THE ANKURA INDIA CYBER RESILIENCE SURVEY 2025

Cyber Resilience Protecting India's Digital Assets

ankura DATA & TECHNOLOGY

INVESTIGATIONS | CYBER SECURITY | eDISCOVERY | DIGITAL FORENSICS | ANALYTICS

Leadership Message

Securing the Digital Frontier:
Insights from our Cyber Resilience Survey

As we reflect on the insights gathered from our Cybersecurity Survey in 2024, we recognize the shifting tides in the digital landscape, prompting us to explore new dimensions of resilience in 2025. Last year's survey highlighted the critical need for robust cyber defenses, laying the groundwork for this year's Ankura India Cyber Resilience Survey. Our journey continues, focusing on not just surviving cyber threats but thriving amidst them.

With contributions from over 50 esteemed companies and cybersecurity leaders, this survey has woven together a wealth of insights, offering fresh perspectives on fortifying defenses and advancing data privacy and governance practices. Each participant has been instrumental in charting a path forward, highlighting both our strengths and areas where innovation can thrive.

Our thanks goes out to all who shared their expertise and candid feedback, which has been crucial in shaping this renewed outlook. This collective insight is the foundation upon which we aim to build security practices that are not only resilient but agile enough to adapt to the ever-changing digital landscape.

The findings presented extend beyond a mere evaluation of the current cybersecurity landscape; they serve as a strategic guide for addressing the evolving challenges that lie ahead. Leveraging these insights, we are well-positioned to direct our future initiatives towards fostering a secure and resilient digital ecosystem for all stakeholders.

Our unwavering commitment to cybersecurity underscores our dedication to preserving trust and confidence among clients, partners, and stakeholders alike. United in purpose, we stand ready to innovate our defense strategies and uphold the highest standards of security, thereby shaping a future where digital trust remains foundational.

Yours sincerely,

Mr. Amit Jaju
Senior Managing Director and India Head
Ankura Consulting

Amit Jaju
Senior Managing Director
amit.jaju@ankura.com | +91 9820073695
@amitjaju

LinkedIn TOP VOICES Technology & Innovation

LEXOLOGY INDEX
Thought Leader Investigations 2025 | Thought Leaders GIR 2024

Contents

Introduction

In an era marked by rapid technological advancement, cybersecurity is more than just a protective measure; it is the cornerstone of digital resilience for organizations worldwide. As cyber threats become increasingly sophisticated, driven by artificial intelligence and complex insider dynamics, the integrity, confidentiality, and availability of information systems are under constant siege. To navigate this challenging landscape and uncover paths to improvement, we conducted the **Ankura India Cyber Resilience Survey 2025**, casting a wide net across multiple industries to gauge and enhance digital resilience.

This report unveils the findings of our India survey, offering a detailed evaluation of cybersecurity across diverse organizations. We identify potential vulnerabilities and scrutinize the effectiveness of current security measures, with particular emphasis on AI-related threats, insider angles, and the critical aspects of data privacy and governance. By gathering insights from cybersecurity leaders across various sectors, we provide a rich, multifaceted perspective on the current cybersecurity status.

OBJECTIVES

Assess Digital Resilience: Assess digital resilience across industries, highlighting vulnerabilities and strengths in cybersecurity to understand readiness for evolving threats.

Examine AI and Insider Threats: Explore AI-driven threats and insider dynamics in cybersecurity, offering insights for strategic adaptation to counter these challenges.

Enhance Data Privacy and Governance: Evaluate data privacy and governance effectiveness, identifying improvement areas to ensure compliance and safeguard sensitive information.

Identify Strategic Improvements: Identify strategies and tactics, including threat actor negotiations and counter-offensive measures, to strengthen defenses, reduce risks, and foster proactive cybersecurity awareness.

TOPICS COVERED IN THE SURVEY

- Data Privacy and Governance
- Vendor Due Diligence
- Incident Response
- Workforce and Talent Pool
- Regulatory Compliance and Mandates
- Roles of CISO in Business-Critical Functions
- Cybersecurity and Privacy Automation
- New Age Threats and Hackers

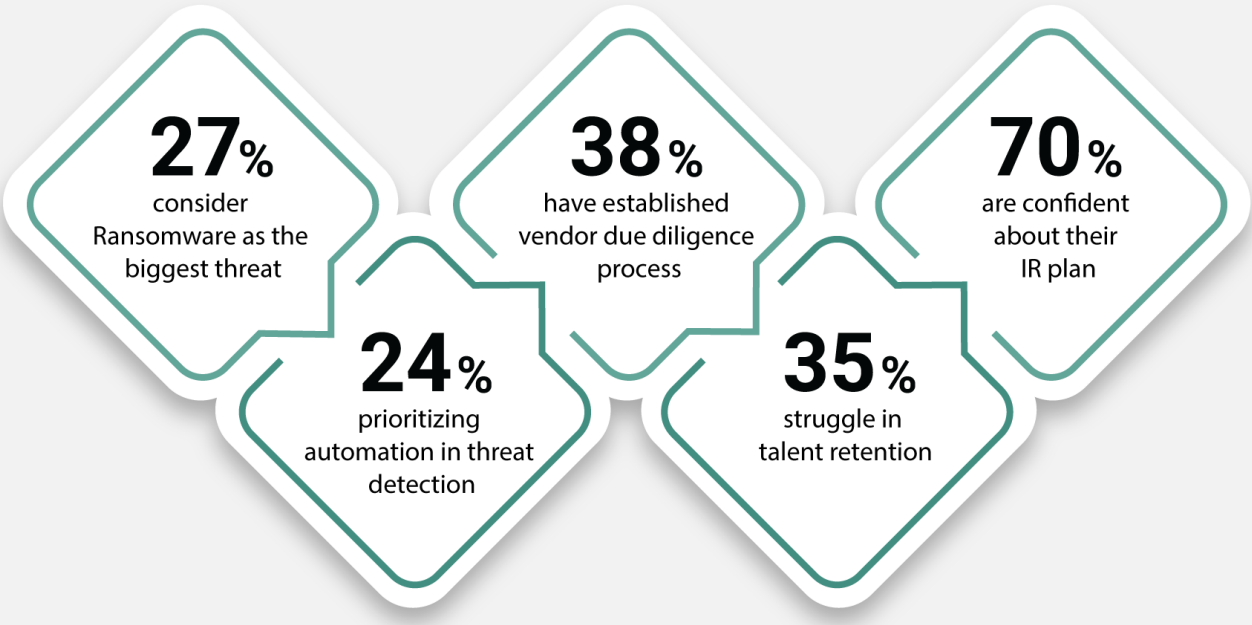
This year's survey explored a broad array of topics, including threat actors, challenges in cybersecurity planning, returns on cybersecurity investments, and the indispensable role of regular security awareness training. It further examined innovative approaches such as negotiations with threat actors, counter-offensive tactics, and key learnings from recent cases. Our goal is to underscore areas requiring immediate focus and propose strategic actions to mitigate risks and strengthen cybersecurity defenses.

This report strives to foster a culture of security awareness and robust data governance, equipping organizations with the knowledge and tools necessary to protect their digital assets. The insights derived from this survey are poised to shape future cybersecurity strategies, paving the way for more resilient and secure organizational environments on a global scale.

Highlights

Unveiling the core insights from this year's survey, the report delves into the intricate dynamics of cybersecurity resilience.

What follows is an in-depth examination of digital resilience, delivering strategic insights and innovative approaches that equip organizations to adeptly navigate and succeed in the rapidly changing cyber landscape.



Executive Summary

WHAT HAS EVOLVED FROM LAST YEAR

Increased Integration of AI/ML Technologies
Organizations have begun to overcome initial skepticism, increasingly integrating AI/ML technologies into their cybersecurity frameworks. This evolution reflects growing confidence in the ability of these tools to enhance threat detection and incident response capabilities.

Enhanced Focus on Incident Response Preparedness
Organizations have significantly bolstered their incident response strategies, emphasizing rapid detection and containment of threats. This evolution highlights a proactive approach to minimizing the impact of cyber incidents and maintaining operational continuity.

Increased Emphasis on Data Privacy Compliance
Organizations have intensified efforts to align with emerging data privacy regulations, reflecting a commitment to protecting sensitive information and maintaining trust in the digital economy.

Ankura shares thoughts with Entrepreneur India
Fight AI with AI

https://tinyurl.com/3e69a5w7

ADOPTING THE CHANGING THREAT LANDSCAPE

Embracing Zero Trust Architecture
Organizations are increasingly adopting Zero Trust principles to address evolving threats, ensuring that all users and devices are continually verified before accessing sensitive data.

Enhancing Threat Detection Capabilities
Organizations in India are focusing on improving threat detection systems to identify and mitigate risks more effectively, adapting to the unique challenges posed by the local cyber landscape.

Ankura shares thoughts with CSO Online
A rapidly growing ransomware threat

https://tinyurl.com/2byzaf4x

Executive Summary

MANAGING PRIORITIES

Aligning Cybersecurity Goals with Business Objectives
There is a growing emphasis on aligning cybersecurity initiatives with overall business objectives, ensuring that security investments support strategic goals and drive organizational growth.

Enhancing Cloud Security Measures
Organizations are increasingly focusing on strengthening security protocols within cloud environments, ensuring robust protection and compliance as they expand digital operations.

Ankura shares thoughts on

Key Challenges in Adopting Zero Trust

https://tinyurl.com/5n8zcwm9

WAY AHEAD

Embracing Digital Transformation
Organizations are prioritizing digital transformation initiatives that integrate advanced security measures, paving the way for innovation while safeguarding assets.

Investing in Scalable Infrastructure
Organizations are focusing on scalable infrastructure development to ensure robust, flexible, and future-ready security systems that can adapt to changing threat landscapes.

Strengthening Cyber Resilience Strategies
Organizations are committed to enhancing their cyber resilience strategies, focusing on robust recovery and continuity plans to swiftly adapt to and overcome potential disruptions.

Ankura shares thoughts with TimesNow on
A Cybersecurity Strategy to Support Every Need

https://tinyurl.com/2ydzymes

Cyber Resilience Survey Report Overview

The Cyber Resilience Survey Report encapsulates the invaluable insights shared by industry leaders, offering a profound understanding of how organizations are navigating the complexities of today's cybersecurity landscape.

Leveraging new-age technologies like AI, these insights reveal innovative approaches to enhancing digital resilience, enabling rapid threat detection and sophisticated incident management.

This report captures the shifting dynamics in regulatory compliance and data privacy, particularly within India's evolving context, highlighting the strategic adjustments organizations are making to adhere to stringent mandates. Industry leaders have candidly discussed the increasing sophistication of cyber adversaries, emphasizing the need for adaptive and proactive security measures.

Through this collective wisdom, the report provides a comprehensive overview of the strategies being deployed to fortify defenses against advanced cyber threats.

Packed with expert analysis and actionable insights, this report equips organizations with the knowledge and strategies needed to enhance their cybersecurity posture, making it an indispensable tool for thriving in the digital age.

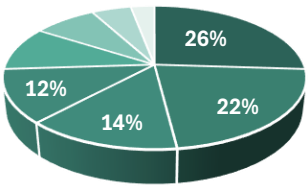
Behind the Research

The Cyber Resilience Survey was meticulously crafted to capture the insights of over 50 seasoned professionals from diverse industries.

With participation from multiple sectors, functions and grades, the survey provides a comprehensive view of cybersecurity challenges and innovations, focusing exclusively on technical expertise. These leaders, many with extensive experience, offered profound insights into the integration of AI within complex, data-sensitive environments.

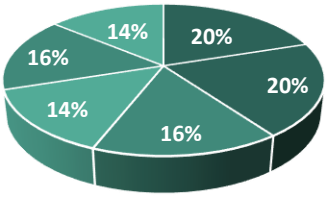
This survey presents a rich tapestry of insights from a mature, multidisciplinary group, driving forward the conversation on AI and cybersecurity. It stands as a testament to the collective expertise and commitment of these professionals to harness technology in fortifying digital infrastructures, providing valuable guidance for organizations striving to enhance their resilience in an ever-evolving digital world.

Sector



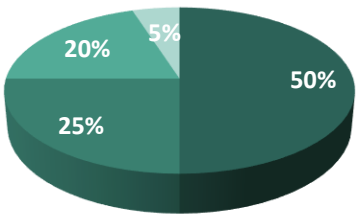
- Technology
- Financial Services
- Healthcare
- Manufacturing
- Retail
- Telecommunications
- Energy and Utilities
- Government

Function



- IT
- Cybersecurity
- Privacy
- Legal
- Compliance
- Information Assurance

Grade

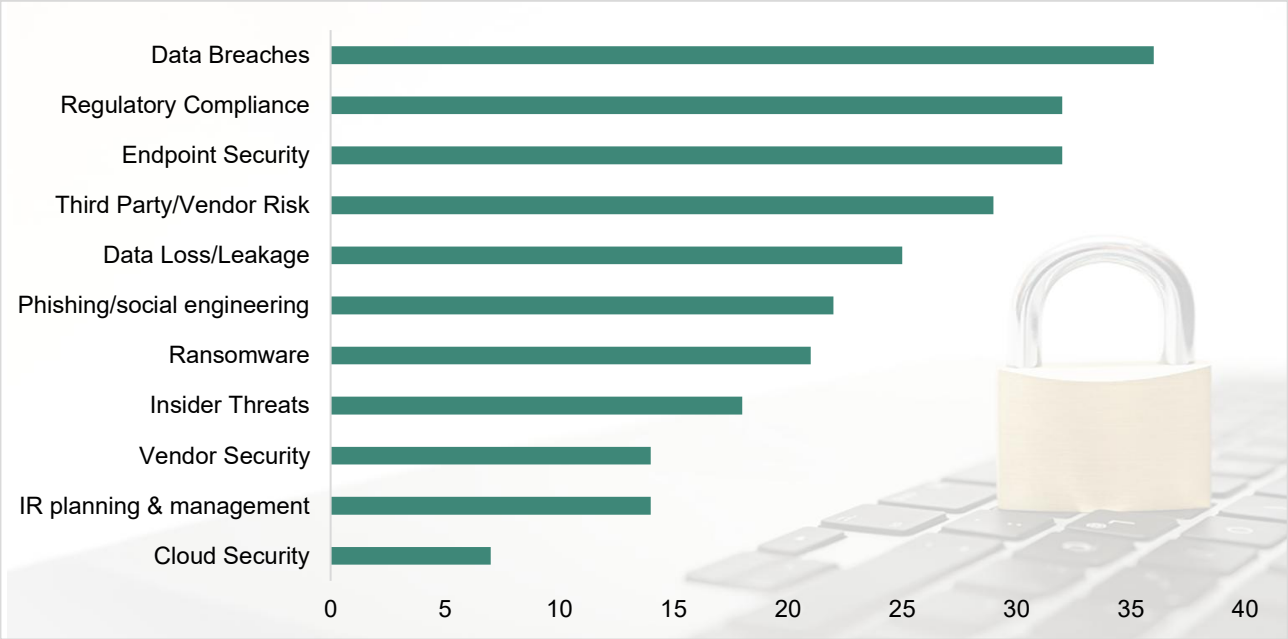


- C-level (CISO/CIO/CTO/CSO)
- Director/Head
- Manager/Senior Specialist
- Other/Unknown

We sincerely thank the following members for their valuable contributions to this survey: Abhishek Tawde, Sherwin Dsouza, Nivedita Bagchi, Sakshi C and Priyanka Basutkar. Additionally, we extend our gratitude to all individuals who responded to the survey but preferred to remain anonymous. Your insights are truly appreciated and have greatly contributed to the success of this report.

Survey Statistics

TOP AREAS OF CONCERN IN DATA PRIVACY & CYBER SECURITY



KEY INSIGHTS

1. Shifting Focus to Emerging and Persistent Threats

While last year's cybersecurity priorities centered on strengthening data and network security, enhancing awareness and compliance, improving incident response and cloud security, and vulnerability management, this year's data reveals specific areas of elevated concern. Organizations are now primarily focused on data breaches, regulatory compliance, and endpoint security, which rank as the top three challenges. This shift suggests growing anxiety about actual breach incidents and the mounting complexity of regulatory demands alongside the expanding attack surface from endpoints.

2. Persistent High Concern About Third-Party Risks and Insider Threats

Third-party/vendor risk remains a significant concern, reflecting the continuous importance of supply chain and vendor cybersecurity management in today's interconnected environments. Insider threats also remain a priority, underscoring the persistent risk from trusted internal actors exploiting access.

3. Continued Emphasis on Social Engineering and Ransomware

Phishing and social engineering attacks continue to trouble organizations, complemented by sustained fears of ransomware attacks, which remain among the top cybersecurity threats despite evolving defensive strategies. These represent tried-and-true attack vectors that exploit human vulnerabilities and system weaknesses alike.

4. Broader Attention to Incident Response and Vendor Security

Concerns about incident response planning and vendor security reflect an increasing effort to prepare for and mitigate impacts of cybersecurity incidents–extending both internally and across third-party ecosystems. Cloud security, while still important, has comparatively lower direct concern, possibly indicating some maturation in cloud protections or shifting risk perceptions.

EVOLVING CYBERSECURITY THREATS: KEY CHANGES FROM LAST YEAR

Disgruntled Employees have become a major concern, rising sharply from **4%** to **17%**, highlighting growing awareness of insider risks linked to employee dissatisfaction.

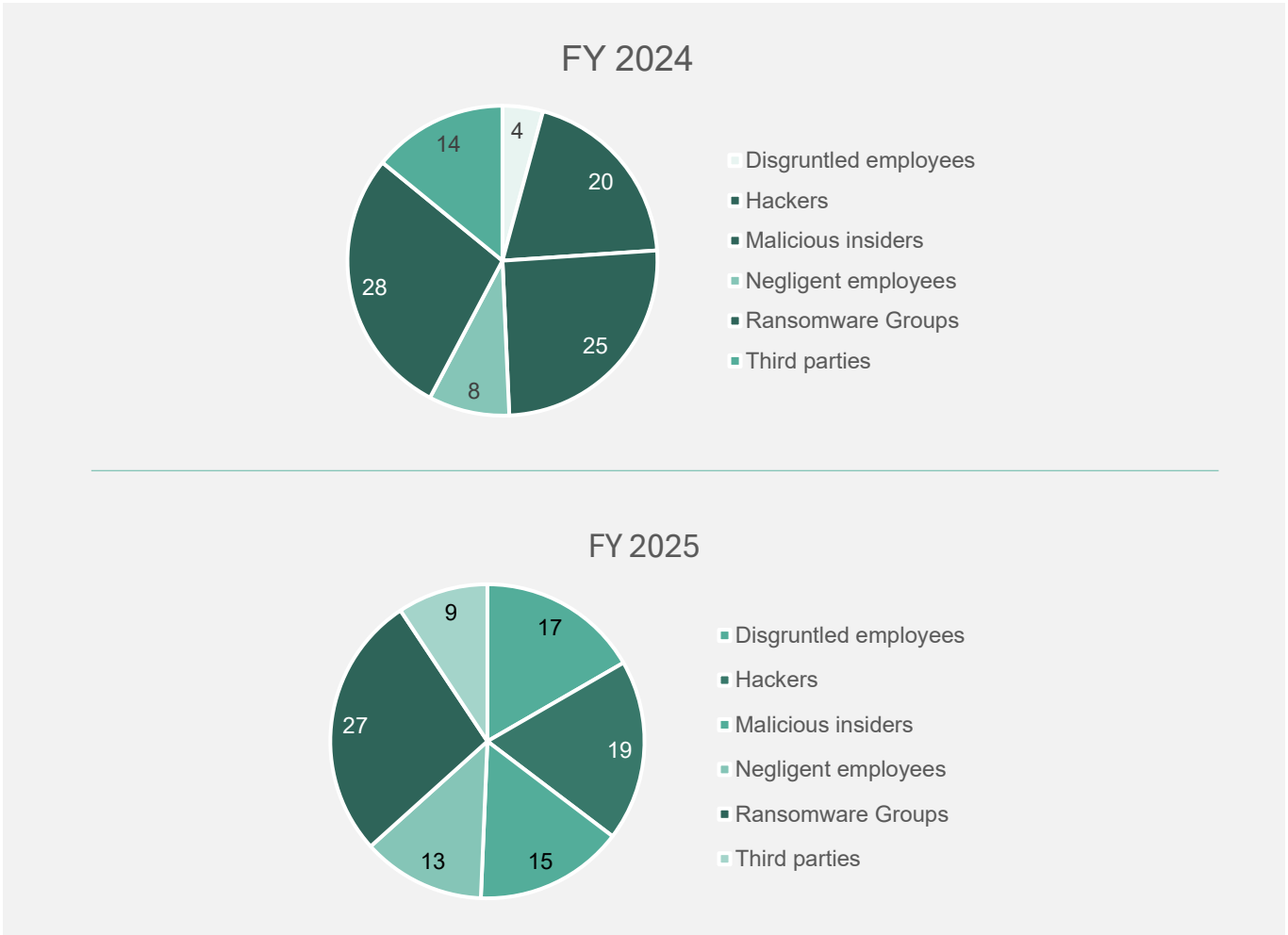
Ransomware Groups remain a top threat, nearly unchanged and still highly prevalent.

Hackers continue to be concerning but have slightly decreased from **20%** to **19%**.

Negligent Employees risks have increased moderately, emphasizing the ongoing need for security training.

Malicious Insiders worries have dropped significantly from **25%** to **15%**, possibly reflecting improved internal controls.

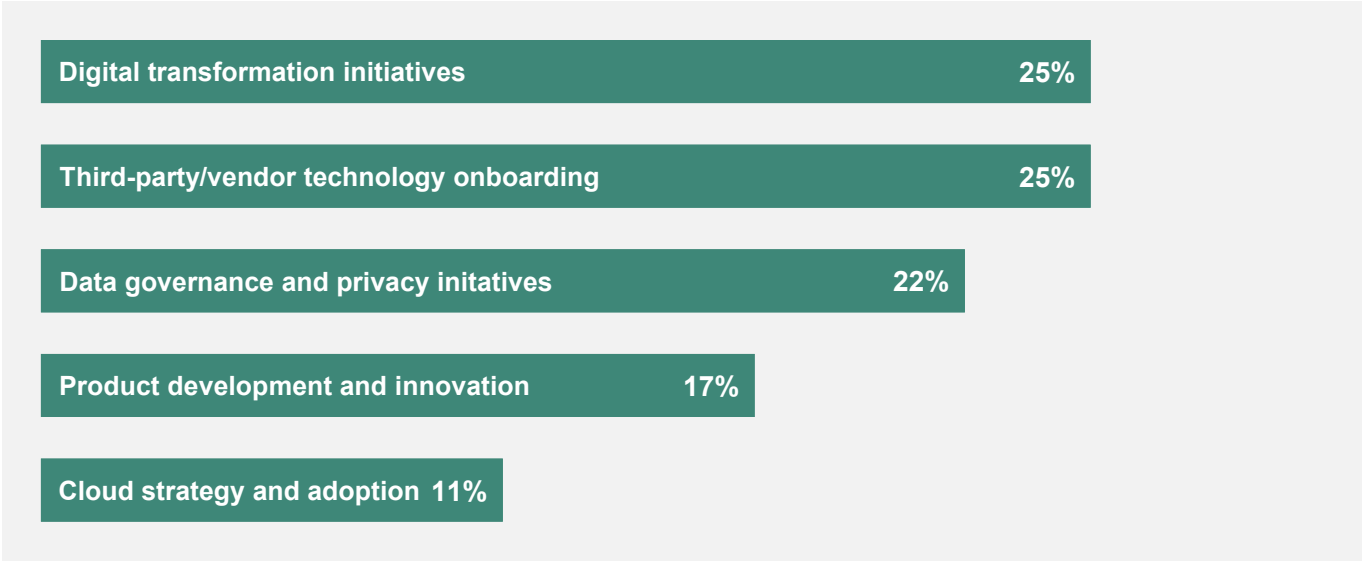
Third-Party Risks have declined, indicating some progress in vendor security management.



This shift calls for a balanced strategy prioritizing both emerging internal human risks and persistent external threats.

ROLE OF CISOs IN BUSINESS-CRITICAL TECHNOLOGY DISCUSSIONS

In today's evolving digital landscape, Chief Information Security Officers (CISOs) play an increasingly strategic role beyond traditional security functions. Their involvement spans key areas that drive business innovation and resilience, reflecting the shift from purely defensive to growth-oriented leadership in technology decisions. Understanding where CISOs focus their efforts provides valuable insight into current organizational priorities.



Digital Transformation Initiatives and **Third-party/ Vendor Technology Onboarding** emerged as the top areas where CISOs are involved. This underscores CISOs' critical role in steering technology adoption and innovation while managing associated risks.

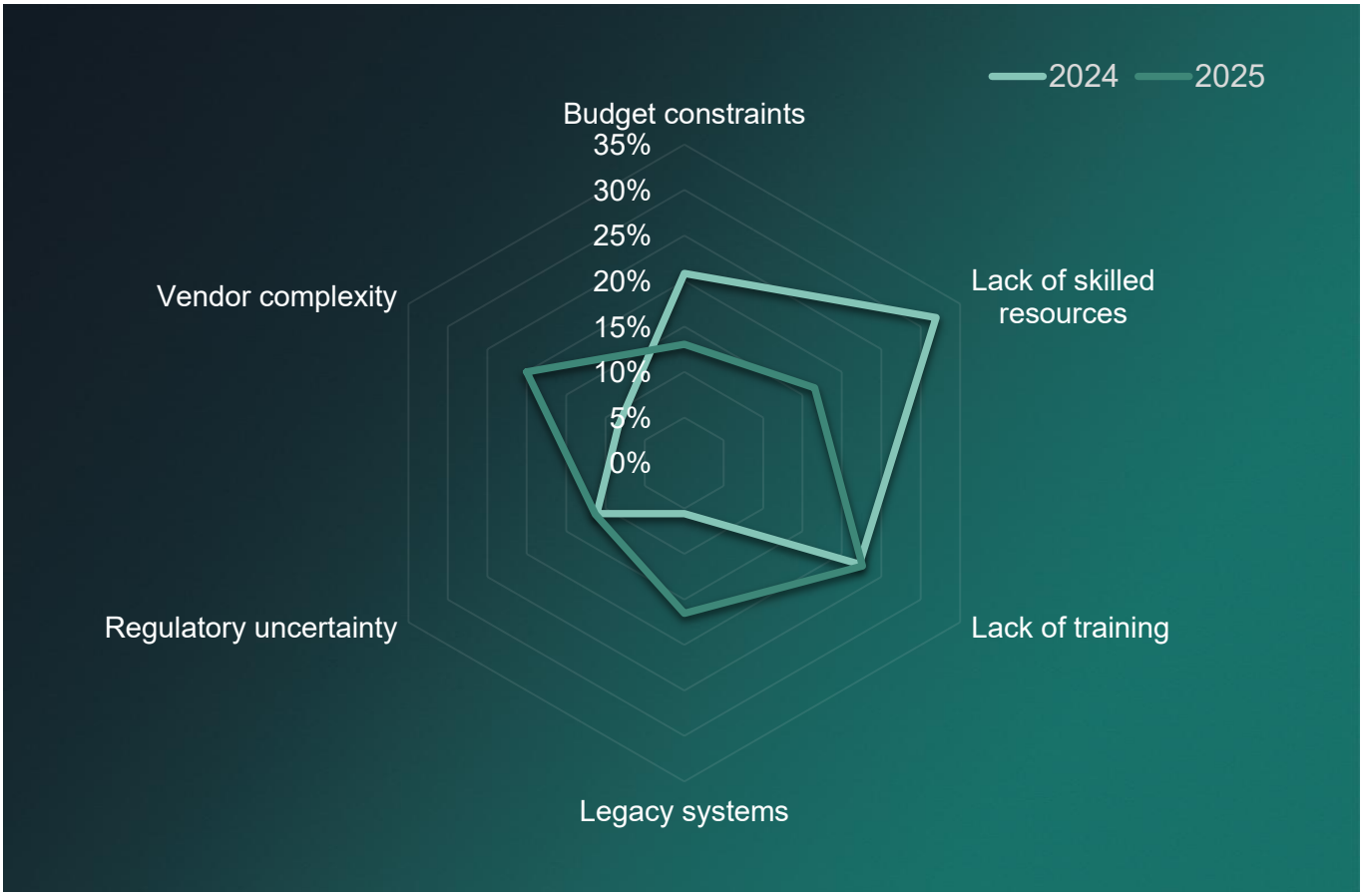
Data Governance and **Privacy Initiatives** highlight the continuing importance of privacy and regulatory compliance in organizational strategies.

Product Development and **Innovation involvement** signals CISOs' growing partnership with product teams to embed security early in the development lifecycle.

Meanwhile, **Cloud Strategy and Adoption** involvement reflects ongoing but more selectively prioritized cloud risk management as organizations mature in their cloud journeys.

33% of organizations currently do not fully engage CISOs in all critical technology discussions, highlighting ongoing opportunities to better integrate security leadership with strategic business planning.

MAJOR OBSTACLES IN PLANNING A CYBERSECURITY AND DATA PRIVACY PROGRAM



Budget constraints remain a significant challenge, though concerns have eased compared to last year's reports of limited resources. Talent shortages persist, with a growing emphasis this year on the need for ongoing training to upskill existing staff. Legacy systems have emerged as a new obstacle, complicating efforts to implement modern security solutions.

Vendor complexity is another new challenge, highlighting increasing difficulties in managing third-party risks. Regulatory uncertainty has also surfaced as an issue, reflecting the complexities organizations face in navigating evolving compliance requirements.

Compared to last year, concerns about insufficient expertise and incomplete inventories have lessened, suggesting some progress. However, the increased focus on **training gaps and legacy infrastructure** points to shifting priorities as threats and technology environments evolve.

Overall, organizations must balance budget realities with investments in talent development, system upgrades, and vendor management to build resilient cybersecurity programs in a changing landscape.

Organizations are increasingly recognizing the critical need for structured investments and strategic planning to build resilience against more sophisticated and varied cyber threats facing the industry.

Organizational Preparedness To Address Emerging Cybersecurity Risks

Effective readiness for emerging cybersecurity risks is critical as threat landscapes evolve rapidly. Organizations vary significantly in their planning and resource allocation to manage these future challenges.

Ankura shares thoughts on
The AI Privacy Dilemma

https://tinyurl.com/2z6rkrxn

Gradual Improvement in Strategic Planning

A notable 38% of organizations have plans to allocate dedicated budgets for emerging cybersecurity risks, reflecting a growing recognition of the importance of proactive investment to enhance resilience over the coming years.

Ad-Hoc and Initial Budget Planning Still Prevalent

About 24% of organizations intend to address these risks on an ad-hoc basis, while 22% already have budget plans in place. This suggests many organizations remain in transitional phases between informal and formalized risk management approaches.

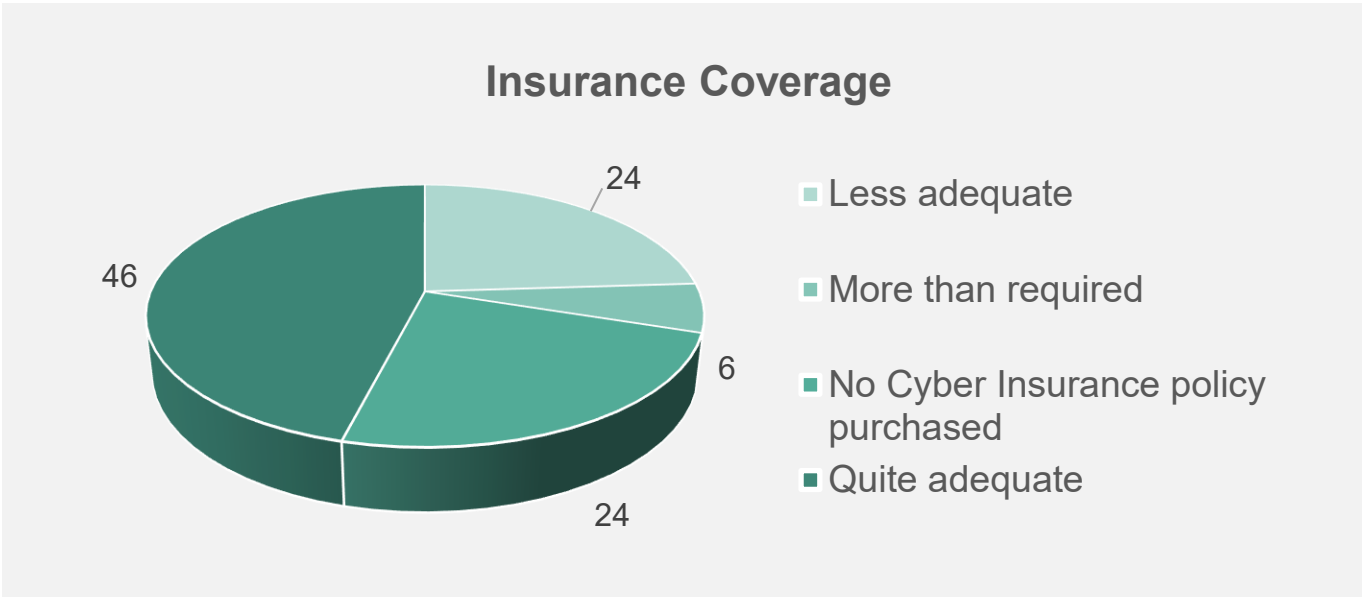
Persistent Gaps in Preparedness

Alarmingly, 16% of organizations currently lack any preparation or planning. This highlights critical gaps that could expose them to significant vulnerabilities in the evolving cybersecurity landscape without timely intervention.

CYBER INSURANCE LANDSCAPE: BALANCING RISK AND READINESS

In today's interconnected world, the importance of cyber insurance cannot be overstated. It serves as a vital component of an organization's risk management strategy, offering a layer of protection against the financial repercussions of cyber incidents.

Reflecting on the survey results, it's evident that organizations approach cyber insurance with varying degrees of confidence and readiness. For Instance, some businesses remain uninsured due to budget or coverage uncertainty, while others proactively secure insurance, occasionally exceeding necessary levels to safeguard digital assets cautiously.



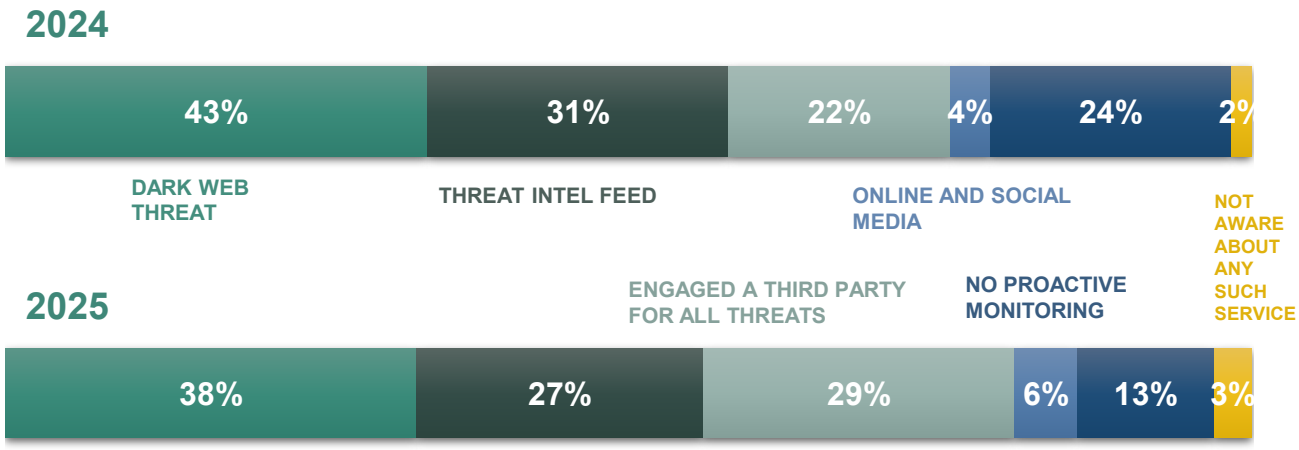
Consider the case of a mid-sized enterprise that underestimated its cyber insurance coverage, opting for a policy that covered only half of its actual exposure. When a major breach occurred, the company faced losses exceeding $2 million, far surpassing its coverage limits.

This stark example highlights the financial peril of inadequate insurance, emphasizing the critical need for organizations to thoroughly assess their risk exposure and ensure their policies are robust enough to cover potential damages in the ever-changing cyber threat landscape.

"While **46%** of organizations are on the right path with insurance coverage, some must rethink their approach for full protection. This slide highlights diverse strategies, urging all to continuously evaluate and adapt policies to navigate the challenges of our evolving digital landscape."- Amit Jaju

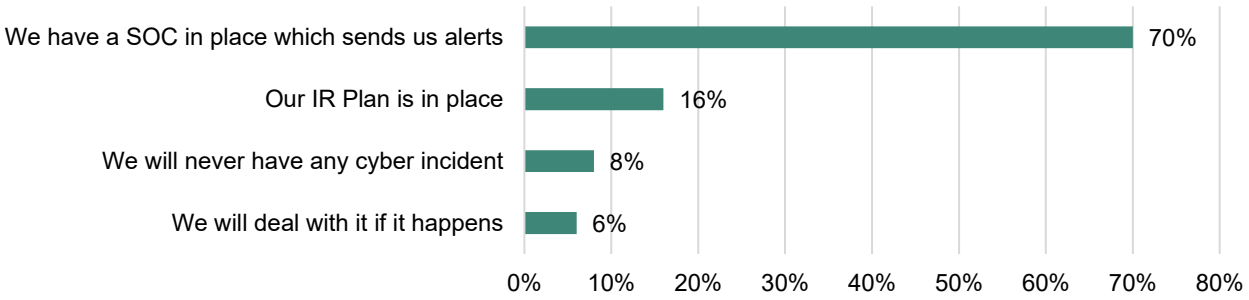
MONITORING ONLINE THREATS AND DARK WEB THREAT

Between 2024 and 2025, organizations have strengthened their focus on dark web threats and increased collaboration with third-party experts to manage all threats. There has been a notable reduction in the number of organizations without proactive monitoring, reflecting broader adoption of advanced security solutions. Awareness about monitoring services has improved slightly, while attention to online and social media threats has grown. Meanwhile, reliance on traditional threat intelligence feeds has decreased somewhat, indicating a shift toward more integrated and comprehensive threat detection strategies.



Confidence in Organizational Cybersecurity Incident Detection & Response

Effective cybersecurity incident detection and response (IR) have become essential as cyber threats escalate in scale, speed, and sophistication. Organizations are increasingly investing in capabilities to not only identify but quickly mitigate incidents before severe operational or reputational damage occurs.



Security Operations Centers (SOCs) are widely established, enabling ongoing threat monitoring and alert generation.

Fully tested and operational incident response plans remain limited across organizations.

Reactive approaches to incident management continue to be present within some entities.

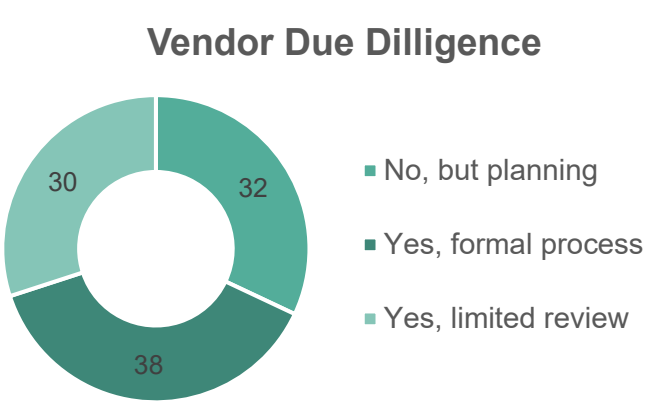
A subset of organizations maintain the view that their systems are fully protected against cyber incidents, which may obscure underlying vulnerabilities.

62% Of Organizations still do not have a formal and established process for carrying out a comprehensive technical vendor due diligence.

STRENGTHENING CYBER DEFENSES: THE IMPERATIVE OF VENDOR DUE DILIGENCE

In today's complex cybersecurity landscape, rigorous vendor and third-party due diligence acts as a critical risk mitigation strategy, essential for safeguarding against potential attack vectors and supply chain vulnerabilities that can jeopardize sensitive data integrity.

Our survey reveals that **38%** of organizations have established formal processes compared to **20%** last year, reflecting their commitment to securing networks and mitigating risks through structured evaluations and compliance with stringent security standards.



Ankura shares thoughts with ETCIO on
How to reduce cyber, data risks in an outsourced environment
https://rb.gy/kjq9v1

However, **32%** of organizations are still in the planning stages, exposing them to significant risks. Delayed implementation of due diligence can create security gaps, as demonstrated by an incident involving a financial services company that suffered a breach due to inadequate vendor vetting. Hackers exploited a vulnerability in a third-party vendor's system, leading to unauthorized access to sensitive client information and resulting in millions of dollars in damages. This incident underscored the urgent need for timely and comprehensive vendor assessments.

Furthermore, **30%** conduct limited reviews, which may lack the necessary depth to uncover hidden vulnerabilities. These superficial evaluations can overlook technical flaws in vendor systems, potentially leaving organizations exposed to cyber threats. To effectively manage long-term risks, comprehensive due diligence processes that incorporate advanced analytical tools and methodologies are essential.

Automating vendor due diligence with AI and modern tools is key to fortifying cybersecurity and mitigating hidden threats.

OVERCOMING WORKFORCE CHALLENGES: BUILDING A RESILIENT TALENT POOL

In the ever-evolving landscape of cybersecurity and digital resilience, organizations face significant challenges in maintaining and hiring a skilled workforce. Our survey highlights these obstacles, providing insights into the areas where organizations struggle most.

A considerable **26%** of organizations report difficulty in recruiting skilled talent, emphasizing the competitive nature of the market and the scarcity of professionals with specialized expertise. This challenge underscores the need for innovative recruitment strategies and partnerships with educational institutions to cultivate a pipeline of future talent.

Retention of skilled employees poses the greatest challenge, with **35%** of organizations struggling to keep valuable team members. This issue highlights the importance of creating a supportive work environment, offering competitive compensation, and providing clear career advancement opportunities to maintain employee satisfaction and loyalty.

Limited training opportunities affect **26%** of organizations, indicating a need for more robust development programs to keep pace with rapidly changing technological demands. Investing in continuous learning and development initiatives is critical to ensuring that existing staff can adapt to new tools and techniques.

Additionally, **13%** of organizations cite inadequate resources for employee development, pointing to budgetary constraints that hinder the growth of their workforce's capabilities. Addressing this challenge requires strategic allocation of resources and prioritization of employee development as a key component of organizational success.

Overall, these findings highlight the pressing need for organizations to reevaluate their workforce strategies, focusing on recruitment, retention, training, and development to build a resilient and skilled team equipped to tackle future challenges.

TRACKING COMPLIANCE WITH REGULATORY MANDATES

60% of organizations face challenges in consistently tracking regulatory compliance mandates, underscoring the importance of strengthening governance and leveraging expert support in complex regulatory environments

In our previous assessment, regulatory compliance tracking showed distinct levels of focus across various bodies, reflecting organizational priorities and challenges in maintaining comprehensive oversight. This year's analysis reveals evolving trends in how organizations approach the monitoring of mandates issued by national and sector-specific regulators.

Inconsistent Tracking of Regulatory Mandates

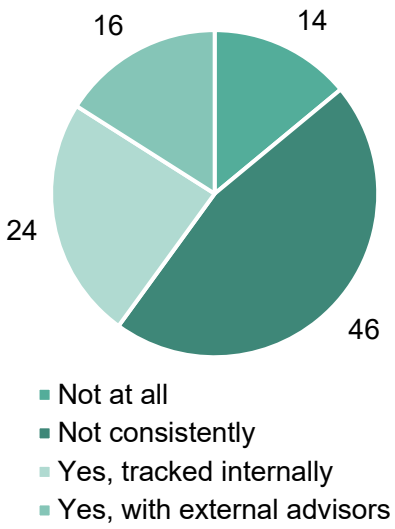
A substantial portion of organizations do not consistently monitor regulatory mandates issued by authorities such as CERT-IN, RBI, SEBI, and DPDPA. This inconsistency points to potential vulnerabilities in compliance management that could lead to regulatory risks and operational disruptions if emerging requirements are overlooked.

Internal Monitoring Dominates Compliance Efforts

Many organizations rely predominantly on internal resources to track regulatory changes. This approach reflects an emphasis on building in-house compliance capabilities, although it may also highlight limitations in specialized expertise or resource allocation needed to keep pace with evolving mandates.

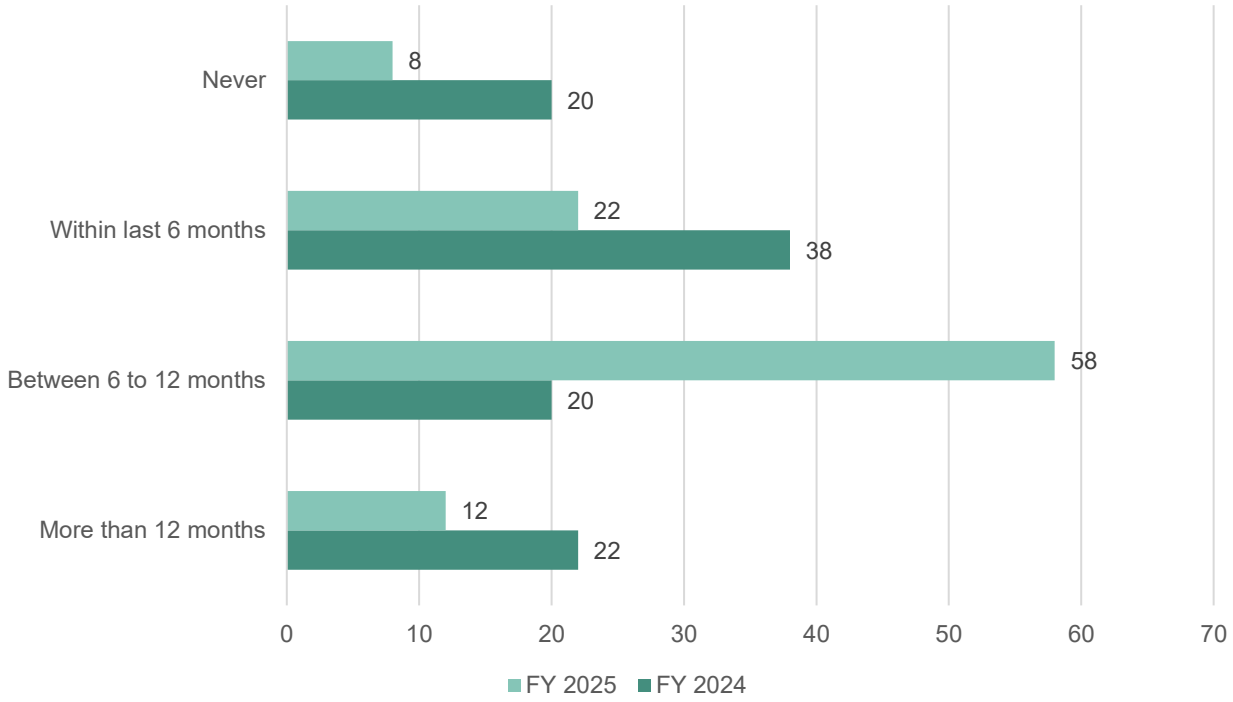
Growing Use of External Compliance Advisors

A notable segment of organizations engages external advisors to support regulatory tracking. This trend highlights growing recognition of the complexity surrounding regulatory landscapes and the value of expert guidance to ensure comprehensive and timely compliance, particularly in highly regulated sectors.



Ankura shares thoughts on Compliance With Data Privacy Regulations
https://tinyurl.com/njnr3cj2

INCIDENT RESPONSE PLAN TESTING FREQUENCY



Increasing Focus on Mid-Term Testing Intervals

The latest data shows a significant shift toward testing IR plans within a 6 to 12 months window. This increase suggests a growing recognition of the importance of periodic validation and updates, balancing operational demands with the need for readiness.

Decline in Long-Interval Testing

Fewer organizations now test their IR plans at intervals exceeding 12 months. This positive trend reflects efforts to maintain more current and effective response measures aligned with the rapidly changing threat landscape.

Reduced Recent Testing and Persistent Gaps

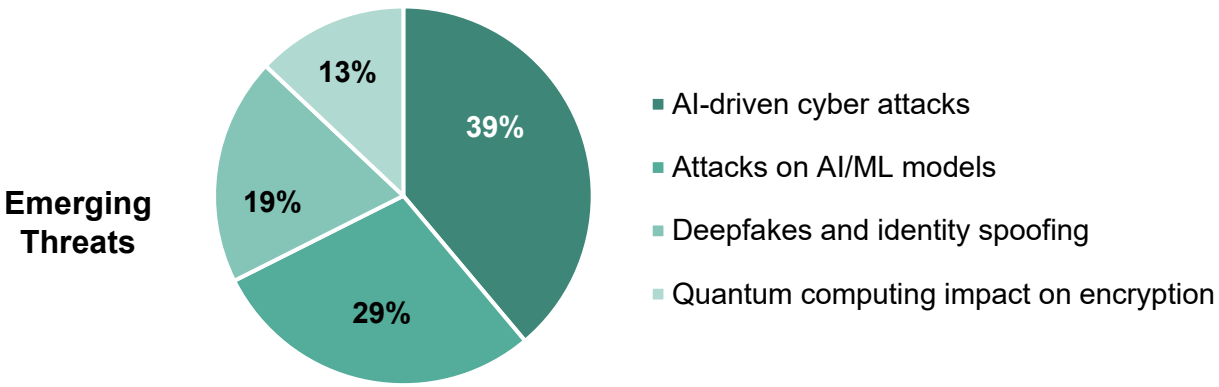
The proportion of organizations testing IR plans within the last 6 months has decreased compared to the previous year, potentially signaling operational challenges or resource constraints. Meanwhile, a smaller but notable segment still reports never conducting IR plan tests, indicating ongoing areas of vulnerability.

Compared to FY 2024, the 2025 survey shows significant improvement in the frequency of incident response plan testing, with **58%** of organizations now testing between 6 to 12 months, up from **20%**, and those never testing dropping from **20%** to **8%**.

68% of organizations are concerned about AI-related threats, combining AI-driven attacks and attacks on AI/ML models.

MOST CRITICAL EMERGING CYBERSECURITY THREATS EXPECTED OVER THE NEXT 3 - 5 YEARS

As cyber threats rapidly evolve, organizations identify emerging and futuristic risks demanding urgent focus. AI-related threats dominate concerns alongside challenges posed by new technologies like quantum computing.



Dominance of AI-Driven Cyber Attacks

AI-driven cyber attacks lead as the most critical risk, with 39% of organizations identifying them. These attacks use artificial intelligence to automate and enhance tactics, increasing sophistication and making detection more difficult.

Vulnerabilities Targeting AI/ML Models

29% of organizations are concerned about attacks on AI and machine learning models themselves. These systems are vital for security and operations, and adversaries aim to exploit or manipulate them for malicious purposes.

Growing Concern About Deepfakes and Identity Spoofing

Deepfakes and identity spoofing are seen as serious threats by 19%, as increasingly realistic fake content raises risks of fraud, misinformation, and trust breaches.

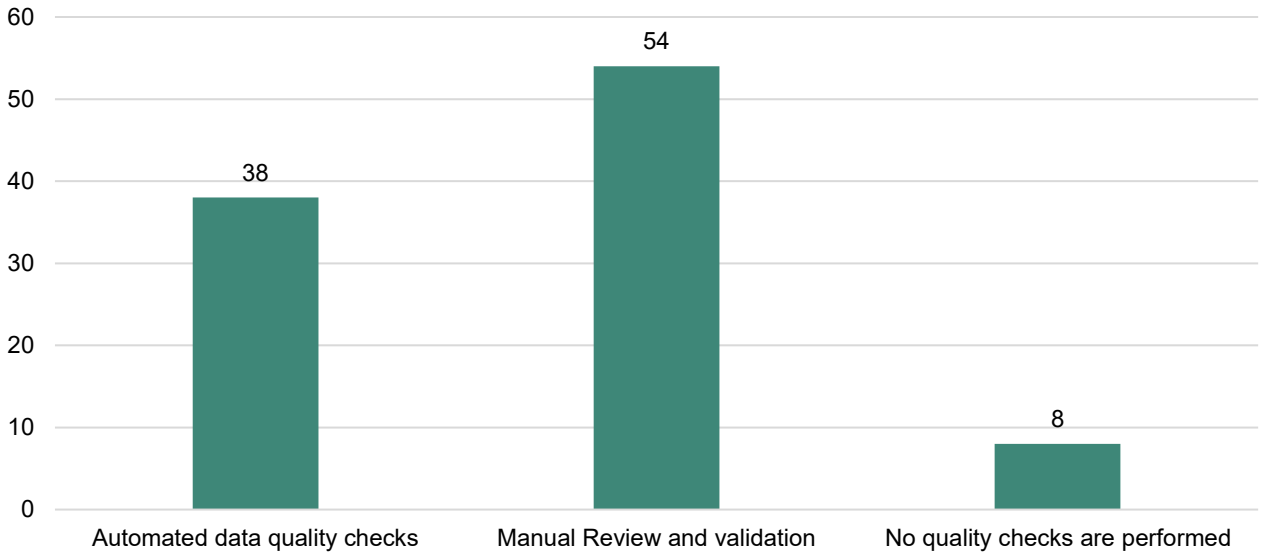
Quantum Computing's Future Impact on Encryption

Thirteen percent worry about the impact of quantum computing on encryption, emphasizing the need to develop quantum-resistant cryptographic measures.

50% of organizations utilize thorough manual validation methods to uphold the integrity and reliability of their security data

ENSURING ACCURACY AND CONSISTENCY OF SECURITY-RELATED DATA

Maintaining accurate and consistent security data is essential for effective threat detection, informed decision-making, and timely incident response. Organizations adopt varying approaches to validate and verify data such as logs, alerts, and incident information.



Predominance of Manual Review and Validation

The majority of organizations rely on manual processes to review and validate security data. This hands-on approach underscores the trust placed in human judgment to detect anomalies and ensure data integrity, though it may also indicate challenges in fully automating quality assurance.

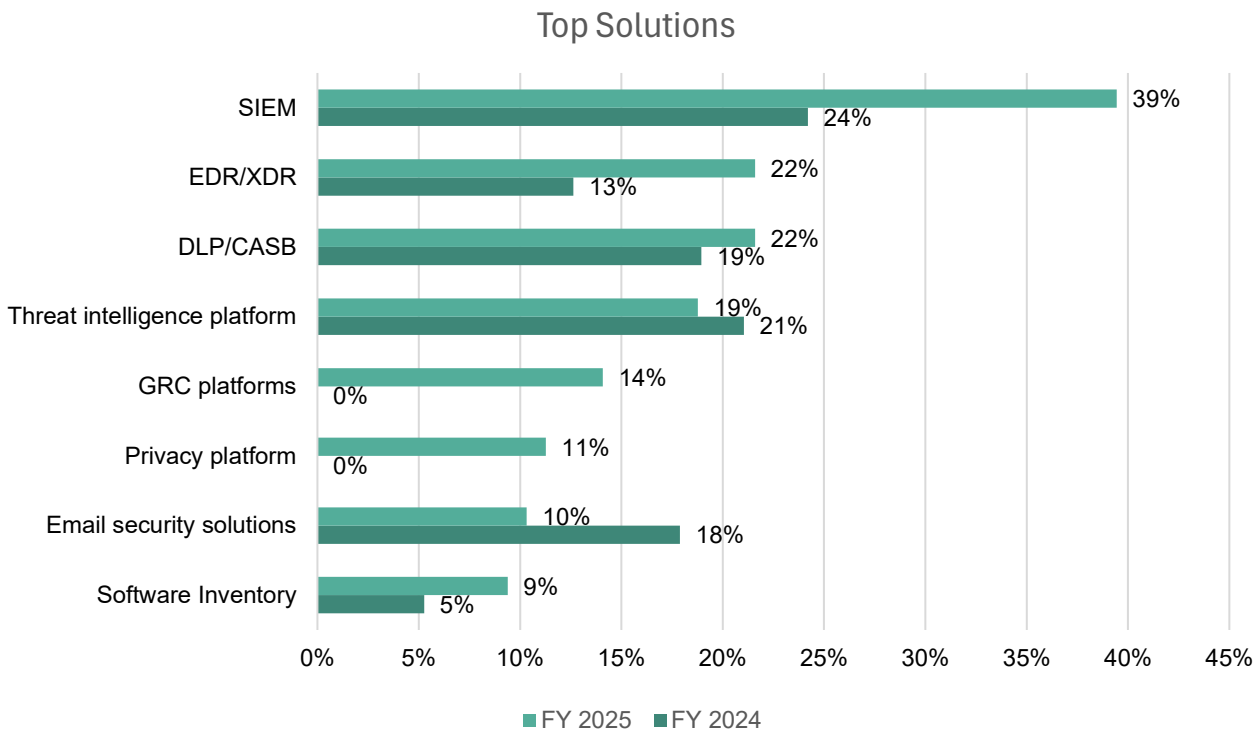
Significant Use of Automated Data Quality Checks

A substantial portion employs automated data quality mechanisms, reflecting growing adoption of technology-driven validation tools. Automation enhances efficiency and consistency, particularly in handling large volumes of security data generated by modern environments.

Presence of Gaps in Data Quality Assurance

A notable minority of organizations do not perform any formal quality checks on their security-related data. This absence of validation could create risks by allowing inaccurate or inconsistent data to impact security monitoring and response effectiveness.

TOP DATA PRIVACY AND CYBERSECURITY SOLUTIONS IN FOCUS



Advanced Threat Detection and Response

A marked increase in adoption of SIEM and EDR/XDR solutions in 2025 highlights a shift toward enhanced centralized monitoring and endpoint threat detection compared to 2024. This reflects growing awareness of sophisticated cyber threats and the need for faster incident response capabilities.

Governance, Privacy, and Asset Management Platforms on the Rise

2025 shows a notable emergence of Governance, Risk, and Compliance (GRC), privacy platforms, and software inventory solutions as organizational priorities. These additions suggest heightened emphasis on meeting complex regulatory requirements, strengthening data protection, and improving visibility into software assets to manage vulnerabilities more effectively.

Shifts in Core Data Security Solutions

While DLP and CASB solutions have maintained focus, their increased adoption in 2025 underscores the accelerated move to secure cloud environments and sensitive data. Conversely, email security has seen reduced emphasis compared to 2024, possibly due to maturing layered defenses and evolving threat landscapes.

84% of organizations prioritize SIEM solutions, underscoring the critical need for advanced security event monitoring

AWAKENING DIGITAL DEFENSES

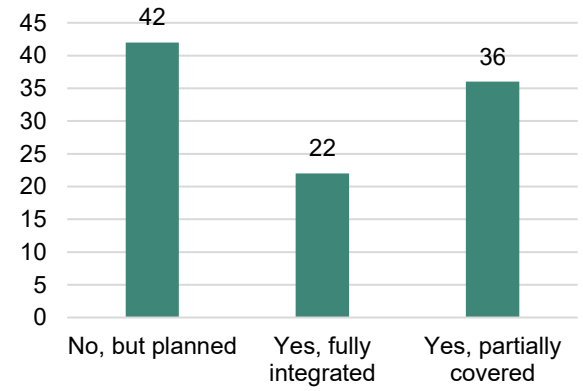
Cybersecurity & Data Privacy Awareness: Key Findings and Progress

In today's evolving threat landscape, organizations recognize the critical role of cybersecurity and data privacy awareness across all levels—from management to frontline employees and external partners.

Our recent survey, compared with last year's data, highlights how organizations are broadening their training efforts, employee engagement, and third-party risk management to build a stronger, more resilient security posture.

Cyber Security Awareness Training Coverage

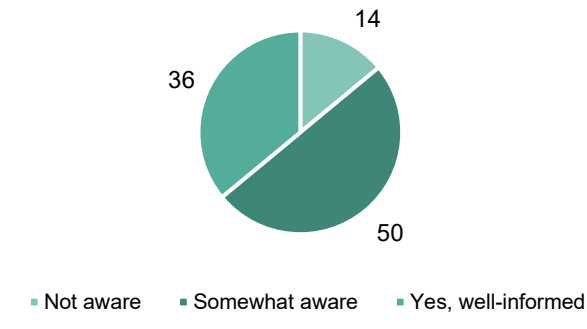
Many organizations have not yet fully integrated data protection and privacy training but are planning to do so. Some have partially covered these areas, while a smaller proportion report comprehensive integration. Last year's focus was heavily on training management and CXO teams, with limited outreach to employees and vendors. This year shows a shift toward expanding coverage beyond leadership to include the wider employee base and third parties.



Employee Awareness of Cybersecurity & Privacy Roles

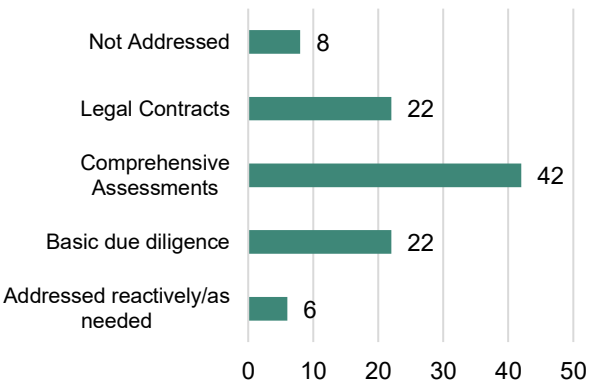
Employee understanding varies. some are well-informed, many are somewhat aware, and a minority are unaware.

The previous year's training emphasis on executives likely contributed to gaps in awareness at the employee level. Organizations are increasingly focusing on improving employee engagement and clarity around individual roles in data protection.



Management of Vendor & Third-Party Cybersecurity Risks

Organizations use varied approaches: comprehensive assessments, legal contracts, basic due diligence, reactive measures, or no approach. Minimal training was provided to third-party vendors in the prior year, likely leaving gaps in vendor risk management. Expanding vendor training and embedding thorough assessments are emerging priorities for holistic risk mitigation.



While 42% of organizations are planning data protection training, only 6% of last year's awareness training covered third-party vendors, pointing to critical areas for enhanced focus and broader reach.

TOP FRAMEWORKS REFERRED BY ORGANIZATIONS

68% of organizations track privacy regulations like DPDPA/GDPR, while approximately 60% rely on ISO and NIST frameworks, underscoring strong adherence to global cybersecurity and privacy standards.

Maintaining accurate and consistent security data is essential for effective threat detection, informed decision-making, and timely incident response. Organizations adopt varying approaches to validate and verify data such as logs, alerts, and incident information.

Preference for Global Standards

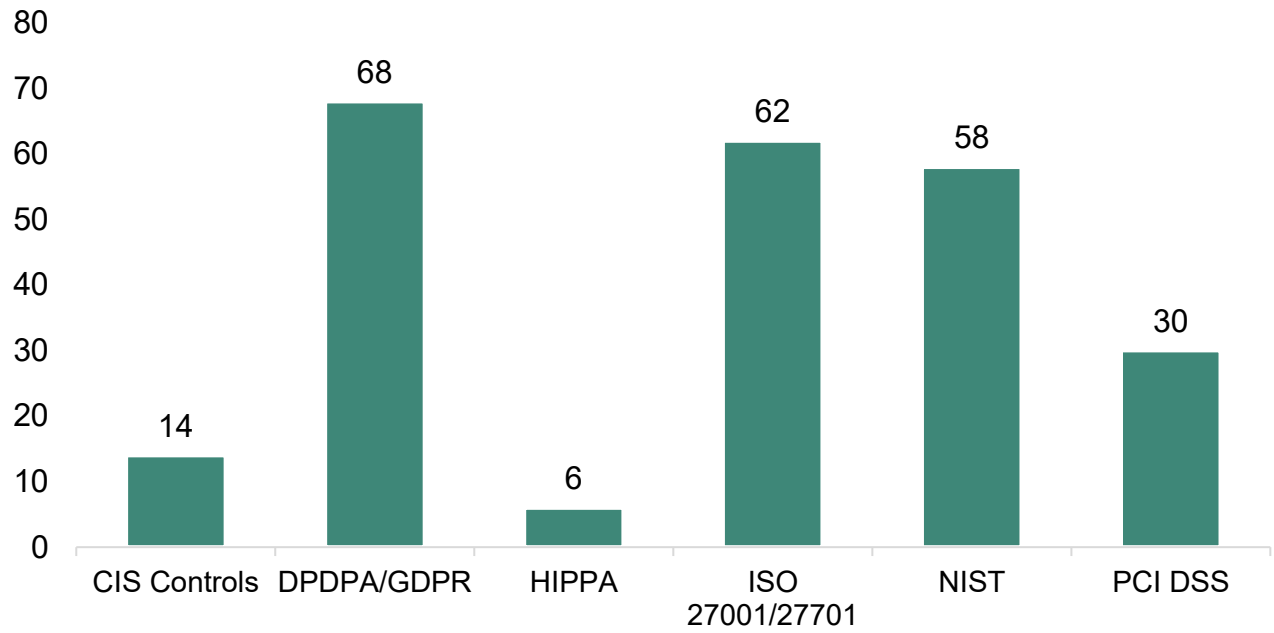
Most organizations continue to rely on internationally recognized cybersecurity frameworks such as ISO 27001/27701 and NIST. High adoption rates for these standards highlight their perceived value in shaping robust, well-structured security programs and in meeting compliance obligations across multiple jurisdictions.

Growing Importance of Privacy and Payment Regulations

There is a notable increase in the use of privacy-focused frameworks, such as DPDPA and GDPR, which have surged in prominence compared to previous years. The ongoing emphasis on regulatory compliance is further supported by the adoption of PCI DSS, especially in organizations handling payment data.

Broader, Yet Selective, Adoption of Other Frameworks

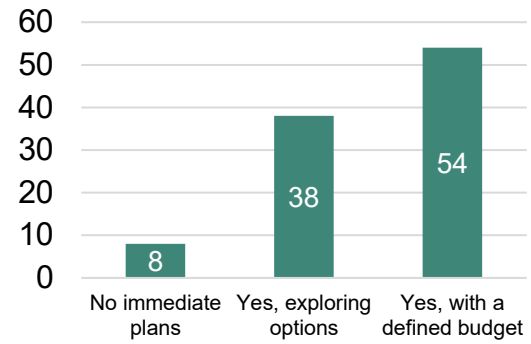
While frameworks like CIS Controls retain a portion of organizational attention, their adoption remains limited relative to more comprehensive standards. HIPPA is referenced by a smaller number of entities, reflecting its relevance in the healthcare sector. Collectively, these trends highlight a focus on aligning cybersecurity practices with both sector-specific and global requirements.



DATA PRIVACY AND GOVERNANCE

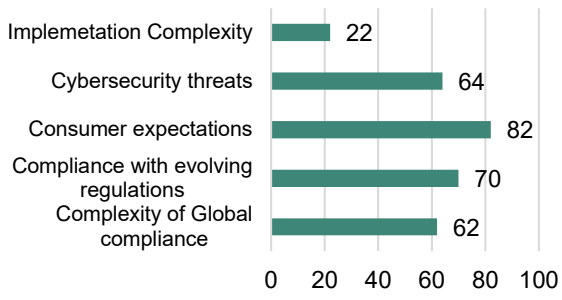
Data Privacy Initiatives & Challenges: Current Insights and Trends

As data privacy regulations grow more complex and consumer expectations rise, organizations are actively planning and investing in privacy initiatives. Compared to last year's focus, which included many organizations not yet planning or just starting data privacy programs, the current landscape shows a stronger commitment with more defined budgets and clearer accountability for privacy management.



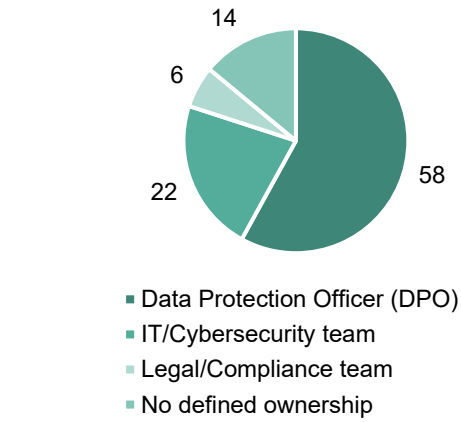
Investment in Data Privacy Initiatives

A clear majority of organizations are prioritizing data privacy, with 54% having defined budgets for related initiatives within the next 12–24 months. Additionally, 38% are actively exploring options, indicating widespread recognition of privacy as a critical business priority. Only a small fraction currently have no immediate plans, showing near-universal engagement on this issue.



Biggest Data Privacy Challenges Ahead

Meeting consumer expectations remains the top challenge, as organizations strive to build trust through transparent and secure data practices. Rapidly evolving regulatory landscapes add complexity, requiring continuous compliance adjustments. Cybersecurity threats compound these issues by increasing risks to sensitive data. Moreover, managing global compliance complexity and overcoming implementation difficulties continue to challenge many organizations.



Accountability for Data Privacy Programs

Data privacy is primarily managed by Data Protection Officers in most organizations, reflecting the growing emphasis on dedicated privacy governance. IT and cybersecurity teams also play key roles in supporting privacy initiatives. However, about one in seven organizations still lack clearly defined ownership, which may hinder effective privacy management and compliance.

50% of organizations now have a defined budget for data privacy initiatives

CYBERSECURITY AND PRIVACY AUTOMATION PRIORITIES FOR THE NEXT 1–2 YEARS

Organizations plan to accelerate automation across various cybersecurity and privacy domains to increase efficiency, reduce manual overhead, and enhance threat detection and response capabilities.

24% of organizations are prioritizing automation in threat detection and response to enhance cybersecurity effectiveness.

Focus on Threat Detection and Log Management

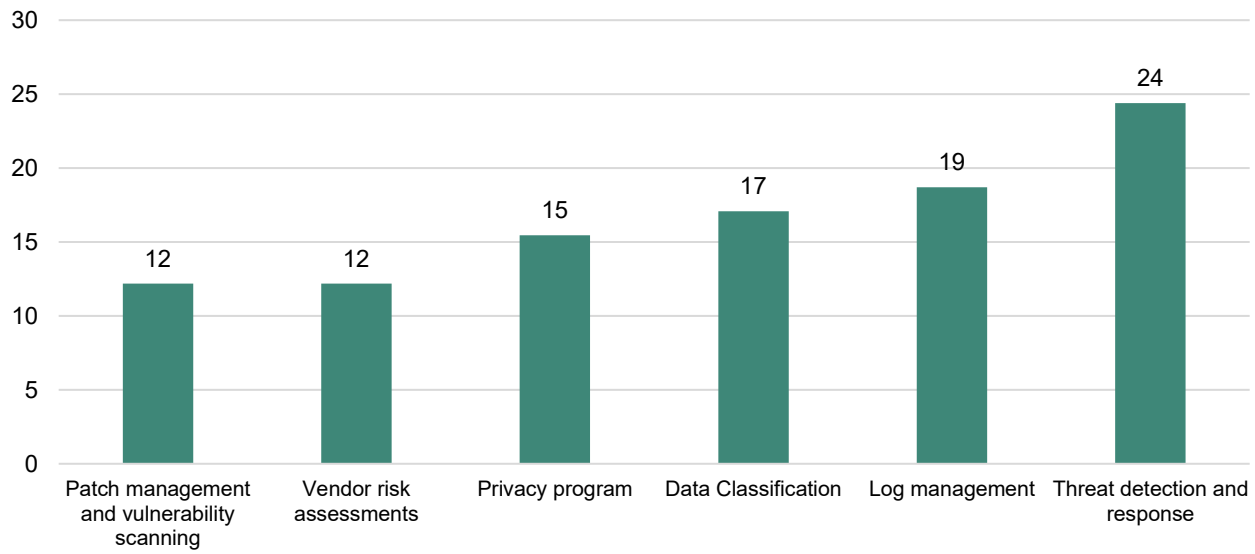
Threat detection and response remains the top priority for automation, with most of the organizations targeting this area. This aligns with industry trends emphasizing AI-driven monitoring and rapid anomaly identification. Log management automation also receives significant attention, facilitating continuous visibility and faster incident analysis across complex IT environments.

Expanding Automation in Data Classification and Privacy

Data classification and privacy programs are key areas slated for automation by 17% and 15% of organizations respectively. These efforts reflect growing regulatory requirements for data governance and the need to safeguard sensitive information efficiently.

Patch Management and Vendor Risk Automation

Automation in patch management and vulnerability scanning addresses one of the most common attack vectors, unpatched systems, by streamlining update deployment. Similarly, automating vendor risk assessments helps organizations manage third-party exposure more effectively, a critical concern as supply chain attacks rise.



Expert Insights – Corporates

What initiatives do you envisage to address the skills gap in cybersecurity and develop a workforce equipped to tackle emerging threats?

Reforming education and training pathways is crucial for cybersecurity preparedness. Early and integrated education should incorporate cybersecurity and digital literacy into K-12 curricula, fostering online safety and security through hands-on activities and competitions. Diverse and accessible learning aims to create entry points into cybersecurity for non-traditional backgrounds, including veterans, women, and minorities.
Continuous professional development involves regular upskilling and reskilling of current employees, both technical and non-technical, to maintain relevant skills and robust security postures. Internal training programs and cross-role experiences enhance versatility, while subsidized certifications encourage ongoing education. Emerging technologies like cyber ranges, AI, and simulations provide real-world practice and personalized learning paths.
Fostering a collaborative and diverse ecosystem requires public-private partnerships to share threat intelligence, conduct joint training, and coordinate large-scale attack responses. Establishing a security-first culture ensures cybersecurity awareness across all organizational levels. Mentorship and community building promote knowledge-sharing among professionals and newcomers.
Addressing new and emerging threats involves specialized training in cloud security, AI, IoT, and OT security, focusing on their unique challenges. Soft skills such as critical thinking, problem-solving, and communication are vital for effective incident response and teamwork.
Key initiatives to close the skills gap include creating clear pathways from school to higher education and vocational training, promoting diversity, encouraging certifications, and supporting public-private partnerships to scale talent initiatives. Introducing cyber skills early in education and broadening access to technology learning opportunities are essential for future readiness.

What role can regulators play in fostering industry-wide digital resilience to effectively counter emerging cyber threats?

Regulators are pivotal in enhancing digital resilience by converting voluntary cybersecurity guidelines into mandatory standards. This ensures a consistent level of preparedness across industries, minimizing vulnerabilities in interconnected sectors. They enforce sector-specific standards based on frameworks like NIST or ISO 27001. The EU's Digital Operational Resilience Act (DORA) exemplifies this by mandating financial institutions to manage, test, and report ICT risks, establishing a unified security baseline.
Mandatory incident reporting forms centralized threat data repositories, which enhance intelligence sharing and accelerate threat detection and response. Transparency encourages organizations to strengthen their security postures to avoid reputational and financial losses.
Regular testing and audits, including third-party assessments and "red team" exercises, ensure practical resilience beyond theoretical compliance. Regulatory demands also drive investment in advanced cybersecurity solutions, fostering innovation.
Regulators promote collaborative ecosystems through public-private partnerships, forums, and programs, vital for combating sophisticated cyber threats and building resilient infrastructures. They boost resilience by setting mandatory standards, requiring ICT risk management, resilience testing, and incident reporting, as mandated by DORA. They encourage cross-sector collaboration, enforce supply chain security, and hold leadership accountable for cyber governance.
In Australia, regulators like APRA and ACSC enforce standards like CPS 230, mandate incident reporting, promote threat intelligence sharing, guide critical infrastructure cybersecurity, and encourage industry collaboration, ensuring sectors remain vigilant against evolving threats.

Anirban Banerjee
Global Head - Business Advocacy & Excellence at Tata Consultancy Services.

Expert Insights – Corporates

What key actions should the industry prioritize to collectively enhance cybersecurity resilience for the future?

For an industry to collectively enhance its cybersecurity resilience for the future, it must prioritize a holistic strategy that goes beyond simple protection. This involves recognizing that an attack is a matter of "when," not "if," and building the capacity to quickly adapt and recover.
The key actions to prioritize include **proactive risk management** and **information sharing**. Instead of just reacting to threats, the industry should conduct continuous risk assessments and penetration testing to identify vulnerabilities before they're exploited. A crucial part of this is implementing a **Zero Trust architecture**, which operates on the principle of "never trust, always verify," and is vital for securing complex, multi-company networks.
Another critical action is **enhancing supply chain security**. As our digital ecosystems become more interconnected, the weakest link can expose the entire chain. Mandating a baseline of cybersecurity standards for all vendors and partners, coupled with regular audits, creates a more robust collective defense.
Finally, the industry needs to invest in **human-centric security** and **collaborative defense**. This means going beyond basic training and fostering a culture where every employee understands their role in security. We must also actively participate in industry-specific threat intelligence sharing to create a collective defense against shared threats, allowing us to respond faster and more effectively.

What role do counter-offensive tactics play in modern cybersecurity strategies, and how can they be responsibly implemented?

Counter-offensive tactics in modern cybersecurity, often called active defense, play a crucial role by moving beyond traditional passive protection to actively deter future attacks, gather threat intelligence, and disrupt ongoing malicious activity. These strategies make an organization a more difficult and less attractive target for adversaries. However, their use requires a highly responsible and cautious approach to mitigate significant legal, ethical, and operational risks.The responsible implementation of these tactics is critical. It must be strictly governed by a principle of non-escalation and proportionality, where any action taken is carefully measured and aimed at neutralizing a threat, not causing disproportionate harm. It is essential to operate within the defined legal boundaries of our jurisdiction and to avoid actions that could be mistaken as cyber-warfare, which can lead to severe consequences. The best practice is to focus on less aggressive forms of active defense, such as using honeypots to lure and study attackers or sinkholing to disrupt their command and control infrastructure. The decision to use any form of active defense should be a strategic one, made at the highest levels of leadership, and executed only by highly skilled and authorized teams to ensure these actions remain controlled and responsible.

Prashant Agarwal
IT & Digital Head - Aditya Birla Group

Expert Insights – Legal

How can the industry build cyber resilience and ensure compliance with evolving regulations while fostering innovation?

As the technology and regulatory landscape evolves, organizations must adopt a structured yet agile approach to cyber resilience that enables compliance without impeding innovation.

A critical first step is the development of a cyber incident response playbook that outlines specific response actions, assigns clear roles and responsibilities across teams, and is regularly updated to reflect both regulatory and threat landscape changes. Equally important is ongoing training and mock drills to cultivate a culture of awareness. Regular sessions across all business functions, not just IT, empower employees to identify and respond to threats quickly and responsibly.

To navigate complex and overlapping compliance requirements, organizations should adopt a unified reporting template that covers obligations pertaining to the reporting to the Indian Computer Emergency Response Team ("CERT-In"), the personal data breach reporting obligations under the Digital Personal Data Protection Act 2023 and rules thereunder (once in force), and relevant sectoral regulators. This centralized approach promotes reporting efficiency and consistency during high-pressure incidents.

Building resilience also demands periodic testing of incident response plans through simulated attack scenarios and tabletop exercises. These help organizations validate preparedness and refine response mechanisms in real-time. Finally, proactive collaboration with regulators and industry bodies is essential to address any emerging challenges in the cyber incident disclosure landscape. Together, these measures form the foundation of a resilient, compliant, and innovation-friendly cybersecurity posture.

How should the industry approach negotiations with threat actors, and what ethical and legal considerations come into play?

Negotiating with threat actors raises complex legal, ethical, and operational concerns. From an ethical standpoint, paying ransom may incentivize criminal activity and fund further attacks. Operationally, there is no guarantee that threat actors will honour their commitments (eg, to restore data or not leak stolen information) even if a ransom is paid.

From a legal standpoint, India does not explicitly prohibit ransom payments. However, such payments, particularly if made to foreign entities or through unregulated means like cryptocurrency, can raise concerns under the Foreign Exchange Management Act 1999, as well as other anti-money laundering and anti-terror financing laws.

As of now, no formal guidance has been issued by the Indian government or CERT-In that permits or bans ransom payments to threat actors, but the broader regulatory posture, as observed from publicly available CERT-In advisories, discourages engagement with threat actors and prioritises timely reporting, investigation and improving resilience. CERT-In has advised that "individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released."

Given this grey zone, organisations should proceed with extreme caution. If negotiation is being considered, it is essential to involve legal counsel early on, document all deliberations, notify regulators, where required and explore non-payment alternatives (like restoration from backups). Organisations should also assess reputational risks and operational impact before making any determination and ensure board-level oversight for such high-stakes decisions.

Supratim Chakraborty
Partner – Khaitan & Co.

Expert Insights – Insurance

Reflecting on recent years, how have shifts in the cyber threat landscape influenced the way organizations approach risk management and insurance policy adjustments?

In recent years, the scale and frequency of cyberattacks have made it clear that cyber risk is now one of the most significant financial exposures facing businesses. High-profile ransomware events, supply chain breaches, and regulatory scrutiny have pushed organizations to reframe cyber risk as a board-level financial and strategic risk, rather than a purely technical concern.

This shift has had several major effects on the cyber insurance landscape:

A dramatic increase in demand for coverage — Organizations that once viewed cyber insurance as optional now consider it a critical part of their risk transfer strategy. Even traditionally conservative sectors are purchasing cover to protect against operational downtime, regulatory penalties, and reputational damage.

Evolving policy structures — Insurance coverage has expanded from basic data breach response to include business interruption, ransomware negotiation, digital asset restoration, supply chain risks, regulatory response, and cybercrime to some extent. This reflects real-world loss experience and changing client needs.

Pricing and capacity challenges — As claims frequency and severity have grown, insurers have adjusted premiums, retentions, and available capacity. Organizations are responding by using tools like risk quantification and modeling to justify limits and negotiate favorable terms. Despite an uptick in claims reported in the last few months, ample capacity is still available at reasonable premiums.

Focus on proactive resilience — Underwriters increasingly assess the strength of security controls during placement. This has elevated the role of brokers and advisors in helping clients demonstrate resilience, adopt best practices, and secure optimal coverage.

Ultimately, the changing threat environment has positioned cyber insurance as an essential partner to enterprise risk management. It is no longer solely focused on recovering losses but also on enabling confidence to operate in a high-risk digital economy.

How can cyber insurance policies be structured to incentivize organizations to adopt comprehensive cyber resilience strategies against emerging cyber threats?

Cyber insurance can be a catalyst for resilience when policies are structured to both protect and incentivize organizations. This requires shifting insurance from a passive risk transfer instrument to an active enabler of stronger security practices.

Cyber risk quantification as a foundation — Quantifying cyber risk enables organizations to understand their potential financial exposures and align policy structures accordingly. This ensures that coverage limits are not arbitrary but tied to modelled risks, motivating organizations to invest in controls that reduce those risks.

Rewarding security maturity — Premium discounts, broader coverage, or deductible relief can be provided to organizations that adopt critical controls such as MFA, EDR, encryption, and offline backups.

Encouraging continuous improvement — Insurers can incentivize insureds to demonstrate year-on-year security improvements, using benchmarks and ongoing monitoring to reward stronger postures with better terms.

Improved wording — While the Indian cyber insurance market is competitive, there is a gap between the coverages available in the global and domestic markets. There are clients in India who are willing to pay extra to get coverages that are available internationally, such as bricking, betterment, and contingent business interruption, which are limited in availability in the Indian market.

At Marsh, we bring this to life by helping clients secure optimized coverage through risk quantification, peer benchmarking, and resilience assessments, while also connecting them to a robust ecosystem of forensic, public relations, and legal vendors. Coupled with our dedicated claims advocacy, this ensures clients not only transfer risk effectively but also continuously improve their resilience against an ever-evolving cyber threat landscape.

Ritesh Thosani
SVP, Cyber Practice Leader- Marsh India

Recent Cases We Worked on

AI-Driven PII/PHI Review: Balancing Efficiency and Compliance

Our team was engaged by a major organization to investigate and validate a suspected data breach by a threat actor. Concern centered around the exposure of personal and sensitive data and identifying breach entry points.

Handling data volumes in terabytes, our team employed local Large Language Models (LLMs) and advanced AI tools for efficient analysis. We scrutinized logs to validate suspicious file downloads and pinpoint breach points, identifying malicious network behavior. Ankura's analytics engine, AI, and eDiscovery solutions helped uncover Personally Identifiable Information (PII) and Sensitive Personal Information (SPI).

Data files were classified into readable, scanned, and encrypted formats. Advanced analytics and AI correlated leaked information with existing data, including dark web sources, to assess risk extent.

Ankura provided a consolidated report with AI-driven insights and recommendations to enhance cybersecurity measures.

Incident Response: When Speed Matters

Our team was engaged by a major organization to respond to a ransomware attack that threatened critical operations. Leveraging advanced log analysis, we swiftly identified patient zero within 30 minutes of the attack's onset, enabling rapid containment measures.

Our investigation revealed the ransomware's entry point and its initial spread, allowing us to implement immediate countermeasures. By isolating affected systems and neutralizing the threat, we curtailed the ransomware's impact and safeguarded sensitive data from encryption.

Following the incident, we prepared a detailed Root Cause Analysis (RCA) report, which was submitted to regulators, ensuring transparency and compliance. The thorough investigation and prompt action led to a satisfactory closure of the incident, reinforcing the organization's cybersecurity posture.

Recent Cases We Worked on

Safeguarding Transition: Expert Guidance on Infrastructure Decommissioning

Our team was engaged by a top media entertainment company to assist in cloud infrastructure decommission supervision. The Head of Legal and the management team were concerned about any implications of their vendor's proprietary software usage in the cloud infrastructure beyond its license expiry. Our team supervised and provided expert advice in relation to the infrastructure decommissioning process. This included:

- Assisting in the creation and preservation of backup copies of the data/information generated
- Analyzing logs to identify any instances of infringement
- Providing a detailed fact-based report capturing the activities along with the findings, outcomes, and other supporting information.

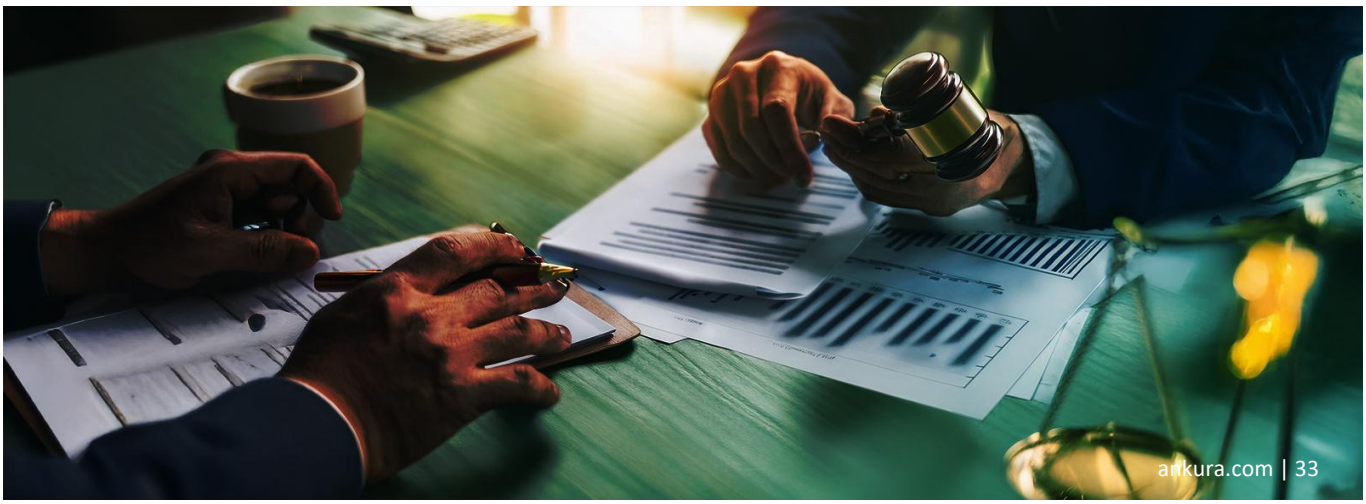
Uncovering Truth: Asset Recovery and Claim Reduction

Our team was engaged by a leading insurance company to investigate a suspicious claim involving asset misappropriation by an employee at a customer location. The management was concerned about the legitimacy of the claim and the potential financial impact.

Utilizing forensic analysis and investigative techniques, our team meticulously examined transaction records, employee communications, and asset inventories. Through detailed scrutiny, we identified discrepancies and patterns indicative of asset siphoning by the employee.

Our investigation revealed the extent of the misappropriation, allowing us to substantiate findings with concrete evidence. As a result, the claim was significantly reduced by approximately 80%, mitigating the financial repercussions for the insurance company.

We provided a comprehensive report detailing our findings, methodologies, and recommendations, empowering the client to implement stronger internal controls and prevent future occurrences of asset misappropriation.



Key Takeaways

CYBERSECURITY EVOLUTION: KEY IMPERATIVES

ADAPTIVE CYBERSECURITY STRATEGIES

Organizations are developing flexible security frameworks capable of evolving with new threats and technological advancements.

INTEGRATED RISK MANAGEMENT APPROACH

Holistic risk management strategies that incorporate cybersecurity into broader business continuity planning, ensuring resilience across all facets.

LEVERAGING AI FOR PROACTIVE DEFENSE

Increased use of AI-driven analytics to anticipate and neutralize threats before they impact operations, enhancing overall security posture.

CULTIVATING A CULTURE OF DIGITAL RESILIENCE

Focus on building a resilient organizational culture where continuous learning and adaptation to cybersecurity challenges are prioritized.

PLAN AND BUILD YOUR FUTURE

BRIDGING SECURITY GAPS THROUGH INNOVATION

Utilizing advanced technologies and adaptive strategies to identify and close vulnerabilities, ensuring robust defense mechanisms.

TRANSFORMING CYBER POSTURE WITH AI INSIGHTS

Leveraging AI-driven analytics to refine defense strategies, enabling proactive protection against a spectrum of cyber challenges.

FOCUSING INVESTMENTS ON NEXT-GEN SOLUTIONS

Channeling resources into cutting-edge security solutions that address emerging threats and enhance organizational resilience.

ACHIEVING COMPLIANCE WITH DYNAMIC STANDARDS

Navigating evolving regulatory landscapes to ensure adherence and protect sensitive data amidst changing requirements.

Key Takeaways

SECURING SENSITIVE DATA IN THE FACE OF EMERGING THREATS

NAVIGATING DATA PRIVACY IN THE AGE OF AI

Implementing AI-enhanced surveillance to ensure compliance with data privacy regulations like GDPR and DPDP, effectively countering sophisticated threat actors and mitigating potential fines.

ENHANCED MONITORING AND INCIDENT RESPONSE

Implementing continuous system surveillance and rapid incident response capabilities to detect and address breaches, maintaining transparency and resilience against diverse cyber threats.

STABLISHING AGILE COMPLIANCE SYSTEMS

Developing dynamic policies and procedures that adapt to regulatory changes, supported by regular audits to counteract the tactics of professional hackers.

COUNTERING UNCONVENTIONAL THREAT ACTORS

Deploying strategic defenses to mitigate risks posed by non-professional hackers and script kiddies, ensuring robust protection of sensitive data in a complex threat landscape.

STRATEGIZING FOR RESILIENCE: FUTURE-PROOFING CYBER DEFENSES

ADAPTIVE THREAT DETECTION

Constantly evolving security measures to swiftly identify and neutralize new and sophisticated cyber threats.

DIGITAL INFRASTRUCTURE RESILIENCE

Ensuring the security and stability of the organization's digital ecosystem to preserve operational integrity and availability.

MULTI-LAYERED SECURITY APPROACH

Implementing a comprehensive strategy that integrates technology, processes, and personnel for robust protection across all fronts.

PROACTIVE VULNERABILITY MANAGEMENT

Regularly assessing and addressing potential weaknesses to prevent exploitation and maintain a strong security posture.

Cybersecurity & Data Privacy

INCREASING DIGITAL RESILIENCE, DELIVERING PRACTICAL COMPLIANCE AND PREVENTING BREACHES

Our cybersecurity and data privacy solutions **Protect, Create, and Recover Value** for our clients by defending them from breaches, building their internal capabilities and processes, and responding swiftly to threats or attacks.

Featured Services

Cyber Incident Response, Intelligence & Investigations |
Data Privacy & Cyber Risk Advisory
Managed Data Protection Services | Records and Information Management

Related Services

Data Strategy & Governance | Digital Forensics | Economic Sanctions
Insurance Claims Preparation & Recovery | Technology Advisory

10,000+

CYBER THREATS IDENTIFIED & NEUTRALIZED

5,000+

CYBER INCIDENT RESPONSE

250,000+

ENDPOINTS MONITORED REGULARLY

Ankura's Cyber Security & Data Privacy Capabilities

PROTECT: CYBER RISK ADVISORY
Leveraging our global footprint, we support our clients in addressing current and future risks as well as meeting long-term business goals. Our integrated cyber and privacy risk solutions are scalable, innovative, vendor-agnostic, and tailored to fit the needs and resources of all organisations.

- Cyber Risk Advisory
- Data Privacy Advisory
- Technical Solutions

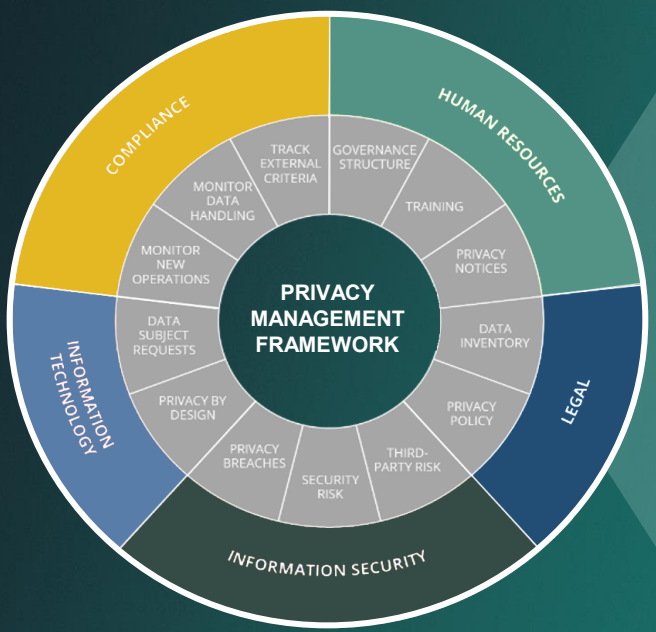
DETECT: MANAGED SERVICES
We help our clients optimise their resources and deliver the benefit of on-demand, 24/7 support from professionals experienced in a range of security domains. Our managed services are designed to become an extension of our clients' team and provide them with the right people and tools at the right time.

- Threat Detection & Response
- Third-Party Risk Management
- Security Analytics & Data Mining

RESPOND: CYBER INVESTIGATIVE SERVICES
Our solutions optimise organisations' actions and decision-making to best respond, mitigate, and recover more quickly. Whether it is a cyberattack, insider threat, or data breach, Ankura professionals have the in-depth experience to solve the most mission-critical and complex cyber challenges for our clients.

- Incident Response
- Investigations
- Threat Intelligence
- Expert Testimony

Privacy Advisory Services and Solutions



1. Conduct Assessment
2. Create Data Inventory
3. Develop Policies & Procedures
4. Operationalize
5. Prepare Readiness Report

Supporting Our Clients

Where industries, disciplines, technologies, and trends intersect and when transformational moments and events overlap – Ankura is there. Every solution, every service, every offering we provide is built to Protect, Create, and Recover Value for our clients.

TURNAROUND & RESTRUCTURING

Our accomplished team, with cross-industry financial and management expertise, adeptly guides organizations through distressed situations.

TRANSACTIONS

Partner with a consulting firm that offers unparalleled support across a variety of transaction types.

RISK & COMPLIANCE

A risk-tailored compliance and ethics program is essential to maintaining regulatory compliance, enforcing ethical standards, and increasing the value of the enterprise.

INVESTIGATIONS

The combination of global regulatory and corporate experience and U.S. federal agency qualifications gives Ankura a leading edge in successfully resolving complex financial, money laundering, bribery, and fraud investigations.

DISPUTES & EXPERT TESTIMONY

As disputes, business risks, and regulatory challenges continue to grow, Ankura provides the expertise to effectively make a winning case.

FINANCE & GOVERNANCE

Builds the organizational infrastructure to support your strategy and growth.

TECHNOLOGY

Cross-functional advice and efficient solutions to help you navigate an increasingly complex information environment.

STRATEGY & TRANSFORMATION

Transform your business with a seasoned team of professionals who translate strategy into results, accelerate business performance outcomes, and minimize risk.

Ankura is a global firm of experts and advisors uniquely built to tackle each challenge or need, by effectively combining the right expertise into solutions, services, and results.

We are a trusted advisor for companies, governments, law firms, and institutions around the world.

Contact Us

Ankura Consulting India Private Limited, part of Ankura Consulting Group, LLC is an independent global expert services and advisory firm that delivers services and end-to-end solutions to help clients at critical inflection points related to change, risk, disputes, finance, performance, distress, and transformation.

The Ankura team consists of more than 2,000 professionals in more than 35 offices globally who are leaders in their respective fields and areas of expertise. Collaborative lateral thinking, hard-earned experience, expertise, and multidisciplinary capabilities drive results, and Ankura is unrivaled in its ability to assist clients to Protect, Create, and Recover Value.

For more information, please visit www.ankura.com

AMIT JAJU
Senior Managing Director and India Head

Amit.Jaju@ankura.com
+91 9820073695
@amitjaju

LEXOLOGY INDEX
Thought Leader Investigations 2025 | Thought Leaders GIR 2024

LinkedIn TOP VOICES Technology & Innovation

LEARN MORE

AMOL PITALE
Managing Director

Amol.Pitale@ankura.com
+91 9833996432
@amolpitale