DSCI
PROMOTING DATA PROTECTION

DSCI Digest

October 2024

DSCI Digest

The DSCI Digest is brought to you for a peripheral understanding of the industry-relevant studies conducted by DSCI. It aims to help you learn and understand the subjects in discussion in a succinct composition.

Table of Contents

Secure in India 2023

GCC empowered global cybersecurity and digital risk management

In an age of increasing digitization, trust and data are the key assets driving global organizations towards cyber GCCs for managing cybersecurity and digital risks. However, cyber GCCs are not only about 'protection' but also focus on 'anticipation', 'collaboration', 'unlocking horizontal value' and 'enabling business growth'.

But worldwide workforce shortage is the biggest concern in achieving these objectives. In this scenario, India's largest youth population and presence of 31.7% of global Science, Technology, Engineering and Mathematics (STEM) graduates, makes it a fertile ground for cultivating cyber talent. India`s emerging cybersecurity market is expected to reach a value of US$13.6 billion by 2025 and can help ensure a continuous pipeline of skilled professionals, positioning the country as a global leader in cybersecurity for years to come. GCCs in India, therefore, have a key role to play as they provide organisations across the world with a platform to access talent, skills and innovation. Therefore, sharing and adopting leading best practices is imperative for the nation. To establish cyber GCCs, top drivers to consider include- availability of cybersecurity skills (86%), cost arbitrage (75%), round the clock delivery (75%), cyber innovation, research and development (58%) and proximity with other business functions (53%). As cyber GCC organisations mature, expectations rise to enable global organisations to innovate, grow and sustain their businesses through continued, proactive and scalable cybersecurity and digital risk management capabilities. Organizations also capitalize on the GCC ecosystem for the same.

Over the years, Cyber GCCs witnessed a significant increase in team size. About 28% of global organisations have more than half of their global cybersecurity team strength in India. Accountability and influence of cyber GCC leadership has also risen. About 67% highlighted that global teams are reporting into the cyber GCC leadership, signifying growing stature and importance of cyber GCCs.

The GCC cybersecurity landscape is also seeing a rise in new functions like cybersecurity engineering, product management and automation, secure development, cloud security, and third-party risk management (including software supply chain security). They are responding by investing in these while maintaining their spending on the 'core functions' comprising cybersecurity and digital risk management.

94% of respondents have reported an increase in services delivered by cybersecurity functions, with more than 42% reporting about 50% increase. No cyber GCC reported de-growth, highlighting continued expansion of cybersecurity functions across cyber GCCs, including a significant rise in emerging functions to manage digital risks. They also act as cybersecurity debt catalysts and optimize the spend by providing strategies like advanced automation, cloud adoption to dedicated cybersecurity experts.

Amidst the surge in demand for cybersecurity skills, cyber GCCs are evolving their talent acquisition and development strategies. While cyber GCCs are looking to implement automation-based strategies, they are also looking to upskill and attract talent in emerging technologies and initiatives. The rise in demand for cyber skills, combined with shortage of specific skills, makes talent retention a key area of focus for cyber GCC leaders. Cyber GCCs have therefore embraced the DE&I (Diversity, Equity & Inclusion) agenda, focusing on inclusivity and empowerment as core values.

Cyber GCCs also plan to implement various strategies including external hire, using service providers, internal training and leveraging the gig workforce. They are exploring gig models for certain skill requirements such as technology, regulatory, audit and standards management and cyber forensics.

GCCs also encourage cross-functional experience or job-rotation, for deeper understanding of the business environment beyond the cyber function. Almost 69% of respondents acknowledge the value of active engagement with industry forums and special interest groups. This has contributed to increased attrition rate over the last 3 years.

With most cyber GCCs experimenting with emerging technologies for competitive advantage, the gap in knowledge and experience between a fresher and an experienced cyber professional is closing rapidly. Cyber GCCs are also adopting various methods to attract new age cyber talent including – mentorship, internship, defining structured cybersecurity curriculum, focused cybersecurity programs, and more.

To enhance the innovation quotient, GCCs are focusing on 1) innovation as a Key Performance Indicator (KPI), making the cyber GCC leadership accountable for defining and implementing the innovation agenda 2) leveraging cyber immersive labs, providing a gamified environment for experiential learning 3) setting up centers of excellence/dedicated teams for innovation in cyber, with clearly established outcomes. In addition, cyber GCCs are embracing open-source technologies, as they help tap into innovation through wider developer

community, open-source components and standards. The survey also found out that for effective cybersecurity management GCCs are actively deploying emerging and existing technologies like Cloud, Robotic Process Automation, Security Orchestration, Automation and Response (SOAR) and Security Operations Centre (SOC) Automation, Risk and Control Automation, Extended Detection and Response (XDR) and Extended Security Intelligence on Automation Management (XSIAM), and actively exploring the use of AI/ML including GenAI in enhancing productivity and improving accuracy of outcome.

GCCs also play a crucial role in cyber risk culture by managing top risks like third-party cybersecurity, software supply chain security, regulatory risk, expansion of cloud platforms and end-points and end-user compromise.. This gets supported by a data-driven risk reporting mechanism. However, GCCs face challenges like emerging tech cyber attacks, changing regulatory landscape, third-party risks, training/ retaining cybersecurity skills, budget constraints and developing and sustaining risk culture, to ones stemming from the OT and cloud fronts. The combat to challenges comes via training and awareness among many other approaches.

Post-pandemic, the imperative for collaboration within the cybersecurity ecosystem has grown. Therefore, Cyber GCCs have imbibed the culture of industry-wide collaboration. They also recognize the importance of harnessing capabilities of advanced, latest, and fit-for-purpose cybersecurity instrumentation to identify, detect, protect, respond, and recover from growing and active cybersecurity threats. Around 56% of cyber GCCs also support global organizations in setting up Cyber Fusion Centers (CFCs) that are central for cross-functional collaboration and innovation to manage cybersecurity with agility and comprehensive response capabilities. Cyber risk quantification and cyber insurance are also areas handled by cyber GCCs, and proactive leverage of global privacy practices to comply with DPDP Act are areas where GCC is pacing.

The entire survey is a lot more detailed and insight-driven, access the report to learn better on the ways to 'Secure in India': https://www.dsci.in/resource/content/secure-in-india-2023

Read the entire report here

INDIA

Cybersecurity Domestic Market Report 2023

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 investing in emerging technologies of Cloud and AI/ML where ~84% and ~97% of the analyzed organizations have invested in them, respectively. GenAI has also garnered significant attention, transforming how organizations approach automation.

Amongst these, cybersecurity has transformed into a central topic in boardroom discussions now. India's cybersecurity market has undergone a remarkable transformation, marked by substantial growth in fortifying digital defenses in the face of evolving threats. A pivotal driver of this expansion has been the investment in cybersecurity products.

Notably, these products have demonstrated extraordinary growth, growing by a CAGR of ~38% and witnessing an 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.

The report here unfolds the growth trajectory within the Indian cybersecurity market. It delves into the dimensions of the current cybersecurity spending and adoption trends, changes in cybersecurity priorities, preparedness, and best practices.

Global spending on information security and risk management has increased whereas spending on cloud and data security, and data privacy emerged as key trends. Coming to the Indian market, it was found that India's cybersecurity market grew at a CAGR of over ~30% during 2019-2023 to reach USD 6.06 billion in 2023. Demand for security offerings including web protection,

endpoint defense, network security, next-gen SOC to threat intelligence services and more are increasing in India. Regulatory requirements, digital transformation, and leveraging emerging technologies have also led to the formation and adoption of cybersecurity and risk management policies, frameworks, and security leaders directly reporting to the board.

The Indian cybersecurity market accounts for ~3% of the global cybersecurity market. The Government of India is actively fostering the growth of the cybersecurity industry, exemplified by allocating INR 400 crore for cybersecurity projects and INR 225 crore for CERT-In in the FY 2023-24 Union Budget. This demonstrates a commitment to fortify the nation's digital defenses.

Stringent regulatory requirements to increase BFSI and healthcare spending on cybersecurity, and remote work enablement are some of the key trends and drivers in India's cybersecurity domestic market. Moving onto cybersecurity procurement, Request for Proposals (RFPs) is the most leveraged medium in India that enables vendor capability validation. Direct Purchase on the other hand stems as another procurement method that gives more flexibility in securing cybersecurity products and services.

At present, India envisions to be a USD 1 trillion digital economy. The government has spearheaded research initiatives in critical areas such as infrastructure security, zero-trust architecture, supply chain trust, etc. Several cybersecurity projects and initiatives like the Indian Cybercrime Coordination Centre (I4C), Cyber Swacchta Kendra, Cybersecurity Grand Challenge, Cyber Surakshit Bharat, etc. have also been aligned.

India's cybersecurity expenditure has surged in response to increasingly stringent regulatory norms and the enactment of the DPDP Act 2023. Brand reputation and growing digital transformation across industries are also driving the investments. Major investments have been channeled into sectors such as BFSI, IT/ITES, government and PSUs, manufacturing, power, oil and gas, healthcare, pharmaceuticals, communication, and telecom, the key drivers of the nation's economic growth.

Product market analysis indicates a strong demand for API security solutions to safeguard products throughout their lifecycle, from development to deployment. Network security has also seen a shift in offerings with the adoption of ZTNA and SASE, from traditional security options like Firewalls, NAC, WAF, and VPNs. Cloud security has seen a massive jump in the last three years thanks to the increased adoption of cloud services. Organizations have also recognized that data security is pivotal to cyber resilience. They invest in security offerings such as Privacy by Design, Data Access Governance, Data Classification, PIA, and DBR to uplift data security.

Similarly, a significant increase in awareness around the importance of personal and sensitive information has driven organizations to invest in privacy offerings. Remote working has also contributed to demands for endpoint security for the endpoint services. IAM offerings are in

demand too and include MFA, identity federation, directory services, IGA, PAM, and API access governance. Risk management offerings that are in demand presently include IT vendor risk management, ITRM solutions, PIA, CASBs, ASRTM, and supply chain risk management.

On the services front, it has been observed that AUDIT & ASSESSMENT, THREAT INTELLIGENCE, and VAPT are leading the wing. Spending on services has been witnessed in security operations accounting for ~45% of the services market, security implementation, security testing, security consulting, and digital forensics and incident response (DFIR). However, the transformation is increasing the attack surface. The talent pool also remains a challenge as the workforce gap is expanding by 40%, and cybersecurity professionals constitute less than 5% of the overall workforce, as indicated by 47% of the corporates.

The constantly evolving threat landscape, constraints in remuneration provisions for skilled cybersecurity professionals, varied cyberattack pathways, and skilled threat actors are a serious challenge to the growth.
The impetus has also been on building cyber resilience where organizations invest in cyber insurance to protect against financial losses due to cyberattack incidents. Emphasis has also been put on enhancing resistance to cyber threats through employee training and awareness initiatives.

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 but organizations can achieve improved protection from unauthorized access and strengthen protection against ransomware by investing in cybersecurity initiatives.

To sum it up, the current scenario looks promising for the cybersecurity product market with a lot more to do and develop as time changes. More details on the domestic market are included in our report 'India Cybersecurity Domestic Market 2023', you can visit to gain more comprehensive insights:
https://www.dsci.in/resource/content/india-cybersecurity-domestic-report-2023

Read the entire report here

INDIA
Cyber Threat Report 2023

India's growing digital ecosystem is estimated to contribute over 20% to the country's GDP by 2026. However, with digital evolution, India has also emerged as the most targeted country regarding cyberattacks, accounting for 13.7% of all attacks worldwide.

A pervasive outbreak of cyberattacks has inflicted substantial financial losses on businesses as India advances its digitalization efforts across sectors. Cybersecurity has ascended to a strategic concern at the board level owing to the multifaceted nature of cyber threats. Therefore, the repercussions of such breaches were studied after analyzing approximately 400 million malware detections from over 8.5 million SEQRITE endpoint installations in India, since malware is a significant peril to the integrity of digital systems.

Cybercriminals are also engineering intricate and diverse attack methodologies. Every day, over half a million instances of malware are discovered. There is also a significant rise in behavior-based detection compared to signature-based detections due to the surge in constantly mutating malware variants such as polymorphic malware, zero-day exploits, and file-less attacks. Furthermore, the report delves into serious threats posed by ransomware attacks. The analysis indicates that the ransomware hit rate is higher than other malware categories. Therefore, the report attempts to bring forth the current cybersecurity landscape, particularly within the Indian context. It also highlights the proliferation of global threat vectors, driven by the increased frequency and sophistication of cyber threats.

Bringing observations from 2023, the predominant threats observed were Malware, Ransome, and Cyprtominers & Cryptojacking. Malware faced challenges with a signature-based approach. Ransomware continued to be the most pernicious manifestation of cybercrime, as a single ransomware security incident emerged for every cluster of 650 detections. Crypto miners and cryptojacking are surfacing as a tenacious menace in the cyberthreat panorama. They impact all significant computing systems and can

remain undetected for an extended period.
Talking about the industries that experienced the most cyber threats we had, the automobile industry, stated-backed threats in India, the education sector, the power and energy sector, the healthcare and manufacturing sector, logistics, banking, and financial sector. India has been a significant target for Advanced Persistent Threats (APTs) based on 500K installations, reveals a discernible uptick in Adware and Potentially Unwanted Applications (PUAs), highlighting the persistent prominence of malware as a significant threat due to the expansion of Android adoption.

Breaking down the threat landscape of Malware that had major domination, it was observed that its subtypes like Trojans (111.9 million), Infector (91.40 million), Worm (29.62 million), Potentially Unwanted application (19.48 million), and Exploits targeting software vulnerabilities (14.47 million) were the principal detections. Apart from these, threats like Ransomware (0.74 million), Cyrptojacking (5.28 million), and Adware (1.50 million) highlighted the multi-faceted threat landscape.

These detections were assisted by behavior-based detection as detecting malware has been a critical challenge with the signature-based approach that fails to effectively detect unknown or polymorphic malware strains that continuously mutate to evade signature recognition. Behavior-based detection focuses on analyzing the dynamic actions and patterns exhibited by potential threats, thereby offering a proactive and comprehensive defense. In 2023, over 12.5% of detections (~49 million) are attributed to behavior-based components. Over the years, we can see that behavior-based detections have increased. To measure the detection efficiency the total incidents vs. total detections ratio was taken as a key measure. This provided the data on ransomware being more difficult than malware due to increased difficulty in its detection. Moreover, cyber adversaries are now leveraging network-based exploits, making it is crucial to identify and comprehend the methodologies used by them as that will help organizations gain edge over the complexity of network infrastructure. Another route that adversaries are making the most of is by indulging in host-based exploits, a critical facet of the digital threat that leads cyber adversaries to compromise system integrity and extract sensitive information.

Mobile devices have replaced traditional systems as the primary internet access point, generating 60% of all internet traffic in 2022. This surge has increased exposure to threats like adware, potentially unwanted applications (PUAs), and malware. Coming to the Indian malware landscape, around 290 million detections have been noted across 10 states including Telangana, and Tamil Nadu which had the highest ratio of detections per installation, while Gujarat and Madhya Pradesh showed an increase in detections.

Sector-wise, the Automotive Supply Chain, Government, and Education sectors experienced the highest malware detections per installation base across the industry.
More to current threat landscape is set to be revolutionized with the coming of the AI-driven era as it is predicted to be governed by threats like:

- Ransomware and digital extortion
- AI-powered malware

- LoLbins- a nightmare for threat researchers
- Multi-factor authentication (MFA) fatigue attacks
- Deepfake for deceptive social engineering
- Hacktivism
- Exploitation of Supply chain vulnerabilities
- Auction of corporate access and sale of breach datasets
- Event-based attacks- like on elections, Olympics, etc
- Phishing/ vishing attacks and dating app scams

But key directives can be undertaken by CISOs to strengthen their preparedness against the evolving threats, these include:

- Maintaining a heightened state of alertness against Advanced Persistent Threats (APTs).
- Devising and implementing a resilient defense strategy to combat ransomware.
- Keeping abreast of the ever-changing cyber regulations and compliance requirements within the industry and jurisdiction.
- Integration of emergent technologies like artificial intelligence, quantum computing, 5G, and the Internet of Things.
- Fostering collaboration and coordination among CISOs and security professionals in your industry and region.

Cyber threats will keep advancing and evolving, as far as the predictions are concerned we have seen a lot of them materialize in the present day with more coming our way. Highlighting the criticalities was therefore important to capture the nuances of the changing times.

The entire landscape is mapped in much more detail including insightful featured stories and in-depth discussion of the mentioned exploits and predictions in our report on 'India Cyber Threat Report 2023' The mentioned details are enclosed and available for you at: https://www.dsci.in/resource/content/india-cyber-threat-report-2023

Read the entire report here

What to Expect in the Next Edition

The DSCI Digest offers a condensed version of all our publications, giving you a quick overview to help you decide on your next read.

The subjects catered here enable you to gain first-hand information on the volumes we bring out for the industry. The information shared is a brief account of the conducted studies. You are requested to visit the reports on our website for better understanding.

https://www.dsci.in/knowledge-center/study-and-reports

Authors

- "Secure in India 2023: GCC empowered global cybersecurity and digital risk management" by Ankit Bhadola
- "INDIA Cybersecurity Domestic Market Report 2023" by Ankit Bhadola
- "INDIA Cyber Threat Report 2023" by Neha Mishra

Compiler and Editor

Mridushi Bose, Content Marketing Manager

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by Nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit https://www.dsci.in/

DATA SECURITY COUNCIL OF INDIA

NASSCOM CAMPUS, FOURTH FLOOR, PLOT. NO. 7-10, SECTOR 126, NOIDA,
UP - 201303
+91-120-4990253 | INFO@DSCI.IN | WWW.DSCI.IN

dsci.connect dsci.connect dscivideo data-security-council-of-india DSCI_Connect