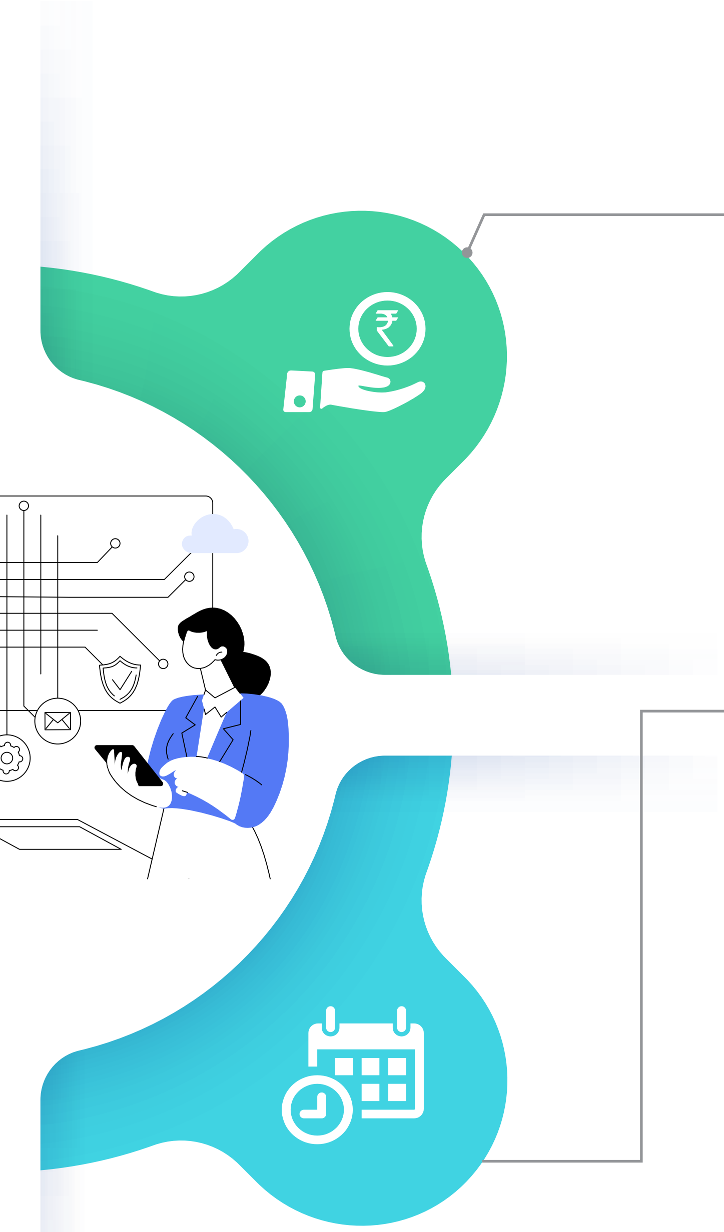
INDIA - MEGA TRENDS

REGULATORY COMPLIANCE

- The increased stringency of norms and regulations has been a key factor in fueling the cybersecurity expenditures in India.
- The Indian government, CERT-In, and regulatory entities such as RBI, SEBI, and IRDAI introduced policies, guidelines, and directives to enhance cyber resilience by enforcing measures, including regular audits, security standards adoptions, and cybersecurity assessment reports.
- In August 2023, the enactment of the DPDP Act 2023 will further drive the spending on data security and privacy offerings in the country.[41]
- IRDAI Information and Cybersecurity Guidelines, 2023, include directions for implementing cybersecurity controls, such as cloud and parameter security.[42]
- In November 2023, RBI issued the Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices. This directive will compel regulated entities to invest in cybersecurity solutions to adhere to the guidelines.[43]
- 81.3% of end-user organizations highlighted that ensuring regulatory compliance is a primary factor motivating their cybersecurity expenditures in India.

TALENT POOL

- The cybersecurity talent shortage has become a significant concern for the country’s end-user organizations and security companies. The ISC2 Cybersecurity Workforce Study[44] shows that the cybersecurity workforce gap has expanded by 40%, reaching approx. 790k in 2023.
- Significant challenges cited by 75% of respondents include a talent shortage. Furthermore, organizations in the country are grappling with the additional challenge of attrition.
- A study conducted by DSCI,[45] 47% of participants reported that cybersecurity professionals make up less than 5% of the total workforce.



DIGITAL TRANSFORMATION

- Digital transformation across all industries increased significantly, leading to an exponential increase in attack surfaces for organizations. The pandemic also aided technology adoption as organizations invested in technology to enable remote workforce.
- According to Nasscom's 2023 State of IT Modernization study[46], most enterprises are placing a high emphasis on modernization, with IT modernization budget constituting 60% of the overall tech budget of 88% of end users.
- As per DSCI's survey, 84% of the respondents reported digital transformation as a critical driver for the increase in cybersecurity investment.
- Cloud plays a pivotal role as a crucial facilitator of digital transformation in India, concurrently elevating security risks for organizations. 59% of end-user organizations express concern about attacks exploiting cloud-based pathways.

CALL FOR ACTION

- The cyber threat landscape has experienced rapid evolution, driven by targeted attacks, growing RaaS incidents, the use of AI/ML to automate attacks and avoid detection, DDoS attacks, and coordinated group cyberattacks.
- Moreover, the data breach cost in India has also increased significantly, with average data breach cost increasing by 28% since 2020, reaching INR 179 million.[47]
- In 2022, CERT-In handled 1,714 phishing attacks and 875,892 vulnerable services.[48]
- Ransomware attacks increased by 53% Y-o-Y in 2022.[49]
- Less skilled threat actors are leveraging RaaS to launch ransomware attacks. RaaS kits are available for them starting at USD 40. Some recognized instances of RaaS kits encompass Shark, Locky, Encryptor, Goliath, Stampado, and Jokeroo.[50]
- As per a Microsoft Study, India accounted for 13.22% of total DDoS attacks, the second-highest volume of attacks after the United States.[51]
- Additionally, vulnerabilities, including zero-day are also being target by attackers.
- In 2022, 41 zero-day vulnerabilities were either disclosed or detected.[52]
- Threat actors are leveraging GenAI for advance malware creation, AI-powered phishing emails, and deepfake generation. AI/ML is being use for brute-force attacks, password guessing and flooding a security system with a multitude of inaccurate positives.[53]

DPDP ACT 2023 TO BOOST SECURITY SPENDING

Compliance with DPDP Act, 2023

DPDP Act 2023 will drive data security and privacy spending in the next few years. Regulatory fines for non-compliance will encourage organizations to ensure compliance with the bill.

- It applies to the processing of digital personal data, collected online and offline, and later digitalized.
- Foreign entities processing personal data to offer goods and services to data principals within India.

Organizations with global businesses, especially in countries with existing data privacy regulations such as the GDPR, California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), Singapore's Personal Data Protection Act, Australia's Privacy Act 1988, and HIPAA, and highly regulated sectors in India such as banking and insurance, will find it easier to comply with the act compared to others.

- According to the United Nations Conference on Trade and Development, 71% of the countries have adopted data protection and privacy regulations.[54]
- Organizations and start-ups catering to Indian organizations must make significant investments to ensure regulatory compliance.

Data protection and privacy offerings, including Data Classification, Privacy Impact Assessment, Privacy by Design, and Data Access Governance, will witness an uptick in adoption in the next five years.

Penalties for Non-compliance

Up to INR
250 Crore
Failure to implement security safeguards for preventing data breach

Up to INR
200 Crore
Failure to notify the board and affected principals of data breach

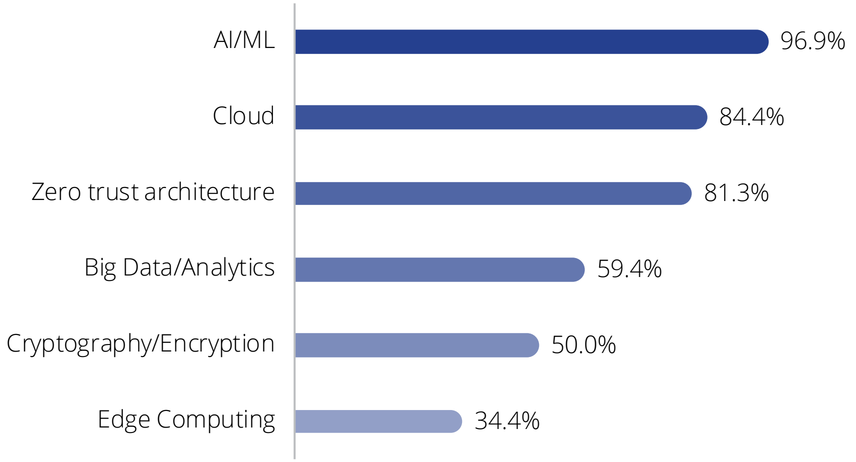
Up to INR
200 Crore
Non-compliance with obligations regarding children's data

Up to INR
150 Crore
Breach of additional obligations by significant data fiduciary

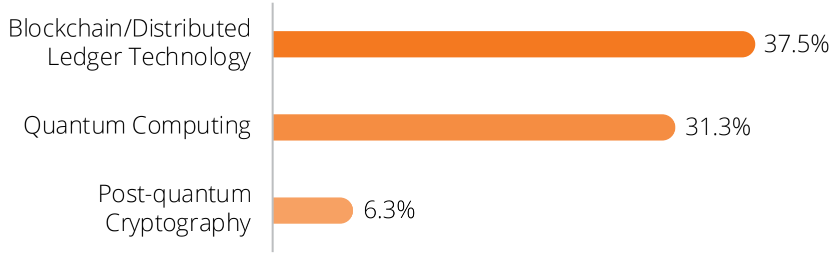
Up to INR
50 Crore
Any other non-compliance penalty

TECHNOLOGY LANDSCAPE

Technologies Leveraged by Organizations



Emerging Technologies to be Leveraged by Organizations



Source – DSCI Survey 2023

Key Drivers

AI/ML and cloud are two areas organizations have invested in or plan to invest in the next two years.

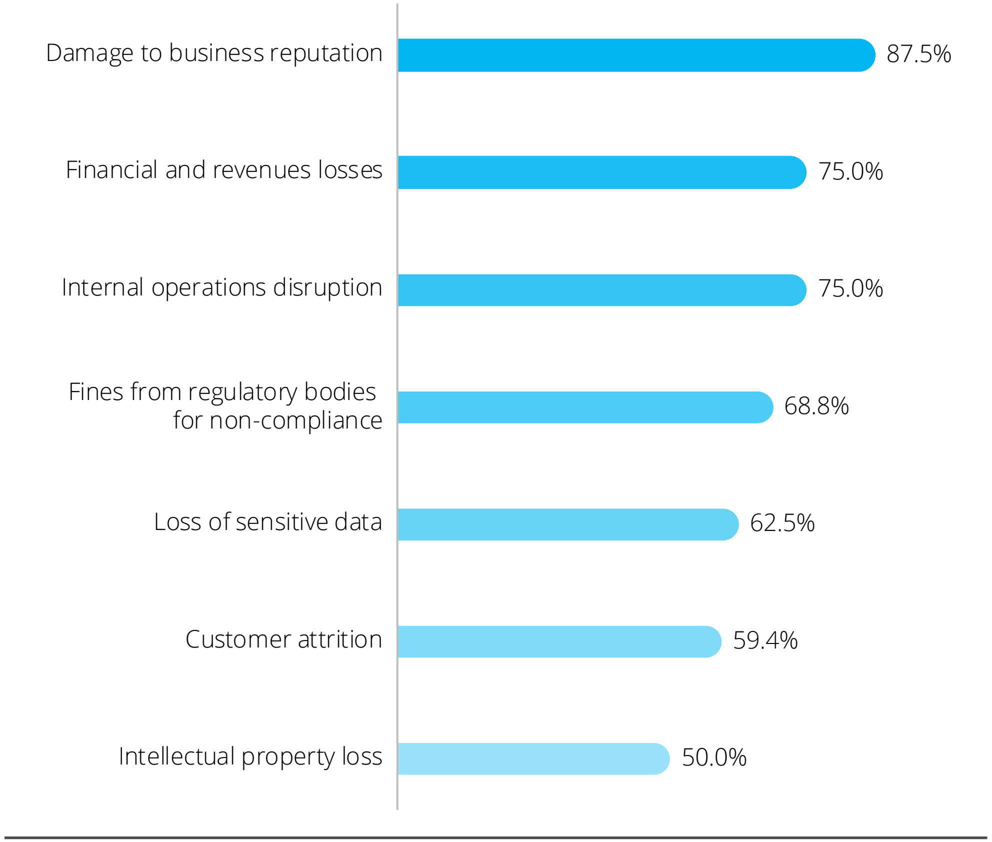
- GenAI has gained significant traction with organizations investing in GenAI to support various functions such as content creation, automating designing, enhancing datasets, drug discovery, and demand forecasting.
- Furthermore, GenAI can be leveraged for anomaly detection, phishing detection, malware detection and analysis, UEBA, password security data protection, and privacy compliance.
- As per a study by Nasscom,[55] between 2021 and May 2023, India GenAI start-ups received USD 475 million in funding.
- Indian government recommended formulating the 'Transparent and Accountable AI and Emerging Technologies Governance Framework' to facilitate responsible use of AI.[56]

Zero trust has emerged as a key area of investment owing to the constantly involving threat landscape.

Organizations are also leveraging big data/analytics to understand the threat landscape better, thereby improving the efficiency of threat detection, response, and mitigation.

Blockchain/Distributed Ledger Technology and quantum computing are gaining prominence as focal points for organizations. They can expedite the analysis and identification of vulnerabilities in cryptographic systems, resistance to tampering or unauthorized alterations, mitigation of the impact of DDoS attacks, and the advancement of quicker and more efficient cryptographic systems.

CYBERATTACK IMPACT



Source – DSCI Survey 2023

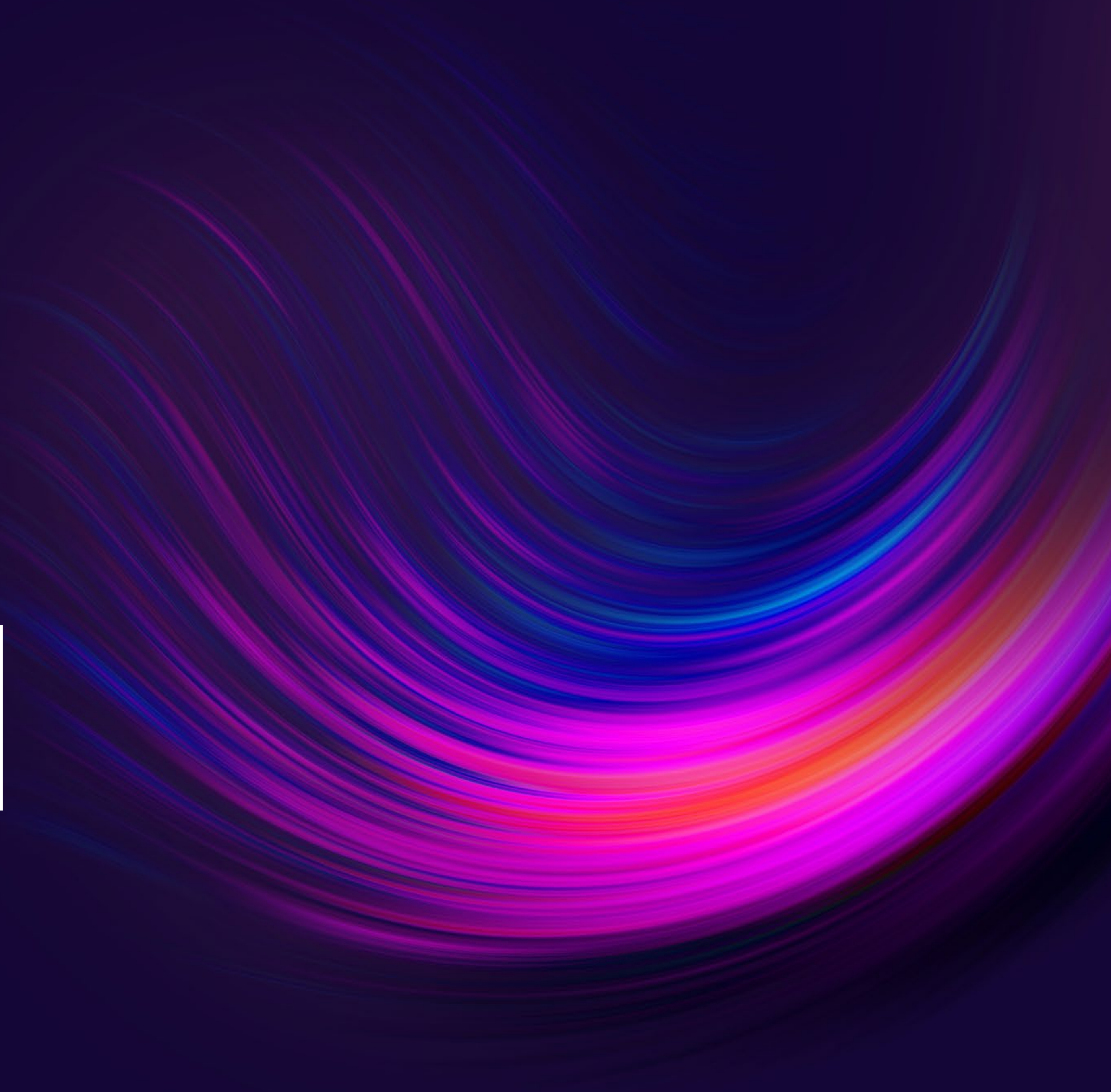
Aftermath Observations

Respondents reported damage to reputation as the significant repercussion of a successful data breach. Negative publicity from the attacks can lead to a loss of stakeholder and customer trust, significantly impacting the organization’s business.

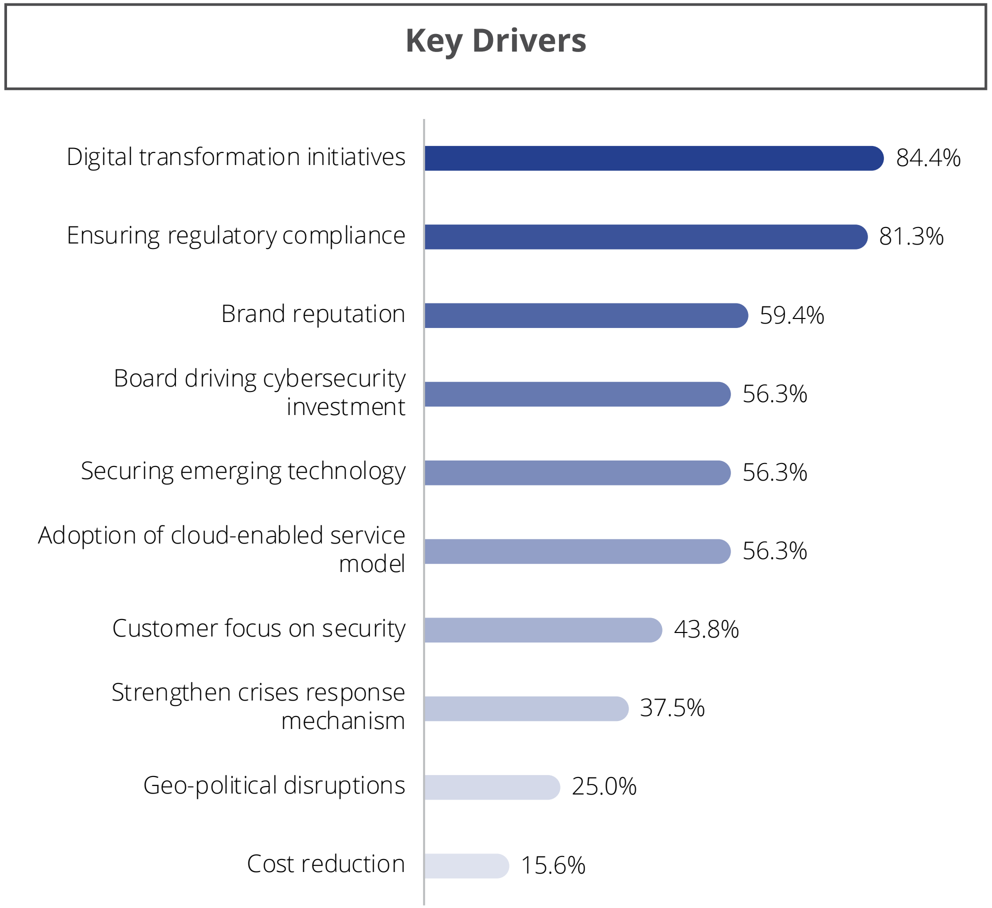
Moreover, the organization may experience enduring consequences, potentially leading to customer hesitancy in utilizing its services and stakeholders expressing apprehension regarding its capability to safeguard sensitive data and assets. Financial and revenue losses, and internal operation disruptions are also a key concern for organizations. Significant fines from regulatory bodies are an essential concern for organizations.

- The changing regulatory environment in India, along with global data protection and privacy laws, have substantially increased the importance of regulatory adherence.
- Failure to comply with the DPDP Act 2023 may result in fines of up to INR 250 crore. These penalties can have a noteworthy effect on an organization’s operations, particularly for those with lower turnovers.
    - Up to INR 200 crore on failure to notify the board and affected principals of data breach.
    - Up to INR 150 crore for breach of additional obligations by significant data fiduciary.

CYBERSECURITY SPENDING DRIVERS



CYBERSECURITY SPENDING DRIVERS



Source – DSCI Survey 2023

The rapid pace of digital transformation, propelled by government initiatives, dynamic startup ecosystem, widespread mobile and internet access, advancements in 5G technology, and the adoption of AI/ML, is fueling increased investment in cybersecurity.

- As per a study by Tenable,[57] owing to adopting emerging technology and cloud services, large Indian organizations, on average, possess 12,000 internet-facing assets susceptible to potential exploitation.

The regulatory framework in India is continuously evolving, with the government, CERT-In, and regulatory entities like RBI and SEBI formulating and issuing new policies, circulars, and directives.

- RBI's Master Direction on IT Governance, Risk, Controls and Assurance Practices, 2023,[58] mandates Vulnerability Assessment bi-annually and Penetration Testing annually and risk assessment of information assets.

Complying with the data residency mandate leads organizations to invest in data security and privacy. RBI's Storage of Payment System Data directive[59], section 94 of The Companies Act, 2013,[60] and IRDAI (Maintenance of Insurance Records) Regulations, 2015,[61] mandate storing specific data like policy issue and claims data, company financials, and payment data.

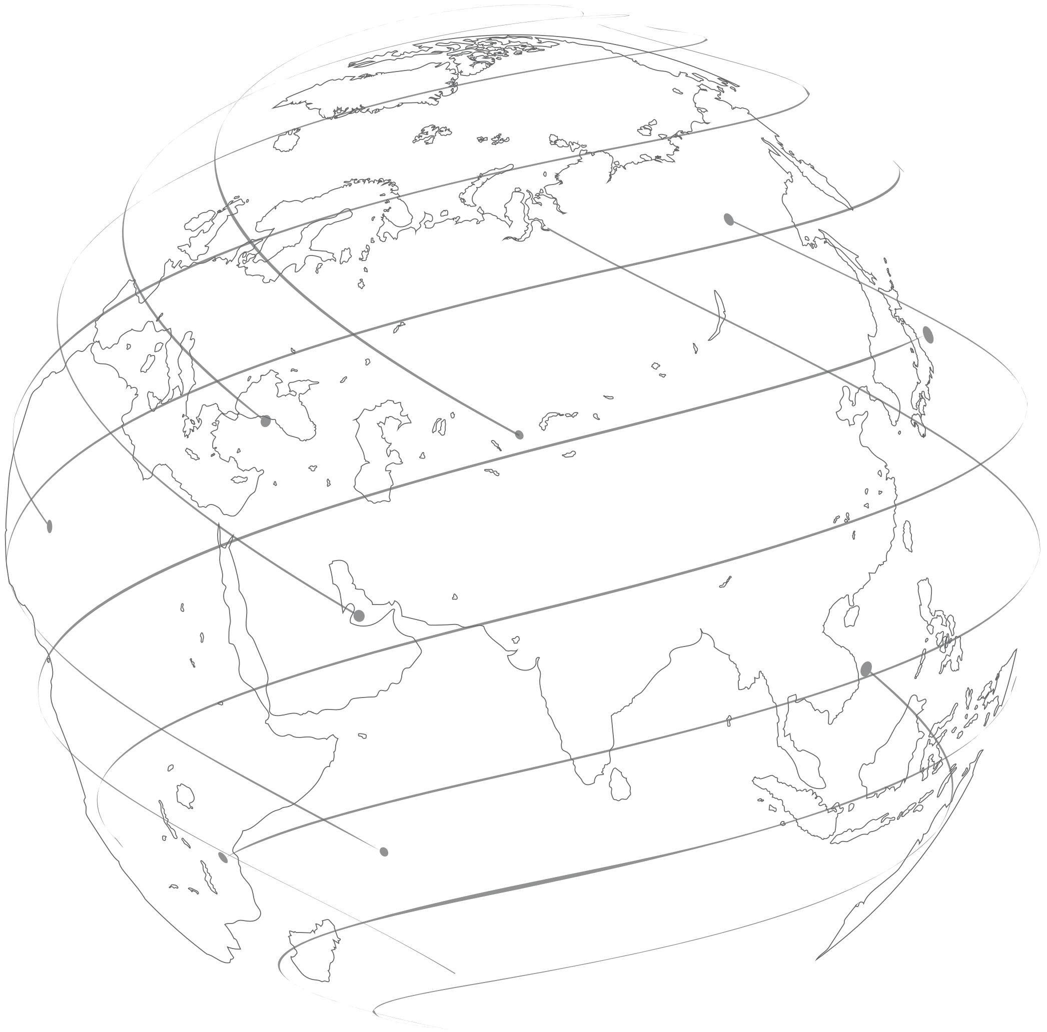
Digital transformation initiatives, regulatory compliance, and brand reputation are the significant cybersecurity spending drivers, as indicated by ~84%, ~81% and ~59% of the analyzed companies, respectively.

Cyberattacks significantly impact brand reputation and lead to customer attrition and financial losses. Consequently, security leaders find it more feasible to secure augmented budgets.

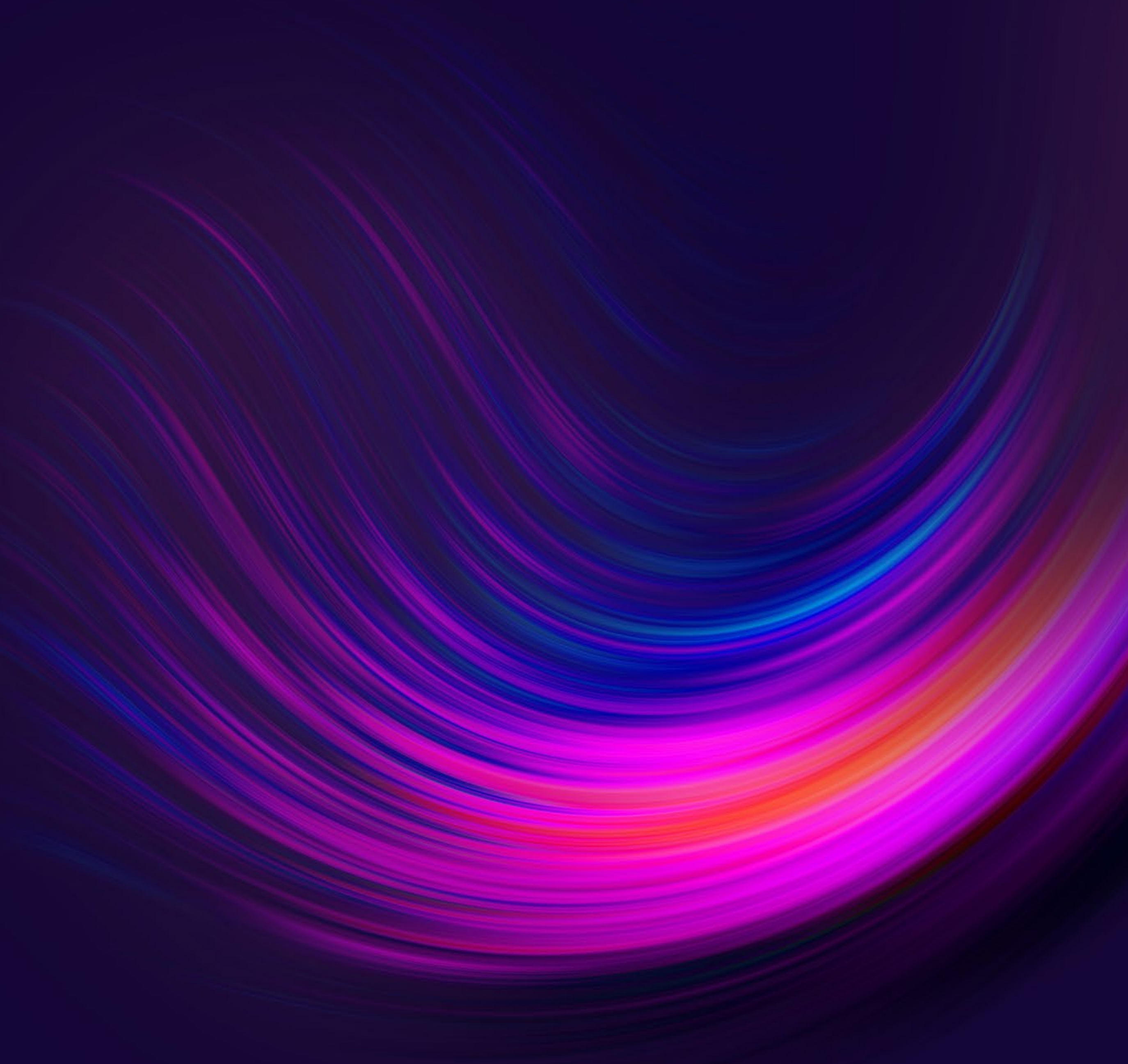
Secure use of advanced technologies such as IoT, AI/ML, GenAI, and edge computing drive companies to invest in security solutions to safeguard them against the ever-evolving threat landscape.

The growing cloud-enabled services model propelled by IT modernization initiatives and focus on digital-first business strategies raises concerns about cloud-related threats. Organizations have acknowledged that securing the cloud is a shared responsibility and are implementing measures to protect their cloud infrastructure.

- As per 2023, Thales Cloud Security Study,[62] 68% businesses in India have over 40% sensitive data on cloud. 35% respondents witnessed data breach on cloud.



CYBERSECURITY CHALLENGES & THREAT LANDSCAPE



CYBERSECURITY CHALLENGES

Talent shortage is one of the biggest challenges end-user organizations face in the country. There is a lack of talent in country, with workforce gap reaching approx. 790k in 2023, which has led to substantial increase in remuneration expectations of skilled cybersecurity professionals.[63]

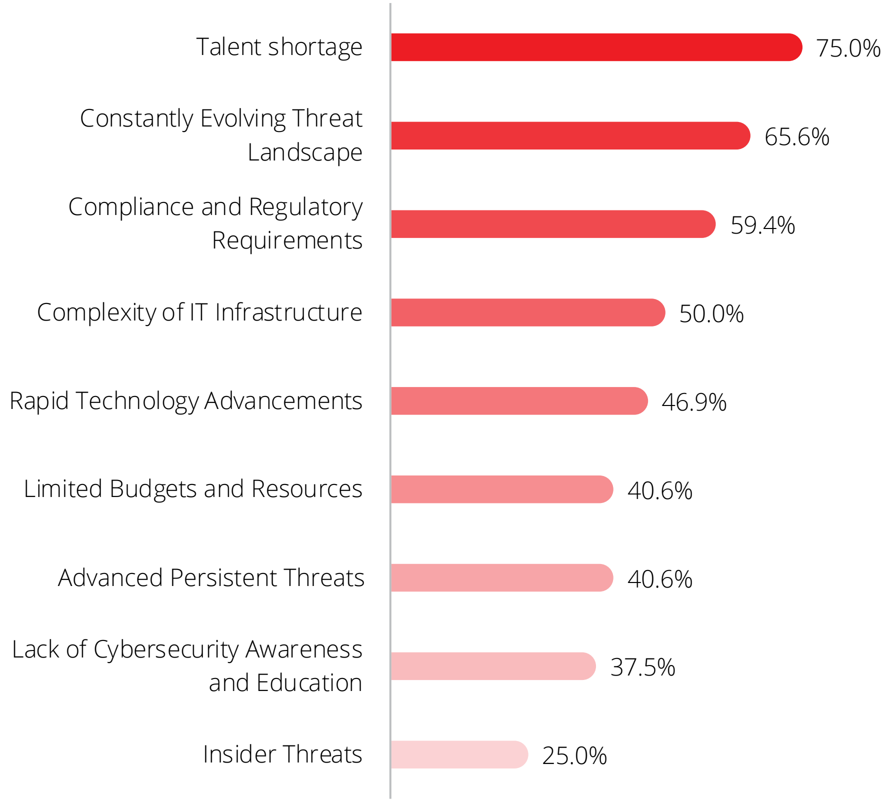
Moreover, substantial remuneration expectations of skilled cybersecurity professionals pose difficulties for organizations with budget constraints in retaining or recruiting them.

The constantly evolving threat landscape remains a crucial worry for end-user organizations. The number of attacks targeting Indian organizations is notably on the rise, with India representing 20% of the 2.29 billion exposures reported in 2022, according to Tenable.[64]

- Additionally, adversaries are employing technologies such as AI and GenAI to enhance the authenticity of phishing attacks and heightened attack frequency.

The proactive approach of the government, ministries, and regulatory bodies to ensure cybersecurity preparedness has led to the need for regulatory compliance and appointment of CISOs. Moreover, organizations must comply with multiple country-specific and global regulations like GDPR.

- In 2021, The Ministry of Power issued the Cybersecurity Guidelines for Power Sector in 2021 aimed at bolstering cybersecurity in the power sector by mandating the implementation of various security controls including access control and authentication.[65]
- In 2020, Department of Telecommunications, Ministry of Communication, published Cybersecurity best practices, recommending enforcing security controls like MFAs, patch management and VAPT.[66]



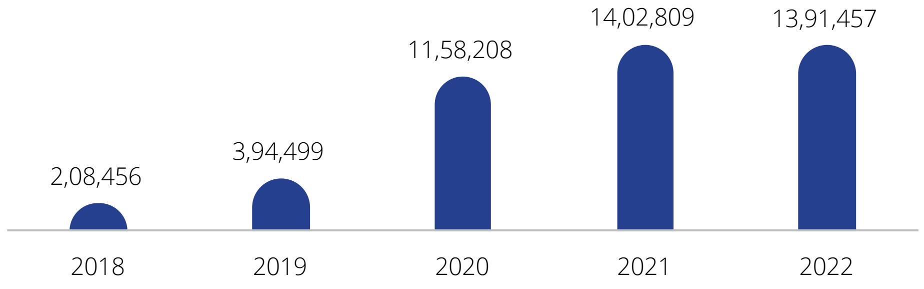
Source – DSCI Survey 2023

CYBERSECURITY THREAT LANDSCAPE

Cyberattack Scenarios

Hardware supply chain attacks	Data exfiltration	Ransomware
State-sponsored attack on critical infrastructure	DDoS	Zero-day exploit
Software supply chain attacks	Business email compromise	Malware
Man-in-the-middle attack	Phishing/ smishing/ vishing	Social engineering
Foreign influence in R&D	URL poisoning	Cryptominer

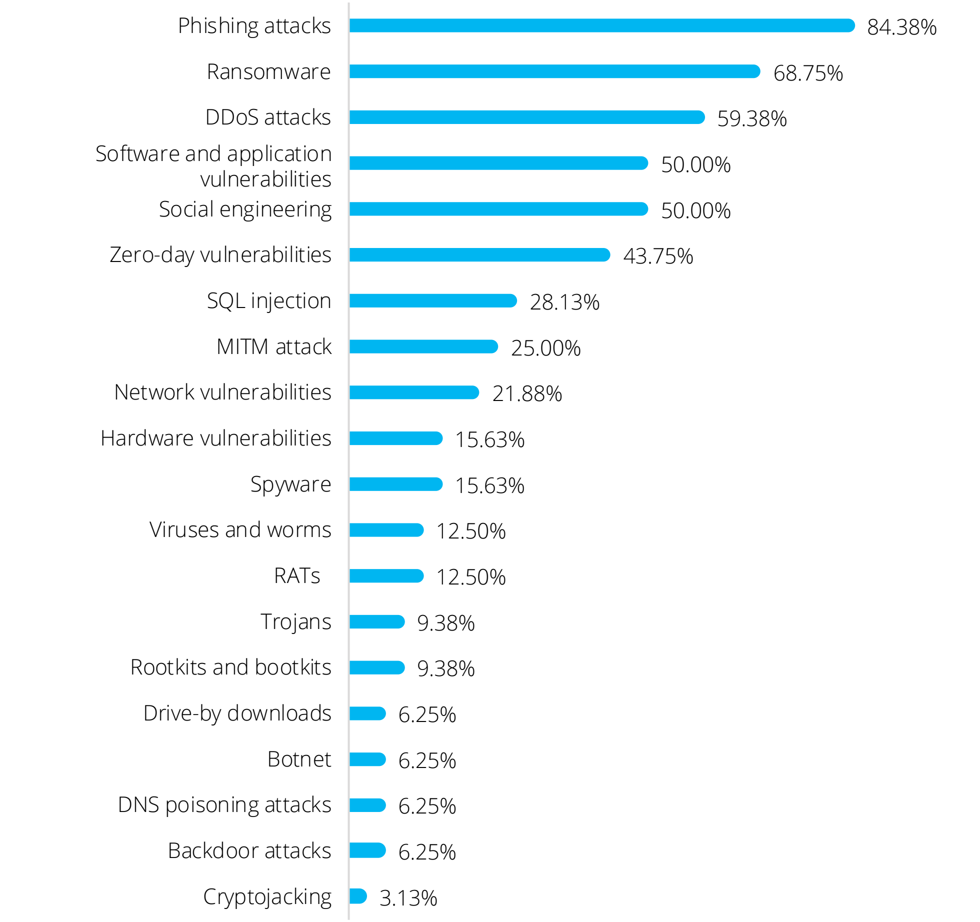
Cyber Security Incidents in India, 2018-2022



Cyber risks have increased as attack surfaces have grown exponentially, predominantly post-COVID-19 pandemic. Cloud services, IT modernization, hybrid workforce, and the Indian Government pushing digital public services are boosting digital assets.

- Cyber security incidents in the country grew by a CAGR of over 60% from 2018 to 2022.[67] From 2018 to June 2023, CERT-In reported 62 and 191 incidents of data leak and data breach, respectively.[68]
- As per SonicWall's 2023 Cyber Threat Report,[69] India ranked 3rd in the number of malware attacks in 2022 and witnessed the most significant volume increase worldwide.

Major Cyber Threats



Source – DSCI Survey 2023

Phishing is a significant concern for most of the end-user organizations in the country. According to Barracuda's 2023 Spear-phishing Trends study,[70] IT teams in Indian organizations receive reports of 15 suspicious emails on a workday, which is 50% higher than the global average.

There has been a significant increase in ransomware attacks, boosted by the emergence of Ransomware-as-a-Service (RaaS). RaaS lowered the entry barriers for threat actors, enabling a broader range of individuals to participate in and contribute to the increasing prevalence of ransomware incidents.

In 2022, there was a 53% surge in ransomware incidents in India compared to 2021. Lockbit, Hive and ALPHV/BlackCat, Black Basta were the prominent ransomware families targeting enterprises in 2022. Medium and small organizations were targeted by Makop and Phobos Ransomware families.[71]

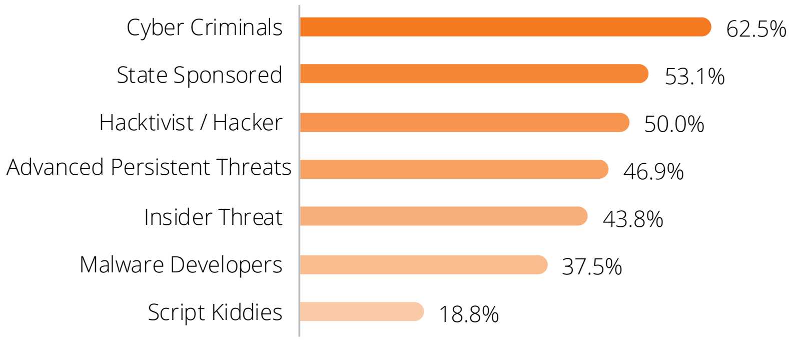
- India accounted for 13.22% of total DDoS attacks, making it the second most targeted nation after the United States, as per the study by Microsoft.[72]
- DDoS exposure fueled by online gaming and an increase in smartphone volume.
- In Q3 2023, 46,000 vulnerabilities were found by Indusface.[73]14,794 critical and high vulnerabilities were open for over 180 days.
- Social engineering attacks led to INR 191 million in losses on an average, positioning it as the costliest attacks vector.[74]

Cyberattack Pathways

Email	90.6%	Third Party and Open-Source Software	71.9%
Web Applications	65.6%	End Point Devices	62.5%
Cloud-based Pathways	59.4%	Software Supply Chain	59.4%
Individuals	53.1%	Mobile Devices	50.0%
Software, OS and Firmware Vulnerabilities	43.8%	Network File Servers	31.3%
Remote Access Portal	31.3%	Firewalls and Switches	28.1%
Network Application Servers	25.0%	IoT Devices	25.0%
Shared Databases and Directories	12.5%	Operational Technology	12.5%

Source - DSCI Survey 2023

Threat Actors

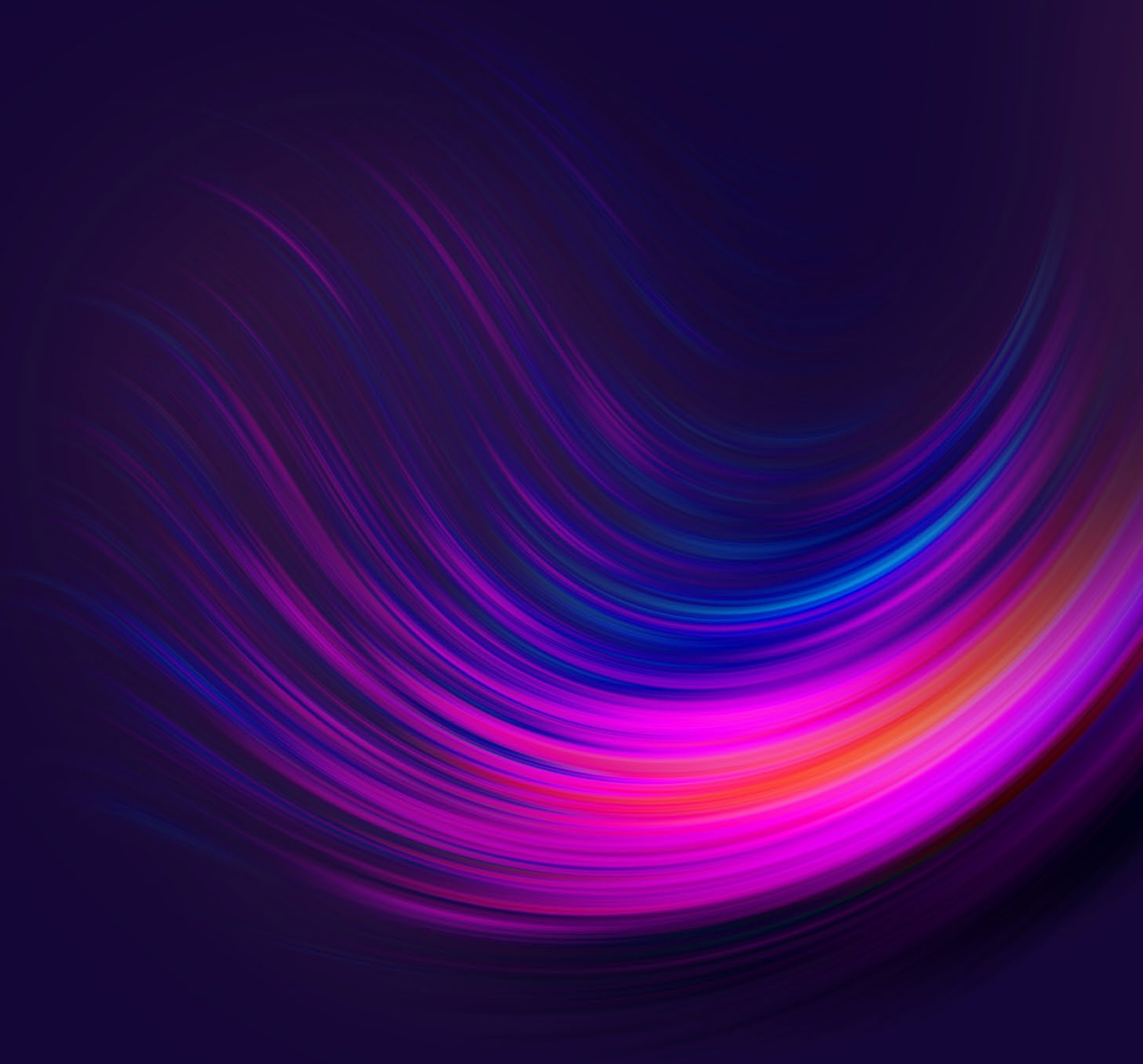


- Emails, third party and open-source softwares, web applications, software supply chain and end points are the pathways majorly being exploited by threat actors to compromise an organizations security posture.
- Cloud-based pathways are also a key concern for end-user organizations due to accelerated adoption of cloud-services.
- AppKnox reported that of the top 100 Indian apps, 75% had critical vulnerabilities, putting business data and customer-sensitive information at risk.[75]
- Successful ransomware attacks have enabled cybercriminals to strengthen their capabilities and increase the effectiveness of their attacks.

Geo-political conflicts are strengthening the intensity of state-sponsored attacks, predominantly targeting critical infrastructure. As per a Cyfirma study, there was a 278% increase in state-sponsored cyberattacks between 2021 and September 2023. Major state-sponsored groups targeting India: Fancy Bear, Turla Group, Lazarus Group and Stone Panda.[76]

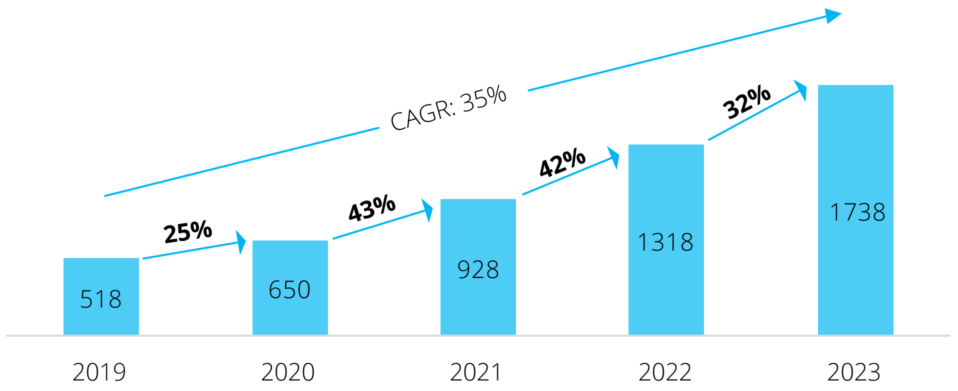
SECTORAL OVERVIEW

Market Analysis



INDIA CYBERSECURITY SPENDING – SECTORAL OVERVIEW

BFSI Cybersecurity Market 2019-2023 (USD million)



BFSI

Accelerated digitalization, adoption of automation, cloud services, AI/ML, and a stringent regulatory landscape led to higher cyber and data security spending in the BFSI sector.

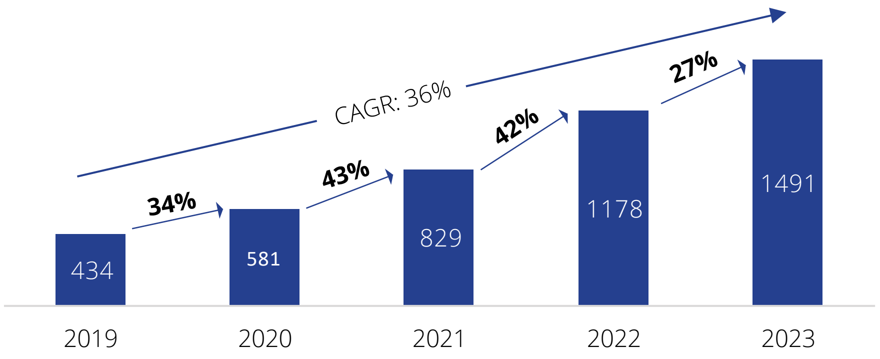
Focus on automation and technology adoption

- Neo-banks and FinTechs like Jupiter, RazorPay, and InstantPay, and the initiatives by Government of India, such as, Digital Banking Units, BHIM-UPI, UPI 123Pay, Aadhaar Payment Bridge, and AePS have bolstered the digital ecosystem.
- Organizations are investing in SOC/Next-gen SOC, security audits and assessments, vulnerability management, CNAPP, network security, and penetration testing to comply with policies, advisories, and guidelines, and to deliver secured customer services.
- Rising use of APIs for account creation, verification, and payment initiation drives API security adoption.
- Phishing remains a critical area of concern. Trend Micro reported the presence of five banking malware families, Elibomi, FakeReward, AxBanker, IcRAT, and IcSpy, employing phishing attacks targeting customers of seven banks in India.[77]

Tightening and granular regulatory compliance

- In November 2023, the RBI introduced the Master Direction on IT Governance, Risk, Controls, and Assurance Practices.[78]
  - This directive mandates regulated entities to establish audit and system logging capabilities for IT applications accessing sensitive data. It further emphasizes the analysis of cyber incidents, including forensic analysis, cryptographic controls, and the adoption of secure, internationally accepted, and published standards.
- In 2023, SEBI launched the Security and Cyber Resilience framework for Portfolio Managers[79] and modified the Stock Exchange's cybersecurity and cyber resilience framework.[80]
- In April 2023, the IRDAI introduced the Information and Cybersecurity Guidelines 2023,[81] establishing distinct standards for regulated entities, considering their degree of access to an insurer's database or systems and gross insurance revenue.

IT/ITeS Cybersecurity Market 2019-2023 (USD million)



IT/ITeS

The IT/ITeS sector is a pivotal contributor India's growth. As of March 2023, its contribution to India's GDP was 7.5%, accounting for 53% of the total export services and 26% of the total FDI in the country. During FY2022-23, the technology industry generate USD 245 billion in revenue, with USD 194 billion in exports. As of March 2023, India is the third largest tech ecosystem with over 27 thousand tech start-ups.[82]

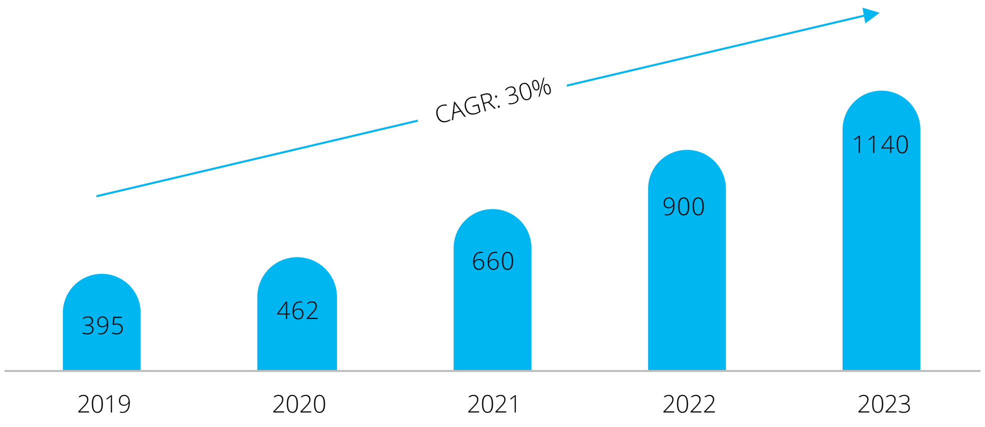
IT/ITeS organizations spend more on security to facilitate integration of advanced technology, such as GenAI, AI/ML, cloud, etc, since they have higher cyber maturity, as organizations collect and process sensitive customer and personal employee data, which they must protect from evolving threat actors.

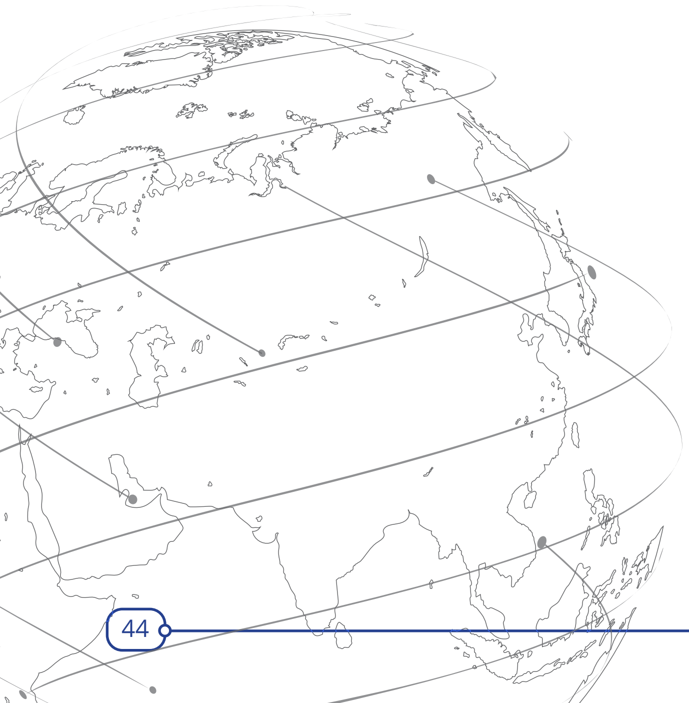
- The pandemic drove remote/hybrid work in the sector, thereby driving the attack surface and the need to secure the expanding digital ecosystem. It also supported growth in cloud adoption, uplifting investment in cloud security.
- According to a nasscom's study, as of March 2023, 36-38% of the 5.4 million workforce in the Indian technology industry was digital.[83]

Growing and Evolving Cyber Threat Landscape

- According to Cyfirma, IT and BPO accounted for 14.3% of the cyberattacks in India.[84]
- AI adoption increases its vulnerability to data breaches and data exposure. It also raises insider threats, as a bad actor can add malicious components to the AI algorithm.
- There has been a significant uptake in GenAI adoption in Indian IT organizations. Their clients are allocating 1-3% of tech budgets to GenAI.[85]
    - Individuals engaging in conversation with GenAI models can share confidential or personal information with the model, increasing privacy risks.

Government and PSUs Cybersecurity Market 2019-2023 (USD million)





Government and PSUs

Cyber activities against Government and PSUs are increasing at an accelerated pace, with state-sponsored threat actors increasingly targeting government agencies.

- Amidst international events hosted in the nation, threat actors increase the intensity of cyberattacks, such as DDoS against government agencies.
- According to a Cyfirma report, government agencies witnessed a 460% increase in cyber-activities between 2021 and September 2023.[86]
- Since the start of the Israel – Hamas conflict on 7 October 2023, there has been a significant increase in state-sponsored cyber activities. Threat actors are targeting critical infrastructure predominantly via web defacement and DDoS operations.[87]
- Furthermore, government agencies and PSUs collect, store, and process citizens' sensitive personal data. It has increased the need to invest in security controls to improve cyber resilience against cyber criminals, APTs, and state-sponsored threat actors. PSUs are actively implementing deploying technologies, including AI and cloud, to deliver services to customers and citizens securely. Therefore, they are investing in security controls to ensure the secure adoption of technology.
- Measure taken by the government to bolster cyber resiliency:
  - 'Guidelines on Information Security Practices' for Government Entities issued by CERT-In in Jun 2023.[88]
  - 74 mock cybersecurity drills, attended by 990 government agencies.[89]

Manufacturing, Power and Oil & Gas

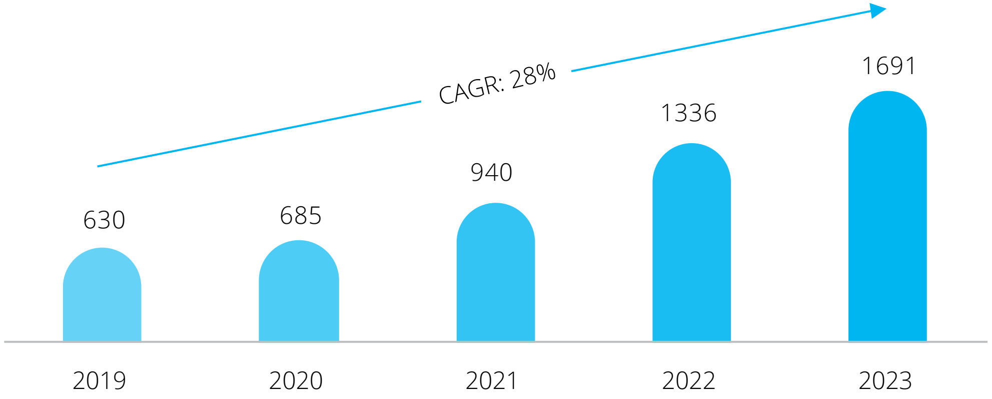
They will witness significant growth as they embrace Industry 4.0 and modernize their IT infrastructure, adopt cloud and IoT technologies.

Convergence of IT and OT will be fueling cybersecurity spending in India.

These sectors are focused on getting their basic security controls such as EDR, XDR, SOC and network firewalls, etc.

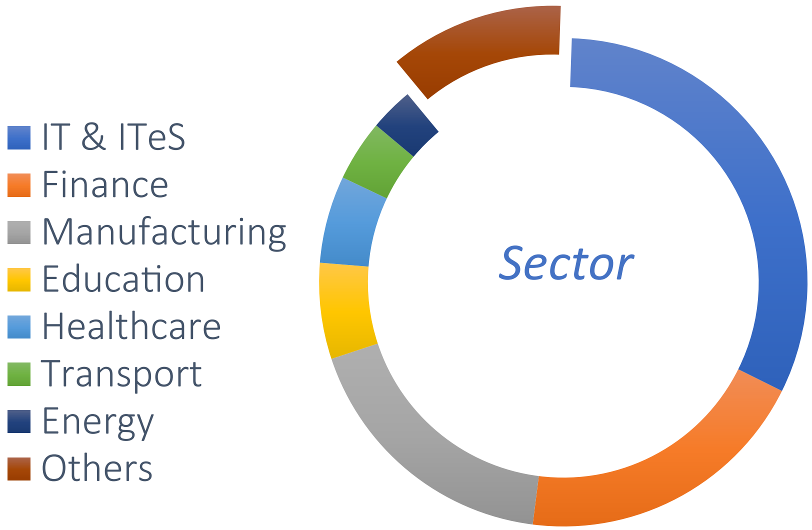
- In February 2023, the government indicated it has approved the National Cybersecurity Reference Framework (NCRF) 2023.[90]
- In 2021, CEA issued ‘Cybersecurity in Power Sector’.[91]
  - It mandates, encompassing the Information Security Division (ISD) led by the CISO, implementation of IDS and IPS for both OT and IT systems, retention of incident cyber logs and cyber forensic records for 90 days, and the formulation of a comprehensive Cybersecurity policy.
  - Establish a matrix showcasing IT and OT cyber risks and define risk acceptance criteria as part of the Cyber Risk Assessment and Mitigation Plan.
- Six sectoral CERTs established by the Ministry of Power, named Thermal, Hydro, Transmission, Grid Operation, Renewable Energy and Distribution.

Other Sectors Cybersecurity Market 2019-2023 (USD million)

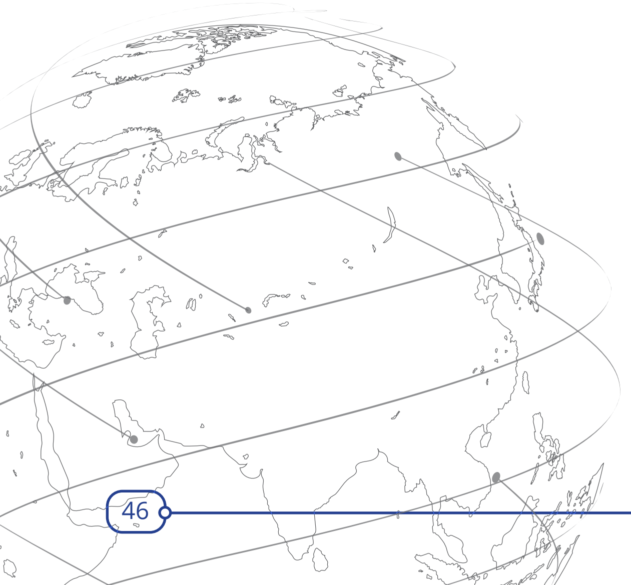


Cybersecurity spending in other sectors grew cumulatively at a CAGR of 28% during 2019-2023 to USD 1.7 billion. Manufacturing, healthcare, and pharmaceuticals are emerging as high-potential markets for cybersecurity organizations.

India Ransomware Incidents, by Sector, 2022



Source –CERT-In India Ransomware Report 2022



Healthcare and Pharmaceuticals

The COVID-19 pandemic pushed healthcare providers to invest substantially in digital resources, enhancing patient experiences, Health Information Systems (HIS), and enabling remote service delivery. Now, driven by the cost and operational advantages of digital transformation, healthcare and pharmaceutical organizations are intensifying their embrace of technologies such as AI/ML and IoT, along with increased utilization of digital data.

Earlier, the sector needed to catch up in cloud adoption. However, the pandemic, cost-efficiency, and remote access to patient data and medical records pushed cloud adoption, with smaller and single-location hospitals shifting the non-core workload to the cloud and investing in BCP, disaster recovery, and data backup. Large hospitals are moving their critical functions to the cloud, driving spending on cloud security.

The emphasis has pivoted to the security of enterprise assets, intellectual properties, as well as the data of patients and employees, spanning both on-premise and cloud environments.

According to a report by DSCI and Deloitte,[92] pharmaceutical companies are embracing Industry 4.0 on the factory floor, emphasizing digital transformation in manufacturing, launch/commercialization, and supply chain processes.

The focus is on cloud, automation, data analytics, and AI/ML adoption.

Accelerated digitalization has driven ransomware attacks against the sector.

Communication, Media and Telecom

Telecom is a critical infrastructure supporting the growth of the country. 5G and ongoing work on 6G implementation has led to significant traction in technology adoption, including AR/VR, AI/ML, and IoT.

The rapid adoption of the OTT ecosystem and the evolving regulatory landscape further increase the need to secure the ecosystem from threat actors.

- In 2018, TRAI published recommendations on 'Privacy, Security, and Ownership of Data in the Telecom Sector.'[93]

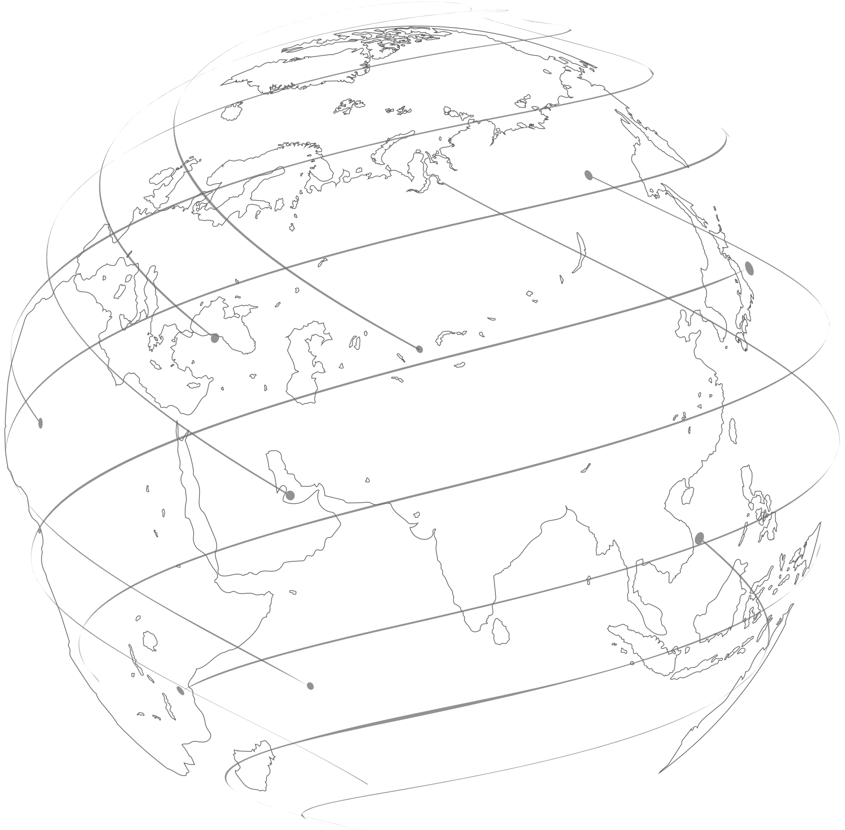
Digitalization and rising threats have led to investment in the Zero Trust model, encryption, MFA, incident response plans, employee training, and threat intelligence.

Companies are spending to achieve regulatory compliance.

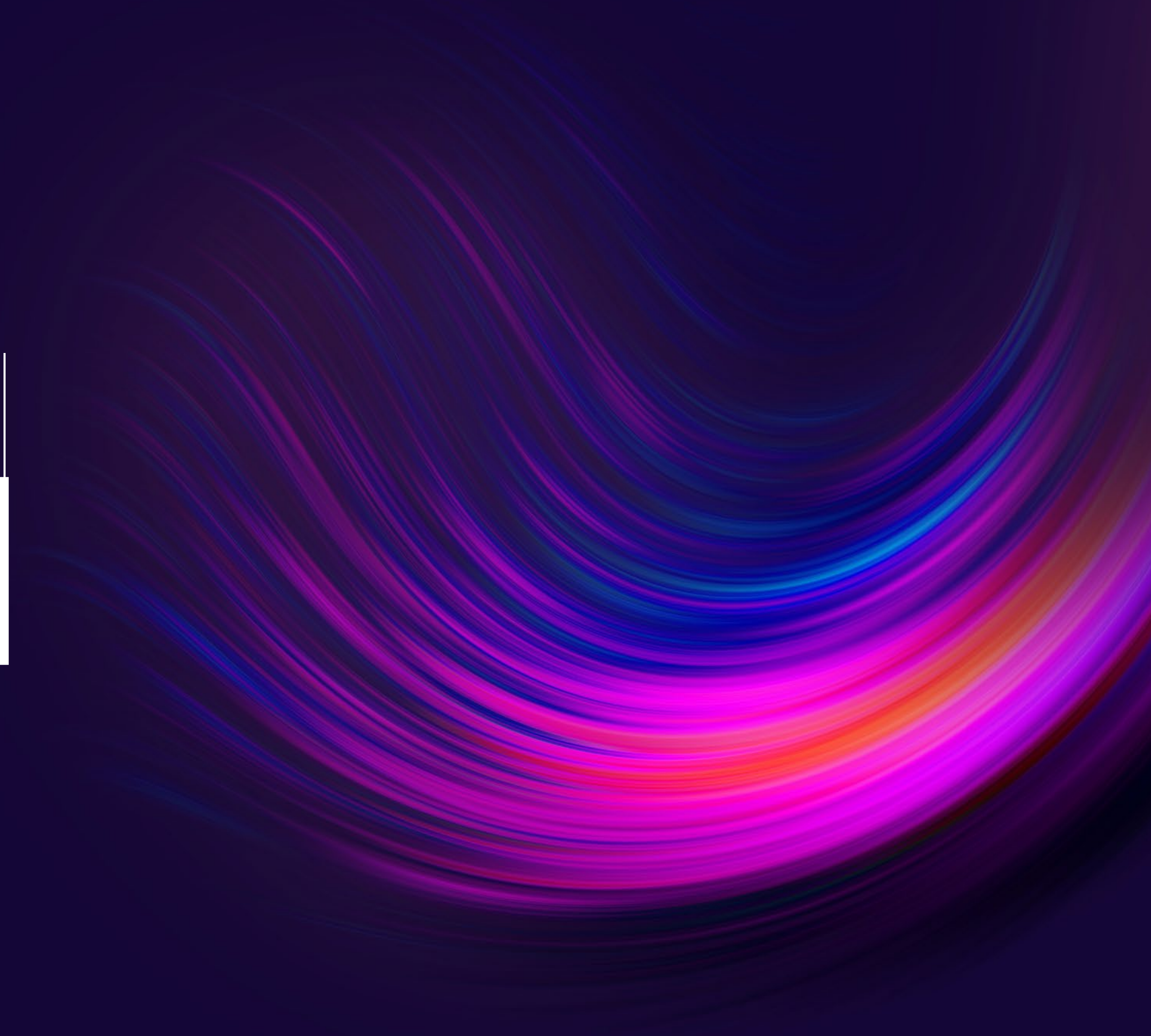
Threats against the telecom sector will increase as successful attacks against telecom infrastructure can significantly impact the country.

- Insider threats, social engineering, service misconfigurations, malware, phishing, third-party vendors, DDoS, and IoT are the significant challenges in the telecom sector phases.
- Cyberattacks have increased against global telecom companies, indicating rising risk against telecom infrastructure in India.
- Content Piracy, Ransomware, Phishing, and DDoS are the major threats faced by India's Communication and Media sector.

Digitalization and rising threats have led to investment in the Zero Trust model, encryption, MFA, incident response plans, employee training, and threat intelligence.

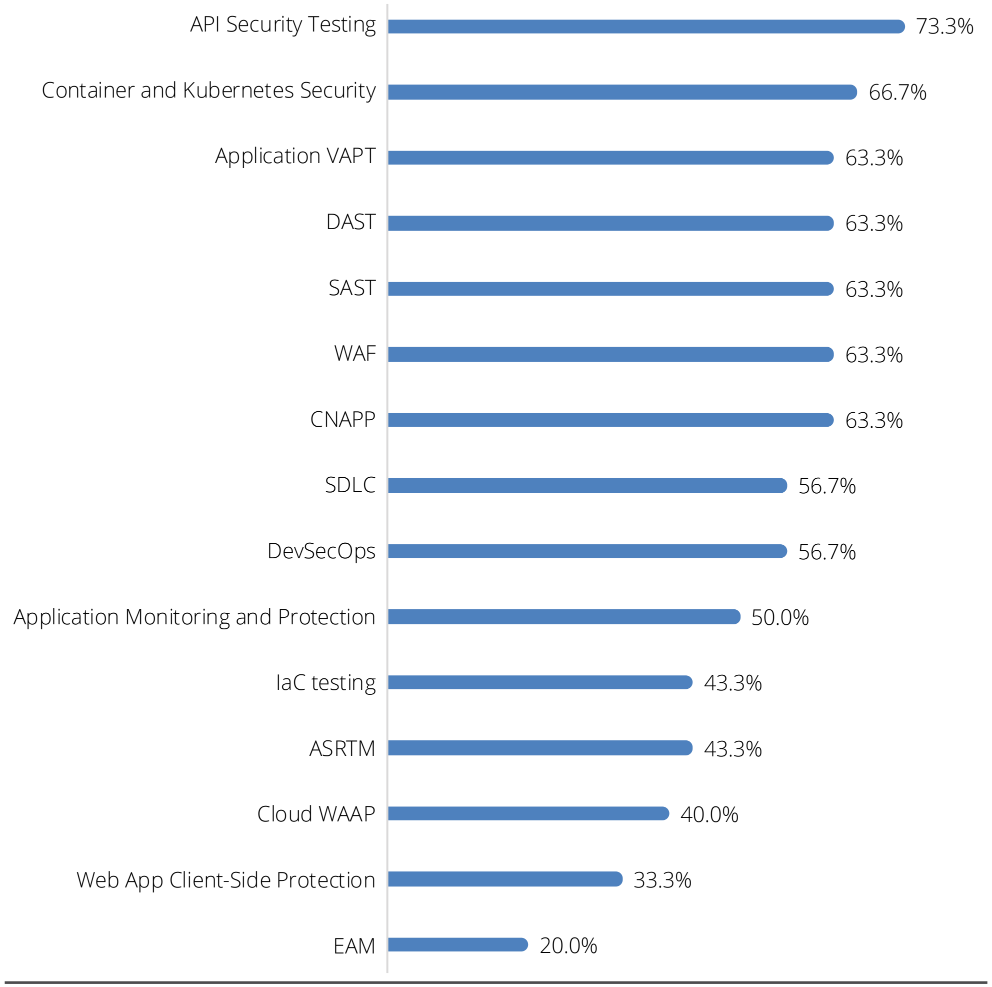


PRODUCT MARKET ANALYSIS



APPLICATION SECURITY

Application Security Offerings in Demand



Source - DSCI Survey 2023

Demand for API security is driving increased deployment of API across industries, including BFSI, healthcare, utilities, and government.

- In 2020, to promote the use of APIs, MeitY launched API Setu to encourage innovation and the sharing of reliable information.[94]

Container and Kubernetes Security and CNAPP adoption is driven by the accelerated adoption of cloud services in India.

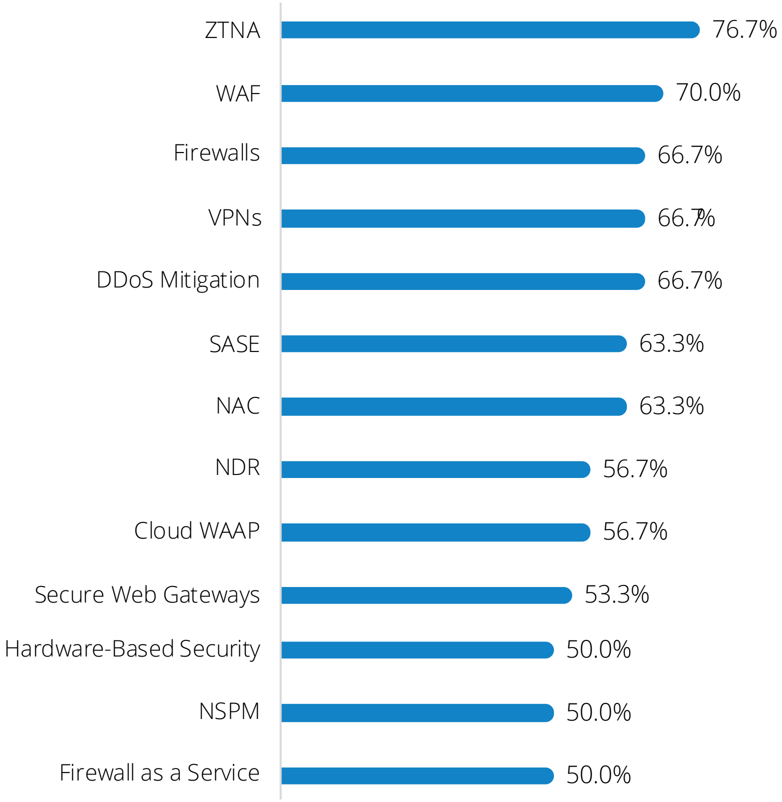
WAF and application security testing (DAST, SAST, and IaC) are driven by the need to protect applications during and after development.

The need to create high-quality, secure software has been the critical impetus driving organizations to invest in Secure Software Development Lifecycle (SDLC) and DevSecOps.

API security testing and Container and Kubernetes security are the key application security offerings. ~73% and ~67% of the analyzed organizations have invested in or plan to invest in the next two years.

NETWORK SECURITY

NetworkSecurity Offerings in Demand



Source - DSCI Survey 2023

The focus has shifted to offerings, including ZTNA and SASE, from traditional security options like Firewalls, NAC, WAF, and VPNs.

The increasing volume of DDoS attacks has driven strong demand for DDoS Mitigation.

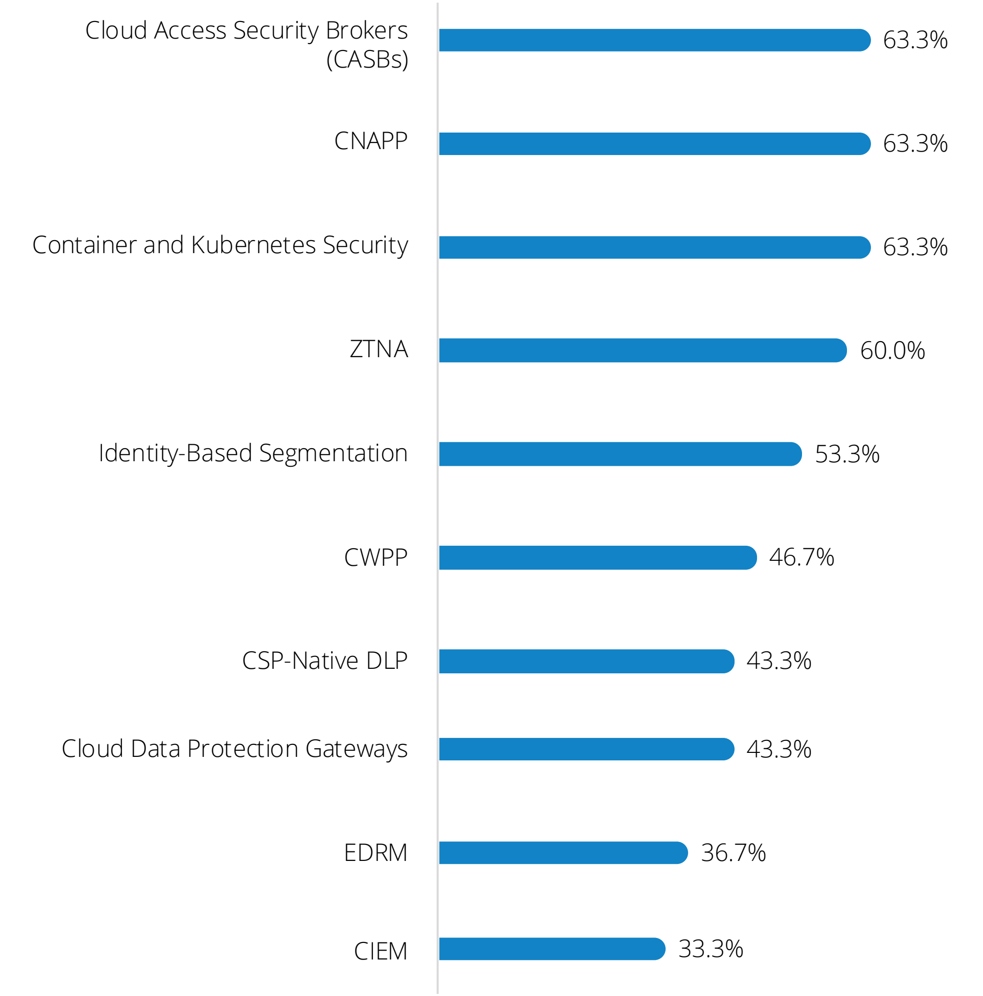
- 60% of the respondents indicated DDoS attacks as a critical concern for their organization’s cyber resilience.

CERT-In’s 2023 guidelines for Government Entities non-uniform highlighted essential controls, including NDR, Firewalls, DDoS Mitigation, and NAC for securing the network.[95]

It also encourages entities to implement Zero trust architecture in addition to the Defense-in-Depth approach.

CLOUD SECURITY

Cloud Security Offerings in Demand



Source - DSCI Survey 2023

Cloud security has witnessed the highest growth in the last three years due to an increasing adoption of cloud services. Organizations have been investing in cloud security to protect their workload, applications, and data.

59% of respondents indicated cloud-based pathways as a critical cyberattack pathway.

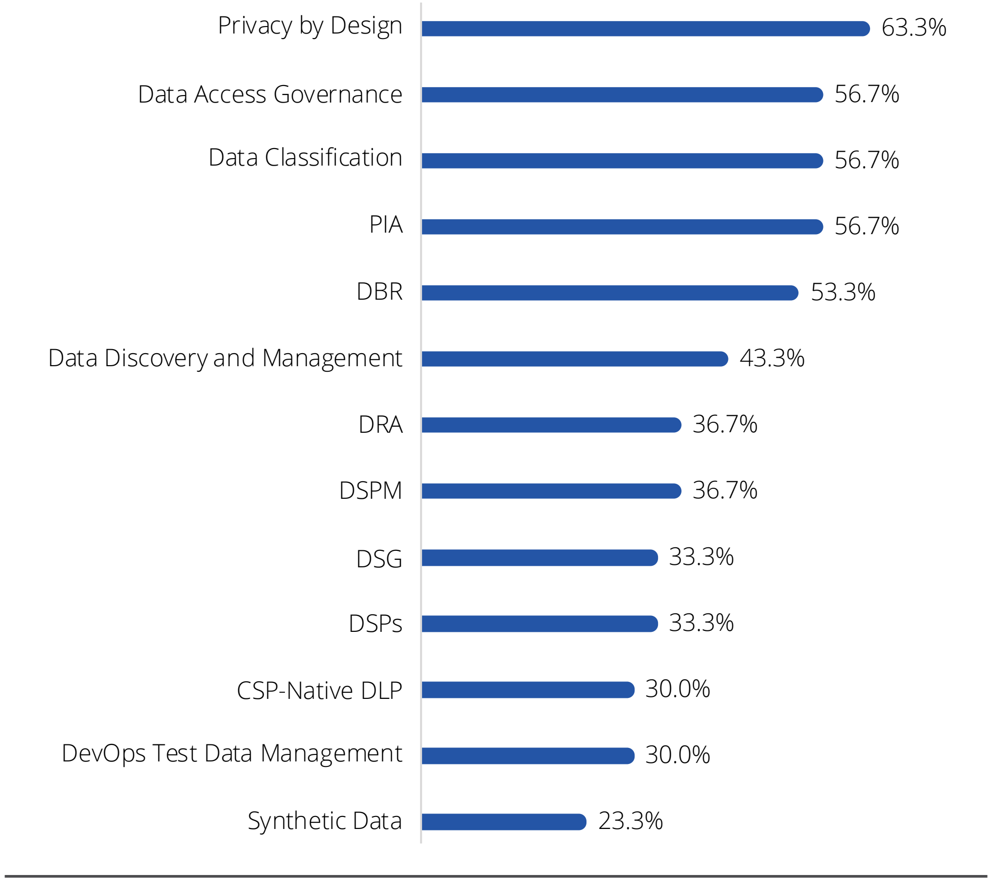
The shared security model of the cloud is leading organizations to protect cloud-based assets from unauthorized user access, malware, and DDoS attacks, as well as mitigate the risk of cloud misconfigurations and insecure interfaces.

CASB, CNAPP, container and Kubernetes security, and ZTNA are offerings organizations are looking to invest in to secure their cloud applications and infrastructure ecosystem.

Cloud adoption has increased substantially in India leading to rising demand for cloud security services. ~63% of the surveyed organizations have invested or plan to invest in CASBs, CNAPP, and Container and Kubernetes Security in the next two years.

DATA SECURITY

Data Security Offerings in Demand



Source – DSCI Survey 2023

Organizations have recognized that data security is pivotal to overall cyber resilience. To uplift data security, they invest in security offerings such as Privacy by Design, Data Access Governance, Data Classification, PIA, and DBR.

DPDP Act 2023 will become a facilitator for the data security offerings in India.

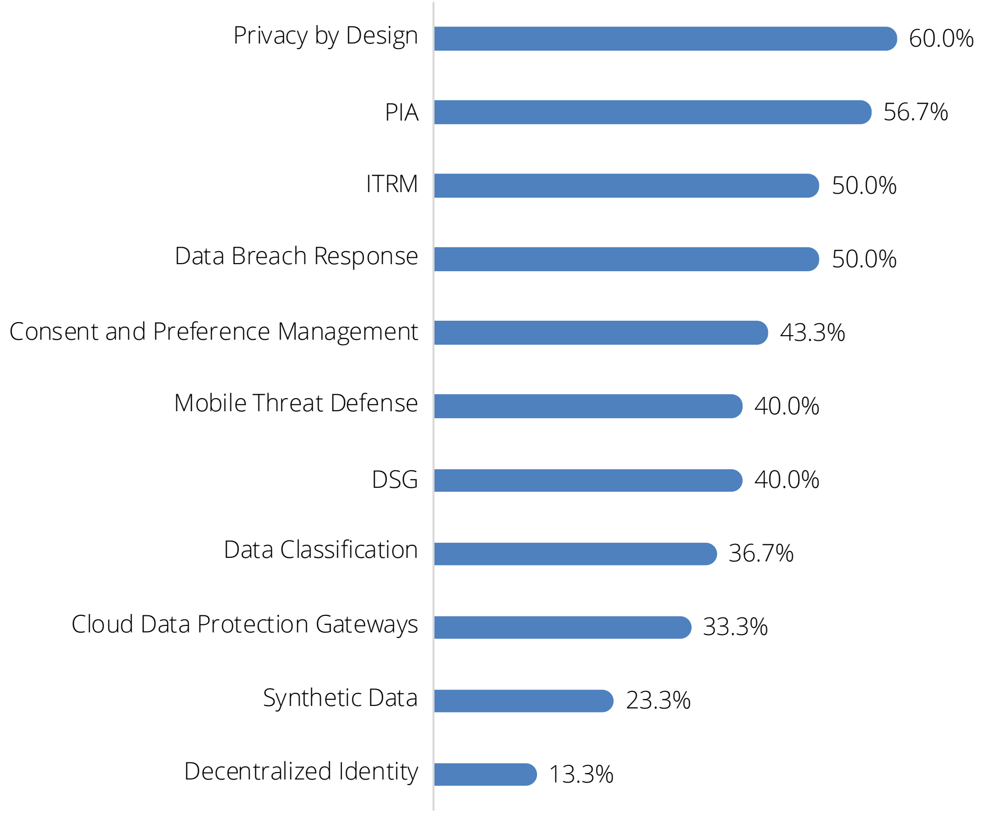
Global regulations, such as GDPR and HIPAA, and regulated sectors in India, such as banking and insurance, have adopted offerings such as Data Access Governance, Privacy by Design, and PIA.

Rising volume of data breaches is also encouraging organizations to invest in data security offerings to safeguard their sensitive data.

- As per Surfshark, from January – October 2023, 4,533,301 personal data breaches were reported in the country.[96]

PRIVACY

Privacy Offerings in Demand



Source - DSCI Survey 2023

Privacy has started gaining traction in the country and is expected to grow significantly in the next five years.

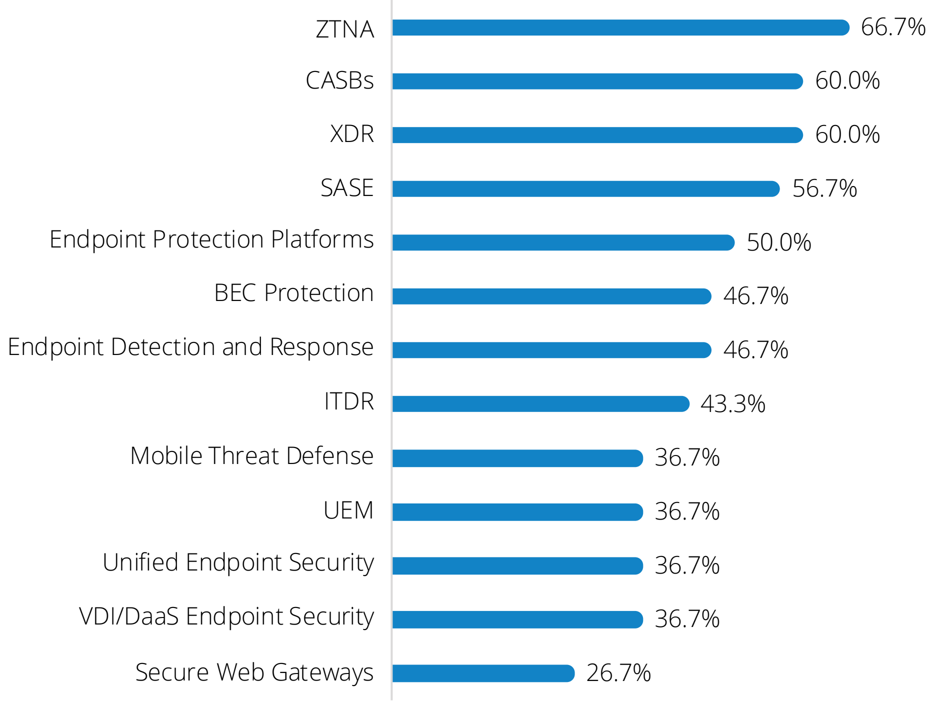
National regulations, policies, guidelines, and frameworks, including the DPDP Act 2023, and global regulations, such as GDPR and HIPAA, are significant drivers for privacy offerings in India. Compliance with international information security and privacy standards, including ISO 27001 and the NIST privacy framework also supports the market growth.

A significant increase in the awareness around importance of personal and sensitive information among organizations and individuals, and the financial impact on brand reputation further drives organizations to invest in privacy offerings.

DPDP Act 2023 will drive spending on privacy offerings in the next few years. Regulatory fines for non-compliance will encourage organizations to ensure compliance with the bill.

ENDPOINT SECURITY

Endpoint Security Offerings in Demand

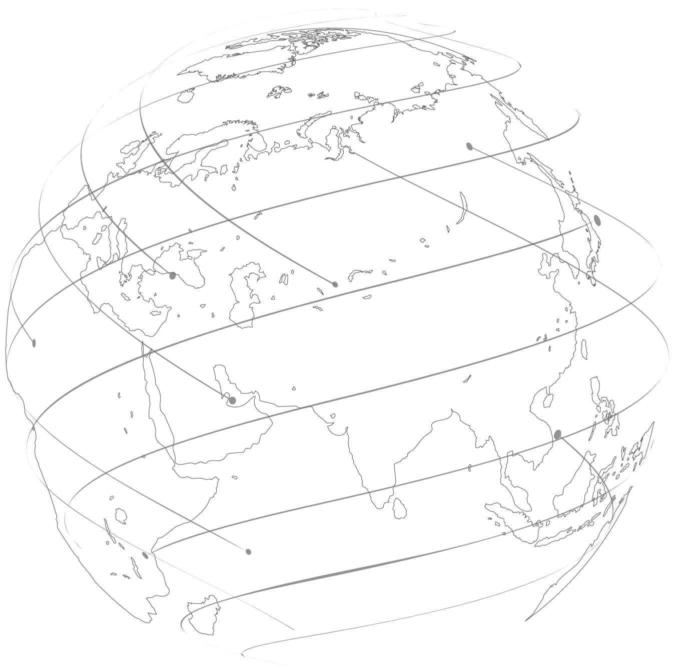


Source - DSCI Survey 2023

Remote work trends, cloud adoption, and Bring Your Own Device (BYOD) work culture have increased the number of attack surfaces an organization needs to secure to protect its ecosystem and uplift its cyber resiliency.

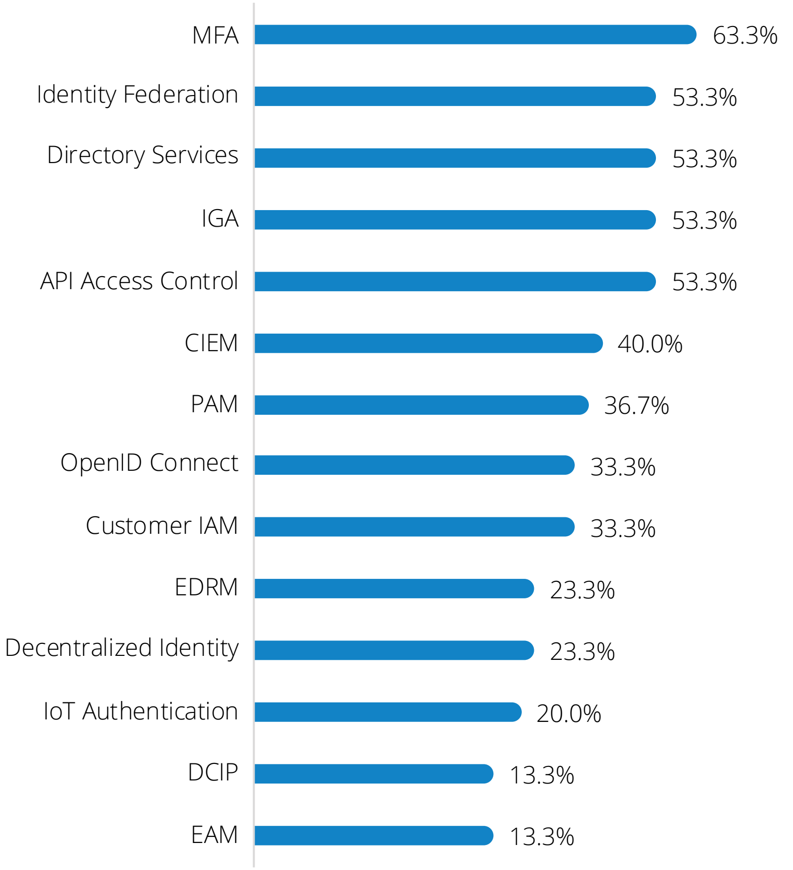
Threat actors are focusing on email, endpoint devices and mobile device, identified by 90%, 62.5% and 50% of respondents, respectively, as significant pathways for cyberattacks.

Organizations are either in the process of implementing or planning to adopt ZTAN, CASBs, XDR, SASE, and Endpoint Protection Platform to enhance the resilience of their endpoint devices.



IDENTITY AND ACCESS MANAGEMENT

IAM Offerings in Demand



Source – DSCI Survey 2023

Need to ensure the management of user authentication and access, as well as secure digital identities, is driving the need for IAM offerings in India.

Regulatory compliance mandates IAM adoption for securing sensitive information and management of data.

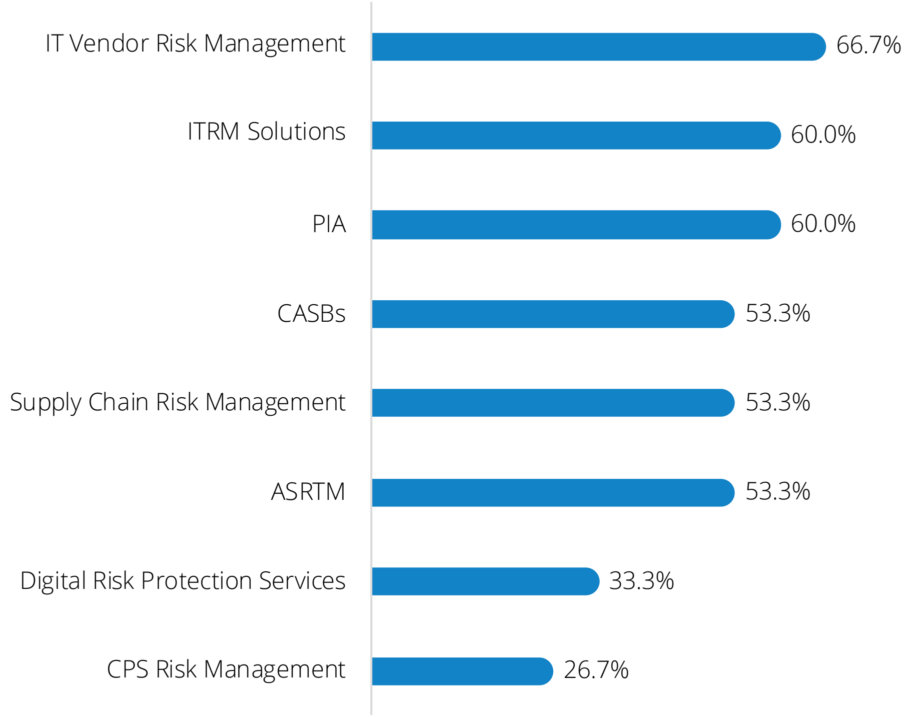
- RBI's Draft Master Directions on Cyber Resilience and Digital Payment Security Controls for Payment System Operators[97] will mandate deployment of controls, policies and procedures, the use of MFAs for admirative and privilege access.
- CERT-In's Guidelines on Information Security Practices for Government Entities[98] encourages the use of MFAs for authentication access management.

Sectors, including banking, IT/ITeS, and healthcare, invest in IAM to protect sensitive data from unauthorized access, thereby reducing data breach risks.

MFA, identity federation, directory services, IGA, PAM and API access governance are gaining traction in India.

RISK MANAGEMENT

Risk Management Offerings in Demand



Source - DSCI Survey 2023

Third-party and open-source software vulnerabilities and attack on software supply chain are the crucial factors driving the need for investing in risk management offerings.

- Threat actors are focusing on third-party and open-source vulnerabilities and software supply chain, identified by 71.9%, and 59.4% of respondents, respectively, as significant pathways for cyberattacks.

The potential impact of cyberattacks on vital infrastructure, including power grids, transportation systems, and healthcare facilities, is significant.

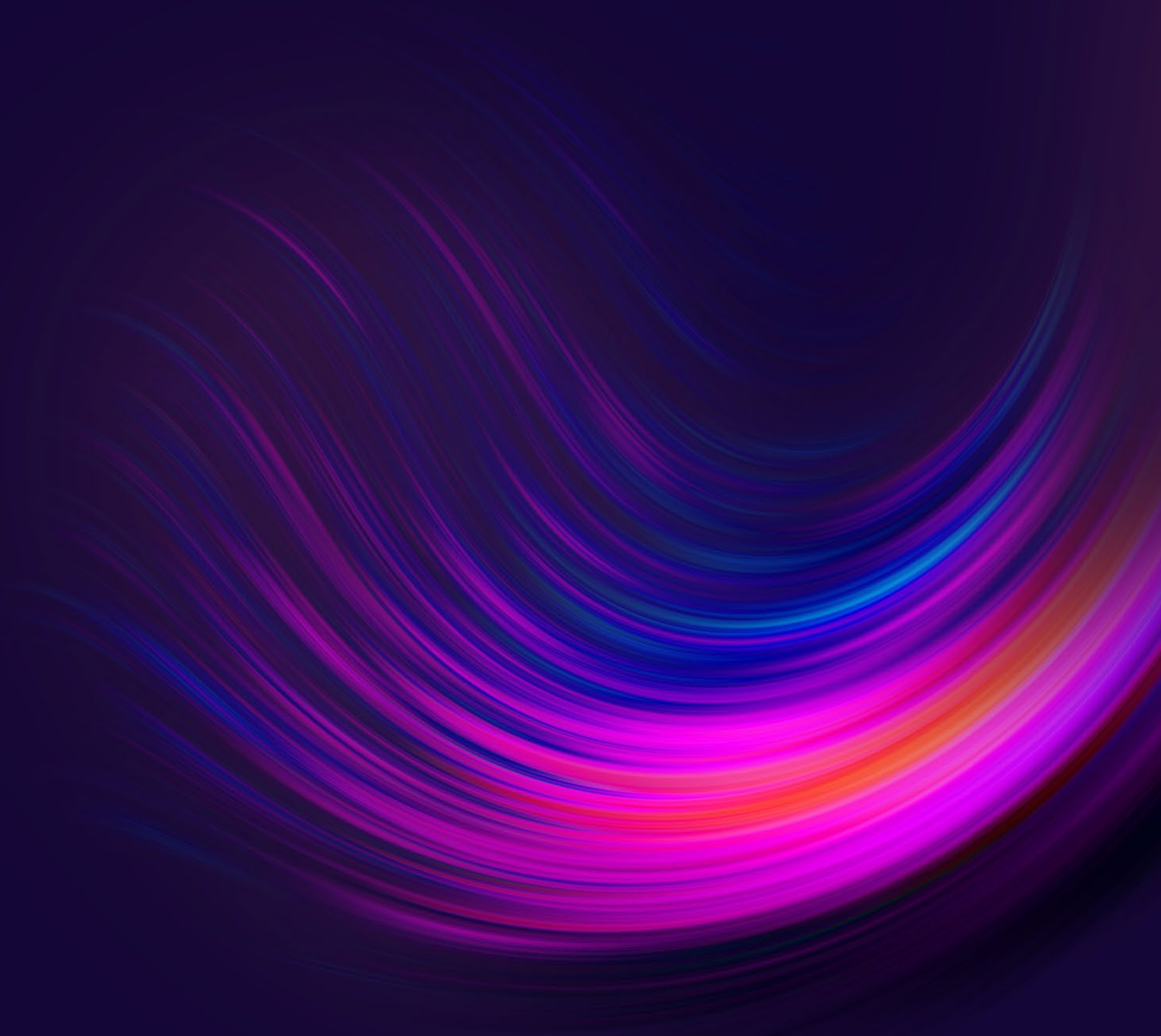
Effective management of cyber risks is imperative to protect and ensure the security of these essential services.

Safeguarding this sensitive data from theft, unauthorized access, and cyber threats necessitates implementing essential cyber risk management measures.

IT vendor risk management, ITRM solutions, PIA, CASBs, ASRTM, and supply chain risk management are expected to grow in the next two years.

SECURITY SERVICES

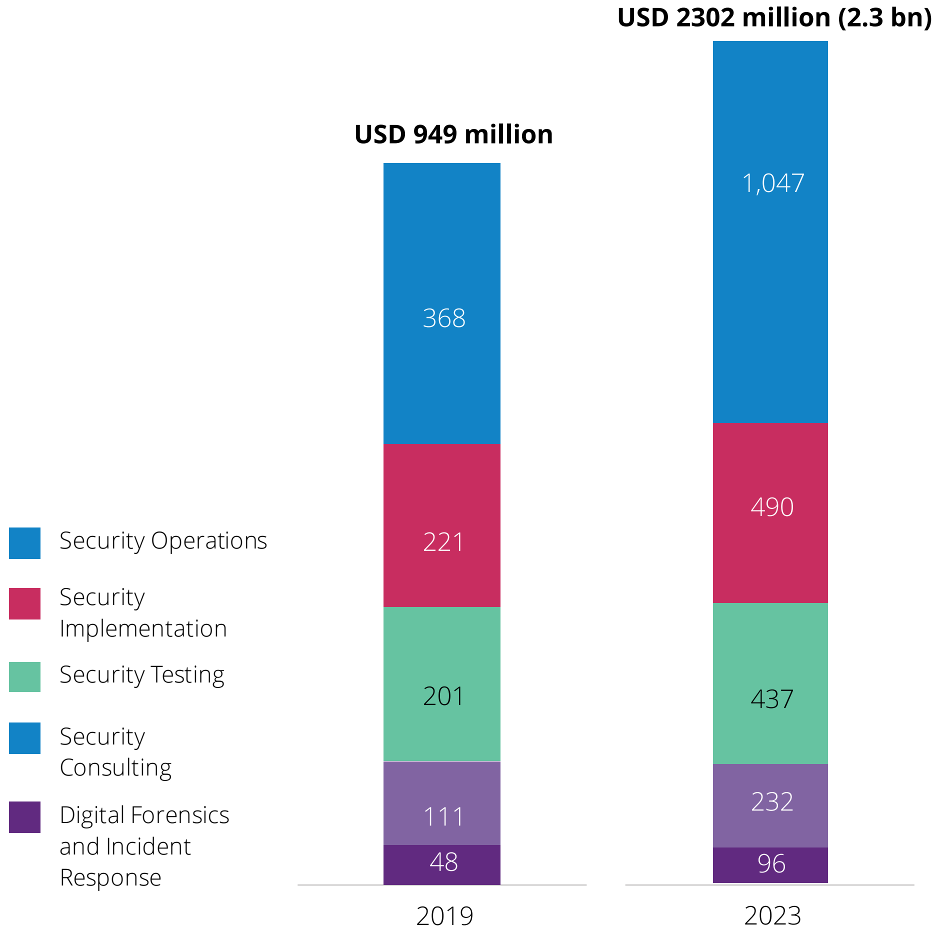
Market Overview



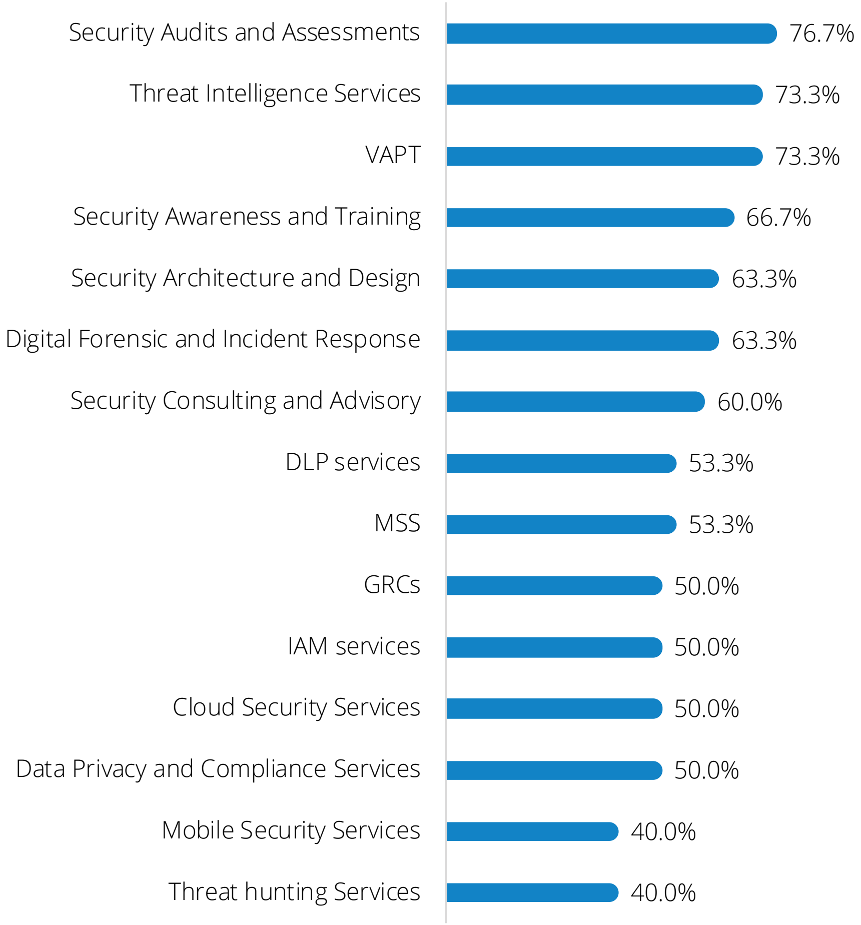
LEADING SECURITY SERVICES

AUDIT & ASSESSMENT, THREAT INTELLIGENCE, and VAPT

India Cybersecurity Services Market (USD million)



Security Services Offerings in Demand



Source - DSCI Survey 2023

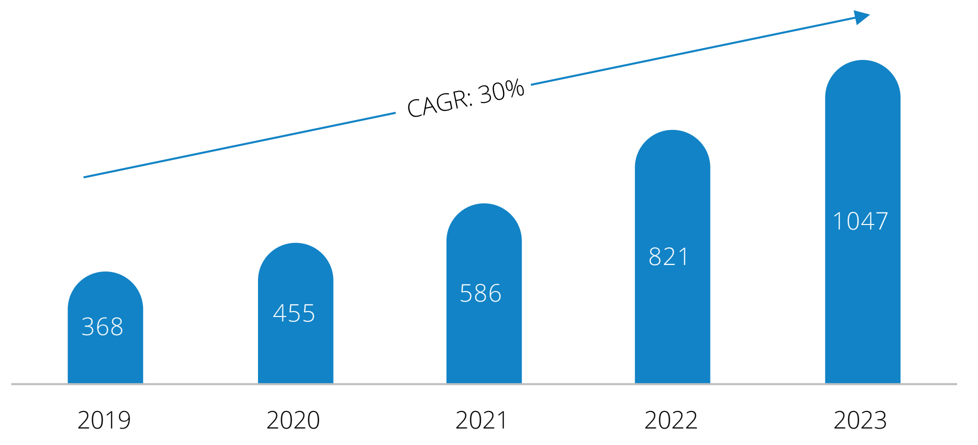
INDIA CYBERSECURITY SPENDING – SERVICES OVERVIEW

Security Operations

Security operations services involve managing and monitoring the configuration and health of security devices. In 2023, it accounted for the highest share in the cybersecurity services segment.

- 73.3% of respondents have invested or plan to invest in threat intelligence services.
- The evolving threat landscape, including APT, supply-chain attacks, zero-day vulnerabilities, OT and IoT vulnerabilities, deepfakes and the expanding attacks surface, resulting from accelerated digital transformation initiatives and hybrid working due to the pandemic, led to demand for security operations services such as SOC/next-gen SOC services, SIEM, vulnerability Management, SOAR, and cloud security.
- Lack of skilled resources and the need to reduce response time to contain and remediate security incidents and mitigate fraud, data theft, and intellectual property loss are driving companies to outsource their security operations.
- Sectors with high cybersecurity maturity, such as banking and IT/ITeS, handle sensitive data. They are leaning towards SOC services to adopt advanced cybersecurity offerings for safeguarding themselves against threat actors.
- Furthermore, sectors, including manufacturing, pharmaceuticals, and healthcare, are implementing technologies such as AI/ML and IoT and moving towards automation, thereby driving the need to secure their ecosystem and implement basic security controls. This has further uplifted the demand for security operations services in India.

India Security Operations Services Market, 2019-2023 (USD million)

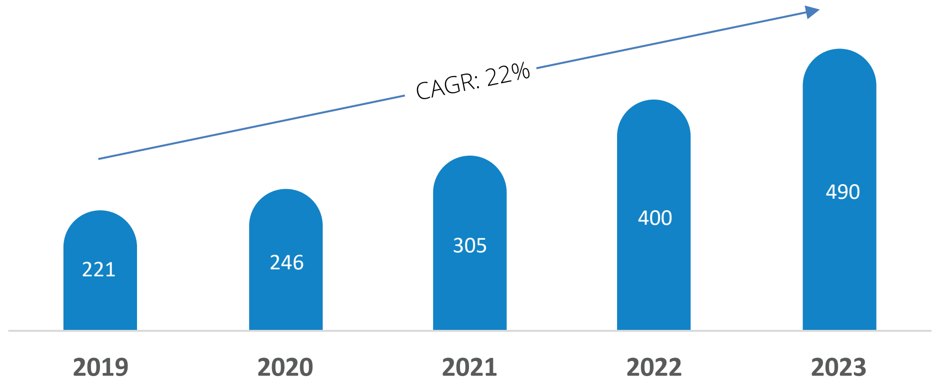


In 2023, Security operation services accounted for ~45% of the services market.

Security Implementation

- Security Implementation encompasses offerings like the design of information security architecture, the deployment and maintenance of hardware and software, and the integration followed by functional and performance testing.
- Accelerated cybersecurity products adoption fueled the demand for implementation services in the country.
- Regulator compliance and lack of skill shortage will drive organizations to opt for security implementation services.
- RBI's 2016 Cybersecurity Framework in Banks[99] mandates the implementation of SoC and security controls, such as firewalls, data encryption, and IDS. SEBI mandates 24/7 SoC and technical safeguard controls for market intermediaries.[100]
- Compliance with the DPDP Act 2023 will drive demand for security implementation services as organizations will invest in data security and privacy offerings.
- Cyber insurance adoption has also risen in the last five years. Due to this, organizations must implement security controls to meet insurance providers' security requirements.
  - As per Deloitte, cyber insurance market in India grew at a CAGR of 27-30% in the last three years to reach USD 50 - 60 billion in 2023.[101]

India Security Implementation Market, 2019-2023 (USD million)



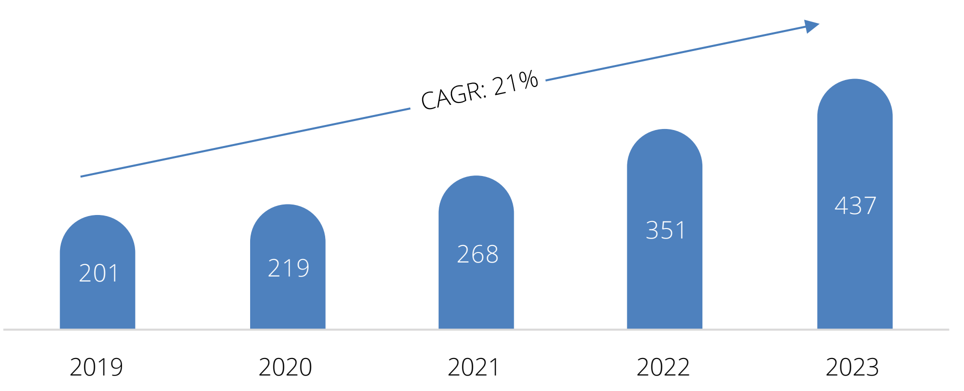
Compliance with the DPDP Act 2023 will drive demand for security implementation services as organizations will invest in data security and privacy offerings.

Security Testing

The security testing services market includes penetration testing, web testing, application security, audits and reviews.

- 76% of the respondents have already invested or plan to invest in security audits and assessments, and 73.3% in VAPT.
- Regulatory requirements, increase in web and mobile application vulnerabilities, supply chain and third-party risks, cyber insurance requirements, and growing concern for APTs, is driving the need for security testing for secure coding practices.
  - RBI requires banks and financial institutions to carry out routine security audits and assessments. SEBI mandates security audits and assessments for entities operating in the securities market.[102, 103]
- Organizations are increasingly embracing DevSecOps to integrate security seamlessly into the entire development lifecycle, consequently driving the need for enhanced demand for security testing services.
- IoT is gaining traction in sectors including manufacturing and healthcare. To ensure the IoT devices are secure, organizations are testing IoT device firmware, communication protocols, and backend systems, for vulnerabilities.
- Organizations utilize services that include blue, red, and purple teaming exercises to strengthen their security stance, fortify defense mechanisms, and encourage collaboration between offensive and defensive security teams.

India Security Testing Services Market, 2019-2023 (USD million)



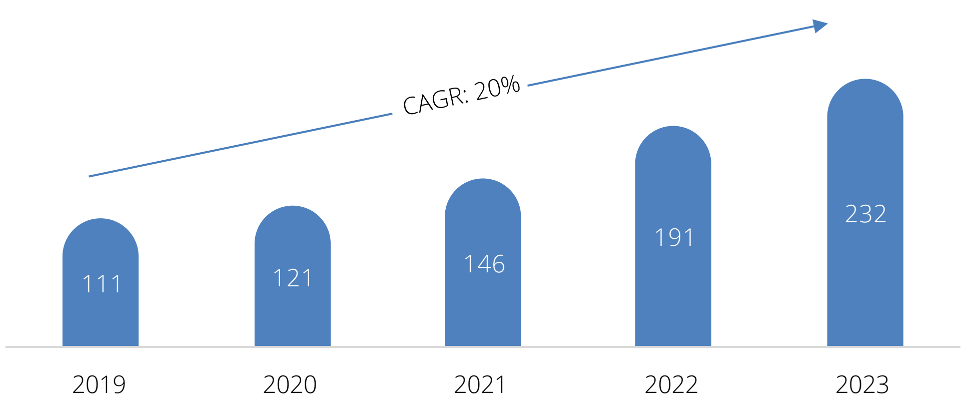
Organizations are increasingly embracing DevSecOps to integrate security seamlessly into the entire development lifecycle, consequently driving the need for enhanced demand for security testing services.

Security Consulting

Security Consulting services include planning of security strategies, policy development, building security architecture, compliance and risk, security awareness and conducting training.

- 66.7% of the respondents have either invested in or plan to invest in security awareness and training services, and 60% in security consulting and advisory services.
- The shortage of skilled talent and rising salaries of security professionals are leading businesses to outsource consulting services.
- Expanding digital footprint due to digital transformation initiatives and technology adoption has driven the volume of attack surfaces an organization needs to manage.
- Consulting services help them with technologies, business processes, and security strategies.
- Third-party risk management and proactive incident response further drive the need for security consulting services for incident response plan development and testing and external partner risk assessment and management.
- Cybersecurity is synonymous with brand reputation; successful data breaches can lead to loss of business, customer attrition, and regulatory fines. They are leading to the need for strengthened cyber resilience, thereby increasing the demand for security consulting services in India.
  - 59% of the respondents indicated that cyber incidents or data breaches will significantly impact brand reputation.

India Security Consulting Services Market, 2019-2023 (USD million)



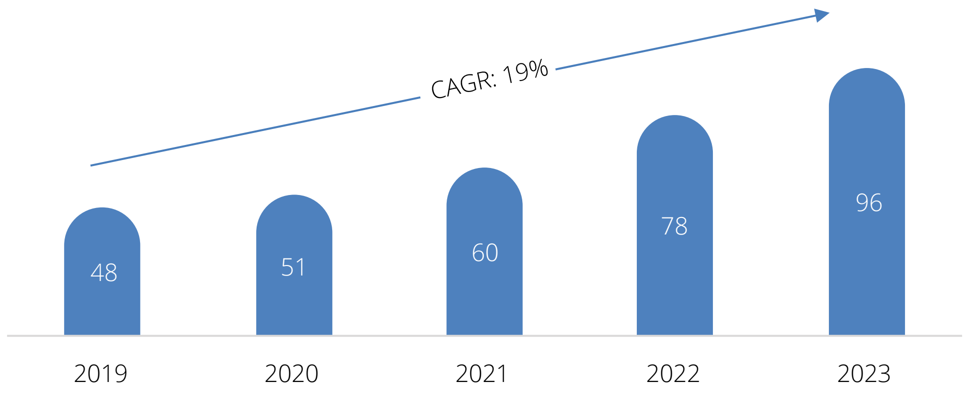
66.7% of the respondents have either invested in or plan to invest in security awareness and training services, and 60% in security consulting and advisory services.

Digital Forensics and Incident Response (DFIR)

The incident response market involves areas such as incident management, digital forensics, evidence capturing and breach reporting. Predominantly, retainer-based model is leveraged for delivering DFIR services.

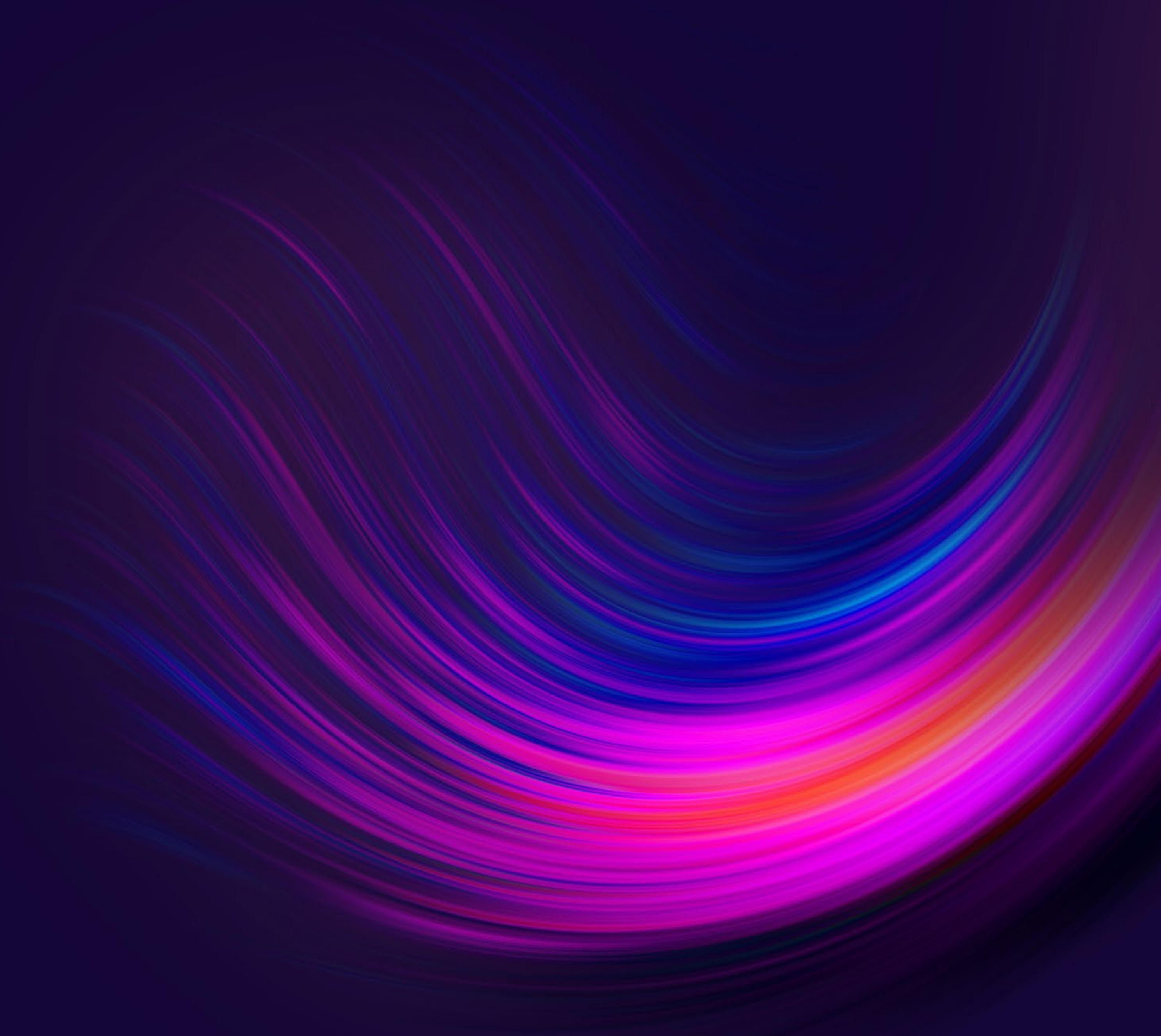
- The sophistication of cyber threats and increasing cyberattacks, including malware, ransomware, and advanced persistent threats (APTs), and data breaches have increased the demand for DFIR services in India to investigate threats and breaches, implement security controls, assess cybersecurity posture, preservation of evidence, and mitigate damage.
  - CERT-In tracked 13,91,457 and 14,02,809 cybersecurity incidents in the country during 2022 and 2021, respectively.[104]
- Regulatory authorities in India mandate organizations to implement incident response mechanisms and follow due process for incident reporting.
  - CERT-In's 2022 directions mandate organizations to report cyber incidents, including DDoS, data breaches, data leak ransomeware, attacks on IoT ecosystems, OT, wireless networks, SCADA, critical infrastructure, and phishing attacks.[105]
  - RBI's 2015 Cybersecurity Framework in Banks mandated banks to report cyber incidents to RBI.[106]
- In 2023, CERT-In launched Guidelines on Information Security Practices for Government Entities, reiterating the need to report cybersecurity incidents to CERT-In and NIC-CERT.[107]
- RBI's 2023 Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices includes, encourages regulated entities to leverage forensic analysis for cyber incidents response.[108]

India Digital Forensics and Incident Response Services Market, 2019-2023 (USD million)



The Digital Forensics and Incident Response services market grew at a CAGR of 19% from 2019 to 2023 to USD 96 million. Regulatory authorities drive the need to implement incident response mechanisms and follow due process for incident reporting.

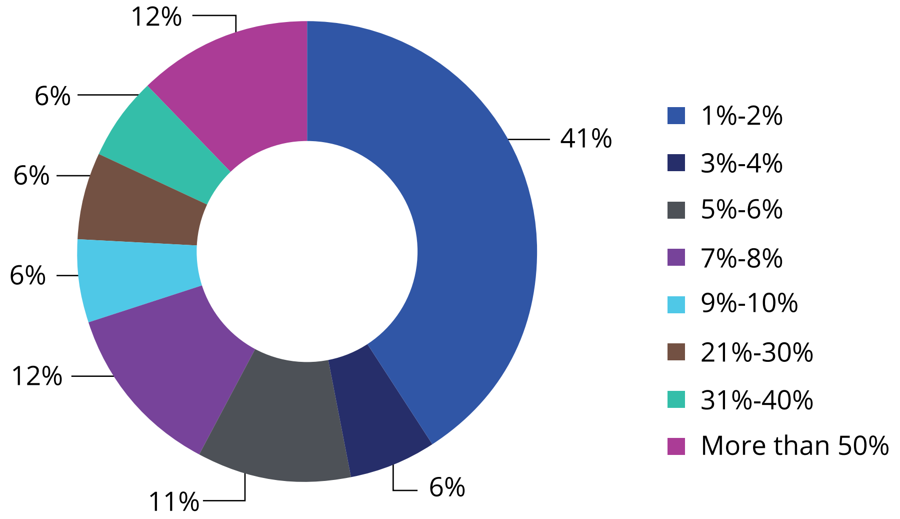
TALENT LANDSCAPE



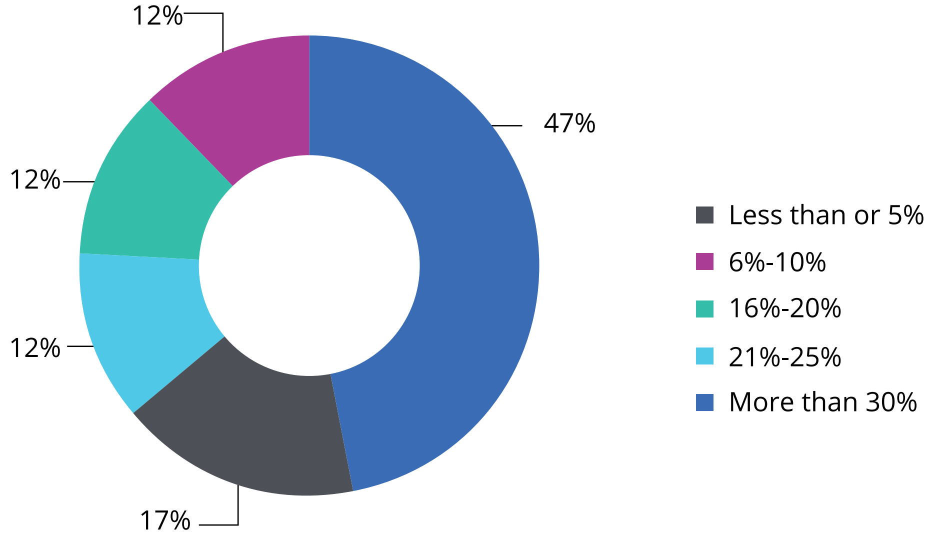
TALENT LANDSCAPE

The below charts show the percentage of cybersecurity workforce compared to their total workforce among the surveyed organizations.

% of Cybersecurity Workforce



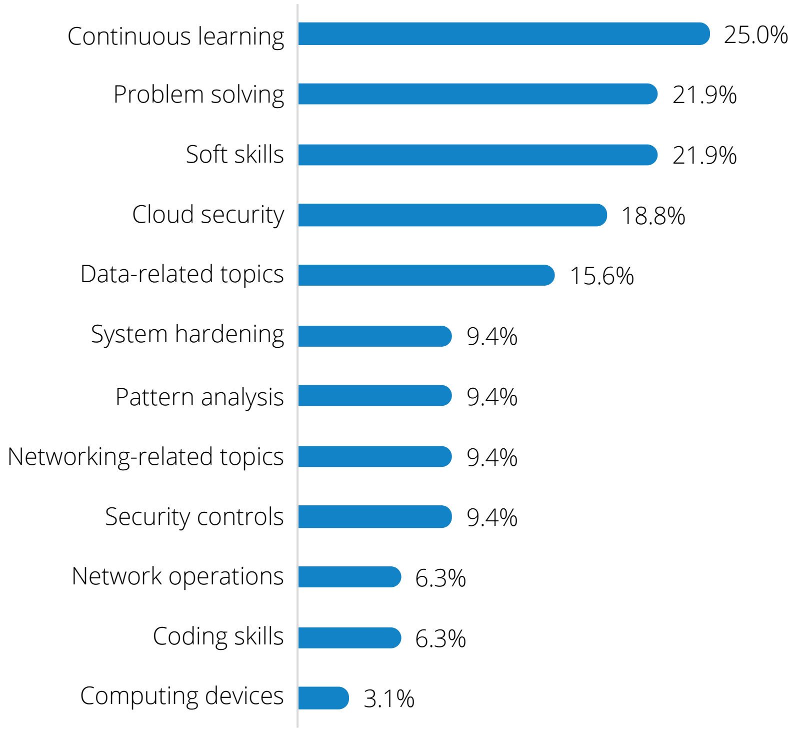
% increase in Cybersecurity Workforce in Next Five Years



As per DSCI's Bridging the Gap report: Identifying Challenges in Cybersecurity Skilling and Bridging the Divide,[109] cybersecurity professionals constitute less than **5%** of the overall workforce, as indicated by **47%** of the corporates.

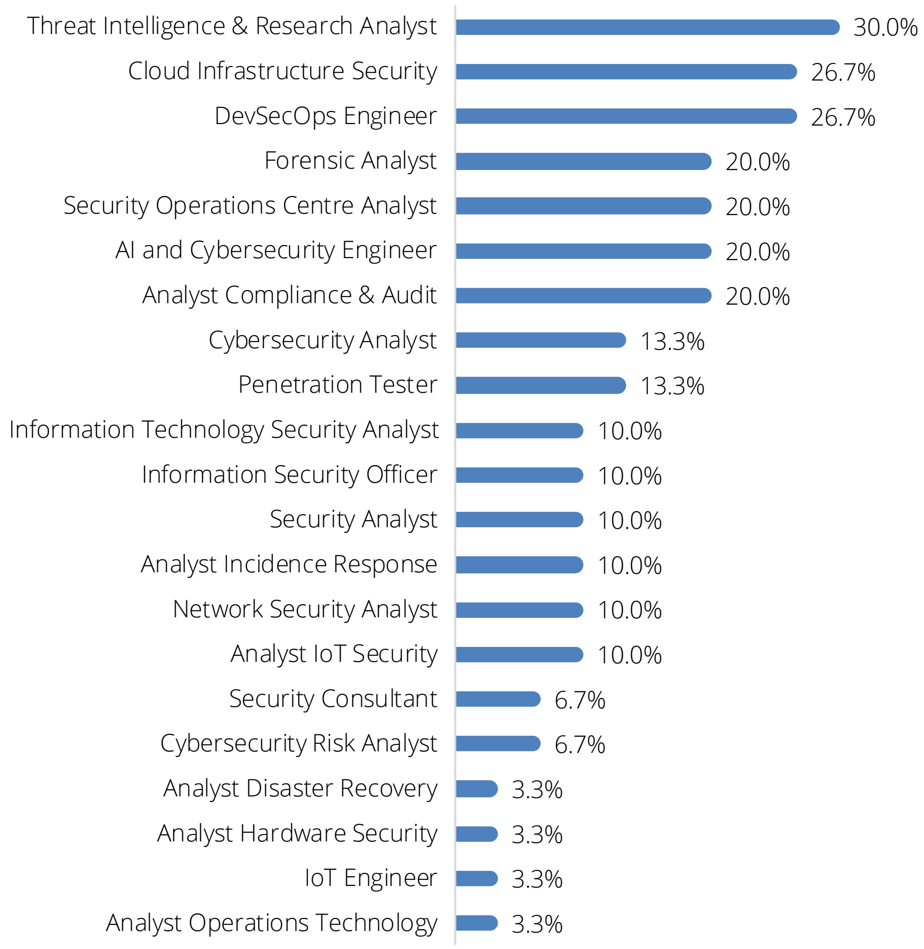
47% of survey participants expressed the aim to augment the count of cybersecurity professionals by over 30% of the existing workforce, signaling a noteworthy surge in the demand for skilled cybersecurity professionals.[110]

Skill Gaps in Workforce



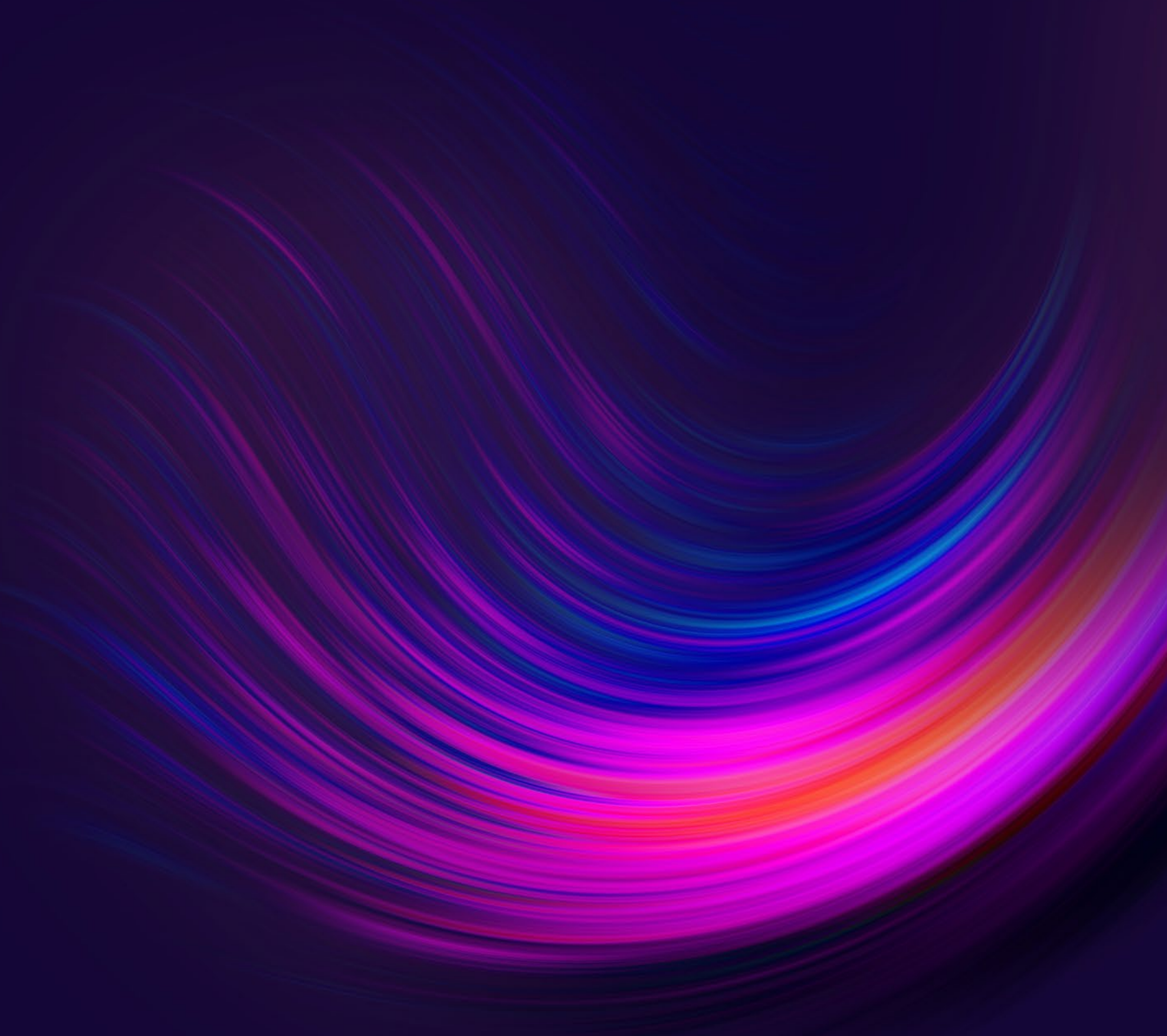
- Continuous learning, problem solving, and soft skills are the key challenges that organizations face with their workforce.
- Cloud security and data related topics are the technical skills, which organizations recognized as a skill gap.

Cybersecurity Roles Expected to Grow in Next Five Years



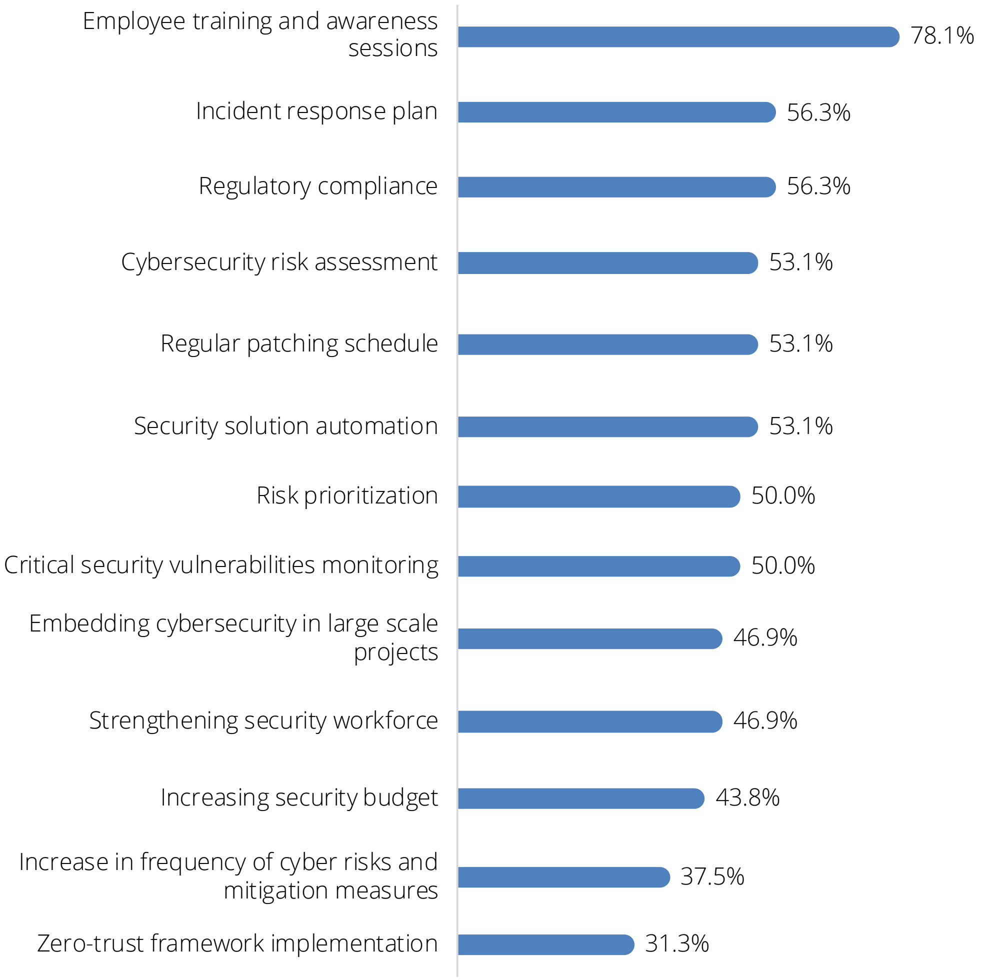
Source - DSCI Survey 2023

CYBER RESILIENCE PRACTICES



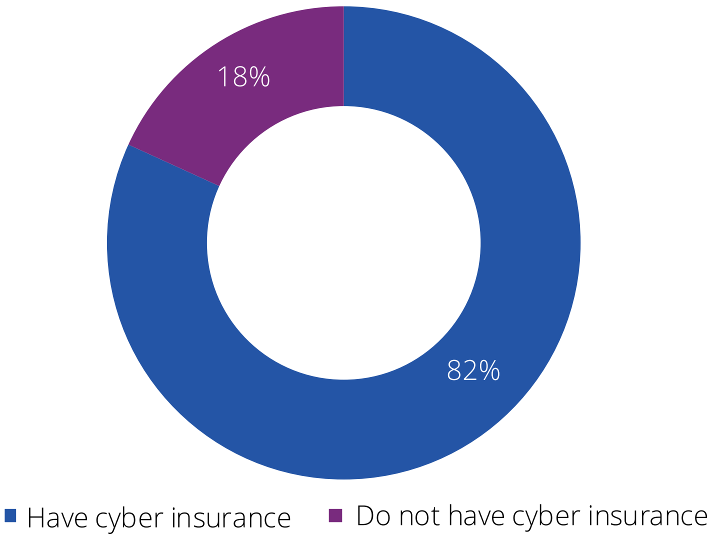
CYBER RESILIENCE PRACTICES

Key Initiatives to Bolster Cyber Resilience



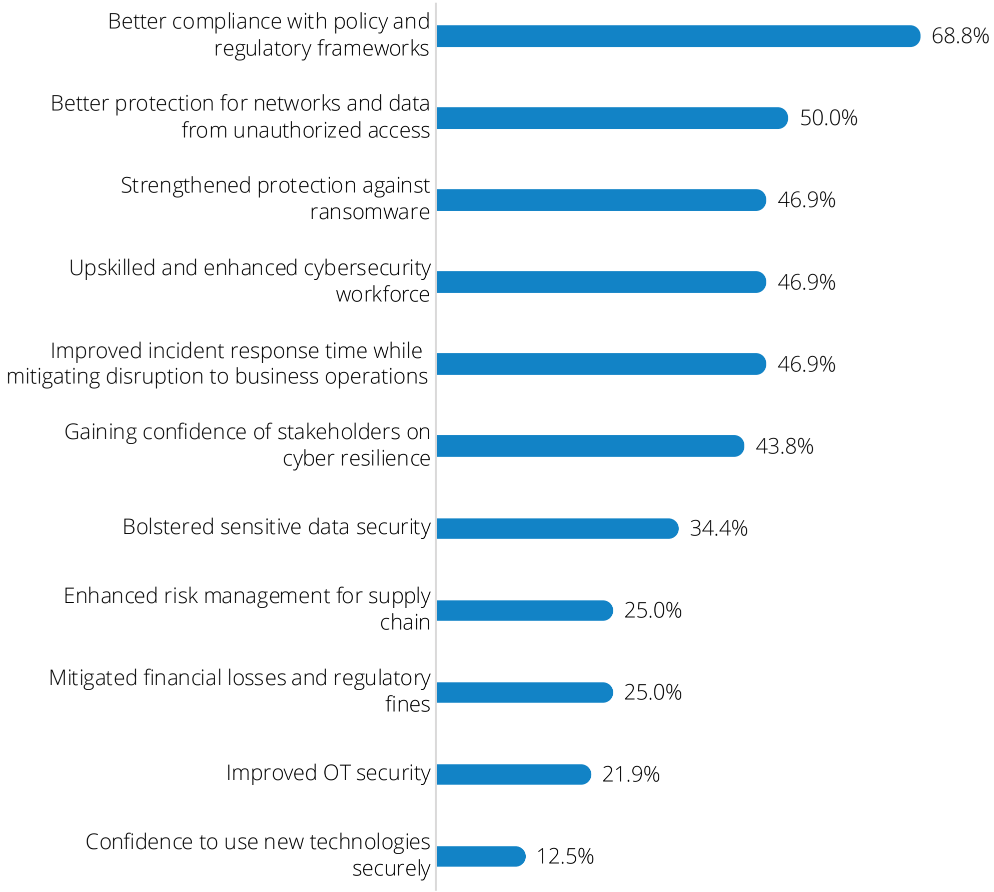
Source: DSCI Survey 2023

Cyber Insurance Adoption



- Organizations invest in cyber insurance to protect against financial losses due to cyberattack incidents. Furthermore, the insurance provider also covers the expenses related to security controls, third-party consultants, and necessary products to mitigate the impact of cyberattacks.
- Companies are placing emphasis on enhancing their resistance to cyber threats through employee training and awareness initiatives. Employing techniques such as gamification, simulations, quizzes with prizes, and case studies, to boost the effectiveness of their training programs.

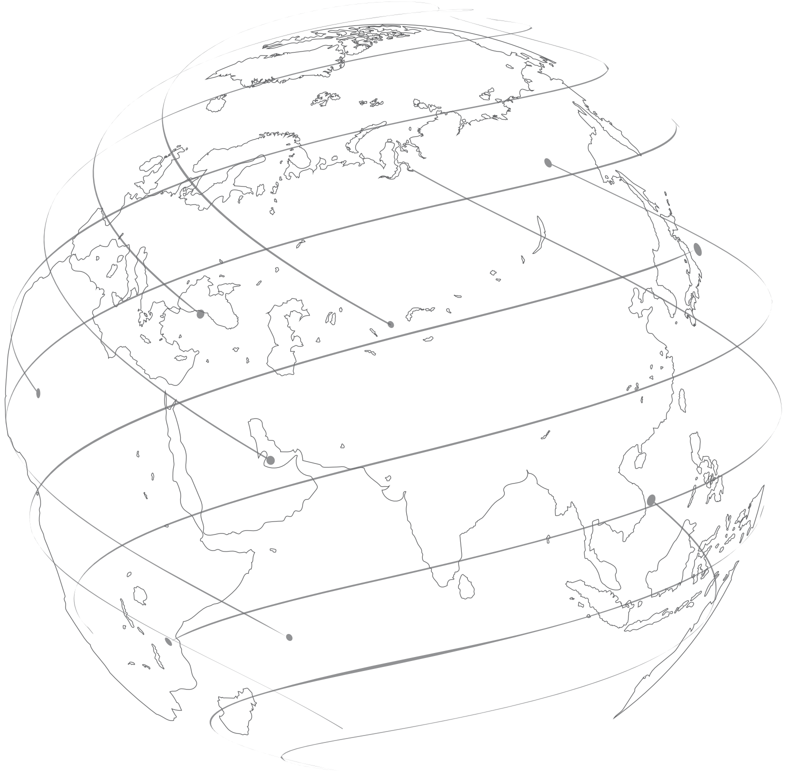
Key Benefits of Cybersecurity Implementation & Initiatives



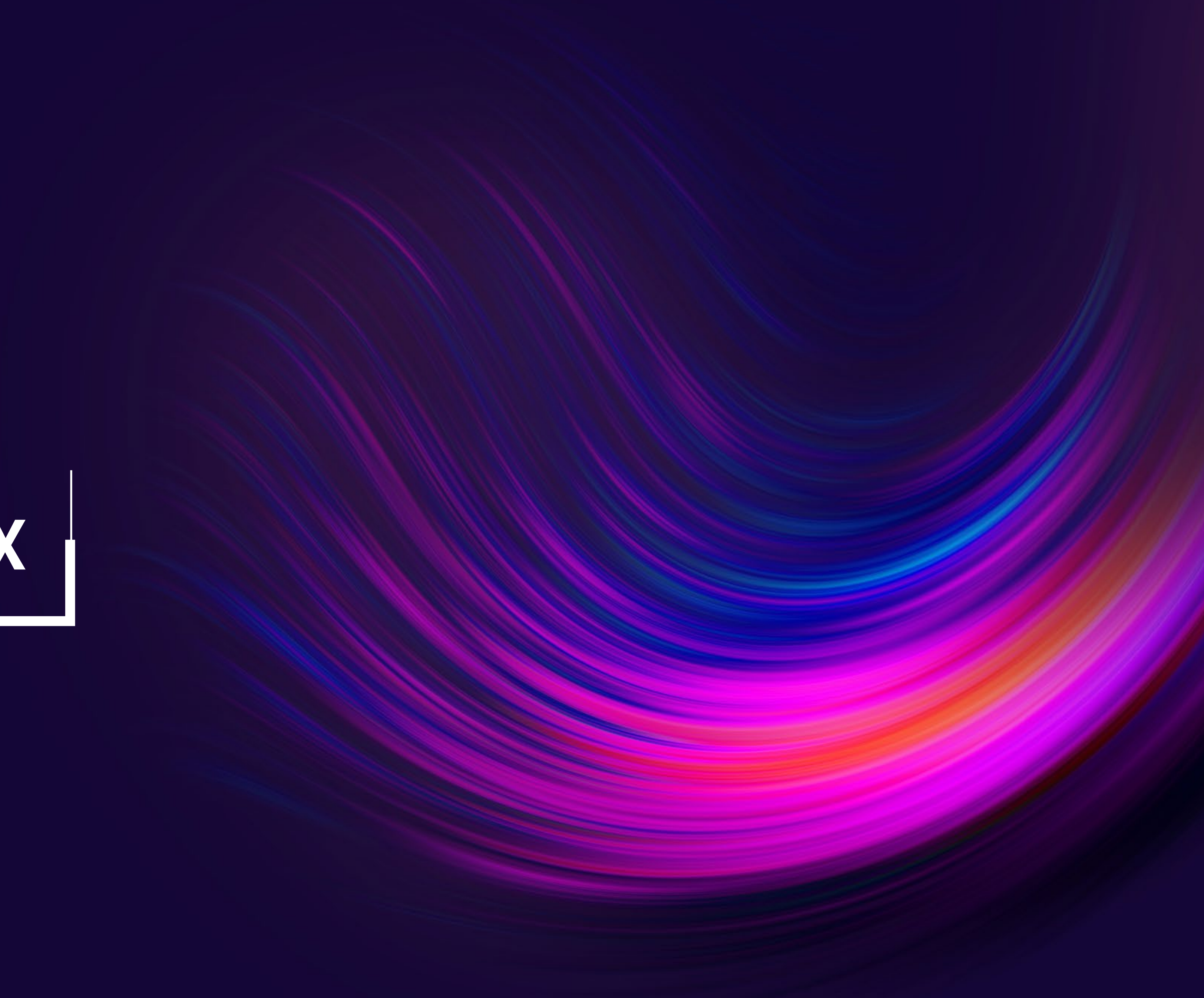
Source: DSCI Survey 2023

Investment in cybersecurity is helping organizations achieve better policy and regulatory compliance. With the constantly evolving regulatory landscape in India and globally, organizations need to comply not only with Indian regulations but with global regulations as well.

DDoS and ransomware attacks have grown significantly in the last few years. The cost of data breaches and regulatory fines have accelerated the need to secure sensitive personal, confidential organizational and customer data from threat actors. Organizations can achieve improved protection against networks and data from unauthorized access and significantly strengthened protection against ransomware by investing in cybersecurity initiatives.



APPENDIX



ABBREVIATIONS AND ACRONYMS

ABHA	Ayushman Bharat Health Accounts
AI	Artificial Intelligence
API	Application Programming Interface
Application VAPT	Application Vulnerability Assessment and Penetration Testing
APT	Advanced Persistent Threat
ASRTM	Application Security Requirements and Threat Modelling
BEC	Business Email Compromise
BFSI	Banking, Financial Services and Insurance
BPO	Business Process Outsourcing
CAGR	Compound Annual Growth Rate
CASB	Cloud Access Security Broker
CASBs	Cloud Access Security Brokers
CCPA	California Consumer Privacy Act
CERT-In	Indian Computer Emergency Response Team
CFCFRMS	Citizen Financial Cyber Fraud Reporting and Management System
CIEM	Cloud Infrastructure Entitlements Management
CISO	Chief Information Security Officer
Cloud WAAP	Cloud Web Application and API Protection
CNAPP	Cloud-Native Application Protection Platform
CPRA	California Privacy Rights Act
CPS	Cyber-Physical Systems
CSP-Native DLP	Cloud Service Provider - Native Data Loss Prevention
CWPP	Cloud Workload Protection Platforms
DaaS	Desktop-as -a –Service
DAST	Dynamic Application Security Testing
DBR	Data Breach Response

DCIP	Document-Centric Identity Proofing
DDoS	Distributed Denial-of-Service
DLP	Data Loss Prevention
DPDP	Digital Personal Data Protection
DRA	Data Risk Assessment
DSG	Data Security Governance
DSP	Data Security Platform
DSPM	Data Security Posture Management
EAM	Externalized Authorization Management
EDR	Endpoint Detection and Response
EDRM	Enterprise Digital Rights Management
eKYC	Electronic Know Your Customer
GDPR	General Data Protection Regulation
GenAI	Generative Artificial Intelligence
GPT	Generative Pre-trained Transformer
GRC	Governance, Risk, and Compliance
HERD	Hardware Security Entrepreneurship Research and Development
HIPAA	Health Insurance Portability and Accountability Act
I4C	Indian Cyber Crime Coordination Centre
IaC	Infrastructure as Code
IAM	Identity and Access Management
IDS	Intrusion Detection System
IGA	Identity Governance and Administration
IoT	Internet of Things
IP	Internet Protocol
IRDAI	Insurance Regulatory and Development Authority of India

IT	Information Technology
ITDR	Identity Threat Detection and Response
ITeS	Information Technology enabled Services
ITRM	IT Risk Management
KYC	Know Your Customer
MDR	Managed Detection and Response (MDR)
MEITY	Ministry of Electronics and Information Technology
MFA	Multi-Factor Authentication
MITM	Man-in-the-middle
ML	Machine Learning
MSSP	Managed Security Services Provider
NAC	Network Access Control
NCCC	National Cyber Coordination Centre
NCoE	National Centre of Excellence
NCRP	National Cybercrime Reporting Portal
NDR	Network Detection and Response
Next-Gen SOC	Next Generation Security Operations Centre
NSPM	Network security policy management
OFC	Optical Fiber Cable
OT	Operational technology
OTT	Over-the-Top
PAM	Privileged Access Management
PIA	Privacy Impact Assessments
PSU	Public Sector Undertakings
PT	Penetration Testing
QKD	Quantum Key Distribution

QRNG	Quantum Random Number Generators
R&D	Research and Development
RaaS	Ransomware-as-a-Service
RAT	Remote-access Trojan
RBI	Reserve Bank of India
RFP	Request for Proposals
RFQ	Request for Quote
SaaS	Software-as-a-Service
SASE	Secure Access Service Edge
SAST	Static Application Security Testing
SDLC	Secure Software Development Life Cycle
SEBI	Securities and Exchange Board of India
SIEM	Security Information And Event Management
SOAR	Security Orchestration, Automation And Response
SOC	Security Operations Centre
SQL	Structured Query Language
Tech	Technology
TRAI	Telecom Regulatory Authority of India
UEBA	User and Entity Behavior Analytics
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
VA	Vulnerability Assessment
VAR	Value-Added Resellers
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network
WAF	Web Application Firewall

REFERENCES

1. Gartner, Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024, https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024#:~:text=Worldwide%20end%2Duser%20spending%20on,estimated%20to%20reach%20%24188.1%20billion.

2. Statista, Spending on digital transformation technologies and services worldwide from 2017 to 2026, https://www.statista.com/statistics/870924/worldwide-digital-transformation-market-size/

3. Gartner, Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024, https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024#:~:text=Worldwide%20end%2Duser%20spending%20on,estimated%20to%20reach%20%24188.1%20billion.

4. Gartner, Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024, https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024#:~:text=Worldwide%20end%2Duser%20spending%20on,estimated%20to%20reach%20%24188.1%20billion.

5. Google, The Ups and Downs of 0-days: A Year in Review of 0-days Exploited In-the-Wild in 2022, https://security.googleblog.com/2023/07/the-ups-and-downs-of-0-days-year-in.html

6. Verizon, 2023 Data Breach Investigations Report, https://www.verizon.com/business/resources/reports/dbir/

7. Verizon, 2023 Data Breach Investigations Report, https://www.verizon.com/business/resources/reports/dbir/

8. Verizon, 2023 Data Breach Investigations Report, https://www.verizon.com/business/resources/reports/dbir/

9. IBM, Cost of a Data Breach Report 2023, https://www.ibm.com/reports/data-breach#:~:text=The%20global%20average%20cost%20of,15%25%20increase%20over%203%20years.&text=51%25%20of%20organizations%20are%20planning,threat%20detection%20and%20response%20tools.

10. Sophos, The State of Ransomware 2023, https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf

11. Microsoft, Microsoft Digital Defense Report 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

12. Gartner, Gartner Forecasts End-User Spending on Public Cloud Services in India to Total $7.3 Billion in 2022, https://www.gartner.com/en/newsroom/press-releases/2021-11-03-india-public-cloud-spending-forecast-2022#:~:text=End%2Duser%20spending%20on%20public%20cloud%20services%20in%20India%20is,onset%20of%20the%20global%20pandemic.

13. Statista, Public cloud services end-user spending in India from 2019 to 2022, with estimates until 2024, https://www.statista.com/statistics/1220691/india-public-cloud-services-end-user-spending/#:~:text=Public%20cloud%20services%20end%2Duser%20spending%20in%20India%202019%2D2024&text=In%202024%2C%20India's%20end%2Duser,2020's%204.2%20billion%20U.S.%20dollars.

14. PwC, Towards a smarter tomorrow: Impact of AI in the post-COVID era, https://www.pwc.in/assets/pdfs/data-and-analytics/towards-a-smarter-tomorrow-impact-of-ai-in-the-post-covid-era-v2.pdf

15. nasscom, Technology Sector in India 2023 : Strategic Review, https://nasscom.in/knowledge-center/publications/technology-sector-india-2023-strategic-review

16. MeitY, Notes on Demands for Grants, 2023-2024, https://www.indiabudget.gov.in/doc/eb/sbe27.pdf

17. MeitY, Meity Annual Report 2022-23, https://www.meity.gov.in/writereaddata/files/AR_2022-23_English_24-04-23.pdf

18. PIB, Union Cabinet approves expansion of the Digital India programme with an outlay of ₹ 14,903 crore, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1949426

19. UIDAI, AADHAAR Dashboard, https://uidai.gov.in/aadhaar_dashboard/, Accessed 18 December 2023

20. PIB, Full text of Union Home Minister Shri Amit Shah's address at the inaugural session of G20 Conference on Crime and Security in the age of NFTs, Artificial Intelligence and Metaverse in Gurugram, Haryana, pib.gov.in/PressReleaseIframePage.aspx?PRID=1939176

21. Statista, Number of smartphone users in India in 2010 to 2023, with estimates until 2040, https://www.statista.com/statistics/467163/forecast-of-smartphone-users-in-india/

22. DigiLocker, DigiLocker National Statistics, https://www.digilocker.gov.in/statistics, Accessed 18 December 2023

23. Telecom Regulatory Authority of India, Highlights of Telecom Subscription Data as on 31st August, 2023, https://www.trai.gov.in/sites/default/files/PR_No.124of2023_0.pdf

24. PIB, Full text of Union Home Minister Shri Amit Shah's address at the inaugural session of G20 Conference on Crime and Security in the age of NFTs, Artificial Intelligence and Metaverse in Gurugram, Haryana, pib.gov.in/PressReleaseIframePage.aspx?PRID=1939176

25. RBI, Payment System Indicators - October 2023, https://www.rbi.org.in/Scripts/PSIUserView.aspx?Id=29, Accessed 18 December 2023

26. UMANG, UMANG Statistics, https://web.umang.gov.in/landing/dashboard, Accessed 18 December 2023

27. API Setu, API Setu Home Page, https://apisetu.gov.in/, Accessed 18 December 2023

28. API Setu, API Setu Home Page, https://apisetu.gov.in/, Accessed 18 December 2023

29. UIDAI, AADHAAR Dashboard, https://uidai.gov.in/aadhaar_dashboard/, Accessed 18 December 2023

30. UIDAI, AADHAAR Dashboard, https://uidai.gov.in/aadhaar_dashboard/, Accessed 18 December 2023

31. DigiLocker, DigiLocker National Statistics, https://www.digilocker.gov.in/statistics, Accessed 18 December 2023

32. DigiLocker, DigiLocker National Statistics, https://www.digilocker.gov.in/statistics, Accessed 18 December 2023

33. National Health Authority, Ayushman Bharat Health Accounts Dashboard, https://dashboard.abdm.gov.in/abdm/, Accessed 18 December 2023

34. National Health Authority, Ayushman Bharat Health Accounts Dashboard, https://dashboard.abdm.gov.in/abdm/, Accessed 18 December 2023

35. UIDAI, AADHAAR Dashboard, https://uidai.gov.in/aadhaar_dashboard/, Accessed 18 December 2023

36. RBI, Payment System Indicators - October 2023, https://www.rbi.org.in/Scripts/PSIUserView.aspx?Id=29, Accessed 18 December 2023

37. PIB, Address by the Hon'ble Minister of State for Electronics and Information Technology; and Skill Development and Entrepreneurship Shri Rajeev Chandrasekhar at GPI Global Summit in Pune on 12.06.2023, https://pib.gov.in/PressReleasePage.aspx?PRID=1931670

38. India TV, India tops world ranking in digital payments in 2022, leaves behind THESE countries including China, https://www.indiatvnews.com/business/news/india-tops-world-ranking-in-digital-payments-89-5-million-transactions-in-2022-mygovindia-data-brazil-china-thailand-south-korea-2023-06-10-875241

39. CERT-IN, CERT-IN Annual Report 2022, https://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT

40. MeitY, Notes on Demands for Grants, 2023-2024, https://www.indiabudget.gov.in/doc/eb/sbe27.pdf

41. MeitY, THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

42. IRDAI, 2023 _ IRDAI Information and Cyber Security Guidelines, 2023.pdf, https://irdai.gov.in/document-detail?documentId=3314780

43. RBI, Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12562&Mode=0

44. ISC2, How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4

45. DSCI, Bridging the Gap: Identifying Challenges in Cybersecurity Skilling and Bridging the Divide, https://www.dsci.in/resource/content/bridging-gap-identifying-challenges-cybersecurity-skilling-and-bridging-divide

46. nasscom, 2023 State Of IT Modernization – Securing Enterprise Competitiveness, https://nasscom.in/knowledge-center/publications/2023-state-it-modernization-securing-enterprise-competitiveness

47. IBM, IBM Report: Average cost of a data breach in India touched INR 179 million in 2023, https://in.newsroom.ibm.com/IBM-Report-Average-cost-of-a-data-breach-in-India-touched-INR-179-million-in-2023

48. CERT-IN, CERT-IN Annual Report 2022, https://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT

49. CERT-In, India Ransomware Report 2022, https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2022.pdf

50. CrowdStrike, RANSOMWARE AS A SERVICE (RAAS) EXPLAINED HOW IT WORKS & EXAMPLES, https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

51. Microsoft, 2022 in review: DDoS attack trends and insights, https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/

52. Google, The Ups and Downs of 0-days: A Year in Review of 0-days Exploited In-the-Wild in 2022, https://security.googleblog.com/2023/07/the-ups-and-downs-of-0-days-year-in.html

53. HCL Technologies, AI and ML for cyber attacks: Boon or Curse?, https://www.hcltech.com/blogs/artificial-intelligence-and-machine-learning-for-cyber-attacks-boon-or-curse

54. UNCTAD, Data Protection and Privacy Legislation Worldwide, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

55. nasscom, Generative AI Startup Landscape In India – A 2023 Perspective, https://nasscom.in/knowledge-center/publications/generative-ai-startup-landscape-india-2023-perspective

56. PIB, Union Home Minister and Minister of Cooperation, Shri Amit Shah addresses inaugural session of the G-20 Conference on Crime and Security in the Age of NFTs, AI and the Metaverse, in Gurugram, Haryana, today, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1939173

57. Tenable, Tenable Study Finds Indian Organisations Cannot Prevent 42% of Cyberattacks, https://www.tenable.com/press-releases/tenable-study-finds-indian-organisations-cannot-prevent-42-of-cyberattacks

58. *RBI, Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12562&Mode=0*

59. *RBI, Storage of Payment System Data, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF*

60. *MCA, THE COMPANIES ACT, 2013, https://www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf*

61. *IRDAI, IRDAI (Maintenance of Insurance Records) Regulations, 2015.pdf, https://irdai.gov.in/document-detail?documentId=604674*

62. *Thales, 2023 THALES CLOUD SECURITY REPORT REVEALS CLOUD ASSETS AS ONE OF THE BIGGEST TARGETS FOR CYBERATTACKS IN INDIA, https://www.thalesgroup.com/en/countries-asia-pacific/india/press_release/2023-thales-cloud-security-report-reveals-cloud-assets*

63. *ISC2, How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4*

64. *CRN, India ranked second in total number of breaches exposed in 2022: Tenable Research, https://www.crn.in/news/india-ranked-second-in-total-number-of-breaches-exposed-in-2022-tenable-research/*

65. *CEA, CEA (Cyber Security in Power Sector) Guidelines, 2021, https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf*

66. *Ministry of Communications Department of Telecommunications, Best Practices - Cyber Security, https://dot.gov.in/sites/default/files/2020_07_09%20Cybersec%20SA.pdf*

67. *RAJYA SABHA, UNSTARRED QUESTION NO. 1043 TO BE ANSWERED ON: 10.02.2023 CYBER SECURITY ATTACKS, https://pqars.nic.in/annex/259/AU1043.pdf*

68. *RAJYA SABHA, UNSTARRED QUESTION NO. 1043 CYBER SECURITY ATTACKS, https://pqars.nic.in/annex/259/AU1043.pdf*

69. *SonicWall, SONICWALL CYBER THREAT REPORT, https://www.sonicwall.com/medialibrary/en/white-paper/2023-cyber-threat-report.pdf*

70. *Barracuda, 2023 spear-phishing trends, https://assets.barracuda.com/assets/docs/dms/2023-spear-phishing-trends.pdf*

71. *CERT-IN, CERT-IN Annual Report 2022, https://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT*

72. *Microsoft, 2022 in review: DDoS attack trends and insights, https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/*

73. *Indusface, The State of Application Security Q3 2023, https://www.indusface.com/resources/research-reports/the-state-of-application-security-q3-2023/*

74. *IBM, IBM Report: Average cost of a data breach in India touched INR 179 million in 2023, https://in.newsroom.ibm.com/IBM-Report-Average-cost-of-a-data-breach-in-India-touched-INR-179-million-in-2023*

75. *Appknox, Evidence-Based Insights of India's Top 100 Android Mobile Apps Tested for Cybersecurity, https://www.appknox.com/hubfs/Ebooks%202022/Security%20Research%20Report%20_%20100%20Indian%20Apps%20%5B42220%5D_Update%204.pdf*

76. *The Economic Times, State-sponsored cyberattacks against India up 278% in three years, https://economictimes.indiatimes.com/tech/technology/india-most-targeted-country-by-cyber-attackers-report/articleshow/104989856.cms*

77. *Trend Micro, Massive Phishing Campaigns Target India Banks' Clients, https://www.trendmicro.com/en_in/research/22/k/massive-phishing-campaigns-target-india-banks-clients.html*

78. *RBI, Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12562&Mode=0*

79. *SEBI, Cyber Security and Cyber Resilience framework for Portfolio Managers, https://www.sebi.gov.in/legal/circulars/mar-2023/cyber-security-and-cyber-resilience-framework-for-portfolio-managers_69521.html*

80. *SEBI, Modification in Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporations and Depositories, https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporations-and-depositories_41244.html*

81. *IRDAI 2023 _ IRDAI Information and Cyber Security Guidelines, 2023.pdf, https://irdai.gov.in/document-detail?documentId=3314780*

82. *nasscom, Technology Sector in India 2023 : Strategic Review, https://nasscom.in/knowledge-center/publications/technology-sector-india-2023-strategic-review*

83. *nasscom, Technology Sector in India 2023 : Strategic Review, https://nasscom.in/knowledge-center/publications/technology-sector-india-2023-strategic-review*

84. *Times of India, 'Most Targeted' Indian Industries Facing Cyber Attacks In 2023, https://timesofindia.indiatimes.com/gadgets-news/most-targeted-indian-industries-facing-cyber-attacks-in-2023/photostory/105035810.cms*

85. *Everest Group, IT Companies Step up GenAI Investments as Clients Ready for Paid POCs | In the News, https://www.everestgrp.com/in-the-news/it-companies-step-up-genai-investments-as-clients-ready-for-paid-pocs/*

86. *Times of India, 'Most Targeted' Indian Industries Facing Cyber Attacks In 2023, https://timesofindia.indiatimes.com/gadgets-news/most-targeted-indian-industries-facing-cyber-attacks-in-2023/photostory/105035810.cms*

87. *Check Point, Evolving Cyber Dynamics Amidst the Israel-Hamas Conflict, https://blog.checkpoint.com/security/evolving-cyber-dynamics-amidst-the-israel-hamas-conflict/*

88. *MeitY, Guidelines on Information Security Practices for Government Entities, https://www.meity.gov.in/writereaddata/files/Guidelines%20on%20Information%20Security%20Practices%20for%20Government%20Entities.pdf*

89. *LOK SABHA, LOK SABHA UNSTARRED QUESTION NO. 2487 CASES OF CYBER FRAUD, https://sansad.in/getFile/loksabhaquestions/annex/1711/AU2487.pdf?source=pqals*

90. *Mint, Govt prepares new cyber security policy to beat malware attacks, https://www.livemint.com/technology/govt-prepares-new-cyber-security-policy-to-beat-malware-attacks-11686717816691.html*

91. *CEA, CEA (Cyber Security in Power Sector) Guidelines, 2021, https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf*

92. *DSCI, Indian pharma takes the digital leap: What does it mean for cybersecurity?, https://www.dsci.in/resource/content/indian-pharma-takes-digital-leap-what-does-it-mean-cybersecurity-2*

93. *TRAI, Telecom Regulatory Authority of India Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector, https://www.trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf*

94. *API Setu, About us, https://apisetu.gov.in/aboutus*

95. *MeitY, Guidelines on Information Security Practices for Government Entities, https://www.meity.gov.in/writereaddata/files/Guidelines%20on%20Information%20Security%20Practices%20for%20Government%20Entities.pdf*

96. *Surfshark, Global data breach statistics, https://surfshark.com/research/data-breach-monitoring*

97. *RBI, Draft Master Directions on Cyber Resilience and Digital Payment Security Controls for Payment System Operators, https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=4267#8*

98. *MeitY, Guidelines on Information Security Practices for Government Entities, https://www.meity.gov.in/writereaddata/files/Guidelines%20on%20Information%20Security%20Practices%20for%20Government%20Entities.pdf*

99. *RBI, Cyber Security Framework in Banks, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0*

100. *SEBI, Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporations and Depositories, https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporations-and-depositories_41244.html*

101. *Deloitte, Cyber insurance gains momentum in India; set to witness exponential growth: Deloitte's report, https://www2.deloitte.com/in/en/pages/financial-services/articles/cyber-insurance-gains-momentum-in-India.html*

102. *RBI, Cyber Security Framework in Banks, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0*

103. *SEBI, Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporations and Depositories, https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporations-and-depositories_41244.html*

104. *RAJYA SABHA, RAJYA SABHA UNSTARRED QUESTION NO. 1043 CYBER SECURITY ATTACKS, https://sansad.in/getFile/annex/259/AU1043.pdf?source=pqars*

105. *CERT-In, Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet., https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf*

106. *RBI, Cyber Security Framework in Banks, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0*

107. *MeitY, Guidelines on Information Security Practices for Government Entities, https://www.meity.gov.in/writereaddata/files/Guidelines%20on%20Information%20Security%20Practices%20for%20Government%20Entities.pdf*

108. *RBI, Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12562&Mode=0*

109. *DSCI, Bridging the Gap: Identifying Challenges in Cybersecurity Skilling and Bridging the Divide, https://www.dsci.in/resource/content/bridging-gap-identifying-challenges-cybersecurity-skilling-and-bridging-divide*

110. *DSCI, Bridging the Gap: Identifying Challenges in Cybersecurity Skilling and Bridging the Divide, https://www.dsci.in/resource/content/bridging-gap-identifying-challenges-cybersecurity-skilling-and-bridging-divide*

ACKNOWLEDGEMENT

We extend our heartfelt gratitude to the esteemed members of the cybersecurity industry who actively participated in our study, study and generously shared their invaluable insights. Our sincere appreciation goes out to all the distinguished industry leaders and dedicated professionals for their significant contribution and unwavering support. It is with great acknowledgment that we recognize their pivotal role, as without their involvement, this report would not have come to fruition. On behalf of DSCI, we express our sincere thanks for their indispensable collaboration.

Authors:

Atul Kumar, Lead – Government Initiatives and Global Trade

Ankit Bhadola, Deputy Manager - Research

Contributors:

Amit Ghosh, Sr. Manager, Communications

Charu Sharma, Assistant Manager, Communications

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by nasscom, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

For more information, visit: www.dsci.in

DATA SECURITY COUNCIL OF INDIA

Nasscom Campus, Fourth Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

☎ +91-120-4990253 | ✉ research@dsci.in | 🌐 www.dsci.in

X DSCI_Connect f dsci.connect dsci.connect in data-security-council-of-india YouTube dscivideo

All Rights Reserved © DSCI 2023