Channel Technologies

CT Cyber Charcha

The State of Cybersecurity in Indian Corporates

A survey conducted by Channel Technologies

Presented at

CT Cyber Charcha Cybersecurity Event

on

7th February 2025 at IIT Delhi

Survey Methodology

This survey was conducted by *Channel Technologies* as part of a broader initiative to assess cybersecurity trends, challenges, and investment priorities within mid-segment organizations. The study gathered insights from key decision-makers, including CISOs, CIOs, industry experts, and IT leaders, to provide a comprehensive analysis of the current cybersecurity landscape.

The research was structured using a quantitative and qualitative approach, incorporating structured survey questionnaires and expert interviews. Participants were carefully selected to represent a cross-section of industries, ensuring diverse perspectives from organizations actively engaged in cybersecurity transformation.

The survey covered key areas such as cyber risk management, technology adoption, regulatory compliance, threat intelligence, and security investment priorities. Responses were collected through online surveys conducted between ***1st Sept 2024 to 20th Dec 2024***. Data validation techniques were applied to ensure accuracy, with redundant or incomplete responses excluded from the final analysis.

The findings presented in this report reflect the aggregated insights from participating mid-segment organizations, offering valuable benchmarks and strategic guidance for cybersecurity leaders navigating today's evolving threat landscape.

Executive Summary

Cybersecurity Investment Priorities:
A significant portion of mid-segment organizations are increasing their **security budgets**, with a strong focus on **cloud security, endpoint protection, identity & access management (IAM), and Security Information and Event Management (SIEM) solutions**. Investments in **SASE (Secure Access Service Edge)** and **Zero Trust Architecture** are also gaining traction.

Regulatory & Compliance Readiness:
Compliance with **data protection regulations** (such as GDPR, DPDP Act, and industry-specific security mandates) remains a key challenge. Many organizations struggle with **data governance, privacy frameworks, and audit readiness**, emphasizing the need for robust **Governance, Risk, and Compliance (GRC) solutions**.

Adoption of Emerging Security Technologies:
The survey highlights an increasing adoption of **AI-driven threat detection, Security Orchestration, Automation, and Response (SOAR), and Extended Detection & Response (XDR)** platforms to improve incident response capabilities. However, skill shortages and integration challenges continue to hinder widespread deployment.

Challenges in Cybersecurity Strategy Execution:
The biggest obstacles for mid-segment organizations include **lack of skilled cybersecurity professionals, fragmented security architectures, and budget constraints**. Many organizations rely on **outsourced security services and Managed Security Service Providers (MSSPs)** to bridge operational gaps.

Introduction

In today's rapidly evolving digital landscape, India's mid-sized enterprises—particularly in sectors such as manufacturing, automobile, and pharmaceuticals—are increasingly vulnerable to sophisticated cyber threats. Despite heightened awareness, a significant number of these organizations remain inadequately prepared to manage and mitigate cyber risks.

A 2024 study by Cisco revealed that only 4% of companies in India have achieved a "mature" level of cybersecurity readiness. The majority are still in the formative stages, with 37% classified as "progressive," 52% as "formative," and 7% as "beginners." This lack of preparedness is concerning, especially as 73% of companies anticipate a cybersecurity incident could disrupt their business within the next 12 to 24 months.

The manufacturing sector has emerged as a primary target for cybercriminals. In 2023, nearly 73% of mid-sized and large companies in India experienced ransomware attacks, with 44% of these organizations paying ransoms ranging between $100,000 and $500,000. The manufacturing industry's reliance on both modern and legacy systems creates significant cybersecurity gaps, making it particularly susceptible to such attacks.

Cybersecurity Quips

"There are only two different types of companies in the world: those that have been breached and know it and those that have been breached and don't know it."

The automobile industry is also facing heightened cyber threats. Smart mobility application programming interfaces (APIs) and electric vehicle (EV) charging infrastructure have become major attack vectors, rendering the sector increasingly vulnerable.

In the pharmaceutical sector, the stakes are equally high. As of 2023, India is the world's largest provider of generic medicines by volume, accounting for 20% of global exports. This extensive global reach makes pharmaceutical companies attractive targets for cybercriminals aiming to exploit sensitive data and intellectual property.

Small and medium-sized enterprises (SMEs) across these industries are particularly at risk. A 2024 report highlighted that cybercriminals are increasingly targeting SMEs, as larger organizations bolster their cybersecurity defenses. In 2023, attacks on SMEs accounted for nearly half of all cyber incidents in India. Notably, 44% of these SMEs ended up paying ransoms, with amounts ranging between $25,000 and $100,000.

Despite these challenges, there is a positive trend toward strengthening cybersecurity measures. A survey conducted in 2024 found that 82% of Indian firms have increased their cybersecurity investments in response to rising threats. Companies are implementing various technical and procedural safeguards, such as formal cybersecurity risk assessments (61%), network segmentation (48%), data classification techniques (46%), and zero-trust network policies (46%).

The cybersecurity landscape has undergone a significant transformation. Instead of solely focusing on the best technology products for defense, cybersecurity must now be a proactive discipline—one that not only protects digital assets but also ensures data privacy, regulatory compliance, and operational resilience. However, the adoption of a strategic approach to technology has been slow, and the shift toward a modern cybersecurity methodology has been equally gradual.

While traditional market indicators suggest a strong future for cybersecurity, the reality is more complex. Global cybersecurity product revenue grew by 15.6% between 2022 and 2023—far outpacing the 3.3% growth in overall IT spending. Looking ahead, the market is expected to maintain double-digit growth, reaching $200 billion by 2028. This steady expansion highlights the increasing importance of cybersecurity in a rapidly evolving digital world.

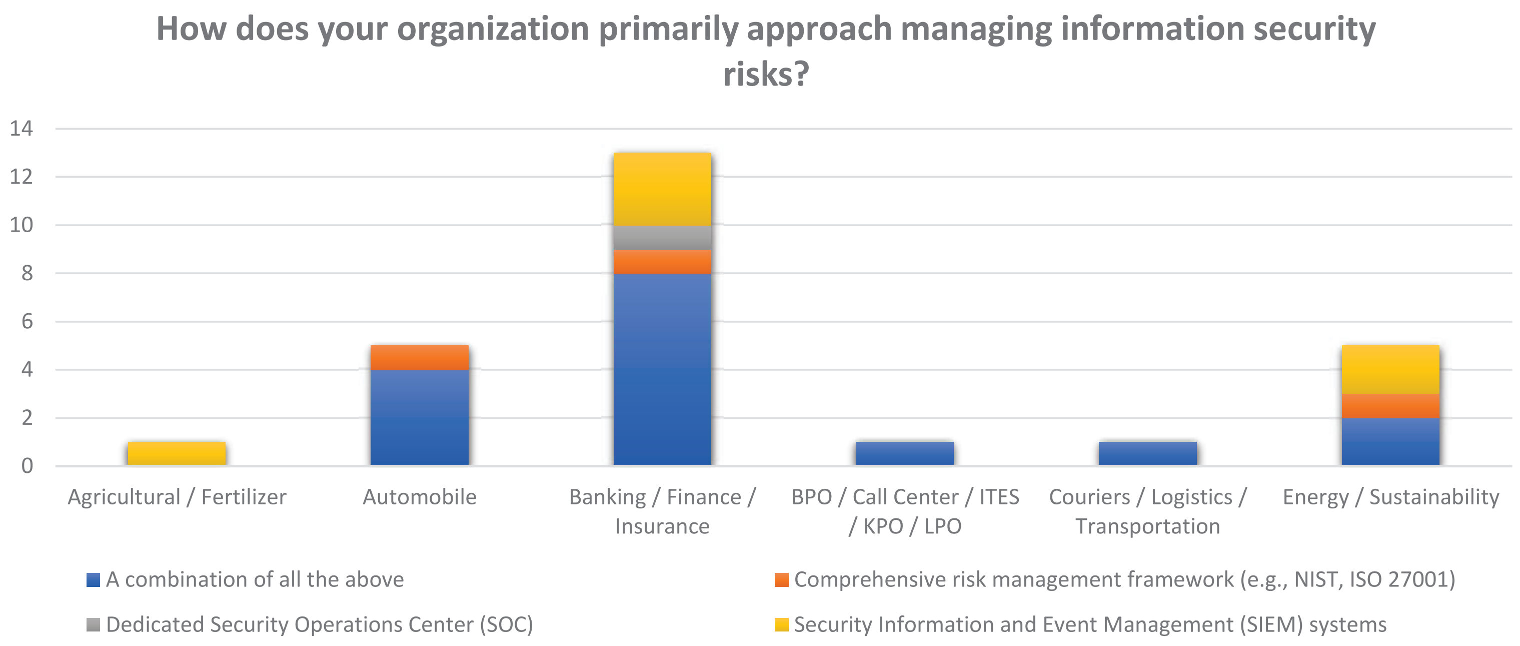
The Indian cybersecurity job market is experiencing significant growth, driven by the country's rapid digital transformation and the increasing need to protect sensitive data. As of May 2023, there were approximately 40,000 open cybersecurity positions in India, reflecting a substantial demand for skilled professionals. However, the industry faces a notable challenge with a 30% demand-supply gap, indicating a shortage of qualified talent.

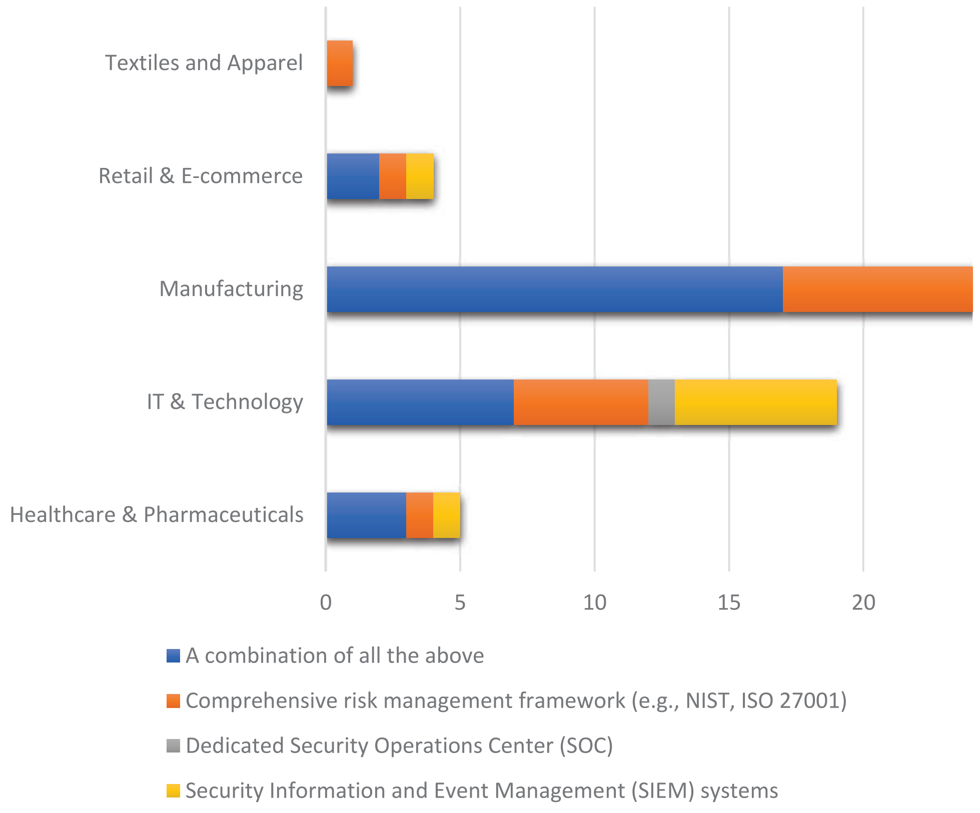
Between 2019 and 2022, job postings for cybersecurity roles in India surged by 81%, highlighting the escalating focus on cybersecurity across various sectors. Despite this upward trend, there was a 25.7% decline in job postings from September 2022 to September 2023, possibly due to the implementation of stricter regulations and controls.

Geographically, Bengaluru leads the nation in cybersecurity job opportunities, accounting for nearly 10% of all listings. This is followed by Delhi-NCR with 4%, and Hyderabad and Mumbai each contributing 2% to the total job postings.

The cybersecurity sector in India is projected to continue its expansion, with the market expected to reach $3.5 billion by 2027, growing at a compound annual growth rate (CAGR) of 8.05%. This growth trajectory underscores the critical need for developing a skilled workforce to bridge the existing talent gap and effectively safeguard India's digital infrastructure.

“Manufacturing and IT Sectors Lead in Comprehensive Information Security Risk Management Approaches”


How does your organization primarily approach managing information security risks?



Manufacturing emerges as the dominant sector in implementing security measures, with a strong emphasis on **Security Information and Event Management (SIEM) systems**, **Comprehensive Risk Management Frameworks (such as NIST and ISO 27001)**, and **Dedicated Security Operations Centers (SOC)**. A large portion of organizations in this sector adopt **a combination of all these measures**, indicating a holistic approach to cybersecurity.

The **IT & Technology** industry follows closely behind, utilizing a mix of security strategies, but with a higher reliance on **SIEM systems and risk management frameworks**. This reflects the sector's awareness of dynamic cyber threats and the necessity for proactive security measures. The **Banking,**

Finance, and Insurance sector also demonstrates a balanced approach, with many organizations favoring a combination of security mechanisms, although **SOC implementations appear to be relatively lower compared to SIEM and risk management frameworks**. Given the critical nature of data protection in financial services, this trend underscores the industry's focus on real-time monitoring and compliance-driven security policies.

Smaller or less technologically intensive industries such as **Agriculture, Textiles, and Couriers/Logistics** exhibit minimal adoption of security risk management measures, indicating a possible lack of investment or awareness regarding cybersecurity threats in these sectors.

Interestingly, the **Retail & E-commerce** industry shows limited implementation of comprehensive cybersecurity measures, which is concerning given the industry's heavy reliance on digital transactions and customer data storage.

Dedicated Security Operations Center (SOC)

How It Helps:

- A **SOC provides 24/7 monitoring** of security threats, enabling rapid incident response and mitigation.

- It ensures **real-time analysis** of logs, network traffic, and security events to detect anomalies before they escalate.

- This is critical for industries such as **banking, IT, and healthcare**, where **quick response to cyber threats** is essential to prevent data breaches and financial fraud.

Security Information and Event Management (SIEM) Systems

How It Helps:

- SIEM systems **collect and analyze log data** from various sources to identify patterns and potential security threats.

- They help organizations **detect anomalies, insider threats, and advanced persistent threats (APTs)** through automated correlation and alerts.

Governance in Cybersecurity

In cybersecurity discussions, "governance" is often associated with regulatory compliance, particularly in highly regulated industries such as healthcare and finance or in specific geographic regions. While compliance remains a critical and evolving requirement, governance extends beyond meeting regulations.

Unlike infrastructure and software development—fields with decades of established frameworks and best practices—cybersecurity and data governance are still maturing. While best practices exist for areas like risk analysis and incident response, a truly holistic cybersecurity framework is still evolving. To be effective, this framework must integrate seamlessly into corporate strategy rather than remain a standalone function.

For cybersecurity professionals, striking the right balance between compliance-driven governance and strategic governance will be essential in shaping long-term security plans and ensuring resilience against evolving threats.

- SIEM is particularly beneficial for industries like **manufacturing, IT, and retail**, where real-time analytics and compliance reporting are crucial.

Comprehensive Risk Management Framework (e.g., NIST, ISO 27001)

How It Helps:

- A well-defined risk management framework **ensures an organization has policies, processes, and governance structures in place** to handle cybersecurity risks systematically.
- Compliance with standards like **NIST, ISO 27001, and GDPR** enhances security posture and **minimizes legal and financial risks**.
- This approach is crucial for industries such as **finance, IT, healthcare, and energy**, where regulatory adherence is mandatory.

A Combination of All the Above (Holistic Security Approach)

How It Helps:

- Organizations adopting a multi-layered security approach benefit from **comprehensive protection**, as they leverage SOCs, SIEM systems, and risk management frameworks together.
- This strategy **reduces attack vectors** by ensuring real-time monitoring, regulatory compliance, and proactive risk management.
- It is best suited for industries with **high-risk exposure**, such as **banking, manufacturing, IT, and healthcare**, where data breaches and cyberattacks can have severe consequences.

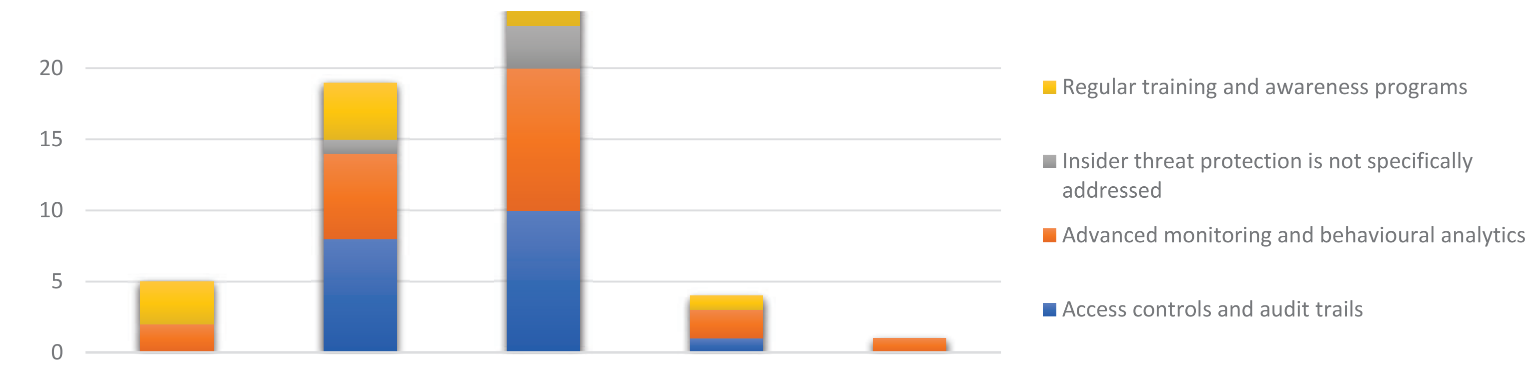
Key Takeaways:

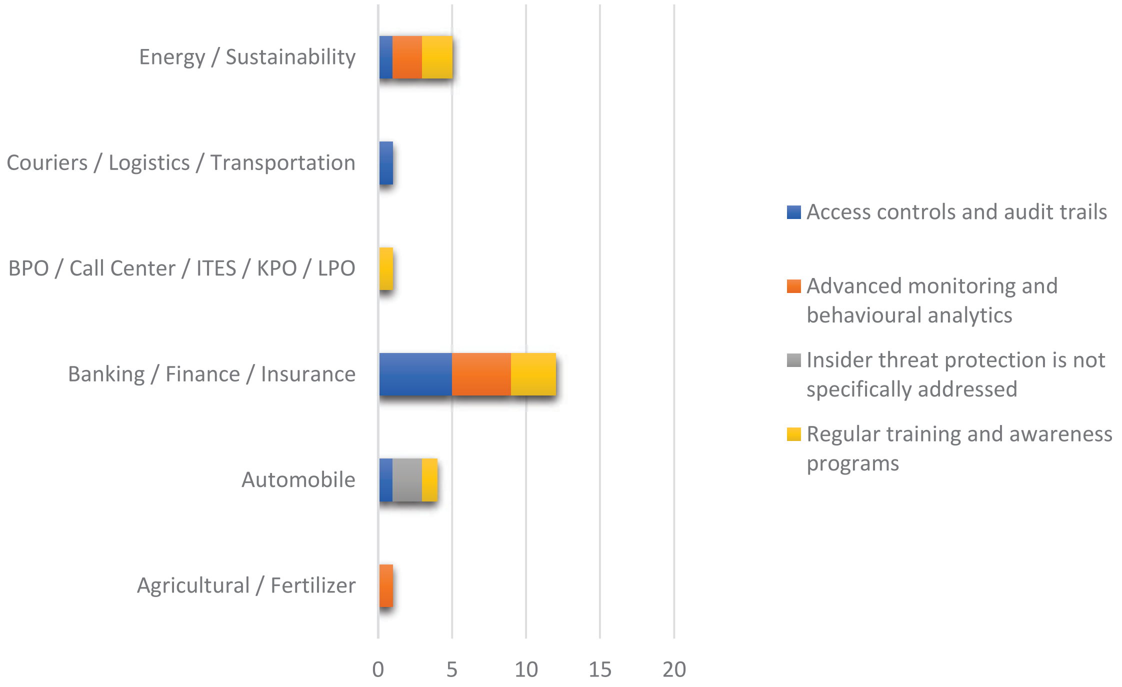
1. **SOC and SIEM work best together for real-time security operations**, helping organizations detect and respond to threats quickly.
2. **Risk management frameworks provide a structured, compliance-driven approach**, ensuring that organizations build resilience against future threats.
3. **A combination of all approaches provides the highest level of security**, offering protection against a wide range of cybersecurity risks.
4. **Industries with high cybersecurity risk exposure (e.g., Banking, IT, and Manufacturing)** benefit the most from implementing a combination of these measures.

“Manufacturing and IT & Technology Sectors Take the Lead in Insider Threat Protection, While Some Industries Remain Vulnerable”

The data reveals that Manufacturing and IT & Technology sectors are the most proactive, implementing a mix of access controls, advanced monitoring, behavioral analytics, and regular training programs. These industries recognize the criticality of insider threats and have adopted multi-layered security measures to mitigate risks.

What is your organization’s strategy for protecting against insider threats?





The Banking, Finance, and Insurance sector also demonstrates a strong security posture, with significant investments in access controls and audit trails, along with monitoring tools to detect anomalies. This is expected, given the highly sensitive nature of financial data and the regulatory requirements imposed on this sector.

However, a notable concern arises from industries like Agriculture, Textiles, and Couriers & Logistics, where insider threat protection appears to be minimal. These sectors show limited investment in security controls, potentially leaving them vulnerable to insider risks, such as data theft, fraud, or sabotage. This could be due to a lower perceived threat level or a lack of regulatory pressure, but the absence of proactive measures increases the potential for security breaches.

Interestingly, the "Others" category, which likely includes smaller businesses or mixed industries, also shows a varied but generally lower level of preparedness. While some organizations have implemented access controls and training, the lack of consistent security measures suggests room for improvement.

This analysis highlights the disparity in insider threat protection across industries. While highly regulated sectors like Finance, IT, and Manufacturing are well-equipped to tackle insider risks, others remain underprepared. Organizations across all industries must recognize that insider threats can emerge in any business environment and should implement a balanced security strategy that includes access controls, behavioral monitoring, training, and awareness programs. A more uniform and proactive approach is essential to safeguard critical data and maintain business integrity in an evolving threat landscape.

Mitigation Strategies

- **User Access Controls** – Implement the principle of least privilege (PoLP) to limit access to only necessary resources.
- **Behavioral Monitoring** – Use User and Entity Behavior Analytics (UEBA) to detect anomalies in employee activities.
- **Security Awareness Training** – Educate employees on cybersecurity best practices and the risks of insider threats.
- **Data Loss Prevention (DLP)** – Deploy tools to prevent unauthorized data transfers or leaks.
- **Strict Offboarding Procedures** – Ensure immediate revocation of access when employees leave the organization.

Insider Threats

Insider threats in cybersecurity refer to risks posed by individuals within an organization who have access to sensitive data, systems, or networks. These threats can originate from employees, contractors, business partners, or other trusted insiders who misuse their access, either intentionally or unintentionally, to harm the organization.

Prevalence of Insider Threats

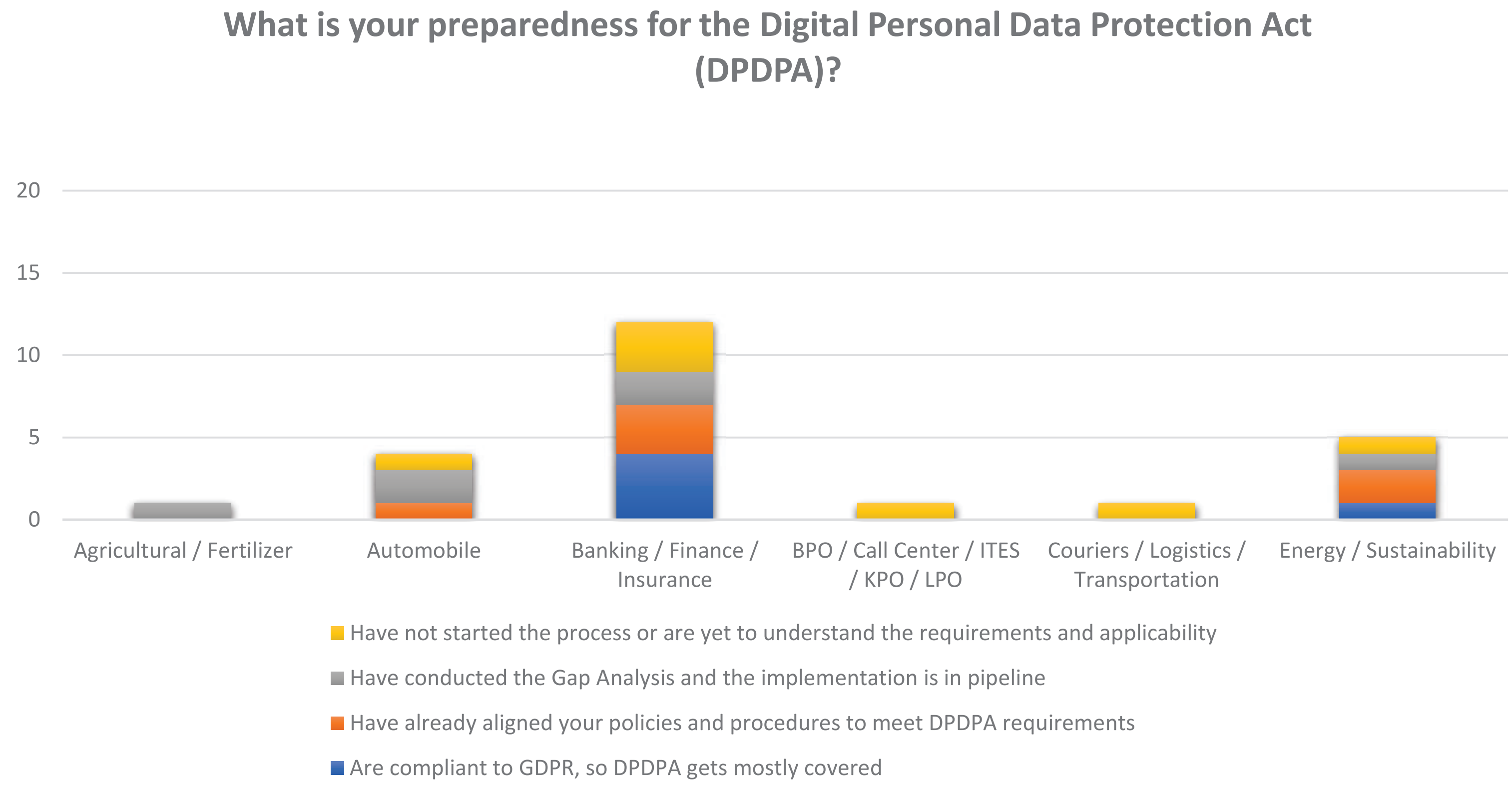
Globally, insider threats account for approximately 43% of all data breaches, encompassing both intentional and unintentional actions.

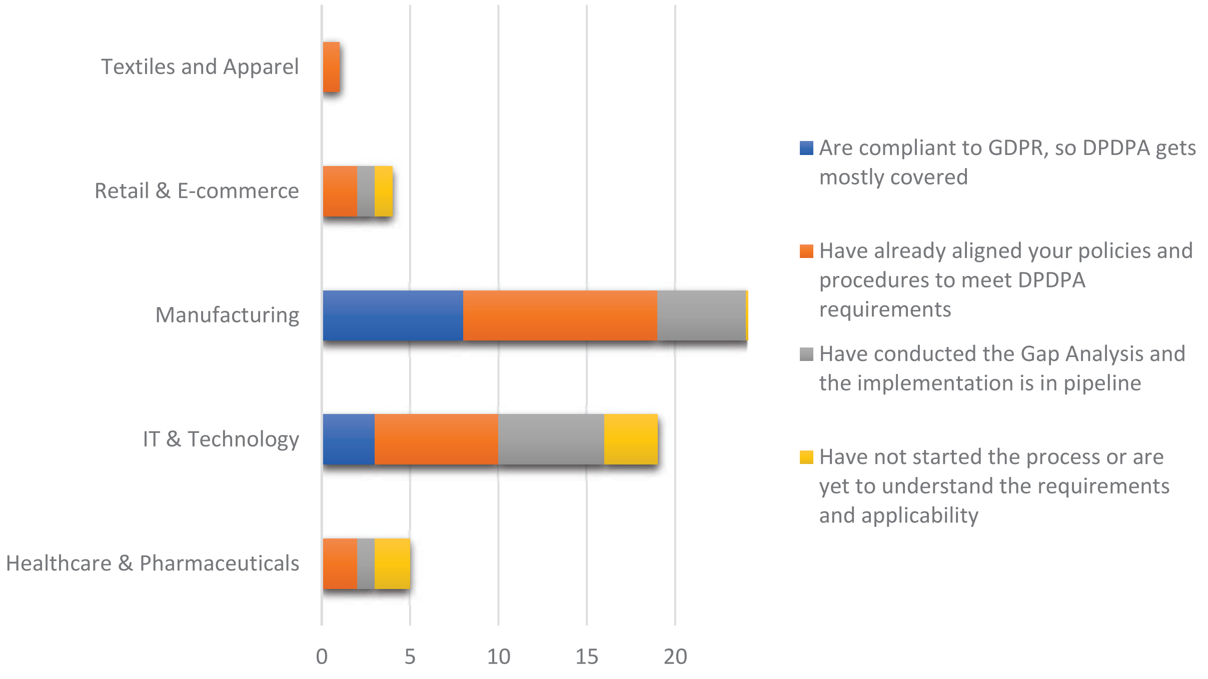
In India, the competitive work environment often leads to high stress levels among employees, making them more susceptible to social engineering attacks and inadvertent errors. Phishing, in particular, is a prevalent method used by attackers, exploiting overwhelmed employees who unknowingly interact with malicious email attachments, leading to data breaches.

Financial Impact

The financial repercussions of insider threats are substantial. A study by Cisco revealed that 62% of Indian startups and small to medium-sized businesses faced cyberattacks costing up to ₹3.5 crore (over US$430,000). These figures underscore the critical need for robust cybersecurity measures to mitigate insider risks.

"Assessing Industry Preparedness for the Digital Personal Data Protection Act (DPDPA): A Sector-Wise Analysis"





Manufacturing and IT & Technology sectors show the highest level of participation in the survey, with a significant number of organizations at different stages of preparedness.

tack. But when companies the insider that is smart has

A Focus on the Indian Market

With the rapid digital transformation in India, the importance of **data privacy and security** has never been more critical. The increasing use of **cloud computing, artificial intelligence, and digital payments** has led to a surge in personal data collection, necessitating robust privacy practices in organizations. The enactment of the **Digital Personal Data Protection Act (DPDPA) 2023** in India underscores the need for businesses to comply with stringent data protection regulations and adopt best privacy practices.

Manufacturing sector has a notable proportion of organizations that have either already aligned their policies or are currently implementing compliance measures. However, a considerable segment has yet to begin the process.

The IT & Technology industry, while also highly represented, displays a more balanced distribution among the three preparedness categories, indicating varying levels of compliance maturity.

The Banking/Finance/Insurance sector has a relatively high number of organizations engaged in compliance efforts, with several already aligning their policies.

Sectors such as Agriculture/Fertilizer, Couriers/Logistics/Transportation, and Textiles & Apparel exhibit low participation, suggesting that either these industries are less affected by the regulation or awareness levels are lower.

Retail & E-commerce and Healthcare & Pharmaceuticals sectors show moderate engagement, with organizations in these fields beginning to align their policies but still lagging behind sectors like IT & Technology or Manufacturing.

The data suggests that while **certain industries, particularly Manufacturing and IT & Technology, are actively working towards compliance, many organizations across sectors remain in the early stages of implementation or lack awareness.**

Growing Digital Footprint and Data Generation

- India had **over 900 million internet users** as of 2023, making it the second-largest digital economy in the world. (Source: TRAI)
- **80% of Indian businesses** store sensitive customer data online, including financial, health, and personal identity information.
- **Digital payments in India surged to ₹149.5 trillion ($1.8 trillion) in 2023**, emphasizing the need for secure transaction mechanisms. (Source: RBI)

Rising Cybersecurity Threats and Data Breaches

- **India witnessed a 15% rise in cyberattacks** in 2023, with over **2,00,000 cybersecurity incidents reported**. (Source: CERT-In)
- A study by IBM found that the **average cost of a data breach in India in 2023 was ₹17.9 crore ($2.2 million)**, a significant increase from previous years.
- Over **61% of Indian companies** reported facing at least one cybersecurity attack in 2023.

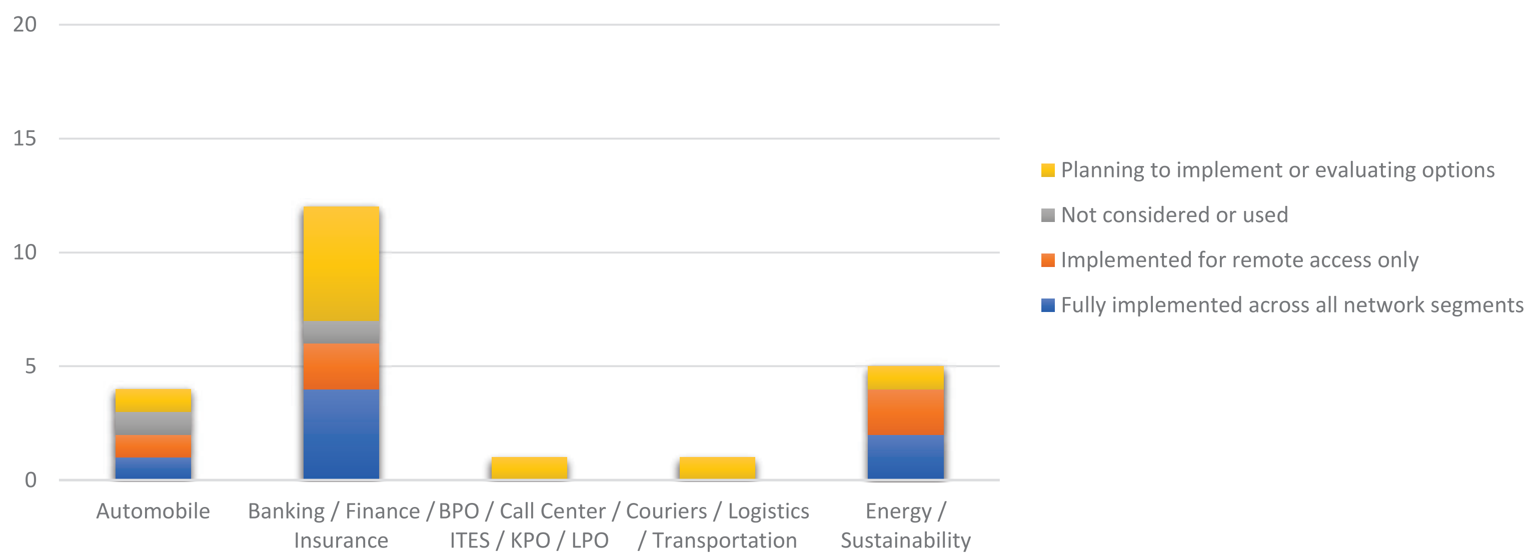
Best Practices for Indian Organizations

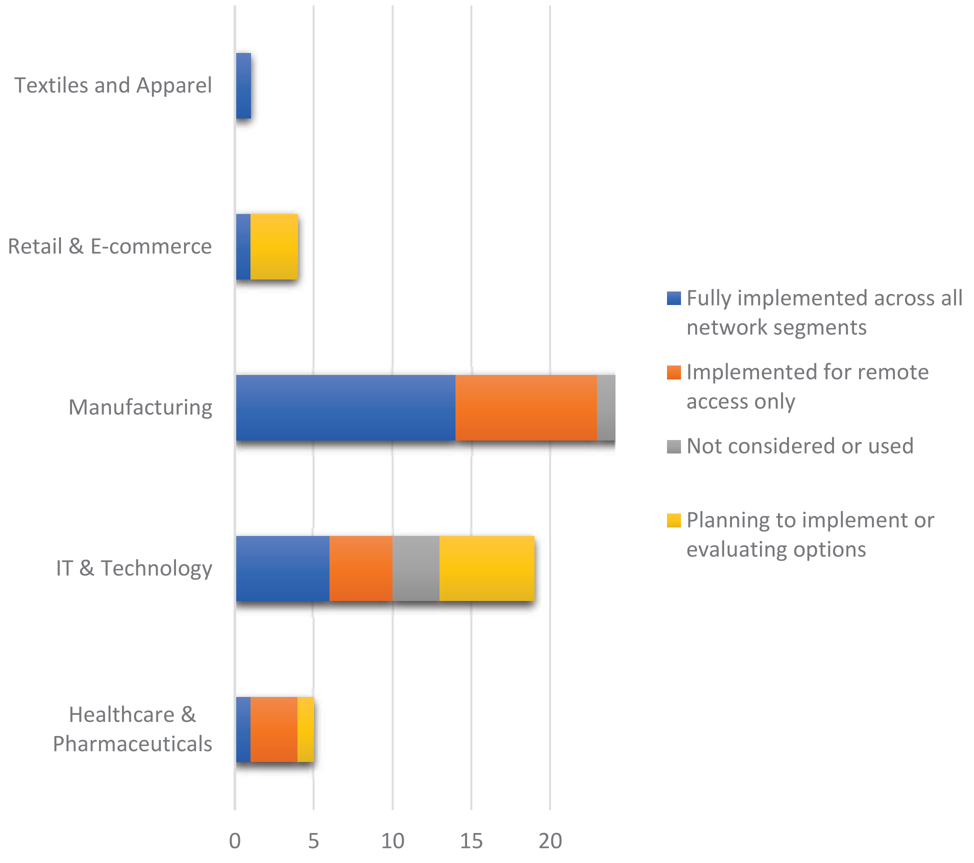
1. **Adopt a Data Protection Framework** – Implement privacy policies in alignment with DPDPA and global standards like **GDPR** and **ISO 27701**.
2. **Enhance Cybersecurity Measures** – Deploy encryption, multi-factor authentication (MFA), and data access controls.
3. **Conduct Privacy Impact Assessments (PIA)** – Regularly evaluate risks associated with data processing activities.
4. **Employee Training and Awareness** – Conduct periodic training on data privacy laws and secure handling of sensitive data.
5. **Incident Response Plan** – Develop a structured approach to handle data breaches and notify affected individuals in compliance with DPDPA requirements.

“Adoption Trends of Zero Trust Network Access (ZTNA) Across Various Industries”

> “Arguing that you don’t care about the right to privacy because you have nothing to hide is no different than saying you don’t care about free speech because you have nothing to say.” — Edward Snowden

Which of the following best describes your organization’s approach to Zero Trust Network Access (ZTNA)?





1. Manufacturing Leads ZTNA Adoption:

- The Manufacturing sector shows the highest engagement with ZTNA, with a significant portion of organizations having fully implemented the approach across all network segments.

- A notable percentage is still in the evaluation or planning stage, while some have implemented it only for remote access.

2. IT & Technology is Actively Adopting ZTNA:

- Many organizations in IT & Technology have fully implemented ZTNA, though a substantial number are still evaluating or in the planning phase.
- A small proportion has implemented ZTNA only for remote access, showing a phased approach toward full implementation.

3. Banking, Finance & Insurance Show Moderate Adoption:

- This sector has a mix of adoption levels, with several organizations fully implementing ZTNA.
- A notable portion is in the planning or evaluation phase, while a smaller percentage has implemented it only for remote access.

4. Healthcare, Pharmaceuticals, and Energy Lag in Adoption:

- Both sectors show limited implementation, with most organizations either planning to adopt or not considering it at all.
- The security-sensitive nature of these industries suggests a potential gap in cybersecurity preparedness.

5. **Retail, E-commerce, and BPOs Have Limited Implementation:**
   - These sectors show a smaller presence in ZTNA adoption, with most organizations still evaluating options.
   - This could indicate either a lack of awareness or lower prioritization of ZTNA in their cybersecurity strategies.

6. **Minimal Adoption in Agricultural, Textiles, and Logistics:**
   - Industries like Agricultural/Fertilizer, Textiles & Apparel, and Couriers/Logistics show very little engagement with ZTNA.
   - These industries may not perceive ZTNA as a priority, possibly due to their operational structures or reliance on traditional security models.

Organizations must recognize that implementing ZTNA is not just a security upgrade but a necessity in the modern cybersecurity landscape. As cyberattacks grow more sophisticated, businesses across all sectors must evaluate their security frameworks and consider ZTNA as a proactive measure to protect sensitive data, prevent unauthorized access, and strengthen overall network security.

Zero Trust and SASE Adoption in India: A Comprehensive Overview

In recent years, Indian enterprises have increasingly recognized the importance of advanced cybersecurity frameworks, notably Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE), to safeguard their digital assets.

Zero Trust Adoption in India

A study by Zscaler indicates that over 96% of Indian IT leaders who have initiated cloud migration have either implemented, are in the process of implementing, or plan to implement a Zero Trust security architecture. This trend underscores a significant shift towards modern security paradigms in the Indian corporate sector.

However, despite this high adoption rate, challenges persist. Fortinet's research reveals that while more organizations are deploying Zero Trust frameworks, the number of complete implementations has decreased, suggesting difficulties in integration and execution.

SASE Adoption in India

The convergence of networking and security through SASE is gaining momentum among Indian enterprises. According to a report by the International Data Corporation (IDC), over 54% of large organizations in India, defined as those with 500 or more employees, plan to implement technologies such as Software-Defined Branch (SD-Branch) and Zero Trust Network Access (ZTNA) as part of their SASE adoption strategy.

Globally, SASE adoption is also on the rise. A survey by Cato Networks found that 88% of respondents reported that security and networking teams are consolidating efforts, reflecting a trend towards integrated solutions like SASE.

Challenges and Considerations

Despite the enthusiasm for these frameworks, organizations face challenges in implementation. A report highlighted that only 8% of organizations have fully implemented SASE solutions, though adoption is accelerating, with 32% currently in progress and 24% planning implementation in the next 12 months. IT teams are confronting challenges in integrating new solutions, managing policies across environments, and maintaining robust expertise in-house.

The Value of Zero Trust

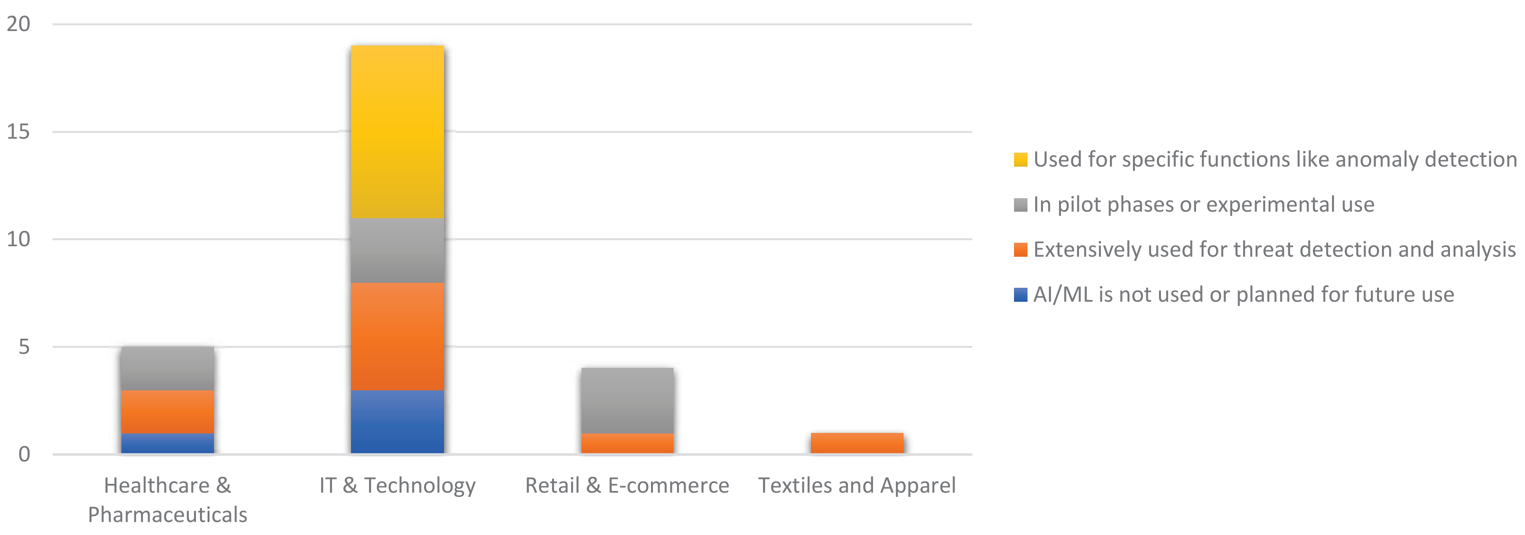
Over the past five years, **zero trust** has emerged as the dominant approach in modern cybersecurity, replacing the traditional **"secure perimeter"** mindset. This shift redefines how organizations approach data protection, application security, and user behavior in an increasingly digital landscape.

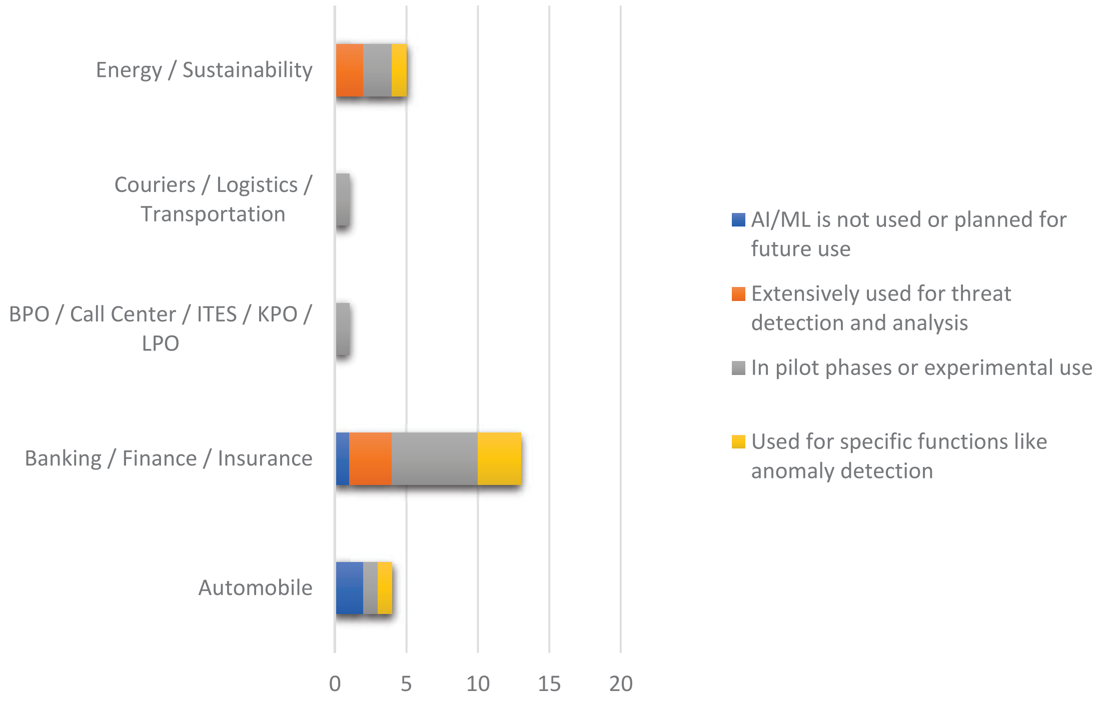
However, the term **zero trust** can often be misunderstood. Given cybersecurity's product-driven history and the growing collaboration between cybersecurity teams and business leaders, there is uncertainty about which products or initiatives truly align with a zero-trust strategy. The lack of clear metrics to measure zero trust success adds to the confusion.

Rather than focusing on the broad concept of zero trust when engaging with executive stakeholders, cybersecurity professionals should emphasize **specific security measures** that contribute to its framework—such as **identity and access management (IAM), multi-factor authentication (MFA), and continuous monitoring**. By doing so, organizations can define **concrete investment priorities and success criteria**, while keeping zero trust as an overarching principle guiding internal cybersecurity strategies.

"AI & ML in Cybersecurity: Industries Leading the Charge vs. Those Falling Behind"

What role does Artificial Intelligence (AI) and Machine Learning (ML) play in your organization's security strategy?





AI and ML adoption for security strategy is highest in Manufacturing, IT & Technology, and Banking/Finance/Insurance due to high cybersecurity risks and the need for proactive threat management.

Many industries, especially Retail & E-commerce, Healthcare, and Automobile, are experimenting with AI-driven security but have not fully integrated it.

The Future of AI in Cybersecurity

AI will continue to revolutionize cybersecurity, with advancements in explainable AI (XAI), federated learning, and AI-driven deception technologies. As threats become more complex, organizations must integrate AI into their security frameworks to stay resilient in an increasingly hostile digital environment.

In conclusion, AI is not just an enhancement but a necessity in modern cybersecurity strategies. Organizations that embrace AI-driven security will have a significant advantage in safeguarding their digital assets and maintaining a robust defense against cyber threats.

Sectors like Textiles, Transportation, and Energy exhibit low AI/ML adoption, possibly due to lower cybersecurity awareness or investment constraints.

Organizations that have adopted AI/ML focus primarily on threat detection, anomaly detection, and security automation, while others are still in experimental phases.

The polarized AI adoption in Manufacturing and Banking suggests a divergence between forward-thinking organizations and those hesitant to adopt AI-driven security solutions.

Future trends indicate that AI-driven security will continue to grow, especially in industries with high cybersecurity risks, while underrepresented sectors may need more awareness and investment to embrace AI-based security strategies.

Strategic Takeaways

- **Leaders in AI Adoption:** Manufacturing, IT & Technology, and Banking & Finance are at the forefront, leveraging AI/ML for threat intelligence and security automation.
- **Sectors at Risk:** Retail, Healthcare, and Automobile need to accelerate AI adoption to mitigate evolving cyber risks.
- **Underserved Markets:** Energy, Logistics, and Textiles remain underutilized in AI-driven security, presenting a growth opportunity for AI security solutions.
- **Future Outlook:** AI will become an indispensable component of cybersecurity, with increased adoption expected across all sectors, driven by regulatory pressures and the rising sophistication of cyber threats.

End Notes

Only 4% of companies in India 'mature' to tackle cyber threats: Study https://www.business-standard.com/companies/news/only-4-of-companies-in-india-mature-to-tackle-cyber-threats-study-124032800361_1.html

Nearly 73% of Indian mid, large companies hit by ransomware in 2023 https://economictimes.indiatimes.com/tech/technology/nearly-73-of-indian-mid-large-companies-hit-by-ransomware-in-2023/articleshow/105518876.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

Manufacturing industry in India most targeted by ransomware attacks: Report https://www.techcircle.in/2024/03/26/manufacturing-industry-in-india-most-targeted-by-ransomware-attacks-report

India's Digital Revolution: Opportunities and Challenges https://website.rbi.org.in/documents/87730/30842423/Chapter1+-+RCF2024.pdf

Cybercriminals target SMEs as large companies beef up security https://economictimes.indiatimes.com/tech/technology/cybercriminals-target-smes-as-large-companies-beef-up-security/articleshow/113102946.cms

82% of Indian Firms Increasing Cybersecurity Investments Amid Rising Cyber Threats in 2024 https://www.businesswireindia.com/82-of-indian-firms-increasing-cybersecurity-investments-amid-rising-cyber-threats-in-2024-88374.html

India saw 81% surge in cybersecurity job postings from 2019-2022: Report https://hr.economictimes.indiatimes.com/news/trends/india-saw-81-surge-in-cybersecurity-job-postings-from-2019-2022-report/104770421

India's cybersecurity job market soars amid rising demand but faces critical talent shortage https://www.cnbctv18.com/education/india-cybersecurity-jobs-hiring-market-rising-demand-talent-shortage-vacancies-indeed-19497404.htm

Inside job: How Indian workforce fuels insider threats https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/inside-job-how-indian-workforce-fuels-insider-threats/105549422

Zscaler Study Finds 96% of Indian Enterprises are Adopting Zero Trust, Yet Have Not Unlocked the Full Business Potential https://cxotoday.com/press-release/zscaler-study-finds-96-of-indian-enterprises-are-adopting-zero-trust-yet-have-not-unlocked-the-full-business-potential/?

Cybersecurity In India: 2024 Global Digital Trust Insights Survey | PwC India https://www.pwc.in/assets/pdfs/digital-trust-insights-india/digital-trust-insights-india.pdf

Unveiling Insights: 2023 SASE Adoption Survey *https://www.catonetworks.com/resources/unveiling-insights-2023-sase-adoption-survey/*

Navigating SASE Adoption: How MSSPs Empower Organizations to Secure Hybrid Networks *https://www.hughes.com/resources/insights/cybersecurity/navigating-sase-adoption-how-mssps-empower-organizations-secure*

Confidentiality and Usage Disclaimer

This report is the exclusive property of Channel Technologies Private Limited and is intended solely for the recipient(s) authorized by the company. Any unauthorized use, distribution, reproduction, or disclosure of this report, in whole or in part, without prior written consent from **Channel Technologies Private Limited ©**, is strictly prohibited.

All information, analysis, and insights contained within this document are proprietary and may not be shared, copied, or utilized for any purpose beyond its intended scope without explicit approval. Violation of these terms may result in legal action.

For permissions or further inquiries, please contact Channel Technologies Private Limited.