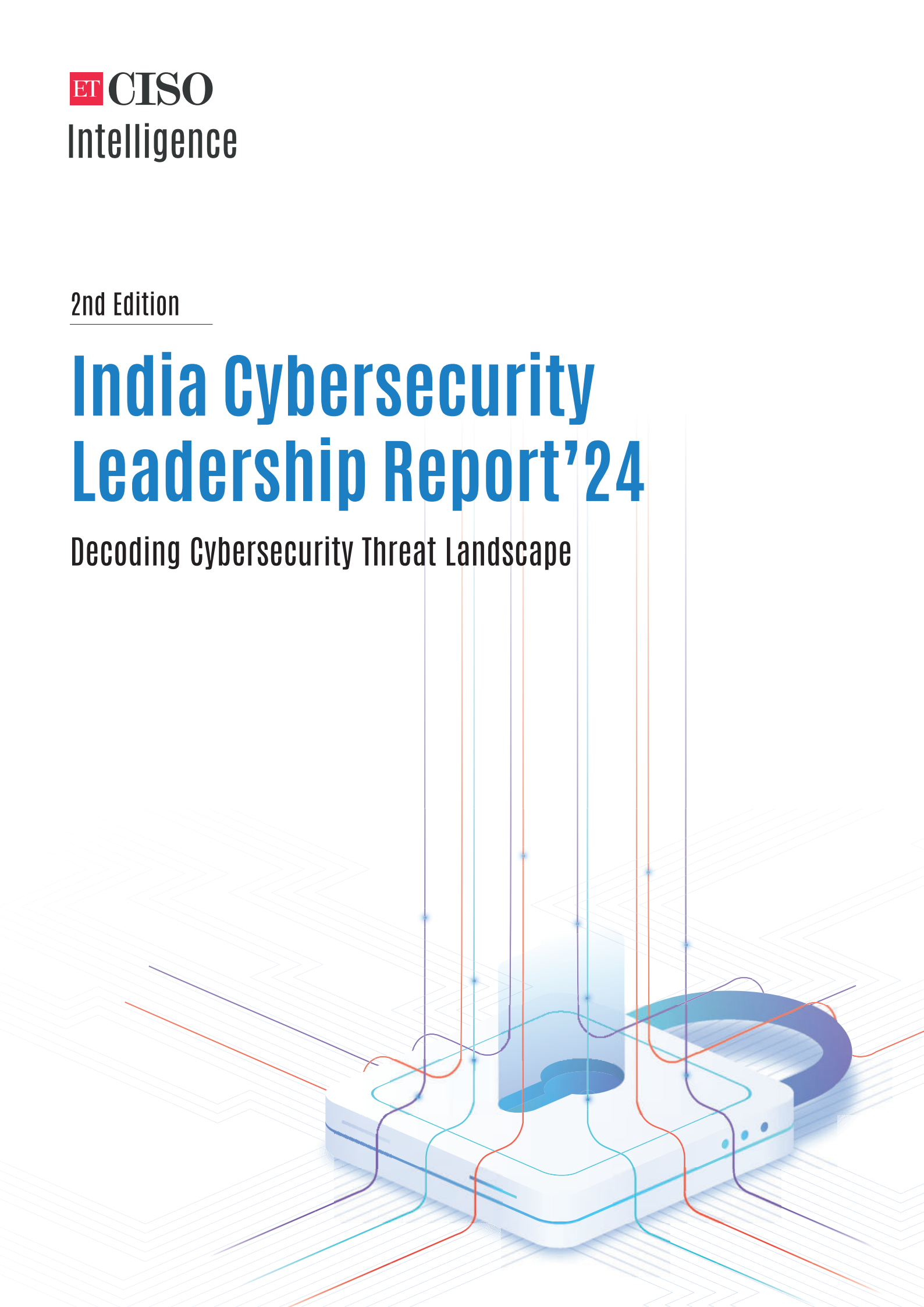
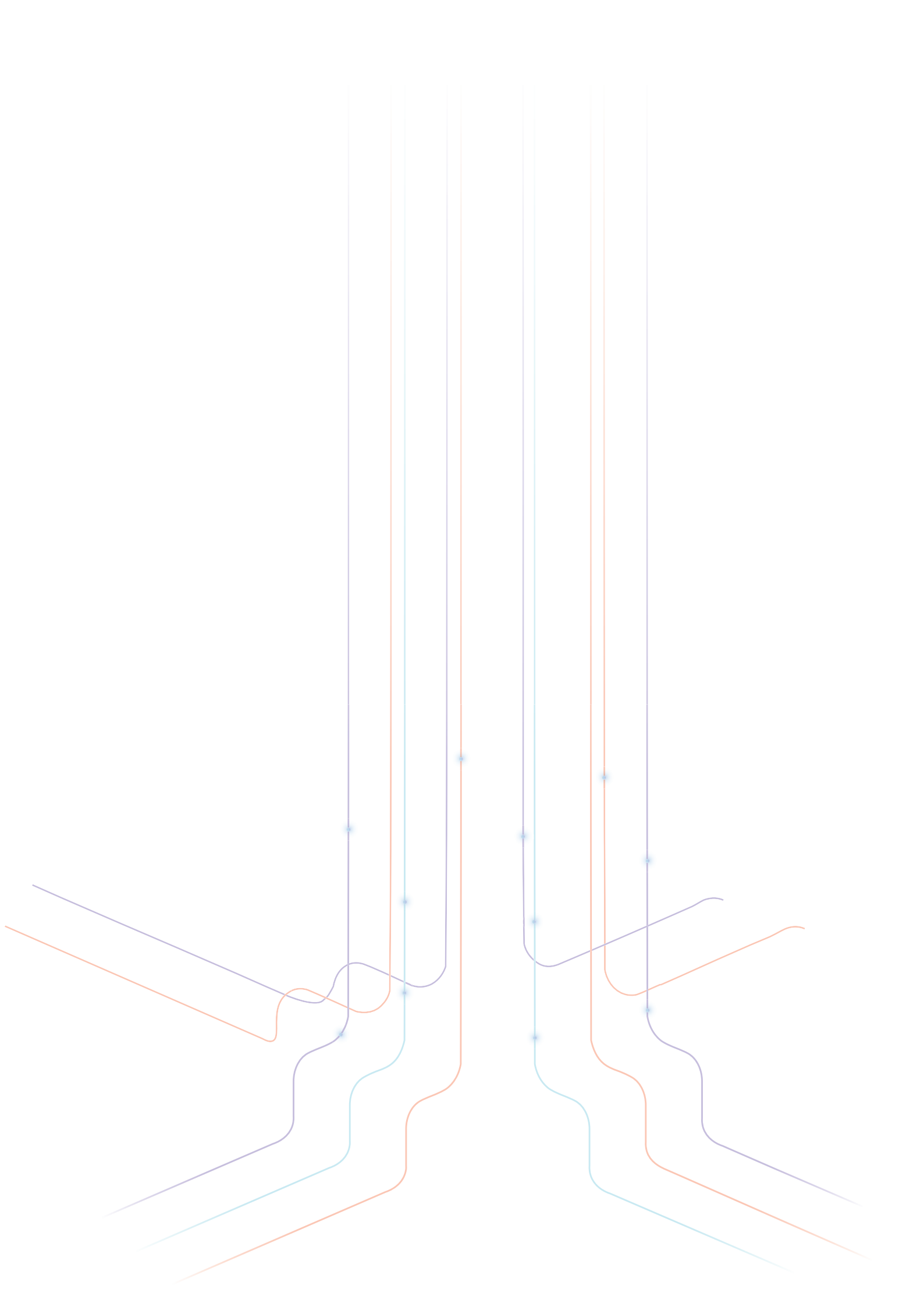
ET CISO
Intelligence

2nd Edition

India Cybersecurity Leadership Report'24

Decoding Cybersecurity Threat Landscape





FOREWORD

Beating the Bad Actors!

Shantheri Mallaya
Editor
ETCISO

Krishna Mukherjee
Senior Lead
Content & Community
ETCISO

In the timeless tale of 'Amrit Manthan', the battle between the asuras and devas symbolizes the eternal struggle between good and evil. Today, in the age of Kaliyuga, this ancient conflict finds a new context in the world of cybersecurity, where CISOs take on the role of devas, defending against the ever-evolving asuras—cybercriminals. The threat landscape continues to expand, with cyber perpetrators growing in strength, forcing organizations to ramp up their defenses.

As a result, cybersecurity has become a top priority, with budgets surging and cyber insurance gaining prominence. The 2nd edition of the ETCISO Intelligence Report highlights this trend, revealing that India Inc.'s average cybersecurity budget has climbed to 8.3% of the overall IT budget in FY'24, marking a 14% increase. This growth is fueled not only by the escalating threat landscape but also by progressive regulations pushing companies to strengthen their cyber defenses.

Emerging tools like GenAI are playing a pivotal role in this transformation, excelling in identifying vulnerabilities, analyzing threats, and enhancing incident response capabilities. With ransomware and cloud misconfigurations emerging as top concerns, the report underscores the growing necessity of making cybersecurity a central element of organizational strategy.

However, many companies are still operating with a "business-as-usual" approach to cybersecurity, relying on fragmented initiatives and navigating an increasingly complicated web of technologies. The challenge lies in overcoming obstacles like failed projects or misguided investments. Given the complexity of today's threats, it's essential to adopt a hedging strategy to mitigate potential losses if a cyber attack materializes.

Cyber insurance, much like traditional insurance, offers a lifeline during times of crisis. CISOs are yet to leverage the full power of cyber insurance.

Nevertheless, cybersecurity controls are no longer confined to individual organizations but must extend across the entire ecosystem—encompassing the broader mesh of digital transformation.

Content

About the Report

The ETCISO Intelligence Report, now in its second edition since its launch in 2023, focuses on cybersecurity threats and risks faced by Indian enterprises. This report serves as a comprehensive resource for understanding various facets of cybersecurity in India.

Key objectives of the study:

- **Current Cyber Threats and Risks:** Analyzing the primary threats and potential cybersecurity incidents that impact enterprises.
- **Financial Impact:** Examining the financial implications of cyber incidents, including the costs of data breaches and associated risks.
- **Cybersecurity Budgets and Investments:** Evaluating how much enterprises are investing in cybersecurity measures and the adequacy of cyber insurance.
- **Vendor Onboarding:** Understanding how enterprises prioritize vendor selection with respect to cybersecurity requirements.
- **Regulatory Compliance:** Reviewing how enterprises comply with existing cybersecurity regulations.
- **CISO Compensation and Reporting:** Studying the compensation structures for Chief Information Security Officers (CISOs) and their reporting hierarchies within organizations.

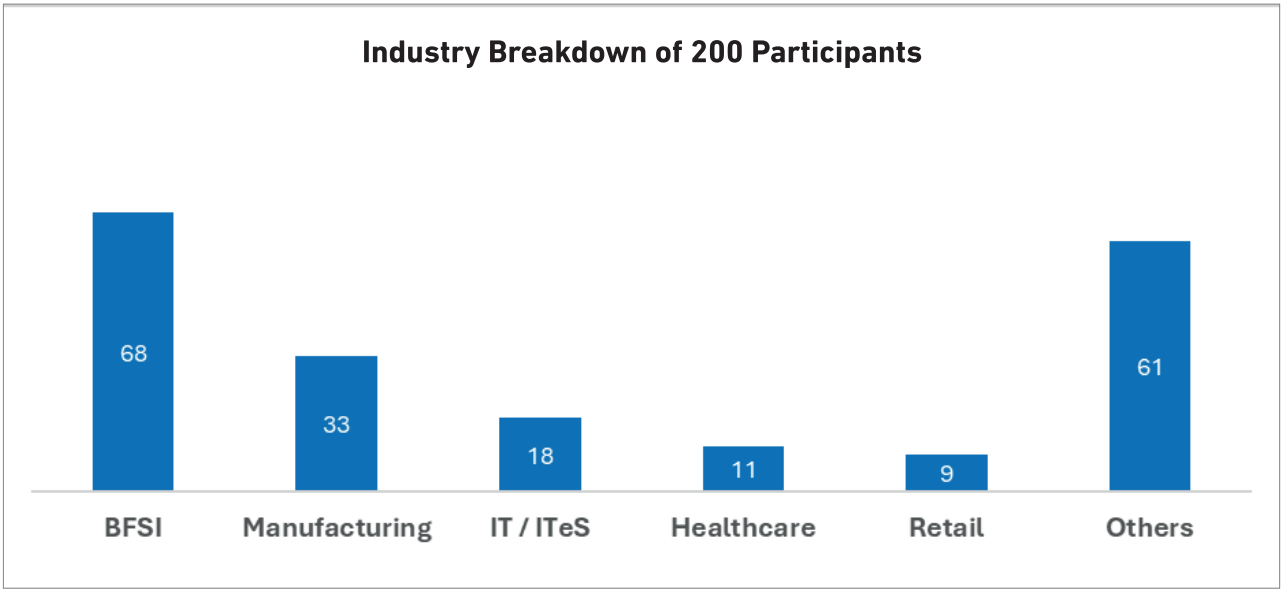
This report provides essential insights into how Indian enterprises are navigating the evolving cybersecurity landscape and what strategies are being employed to mitigate associated risks

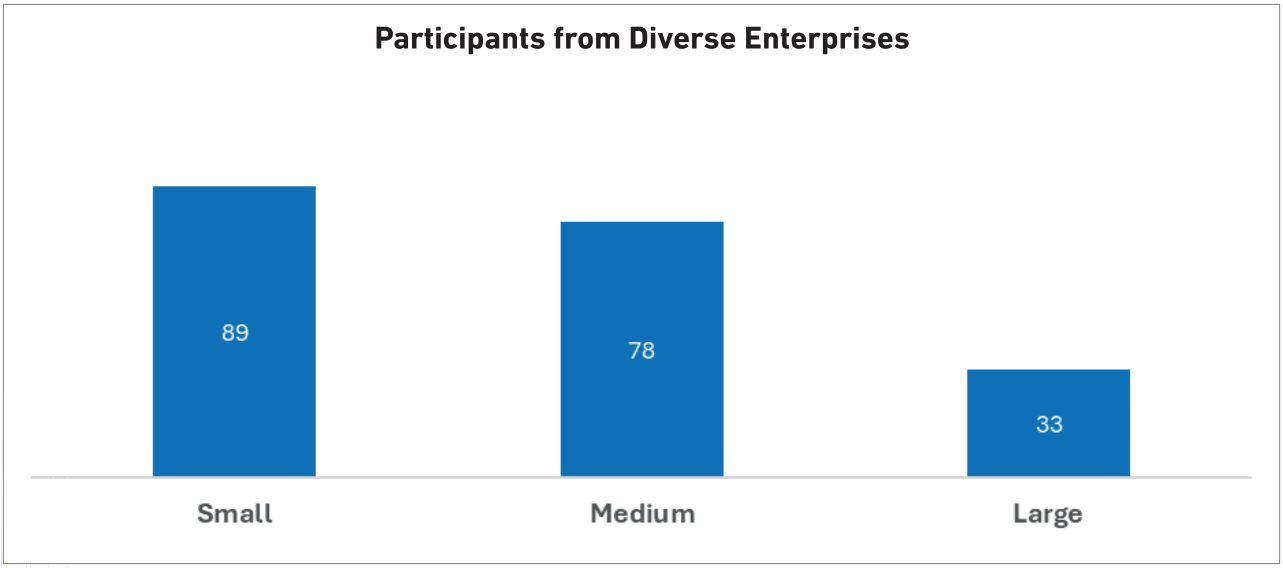
Methodology

The survey was conducted online through a structured questionnaire. The survey link was distributed to CISOs from various sectors, including BFSI, Manufacturing, IT/ITeS, and others, representing enterprises of different sizes. A total of 200 CISOs participated in the survey.

Enterprise Classification by Revenue (INR):

- Large enterprises: INR 30,001 Crore and above
- Medium enterprises: INR 2,001 Crore to INR 30,000 Crore
- Small enterprises: Less than INR 2,000 Crore





Executive Summary

DECODING CYBERSECURITY THREAT LANDSCAPE

In India's evolving digital ecosystem, enterprises are contending with critical cybersecurity threats, including ransomware (21%), cloud infrastructure vulnerabilities (17%), data breaches (12%), business email compromise (11%), and supply chain attacks (9%). These threats pose serious operational, financial, and reputational risks across multiple sectors.

FINANCIAL IMPACT OF CYBERSECURITY INCIDENTS

Cyber incidents in Indian enterprises can result in substantial financial losses (16%), operational disruptions (16%), reputational damage (14%), regulatory fines (13%), and the severe consequences of data breaches (11%). The financial toll of data breaches varies by sector. The BFSI sector faces the highest average losses due to the sensitivity of data involved, incurring losses of up to INR 17 crore per breach, while retail, despite frequent breaches, experiences lower costs, averaging INR 1 crore per breach.

ENTERPRISE SIZE AND RISK

Larger enterprises are particularly vulnerable to data breaches, with average financial losses reaching INR 21 crore per incident. In comparison, medium-sized enterprises face losses of INR 9 crore, and smaller enterprises bear losses averaging INR 7 crore.

CYBERSECURITY BUDGETS

The focus on cybersecurity is reflected in budget allocations, which now average 8.3% of overall IT budgets in Indian enterprises, marking an 11% increase over the previous year. The BFSI sector leads the way with the highest budget allocations, signaling its priority in defending against cyber threats.

PREPAREDNESS FOR REGULATORY COMPLIANCE

Indian enterprises display moderate readiness for the Digital Personal Data Protection (DPDP) Act 2023, with only 7% fully prepared and 17% very prepared. The IT/ITeS sector is the most advanced, with 41% of companies either fully or very prepared to meet the new regulatory requirements.

CYBERSECURITY INSURANCE

More Indian enterprises are adopting cybersecurity insurance to mitigate risks, although coverage limits differ across industries. The BFSI sector has the highest average coverage, at INR 200 crore.

VENDOR PARTNERSHIPS FOR CYBERSECURITY

Collaborating with vendors for endpoint security (21%), network security (14%), and cloud security (13%) is essential for enterprises to manage the diverse cyber threats prevalent across different sectors.

CISO COMPENSATION AND REPORTING

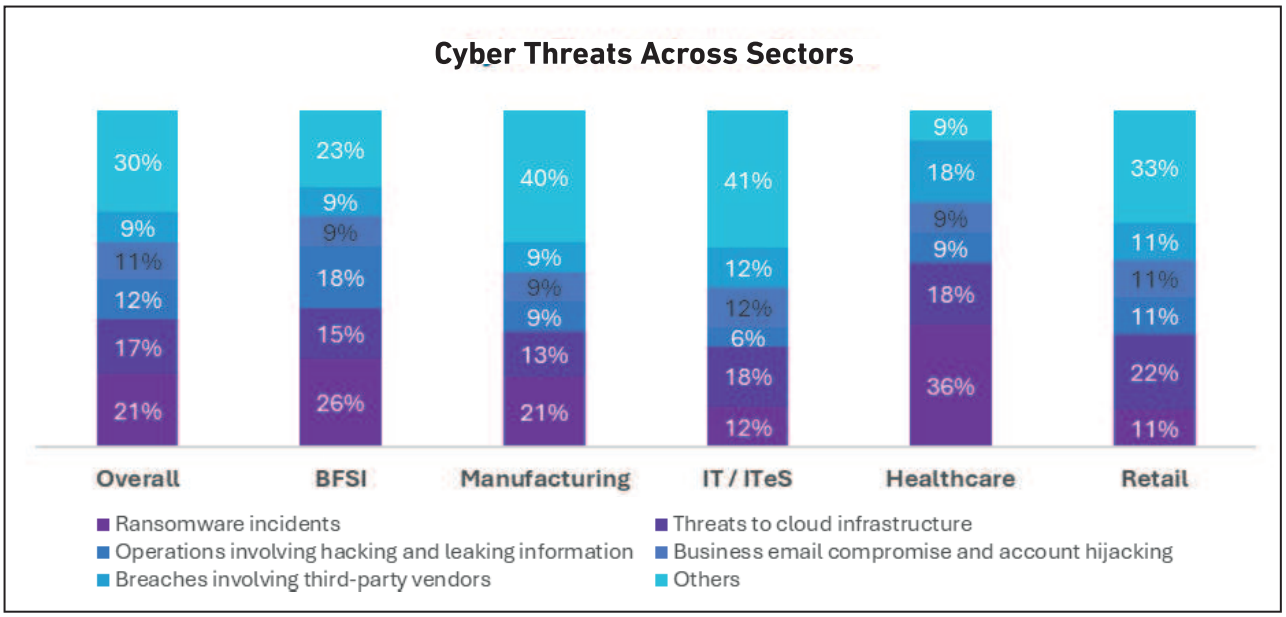
The average annual salary of CISOs in India has risen to INR 73 lakhs, reflecting an 11% increase from last year, driven by the rising complexity of cybersecurity challenges. Most CISOs (38%) report to CIOs, although many express a preference for direct reporting to CEOs or CROs to enhance strategic decision-making in cybersecurity.

CONCLUSION

As Indian enterprises adopt digital technologies, the cybersecurity landscape becomes increasingly complex. Managing the growing array of threats requires a multifaceted approach involving adequate budgets, robust vendor partnerships, regulatory compliance, and strong leadership from CISOs. This narrative sheds light on the challenges faced by Indian enterprises and the strategies they are employing to safeguard their operations and data in this digital age.

The Rising Tide of Cyber Threats

Ransomware and cloud-related risks are among the top cyber threats; BFSI sector particularly vulnerable to hacking and data breaches



In the coming year, Indian businesses must stay vigilant to several ongoing cyber threats:

- **Ransomware: A Persistent Menace**
  Ransomware remains a major concern, with attackers demanding large ransoms to unlock encrypted data. This threat poses significant risks across industries, particularly in the industrial and healthcare sectors, where the consequences can be catastrophic.

Driven by rising cyber threats and the push from progressive regulations, budgets for cybersecurity have increased substantially. A few years ago, they ranged from 5% to 8%, but now, in the BFSI sector, they exceed 10% to 15% of IT budgets. Cybersecurity investments have become central to IT budget planning. Given the complexity of cyber threats, it's crucial to implement hedging strategies to offset the steep losses in case of a cyberattack.

SAMEER RATOLIKAR, *CISO, HDFC Bank*

Cybersecurity is not just a shield, it's a strategic enabler for India's digital growth. As we journey towards a digitally secure India, we must harness cutting-edge technologies while upholding our national values. By implementing SOAR solutions, we're streamlining our cybersecurity operations. Incident response and cyber hygiene must become second nature to every Indian netizen. A secure digital India is not just a dream, it's a collective responsibility. By embracing this holistic approach, we're not just shielding our digital assets, but igniting a beacon of technological sovereignty that will illuminate India's future for generations to come.

DR. KUSHAL PATHAK, *Joint Secretary (Systems, Capacity Building and CISO), Rajya Sabha Secretariat, Parliament of India*

- **Cloud Infrastructure Security: A Growing Concern**
  As more organizations move to cloud computing, securing cloud infrastructure is becoming critical. Common issues like misconfigurations, unauthorized access, and data breaches are on the rise. The IT/ITeS, healthcare, and retail sectors, in particular, are experiencing an increase in cloud-related security threats, emphasizing the need for robust cloud security practices.

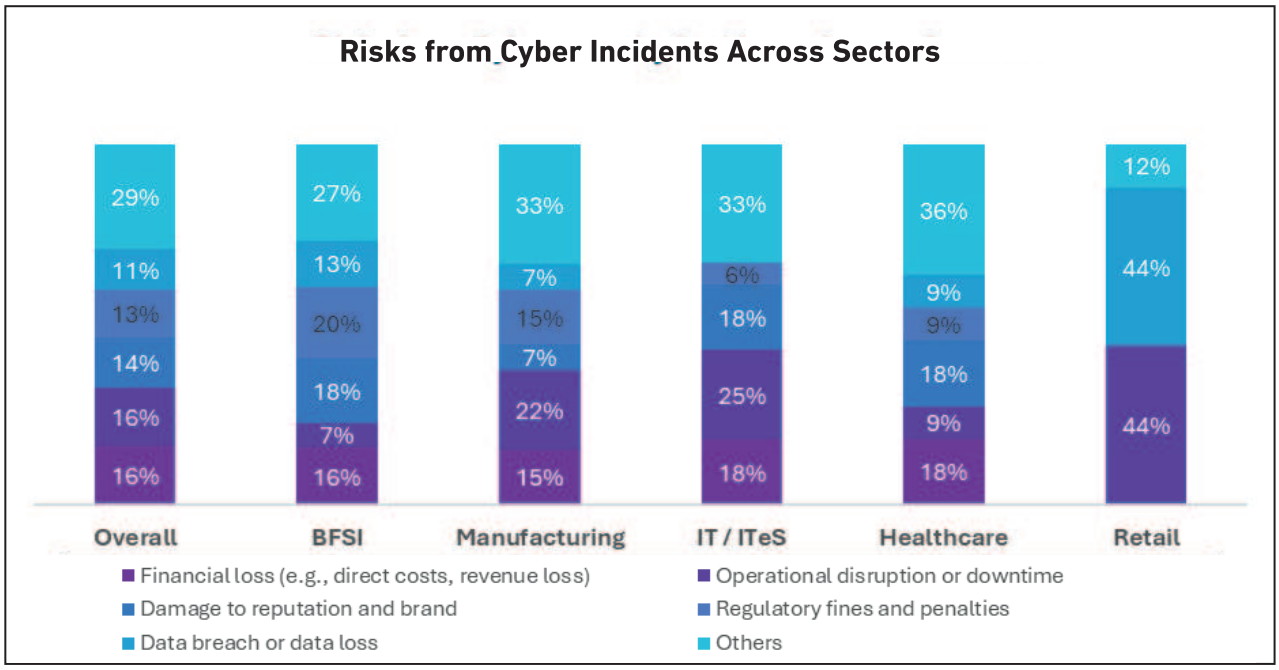
- **Data Breaches and Information Leaks**
  Data breaches involving unauthorized access and the leakage of sensitive information continue to be a pressing concern. The BFSI (Banking, Financial Services, and Insurance) sector is especially vulnerable, with breaches leading to significant financial losses and reputational damage.

- **Business Email Compromise (BEC) and Account Hijacking**
  BEC and account hijacking present major risks, where attackers gain unauthorized access to legitimate email accounts. These attacks can result in financial loss, data theft, and reputational damage across various sectors.

- **Supply Chain Attacks**
  Supply chain attacks, in which cybercriminals exploit vulnerabilities in third-party vendors, are a growing threat to all industries. Companies must rigorously evaluate and monitor their suppliers to reduce this risk.

Mitigating Cybersecurity Incident Risks

Financial loss & downtime are top risks from cybersecurity incidents; BFSI faces higher fines, healthcare reputational damage



Cybersecurity incidents can have significant and widespread consequences for Indian enterprises:

- **Financial Loss:** Financial damage is a major concern for businesses facing cybersecurity threats, resulting in direct financial losses, revenue disruptions, and regulatory penalties. Nearly all sectors are at risk of experiencing substantial financial setbacks.

Top attack vectors which can cause maximum potential impact to any organisation are ransomware, DDOS, software supply chain attack and technology obsolescence. As is indicated by the survey, to mitigate these and similar risks, organizations have significantly increased their investments in strengthening their IT risk observability/ visibility of events, layered defenses, cyber resilience, and build advanced testing and simulation capabilities. Many CISOs still find them inadequate. I recommend regular efficacy assessments to optimize tool use, measure ROSI, and justify any additional funding needed to tackle the evolving threat landscape.

RAJESH THAPAR, *CISO, NSE*

- **Operational Disruption and Downtime:** Cyber incidents can cripple business operations, particularly in industries that depend on continuous functioning like retail, IT/ITeS, and manufacturing. Such disruptions often lead to considerable financial losses, reputational damage, and long-term economic struggles.

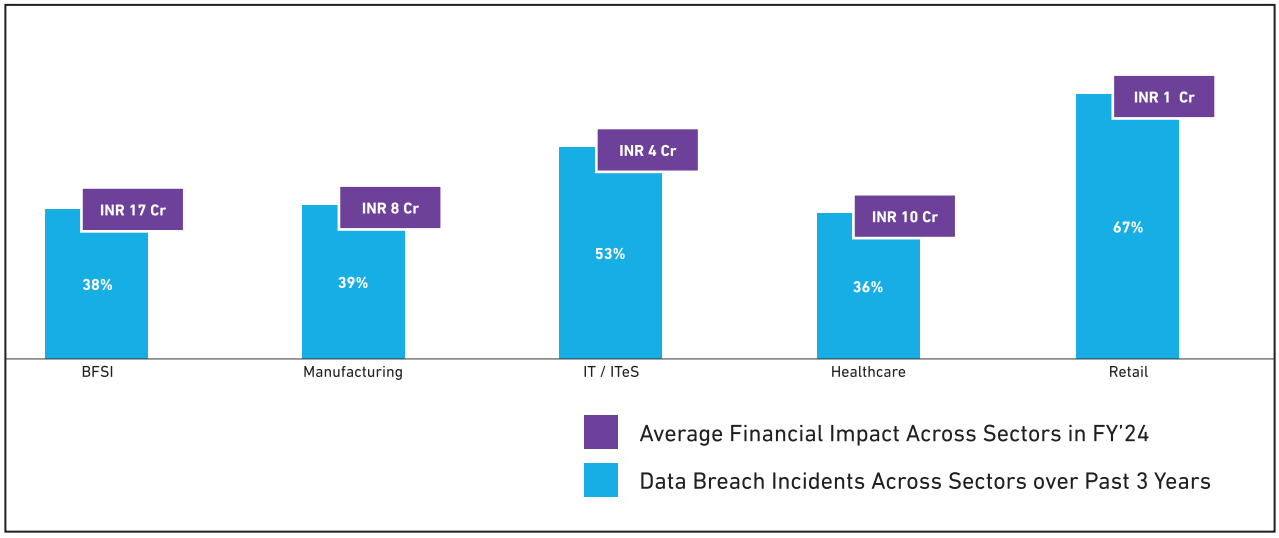
- **Damage to Reputation and Brand:** Reputational harm is one of the most enduring consequences of a cybersecurity breach. Unlike financial or operational losses, damage to a company's reputation can severely impact customer trust and brand value, particularly in sectors such as BFSI, IT/ITeS, and healthcare.

- **Regulatory Fines and Penalties:** In India, failing to comply with data protection and cybersecurity regulations can result in hefty fines. The government has enforced regulations such as the Personal Data Protection Bill (PDPB), the Information Technology Act, and CERT-In guidelines. The BFSI sector faces particularly stringent regulations, with severe penalties for non-compliance.

- **Data Breach and Data Loss:** The risk of data breaches is high due to increased reliance on technology. Sectors like retail and BFSI are especially vulnerable, with breaches leading to significant financial and operational consequences.

Financial Impact of Data Breaches

India Inc's average data breach cost stands at about INR 10 CR in FY'24



The financial impact of data breaches varies across sectors:

- **BFSI:** The sector incurs the highest average financial loss at INR 17 crore per breach due to the sensitivity of financial data.
- **Retail:** Despite accounting for 67% of data breaches, the retail sector faces the lowest average financial loss at INR 1 crore, reflecting frequent attacks but lower costs per breach.
- **Healthcare:** With an average loss of INR 10 crore, healthcare is increasingly targeted due to the rise in digital health technology and sensitive patient data.
- **Manufacturing and IT/ITeS:** These sectors see moderate financial losses, averaging INR 8 crore and INR 4 crore per breach, due to their heavy reliance on technology and potential for operational disruption.

The increasing dependence on digital ecosystems means that organizations can no longer afford to ignore the risks posed by cyber vulnerabilities. Cybersecurity strategies must continuously adapt to keep up with evolving threats. From updating security toolsets to adopting advanced AI-driven solutions, enterprises are recognizing the need to strengthen their defenses against both current and emerging risks. Even conservative sectors are investing heavily in tools, technologies, and policies to address emerging risks.

KALPESH DOSHI, *CISO, HDFC Life*

Additionally, enterprise size plays a role:

- **Small Enterprises:** 50% of small businesses experienced a data breach over the past three years, with an average financial impact of INR 7 crore.
- **Medium Enterprises:** 30% have faced breaches, with average losses of INR 9 crore.
- **Large Enterprises:** One in three large enterprises has experienced breaches, facing significantly higher losses averaging INR 21 crore.

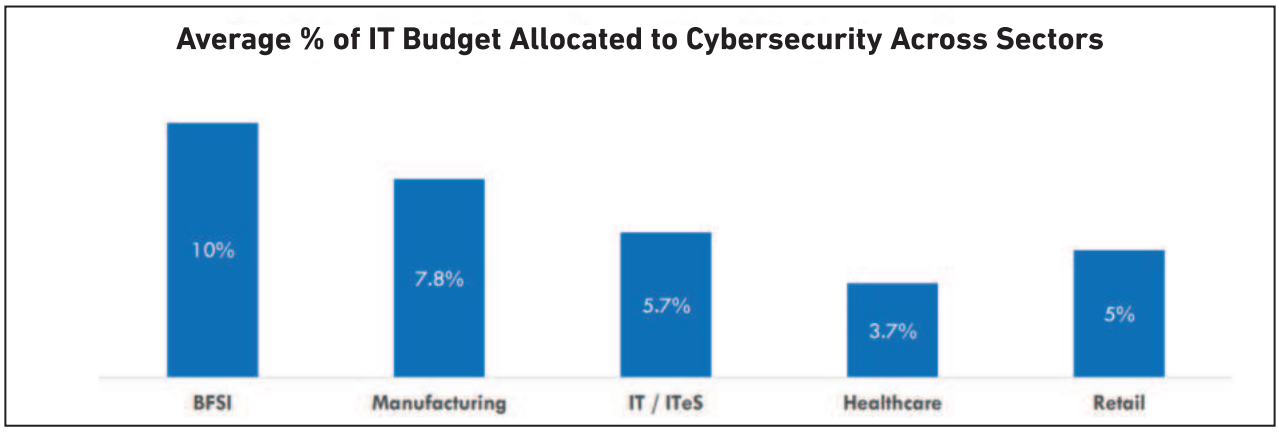
STRATEGIC MEASURES FOR INDIAN ENTERPRISES

To effectively address cybersecurity threats and reduce risks, Indian enterprises should:

- Develop comprehensive cybersecurity strategies to counteract diverse threats such as ransomware, cloud security risks, and data breaches.
- Invest in employee training, advanced security technologies, and incident response preparedness.
- Ensure regulatory compliance with data protection and cybersecurity laws to avoid penalties and maintain operational continuity.

Cybersecurity Investment Scenario

India Inc's average cyber security budget reached 8.3% of IT budget in FY'24 from 7.5% last year

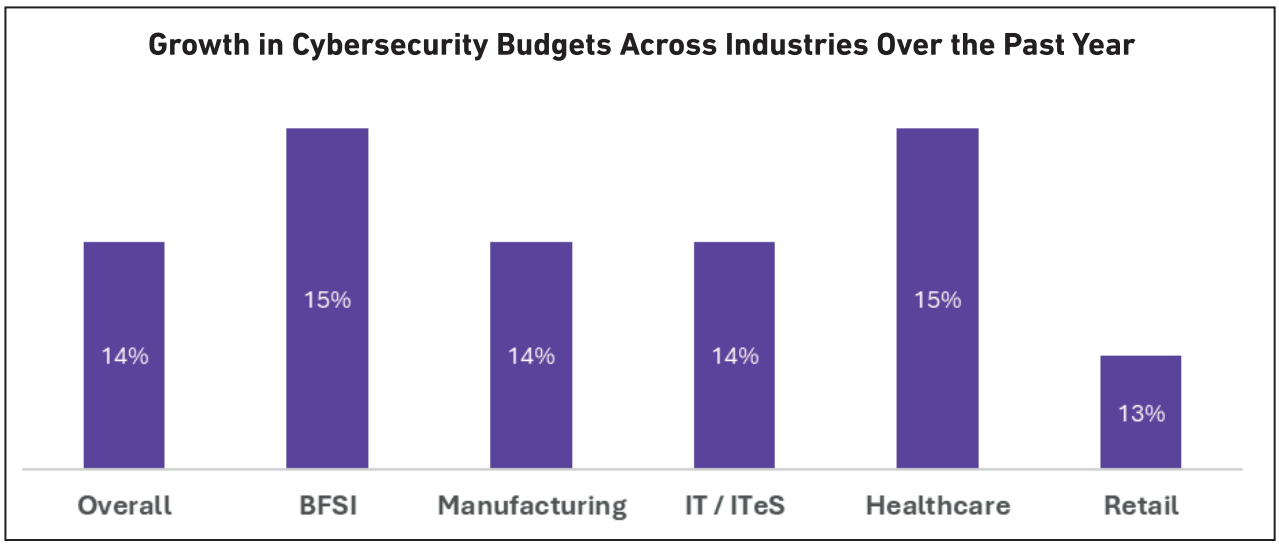


In the dynamic realm of cybersecurity, Indian enterprises are increasingly realigning their investment strategies. For FY'24, the average cybersecurity budget allocation of IT budget rose to 8.3%, up from 7.5% the previous year. This growth underscores the heightened awareness of the importance of robust cybersecurity measures in response to the rising threats.

Among the sectors, the BFSI (Banking, Financial Services, and Insurance) industry leads with the highest average cybersecurity budget allocation at 10%, reflecting the sector's pressing need to protect sensitive financial data from cyber threats.

Rise in Cybersecurity Budgets Across Industries

India Inc's average cybersecurity spending up by 14% in FY'24



India Inc raised its average cybersecurity spending by 14% in FY '24, driven by an intensifying threat environment and the need for advanced cybersecurity solutions. The increase in budgets was seen across all sectors, including BFSI, manufacturing, IT/ITES, healthcare, and retail, as businesses recognize the need to bolster cybersecurity to safeguard operations and reputations.

CISOs project further budget increases, with cybersecurity professionals anticipating a potential 20% rise in the near future. This highlights the sustained importance of cybersecurity investments.

By prioritizing cybersecurity, organizations can allocate sufficient resources to meet evolving threats. Developing a comprehensive cybersecurity plan tailored to specific risks, conducting regular security assessments, and collaborating with industry peers to share knowledge and best practices are essential strategies for staying ahead of emerging threats.

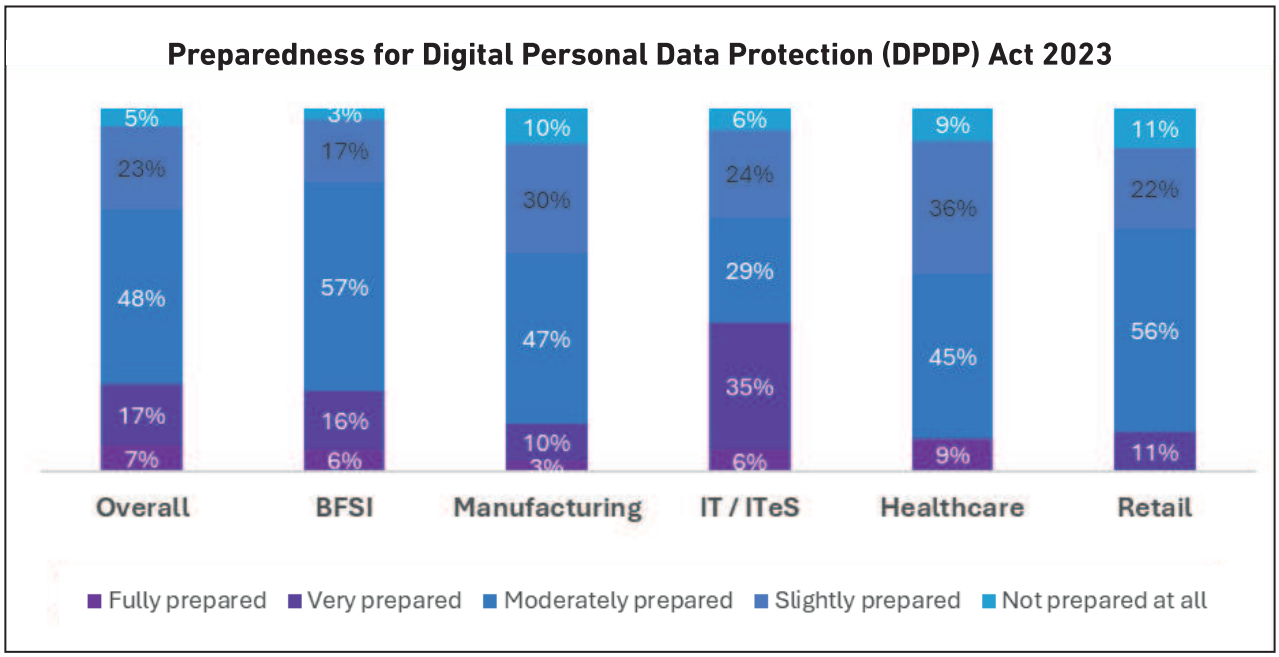
Since 2021, the cybersecurity budget has been increasing by leaps and bounds. While the standard metric is typically the percentage of the IT budget, I believe this should be reconsidered with a broader base. It could instead be a function of factors such as the number of users, the overall IT budget, and company profits. Soon, cybersecurity will likely account for a double-digit percentage of the IT budget.

DR DURGA PRASAD DUBE, *EVP & CISO, Reliance Industries*

Navigating the Digital Personal Data Protection (DPDP) Act 2023

Enterprises show a moderate level of readiness for the DPDP Act, with IT/ITES leading the way at 41% being fully or very well-prepared

The Digital Personal Data Protection (DPDP) Act 2023 introduces stringent requirements for Indian enterprises. Key mandates include appointing a Data Protection Officer (DPO), obtaining explicit consent, minimizing data collection, ensuring data retention aligns with its purpose, securing cross-border data transfers, and promptly notifying breaches.



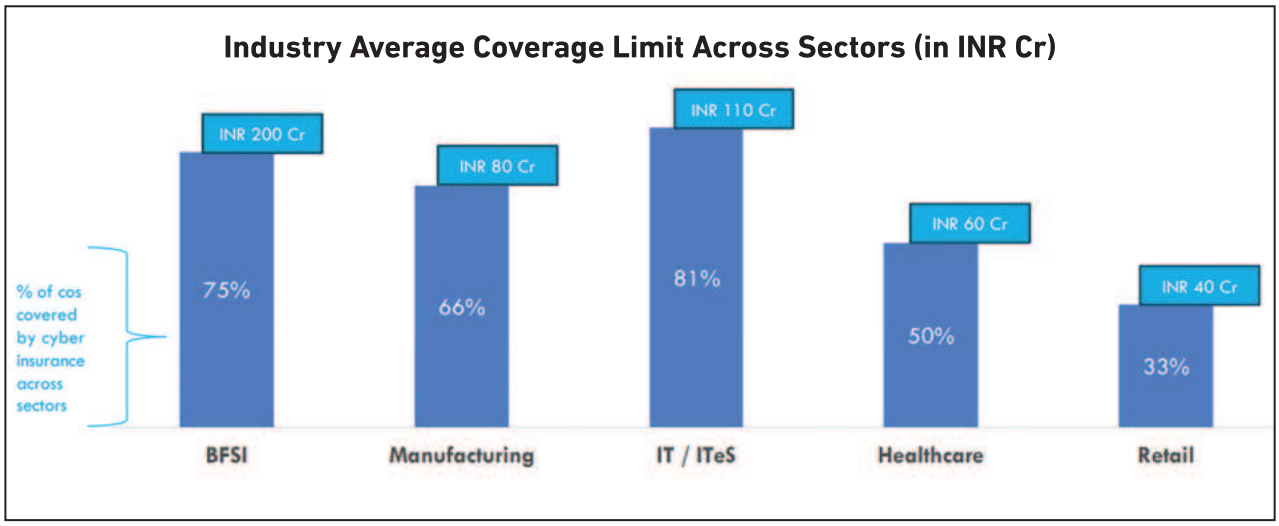
While enterprises show moderate preparedness for the DPDP Act, only 7% are fully prepared and 17% are very prepared. The IT/ITES sector leads in compliance readiness, with 41% of companies either fully or very prepared. In contrast, the healthcare and retail sectors report the lowest levels of readiness.

Non-compliance with the DPDP Act can result in severe penalties, including fines of up to INR 500 crore or imprisonment, along with increased risks of data breaches and reputational harm. To avoid these consequences, organizations must build strong compliance frameworks, conduct thorough assessments, create dedicated DPDP teams, train employees on data privacy, update policies, and carry out regular audits. While the IT/ITES sector is ahead in preparedness, other sectors, particularly healthcare and retail, must accelerate their efforts to mitigate risks and avoid penalties.

India Inc's Cybersecurity Insurance Coverage: A Growing Imperative

India Inc's average annual cybersecurity insurance coverage is INR 100 crore, with 62% of companies insured

Cybersecurity insurance is becoming a crucial risk management tool. As cyber threats continue to evolve, cybersecurity insurance can provide financial protection in the event of a data breach or other cyber incident.



More than 3 in every 5 companies own a cybersecurity policy implying that Indian businesses are taking proactive steps to protect themselves against cyber threats.

India Inc's average cybersecurity insurance coverage limit stands at INR 100 crore annually which indicates a growing awareness of the importance of cybersecurity insurance among Indian businesses.

BFSI/ITES sectors have the highest average insurance coverage limit as they often handle sensitive data recognizing the need for greater cybersecurity protection.

There remains a gap in coverage limits across sectors as every enterprise should have a cybersecurity policy.

There is a significant difference in coverage limits across company sizes. Large companies have the highest average coverage limit at INR 115 crore, followed by medium-sized companies at INR 110 crore. Small companies have the lowest average coverage limit at INR 73 crore.

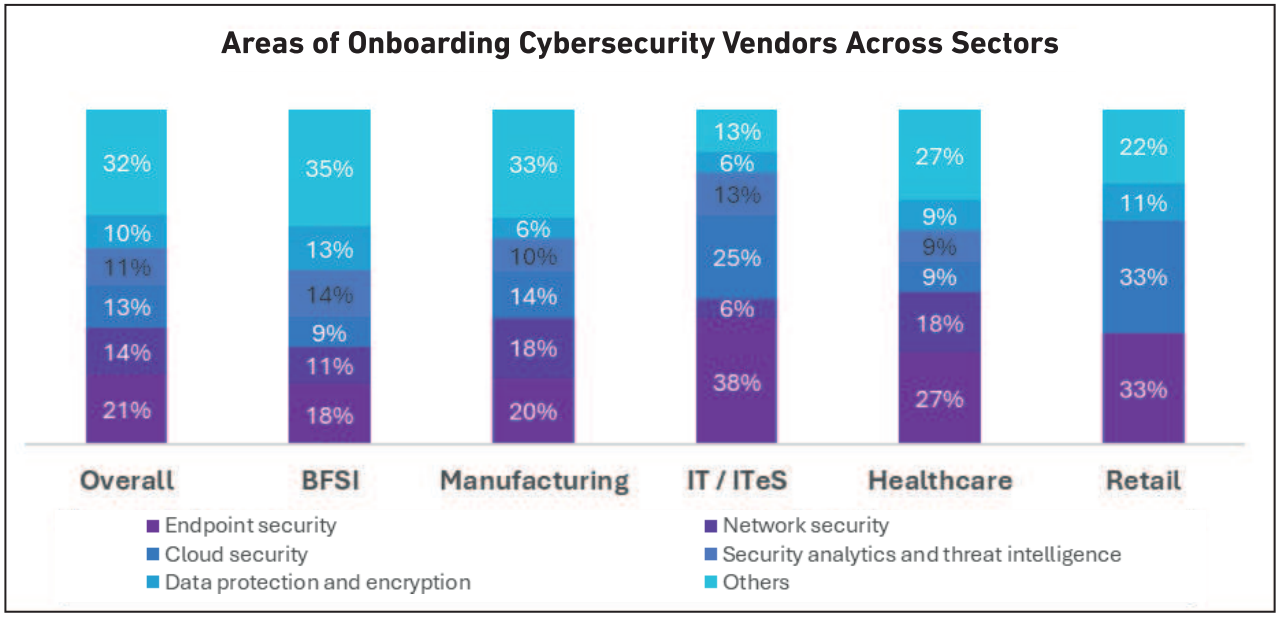
A majority of companies in all size categories own cybersecurity policies. About 67% of large companies, 65% of medium-sized companies, and 58% of small companies have cybersecurity insurance coverage.

Enterprises should routinely evaluate their cybersecurity risk in order to determine the proper coverage levels. They must regularly assess their cybersecurity policies to ensure that they remain effective and resilient against new attacks as the threat landscape changes.

The Strategic Advantage of Partnering with Cybersecurity Vendors

Endpoint security is the top priority for vendor onboarding across all sectors, while cloud security is also critical for IT/ITES and retail

Partnering with cybersecurity vendors gives organizations access to expert knowledge and advanced technologies to manage and reduce security threats. Vendors offer scalable, cost-effective solutions that align with the organization's growth and budget, often more affordable than an in-house team. Outsourcing cybersecurity helps reduce risks, meet regulatory requirements, and improve overall security, allowing organizations to focus on their core business while experts protect their sensitive data.



Endpoint security is the top priority for vendor onboarding across all sectors, highlighting a strong focus on protecting devices and systems from cyber threats. These solutions help prevent malware infections, data breaches, and other cyber incidents.

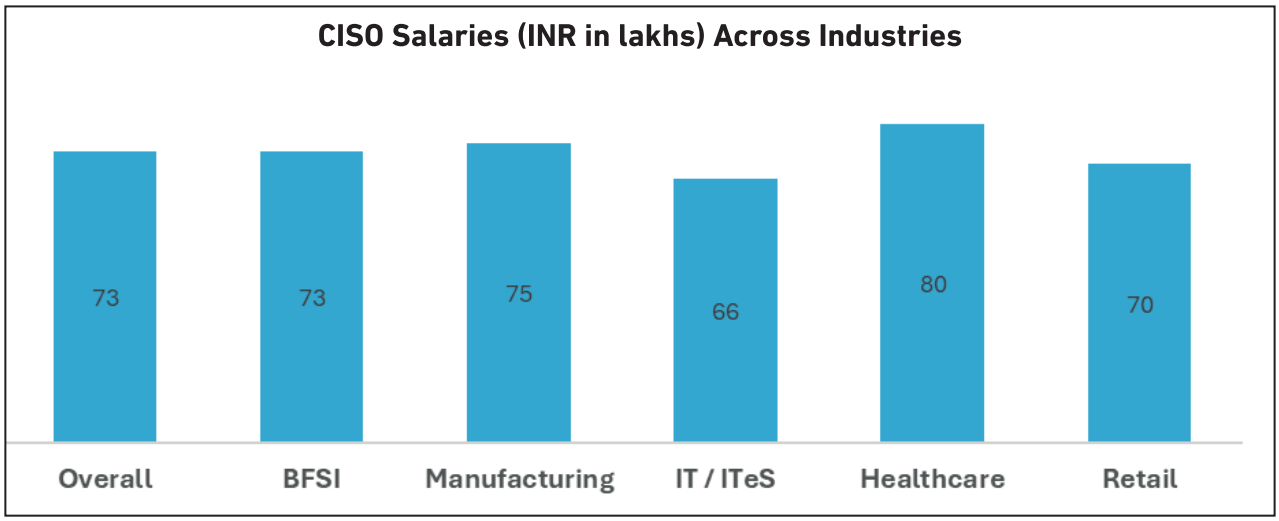
Network security is crucial for the manufacturing and healthcare sector for onboarding vendors. These industries often handle sensitive data, critical infrastructure, and patient information, making them particularly vulnerable to cyber threats.

Cloud security is a crucial area for IT/ITES and retail sectors, which often rely heavily on cloud-based infrastructure and recognize the importance of securing their cloud environments.

A comprehensive cybersecurity strategy requires a focus on multiple areas. Organizations should consider a range of cybersecurity measures, including endpoint security, cloud security, network security, data protection, and threat intelligence, to protect themselves from cyber threats.

The Evolving Role and Compensation of CISOs in India

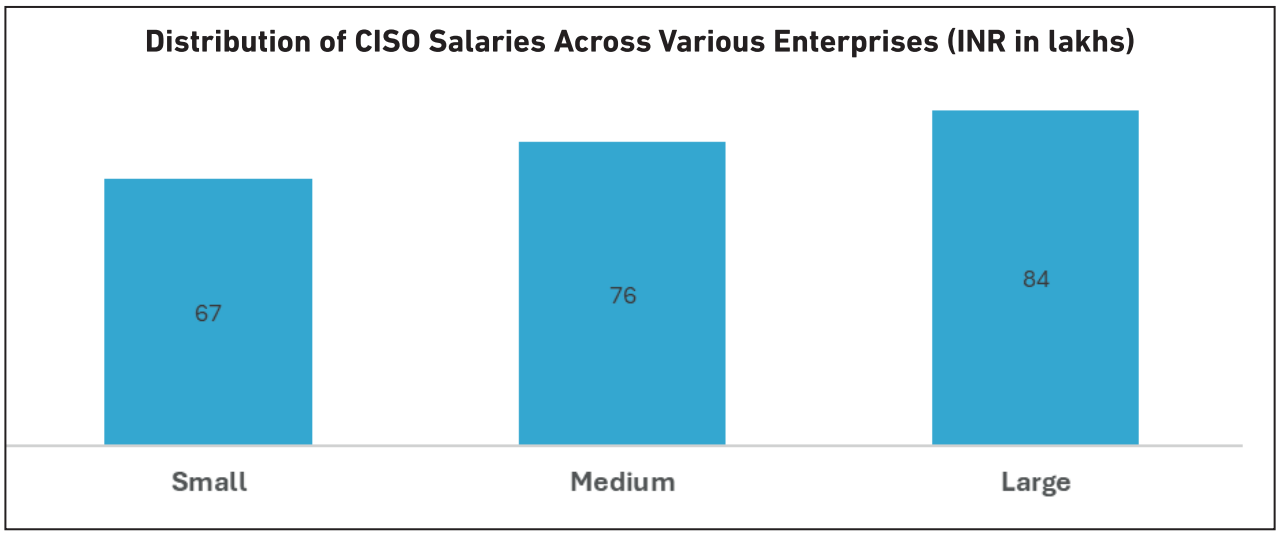
Average annual salary for CISOs stands at INR 73 lakhs



CISOs in India command a substantial average annual salary of INR 73 lakhs with a growth rate of 11% over last year. The rising salary levels suggest a growing demand for CISOs in India, driven by the increasing complexity of cybersecurity threats and the need for robust data protection measures.

The healthcare sector offers the highest average annual salary for CISOs at INR 80 lakhs, with a growth rate of 12.3%, reflecting the critical role they play in protecting sensitive patient data and securing medical infrastructure.

The consistent salary growth likely reflects the premium placed on the specialized skills and expertise required to effectively manage cybersecurity risks. The increasing demand for their skills, coupled with the growing complexity of cybersecurity threats, is likely to drive further salary growth in the coming years.



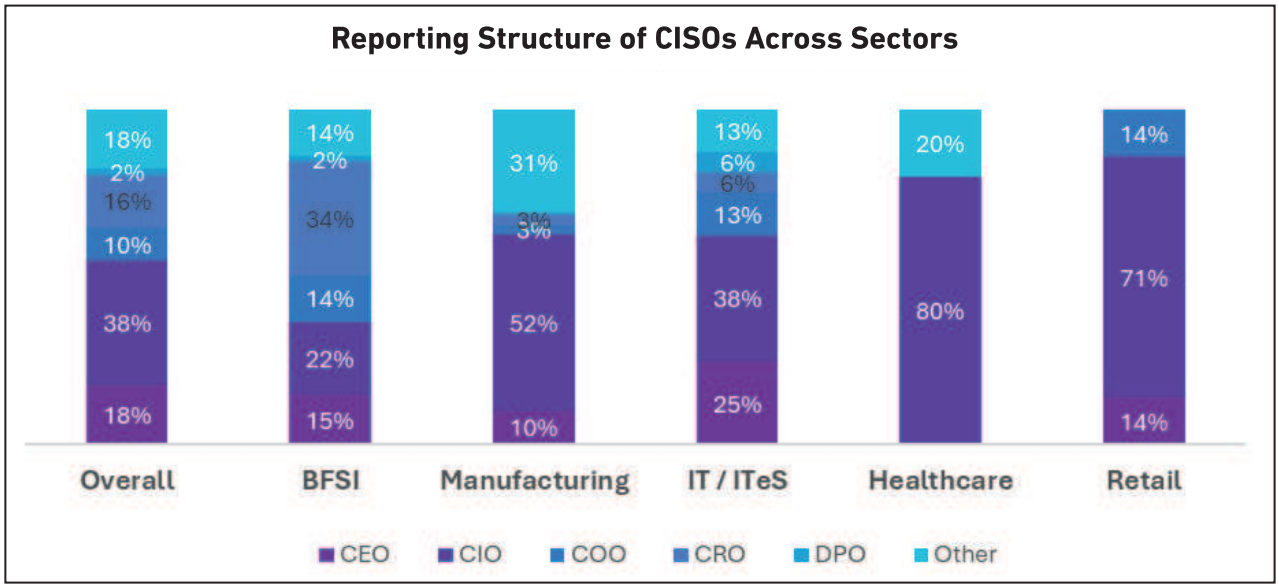
The average annual salary of CISOs increases with the size of the enterprise.

Medium-sized enterprises have experienced the most significant increase in CISO salaries over the past year, with a growth rate of 11.4%. The higher growth rate indicates a greater emphasis on cybersecurity as a strategic priority for this segment.

All enterprise sizes have seen salary growth for CISOs, indicating a rising demand for cybersecurity expertise across the board.

The Evolving Reporting Structures of CISOs

Five out of seven CISOs prefer not to report to the CIO

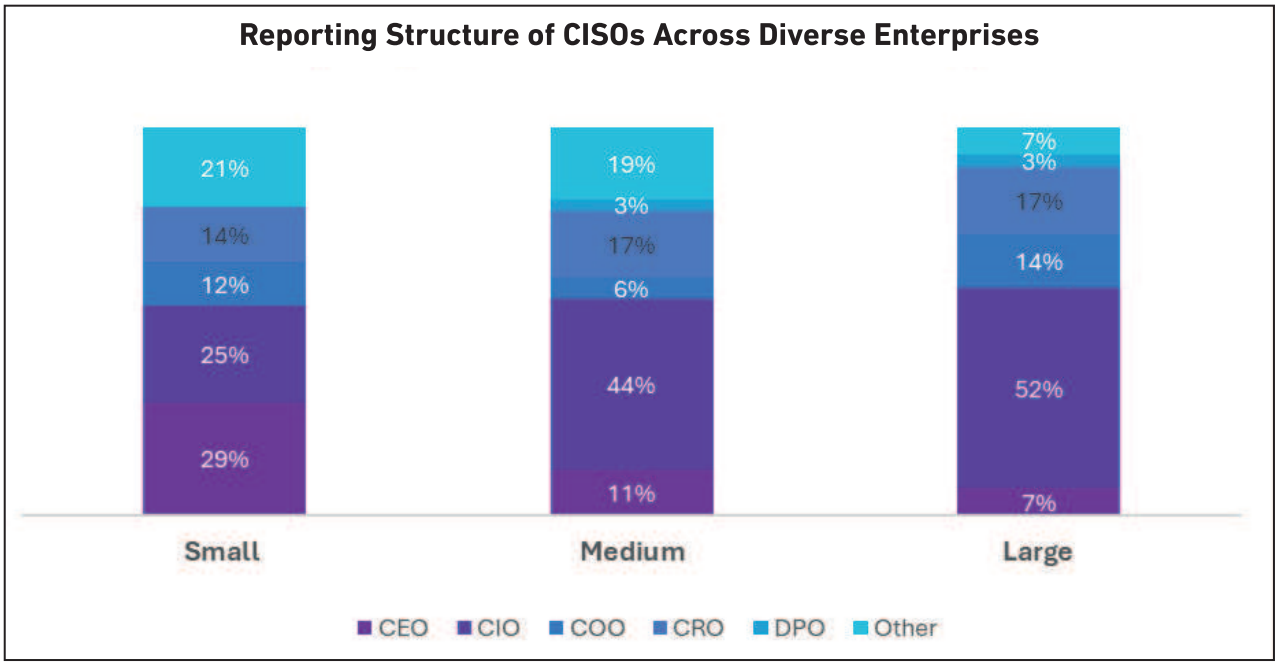


(FY'24)

CISOs most commonly report to Chief Information Officers (CIOs), demonstrating a strong alignment between cybersecurity and IT functions.

A significant percentage of CISOs report directly to Chief Executive Officers (CEOs) or Chief Risk Officers (CROs), highlighting the strategic importance of cybersecurity at the highest levels of organizations and positioning CISOs as key players in risk management.

CISOs of BFSI enterprises mostly report to CROs.



The reporting structure for CISOs varies slightly based on enterprise size. In smaller enterprises, CISOs are more likely to report to CEOs, while in medium and large enterprises, reporting to CIOs is more common.

A majority of CISOs are not inclined to report directly to Chief Information Officers (CIOs). The desire for a separate reporting line underscores the strategic importance of cybersecurity and the need for CISOs to have autonomy in decision-making.

CISOs value a separate reporting line to ensure they are not unduly influenced by IT priorities that may not align with overall security needs.

ET CISO Intelligence

About ETCISO Intelligence

ETCISO Intelligence is a comprehensive research and report product tailored for Cybersecurity leaders, specifically Chief Information Security Officers (CIOs), aiming to equip them with transformative insights essential for navigating the rapidly evolving digital cybersecurity landscape.

ETCISO Intelligence goes beyond data aggregation to actively gather insights from industry experts, thought leaders, and security practitioners. It employs a multi-faceted research approach, combining quantitative analysis, qualitative assessments, industry benchmarks, and expert opinions to provide a holistic understanding of key trends, opportunities, and risks in the cybersecurity domain. ETCISO Intelligence not only provides information but also distills it into valuable knowledge that cybersecurity leaders can leverage to drive meaningful change within their organizations.