



A Research Study on

A STUDY ON CYBER RISK UNDERWRITING IN INDIA

– Implications for Insurance Industry

Foreward

It is with great pleasure that I present this insightful report on **Cyber Risk Underwriting in India**, a collaborative endeavour with Marsh India Insurance Brokers that underscores our commitment to advancing knowledge within the Indian insurance sector.

The study on Cyber Risk Underwriting in India is pivotal in the evolving world of cyber risks and the expanding insurance market. The objectives of this report align with the NIA's mission to enlighten and develop the insurance sector, providing real-world perspectives that enrich the understanding of both challenges and opportunities within the landscape of cyber risk insurance. As the digital ecosystem grows and cyber threats become more sophisticated, the need for comprehensive underwriting practices is highly imperative.

Moreover, the findings and conclusions drawn from this study provide certain vital strategic recommendations to key stakeholders, including regulators, policymakers, underwriters, industry professionals, customers, and academics. The study report is particularly valuable, as it delves into the critical areas where underwriting practices may fall short in addressing the full spectrum of cyber risk exposure. It offers an in-depth analysis of current trends, identifies gaps in coverage, and examines the dynamic interplay between insurers and policyholders. The report aims to provide actionable insights to strengthen cybersecurity resilience and informed policy decisions shaping India's cyber risk mitigation.

I extend my heartfelt gratitude to Mr. Sanjay Kedia, CEO, Marsh McLennan India, President & CEO, Marsh India Insurance Brokers Pvt. Ltd, and his team, for their invaluable support as the sponsor of this study. I extend my sincere appreciation to the dedicated project team—comprising Mr. Renjit Gangadharan, Dr. Steward Doss, Ms. Jayashree Sridhar, and Mr. Indraneel Roy—whose unwavering efforts have culminated in the comprehensive review and exploration of the cyber risk underwriting environment in the Indian market. I also acknowledge the significant contributions from experts across the insurance industry, academia, and cyber security professionals whose insights have enriched this work.

I encourage all stakeholders to engage with the contents of this report. I hope that the findings presented here will ignite crucial discussions and drive meaningful action within the insurance sector. Further, it helps organisations better manage their cyber security risks, ultimately fostering the growth and adaptability of the Indian insurance sector.

Kind Regards,



A handwritten signature in black ink, appearing to read 'B.C. Patnaik', written in a cursive style.

B.C. Patnaik
Director, National Insurance Academy

Acknowledgement

We are happy to present this insightful report on the **Cyber Risk Underwriting in India**, a collaborative effort that accentuates the commitment of the National Insurance Academy (NIA) to advancing knowledge landscape and curtailing gaps, within the Indian Insurance sector.

This study connotes the culmination of our comprehensive research on the Cyber Risk Underwriting in India, inclusive of the current underwriting practices and gaps in the cyber insurance coverages, and exclusions in the Indian market. First and foremost, we extend our sincere gratitude to Mr. B.C Patnaik, Director of NIA, for his active encouragement and support during the completion of the project.

We are extremely grateful to Mr. Sanjay Kedia, CEO, Marsh McLennan India, President & CEO, Marsh India Insurance Brokers Pvt. Ltd, and his team, who played a paramount role as the sponsor of this study, as well as for their constant encouragement and valuable inputs. Our sincere appreciation also goes to Mr. Renjit Gangadharan, our project leader, for his guidance and valuable insights which have led us to the successful completion of the project. We sincerely thank Dr. N Raveendran, Principal Consultant and Mr. B Suresh, Consultant, Xsentinel Risk and Claim Advisory Pvt Limited, for their technical advice and guidance throughout the study which has enriched the quality of the report.

We also express our esteemed gratitude to Mr. Anil Srivastava for his support and contributions during the colloquium. We are also grateful to the industry leaders, practitioners, subject experts and corporate customers who provided us with their valuable practical insights that helped to enrich the quality of the project. Furthermore, our gratitude is extended to various insurance companies, brokers and other collaborated organizations and individuals for their assistance in the compilation of significant responses and other relevant information. Heartfelt thanks to all the organizations and key managerial individuals who participated in our survey for their invaluable response and contributions.

Special thanks are extended to all the Senior Professors and Faculty colleagues for their valuable input, and to the administrative staff for their constant support. Lastly, we express our appreciation to Ms. Chaturthi Shetty and Mr. Aman Rehman K P as project assistants, who have helped us relentlessly throughout the project.

Project Team

- **Mr. Renjit Gangadharan**
- **Dr. Steward Doss**
- **Mrs. Jayashree Sridhar**
- **Mr. Indraneel Roy**



Index

Acknowledgement

Executive Summary **01**

1 Introduction **15**

2 Need and Importance of the Study **19**

3 Objective of the Study **23**

4 Methodology Adopted **24**

5 GAP Analysis of Cyber Insurance Products **27**

6 Analysis and Findings of the
Corporate Customers Perceptions
about Cyber Risks and Insurance **39**

7 Managerial Implications and Suggestions **87**

8 Conclusion of the Study **91**

The Project Team Members **93**



Executive Summary

Introduction

The emergence of cybersecurity as a critical global imperative is evidenced by its designation as the fifth most significant risk in the World Economic Forum's World Risks Report 2024. The accelerating digital transformation across sectors, combined with the proliferation of interconnected devices, has exponentially expanded the attack surface for cyber threats. Contemporary organizations, governmental institutions, and private entities face an increasingly sophisticated spectrum of cyber risks that compromise critical infrastructure integrity, data sovereignty, and operational resilience.

The trajectory of cybercrime demonstrated persistent escalation throughout 2024, resulting in unprecedented financial implications globally. Cybersecurity Ventures' analysis indicates that the global economic impact of cybercrime reached approximately \$9.5 trillion USD in 2024. Data breach incidents remained particularly concerning, with the average cost per breach escalating to \$4.88 million, representing a 10% year-over-year increase and establishing a historical peak. The financial sector exhibited vulnerability, accounting for approximately 20% of documented cyber incidents, with median direct losses approximating \$0.5 million, while the probability of catastrophic losses exceeding \$2.5 billion demonstrated significant elevation. Within this context, India experienced a marked intensification of cybercrime incidents, resulting in substantial financial repercussions. According to the Indian Cyber Crime Coordination Centre (I4C), reported losses surpassed ₹11,000 crore (approximately \$1.3 billion) during the initial three quarters of the year.



India's digital economy exhibits substantial growth potential, with projections indicating the deployment of over 50 billion connected devices and the integration of nearly 1 billion Internet users by 2025. While this digital transformation catalyses economic advancement, it simultaneously introduces unprecedented cybersecurity vulnerabilities. The proliferation of cyberattacks across diverse sectors underscores the systemic weaknesses within India's digital infrastructure. Notable examples include the education sector's experience of a 33% year-over-year increase in weekly cyberattacks during early 2024, while the healthcare industry confronted a 22% surge in ransomware incidents, compromising both patient confidentiality and service delivery protocols.

Despite these demonstrable threats, India's cyber insurance market remains embryonic. Insurance penetration remains suboptimal, particularly within the Small and Medium Enterprise (SME) sector, accompanied by limited awareness regarding the strategic value of cyber insurance as a risk management instrument. This research initiative examines critical dimensions including cyber risk perception paradigms, assessment methodologies, insurance product inadequacies, claims analysis frameworks, and mitigation strategies. The objective is to

While regulatory frameworks, including directives from the Reserve Bank of India (RBI), Insurance Regulatory and Development Authority of India (IRDAI), and Securities and Exchange Board of India (SEBI), have initiated organizational momentum toward enhanced cybersecurity measures and insurance adoption, significant implementation gaps persist.

enhance the sophistication of India's cyber insurance ecosystem through alignment with international best practices. Beyond mere problem identification, this investigation presents empirically grounded recommendations to address existing vulnerabilities, facilitating enhanced organizational preparedness and incident recovery capabilities. The findings provide a comprehensive analysis of the cyber threat landscape, enabling stakeholders to implement proactive risk management measures and develop sustained operational resilience against emerging challenges.

Cyber Threat Perception

The comprehension of cyber threat dynamics across industrial sectors represents a fundamental prerequisite for addressing systemic vulnerabilities. India's heterogeneous industrial landscape exhibits varying degrees of threat awareness, with BFSI and IT/ITES sectors demonstrating heightened vigilance due to persistent targeting, and stringent regulatory compliances, while sectors such as Manufacturing and Oil & Gas exhibit subdued risk recognition.



The proliferation of cyber-attacks across Indian industries is evidenced by CERT-In's documentation of over 1.5 million incidents in 2024. Critical sectors, including Education, Healthcare, and BFSI, have experienced significant impact. Notably, the education sector exposed to approximately 2,800 weekly cyber incidents in early 2024, representing a 33% year-over-year escalation. Concurrently, the healthcare sector confronted a 22% increase in ransomware attacks, compromising patient data confidentiality and operational continuity. These metrics underscore the substantial increase of cyber threats across sectoral boundaries, despite diminished threat perception among key organizational stakeholders.

This analysis further examines the evolutionary trajectory of cyber risks. Advanced Persistent Threats (APTs), state-sponsored cyber operations, and insider threats increasingly target organizational infrastructure, exploiting inadequate preparedness against these sophisticated attack vectors. Organizations frequently underestimate these threats, resulting in suboptimal defence mechanisms.



■ Key Observations:

- While BFSI, IT/ITES, and Healthcare sectors demonstrate elevated threat awareness due to recurring targeting patterns, the Manufacturing and Oil & Gas sectors exhibit diminished risk perception despite substantial exposure.
- The sophistication of Advanced Persistent Threats (APTs), state-sponsored cyber operations, and insider threats continues to evolve, yet remains inadequately represented in organizational risk assessments.
- Large enterprises demonstrate enhanced threat perception owing to extensive digital footprints and regulatory compliance requirements, particularly BFSI, IT/ITES, etc, whereas Small and Medium Enterprises (SMEs) frequently underestimate their risk exposure.
- Industrial sectors demonstrate significant disconnection from actual threat landscapes. Empirical evidence indicates 95.7% of BFSI entities experienced phishing attacks, while Healthcare witnessed a 22% increase in ransomware incidents. Manufacturing and IT/ITES sectors confronted a 66% escalation in ransomware and malware attacks.

■ Recommendations:

- Implementation of sector-specific workshops targeting under represented industries to bridge the perception-reality gap.
- Promotion of standardized risk perception frameworks customized for diverse organizational scales and industrial sectors.
- Development of comprehensive market awareness regarding evolving cyber threats, supported by adequate resources and information dissemination.

Cyber Risk Assessment

Cyber risk assessment plays a critical role in identifying and evaluating potential vulnerabilities within an organization's digital infrastructure, enabling informed decision-making for effective cyber underwriting and risk management strategies. The implementation of robust risk assessment methodologies constitutes the foundational element of comprehensive cybersecurity frameworks. The same assessments are also key notaries which are significantly employed in the process of underwriting. However, this investigation reveals significant heterogeneity across Indian industries. While certain sectors demonstrate excellence in periodic risk evaluations, many organizations exhibit deficiencies in critical components, particularly regarding vendor and third-party risk assessments.

The execution of cyber risk assessments demonstrates marked inconsistency across Indian industrial sectors. While BFSI and IT/ITES sectors maintain regular evaluation protocols, other sectors, notably manufacturing and services, exhibit substantial deficiencies. Furthermore, the integration of emergent technologies, including Artificial Intelligence and Internet of Things (IoT), introduces novel vulnerabilities that current assessment frameworks inadequately address. Despite the imperative nature of these assessment practices, numerous organizations demonstrate limited engagement with cyber auditing and pre-incident response protocols.

A significant finding indicates that third-party risk assessments, crucial for supply chain security integrity, frequently remain unaddressed.



Key Observations:

- While specific industries demonstrate excellence in cybersecurity assessments, MSMEs exhibit deficiencies in maintaining fundamental evaluation protocols.
- In the assessment ground, numerous methods are in consumption to assess and evaluate the intensity of the cyber risks. However, the comprehensive and effective use of these methods is still in question. Organizations constantly choose the most traditional and available method for assessment, completely neglecting the current growing landscape of cyber threats.
- Almost 26% of the total companies adopt the Vulnerability Scanning test, which is seen to be the main utilized method for assessing cyber risk, while Cloud Security testing and API Security testing only sum up to around 12%. The pioneering methods including, Web Security testing and Mobile Application Security are only employed by 14% and 6% respectively. This wide disparity and retrenchment clearly outlay the gap in the assessment tools.

- Advanced technological integration amplifies systemic vulnerabilities, emphasizing the necessity for comprehensive assessment methodologies.
-
- While breaking down industry-wise, most of the companies have only a moderate level of cyber threat assessment measures in position, which reveals that the organizations are inadequately equipped to counteract the existing cyber threats. Only about 46% of industries have comprehensive cyber security in place to assess and react. Among them, BFSI along with the IT/ITES sector, demonstrate relatively higher adoption rates, accounting for approximately 21% and 15%, respectively.
-
- Supply chain and third-party risk evaluation remain a significant oversight, with a limited assessment of external vulnerabilities. The utilization of these assessment variabilities has a strict correlation to the turnover of the organizations,
-
- The adoption of third-party risk assessment has yet to progress. Throughout the industry, cyber risk assessments are performed occasionally. Even among the most vulnerable sectors such as Healthcare, Telecommunications, and Power & Utilities, only 27% of all these organizations adopt third-party security assessments as part of their cyber security risk evaluation.
-
- Vendor reputation, a critical factor in cybersecurity and risk management, is inconsistently prioritized across industries, highlighting a lack of emphasis on its role in cyber risk assessment. Among all industries, only 22% engage top-tier vendors for cybersecurity solutions. Within this group, the Manufacturing sector lags, with only 9% relying on top-tier vendors for their cybersecurity needs. Although the BFSI sector demonstrates relatively higher adoption, only 4% of organizations overall engage top-tier vendors for cybersecurity equipment procurement in the process of countering and assessing cyber risk. However, these sectors have experienced a higher incidence of cyber threats or exposures in recent years.

■ Recommendations:

- Establishment of mandatory industry-wide cybersecurity assessment protocols ensuring standardized, comprehensive evaluations across all sectors.
-
- Implementation of regular third-party risk evaluations and audits to proactively address supply chain vulnerabilities and emerging threats.
-
- Integration of AI-driven predictive analytics for continuous, real-time threat monitoring, analysis, and response optimization.



- A periodical cyber security auditing of the entire cyber security system must be ensured and made into a mandatory activity, and one of a key eligibility under cyber underwriting.
- Institute a pre-incident report and a cyber forensic report into the cyber protocols, and the same should be mandatory for the cyber loss assessment procedures.

Cyber Insurance Gap Analysis

Cyber insurance functions as a critical financial risk mitigation instrument for organizations, ameliorating the economic impact of cyber incidents. However, this investigation identifies substantial gaps within India's cyber insurance ecosystem, necessitating an address to ensure comprehensive coverage aligned with international standards.

Additionally, the research highlights that a significant proportion of industrial entities remain uninsured against cyber-attacks, attributable to various factors ranging from threat perception to budgetary constraints.

The cyber insurance market in India remains in its nascent stage, exhibiting significant coverage disparities compared to international benchmarks. Contemporary policies address fundamental risks including ransomware and data breaches but demonstrate inadequate coverage for sophisticated threats such as APTs, cloud system failures, and insider activities. Moreover, coverage for human error and outsourced service provider failures exhibits significant variation across insurers, reflecting inadequate standardization.



■ Key Observations:

- Analysis reveals that most of the respondents find that the current insurance products do not sufficiently meet the growing risk requirements. Critical risk domains, including APTs, intellectual property theft, and social engineering risks, remain inadequately addressed.
- International insurers demonstrate comprehensive incident response and cyber security risk management services and supply chain risk coverage, while Indian insurers exhibit limitations in addressing emerging threats like APT and IoT etc.
- Enhanced regulatory oversight has driven increased insurance adoption in BFSI and Healthcare sectors, though remaining inadequate by SMEs. The current DPDP Act imposes non-compliance fines, which can reach up to 250 crores for significant data breaches. Furthermore, the Act is in its early stage and could witness further growth. Subsequently, this could enhance the overall demand for cyber insurance in the next 2 to 3 years.

- Limited comprehension of existing cyber insurance products represents a significant barrier to organizational adoption, with various entities demonstrating unawareness or unilateral hesitance to cyber insurance adoption. The demand for add-on/ specific coverages, and subsequent measures to meet the demand, could potentially address this gap.

■ Recommendations:

- | | |
|---|---|
| <ul style="list-style-type: none"> • Development of modular insurance frameworks enabling customization for sector-specific risk profiles. <hr/> <ul style="list-style-type: none"> • Implementation of comprehensive policies addressing advanced threats including APTs, insider risks, and cloud infrastructure failures. <hr/> <ul style="list-style-type: none"> • Establishment of strategic partnerships with global insurers to incorporate international best practices and expand product offerings. | <ul style="list-style-type: none"> • Institution of periodic policy updates to mitigate potential financial losses arising from evolving cyber risks. <hr/> <ul style="list-style-type: none"> • Creation of innovative insurance frameworks transcending standard coverage parameters to enhance market attractiveness and customer value proposition. |
|---|---|
-

Cyber Insurance Coverages

Cyber insurance is a critical instrument in mitigating financial and operational risks associated with cyber incidents. However, as cyber threats become increasingly sophisticated, insurers must continuously adapt their policies to ensure comprehensive and effective coverage. This study identifies significant discrepancies across insurers, underscoring the necessity for standardization and expansion to address emerging risks. While policies generally encompass ransomware, business interruption, and data breaches, they frequently lack provisions for advanced threats such as Advanced Persistent Threats (APTs), insider threats, and cloud system failures. Moreover, the inconsistent inclusion of human error—a primary vector for security breaches—exposes businesses to substantial financial liabilities. Additionally, insufficient coverage for supply chain vulnerabilities, third-party vendor failures, and regulatory non-compliance presents considerable challenges, particularly for industries handling sensitive data, such as healthcare, IT, and manufacturing.

A fundamental concern in cyber insurance underwriting is the determination of the sum insured, which often lacks alignment with actual risk exposures. Empirical evidence suggests that policy limits are frequently inadequate relative to incurred losses, exacerbating financial strain during claims settlements. The exclusion of state-sponsored cyberattacks, despite their increasing prevalence, further amplifies the coverage gap. Additionally, procedural inefficiencies in claims processing—



characterized by ambiguous policy language, stringent documentation requirements, and delayed settlements—diminish policyholder confidence and impede market adoption. To enhance policy efficacy, insurers must transition towards modular frameworks that enable industry-specific customization. Furthermore, integrating pre-breach mitigation strategies—such as cybersecurity audits, workforce

training, and proactive threat intelligence—can significantly fortify organizational resilience. By fostering regulatory alignment, refining claims protocols, and ensuring risk-appropriate coverage, the cyber insurance sector can evolve into an indispensable pillar of contemporary corporate risk management frameworks.

■ Key Observations:

- Even when the reality is that the cyber incidents have been increasing daily exponentially both in numbers and intensity of the attack, there indeed exists a trivial number of organizations without cyber insurance in existence. It is marked that over 76% of the total 674 surveyed companies do not indeed have comprehensive cyber insurance cover.
- Moreover, nearly 18% only have a cyber business interruption policy to mitigate to some extent. In reality, even this policy would not be enough to counteract potential losses from cyber incidents.
- However, out of the balance 80%, almost 42% has only a standalone cyber policy, which would not be entirely effective to mitigate the losses, if a cyber incident occurs.
- In the steadfast world of cyber threats, the current insurance policy has its drawbacks of being unable to cover each and every cyber threat and even the prominent cyber threats. For instance, almost 25% of responses seek to cover the operational shutdown under the insurance, which is yet to be included perfectly. Subsequently, a total of over 20% of the respondents seeks to cover Property damages, crypto jacking and IPR thefts/loss.
- The different indicators for the basis of sum insured are also an integral component of evaluating the current and future insurance products. A vast proportion of the respondents depends on the 3rd party risk and self-risk assessment as the indicators for the basis for sum insuring, rather than a wider understanding of the cyber threats. Thus, reassuring the cyber threat perception variation from the reality of the situation.



■ Key Challenges in Cyber Underwriting:

As the market for, both domestically and internationally, cyber insurance products are still in advancement, there exist consequent challenges in cyber underwriting. It is fundamental to address the obstacles both from the perspective of underwriters and consumers.

- The accessibility of only limited historical data hinders accuracy in pricing and proper risk assessment.
- Traditional statistical models (e.g., Log-normal and Gamma distributions) are seen to be unsuitable for advancing cyber risks; incorporation of extreme tail models is required.
- The leakage or exclusion of key underwriting information relating to supply chain security lapses, AI integration and data usage, IoT/Connected devices, etc) is often overlooked by the underwriters leading to increased cyber liability and severe financial challenges by the clients at the time of claims.
- The legal ambiguities and cross-border data laws have complicated breach assessments and claim settlements, for both the underwriters and consumers.



- The lack of industry-wide standardizations and clear definitions of cyber risk terminologies and data standards have been an integral reason for inefficient claim handling and settlements, which need to be addressed accurately.

■ Recommendations:

- Broaden coverage to include APTs, insider threats, and cloud system failures while integrating operational shutdown, property damage, cryptojacking, and intellectual property theft. Introduce modular policies tailored to industry-specific risks for comprehensive protection.
- Establish standardized benchmarks for sum insured calculations, aligning policy limits with actual cyber risk exposure. The shift from reliance on third-party assessments to holistic risk evaluations, incorporating real-time threat intelligence and data-driven risk modeling.

- Incorporate extreme tail statistical models to improve cyber risk pricing and move beyond traditional methods like Log-normal and Gamma distributions. Develop a centralized cyber risk data repository for better underwriting insights and market stability.
- Address inefficiencies by eliminating ambiguous policy language, reducing excessive documentation, and adopting faster settlement mechanisms. Standardize breach assessments and forensic investigations to improve claim evaluation accuracy and policyholder confidence.
- Integrate cybersecurity audits, penetration testing, and employee training as mandatory components of cyber insurance policies. Incentivize organizations to adopt proactive security measures through premium adjustments and insurer-supported cybersecurity programs.
- Establish clear regulatory guidelines for cross-border data breaches, align policies with evolving cybersecurity laws, and promote industry-wide standardization in underwriting, policy structures, and claims handling to enhance market trust and compliance.

Cyber Insurance: Loss and Claims Analysis

The evaluation of cyber insurance claims processing and settlement mechanisms represents a crucial metric for assessing policy effectiveness. This analytical section examines the operational challenges encountered by organizations during claims settlements, identifying critical gaps and opportunities for enhancement.

This investigation analysed loss and claims trends, revealing that data breaches, ransomware attacks, and business interruptions constitute predominant claim categories. However, persistent dissatisfaction with settlement processes emerges from policy limitations and documentation inadequacies. Insurance data analysis revealed significant sectoral variation in cyber incident impact, emphasizing the necessity for industry-specific policy frameworks. While larger organizations generally secure comprehensive coverage, smaller enterprises encounter challenges in obtaining adequate protection. Despite insurance coverage, numerous organizations continue to experience financial strain due to coverage limitations. Mid-sized enterprises demonstrate vulnerability, experiencing elevated losses due to restricted cybersecurity resources. The evolution of cyber threats necessitates tailored, scalable insurance solutions addressing diverse risk profiles and financial impacts.



Key Observations:

- While various organizations express satisfaction with settlement processes, this sentiment predominantly correlates with higher turnover entities, indicating suboptimal satisfaction among MSMEs.
- Multiple factors contribute to settlement process friction. Furthermore, partial loss coverage proves particularly problematic for organizations with long-term profitability objectives.
- The financial challenges associated with the claim settlement are a contributing factor to the friction of claim settlement. The majority of the respondents do experience severe financial challenges after claim settlement, indicating inadequate coverages and lack of customization.
- The absence of standardized documentation frameworks frequently results in claim rejections or reduced compensation. Industrial diversity in organizational scale creates knowledge gaps in maintaining adequate claim documentation.
- Substantial residual costs post-claim settlement indicate structural policy inadequacies, representing a primary deterrent for uninsured organizations. The turnover disparity across industries creates unsustainable premium structures, particularly for MSMEs.
- More than 50% of the cyber loss, among the respondents, was in the nature of a data breach. This can be marked as an indication of a larger number of cyber threats in the form of data breaches.

Recommendations:

- Enhancement of claim models to accurately reflect and compensate actual losses, incorporating industry-specific turnover metrics for optimized settlement processes.
- Implementation of comprehensive documentation guidelines and information dissemination protocols to minimize settlement conflicts and enhance customer service quality, thereby incentivizing cyber insurance adoption.
- Introduction of pre-breach risk mitigation services addressing the evolving threat landscape and reducing claim frequency.



Cyber Risk Mitigation and Awareness

The analysis of cyber security risk mitigation examines proactive measures adopted across industries. This section evaluates the alignment between specific mitigation strategies and perceived risk levels, demonstrating organizational approaches to threat prevention. These insights prove fundamental in understanding preventative

methodologies that reduce the incident probability, directly informing the structure and requirements of effective cyber insurance frameworks. Mitigation protocols and awareness initiatives constitute critical elements in enhancing organizational resilience, although significant challenges persist in training implementation and proactive strategy adoption.

Analysis reveals a direct correlation between organizational scale and cybersecurity investment, with larger enterprises demonstrating enhanced awareness and effectiveness through superior resource allocation. Smaller entities frequently encounter challenges in accessing expertise and threat intelligence, increasing their vulnerability.

Industry preparedness exhibits significant variation, with sectors such as Oil & Gas demonstrating vulnerability due to legacy infrastructure constraints. While vulnerability scanning demonstrates widespread adoption, reliance on fundamental assessment protocols indicates potential deficiencies in comprehensive security testing. These patterns emphasize the necessity for balanced, scalable approaches to cybersecurity enhancement across diverse organizational scales and sectors.



Key Observations:

- Despite employee error/ inappropriate response behaviours/ break of standard security protocols, representing a primary breach vector, training initiatives remain inadequately implemented. Organizational capacity development and workforce cybersecurity capability enhancement have not achieved optimal prioritization.
- Organizations demonstrate a predominant focus on reactive methodologies, such as data recovery, rather than preventative security strategy investment. Limited awareness of evolving cyber risks has resulted in inadequate adoption of innovative mitigation measures.
- Most of the companies including MSME only have a low to medium level of cyber security awareness. The level of this awareness has been increasing as the turnover increases, although even large turnover companies are equipped with a medium level of awareness of cyber security.

- The IT/ITES and Manufacturing has a comparatively higher level of cyber security awareness although at a moderate level. It is followed by other industries including BFSI, Healthcare, Power & Utilities, etc with a similar moderate level of cyber security awareness.

- Across all industries, only 25% have implemented a highly effective cyber risk mitigation system. Among them, the BFSI and IT/ITES sectors exhibit relatively higher adoption rates, accounting for approximately 5% and 4%, respectively. Additionally, 36% of organizations maintain only a moderately effective cyber risk mitigation framework. Within this category, the BFSI and IT/ITES sectors lead with 13% each, followed by the Pharmaceuticals and Healthcare sectors, each at 12%.

- In examination, evidently there is much room for growth for the data storage and protection methods of organization in lieu. While 42% utilize Data Backup and Recovery, and network security upgrades which are standard /traditional security measures adopted, while only 14% apply Data Encryption and 9% employ Intrusion Detection systems.

- Budgetary limitations significantly impact developing and small enterprises' ability to implement proactive mitigation measures and maintain threat awareness.

Recommendations:

- Implementation of comprehensive, mandatory cybersecurity training programs across industrial sectors to mitigate potential threats and financial losses.
- Establishment of accessible awareness resources and mitigation tools for resource-constrained sectors.
- Facilitation of inter-industry collaboration for shared threat intelligence and defence strategy development.
- Deployment of non-traditional testing methodologies like APT testing, Auto Intrusion Detection System, web server security upgradation and application testing, both independently and in conjunction with established conventional techniques.
- Systematic and timely updates, alongside specialized technical seminars, webinars, cyber intelligence reports, etc., to improve technical knowledge and capabilities of cyber security personnel including users and service providers/vendors on the evolving landscape of cybersecurity threats, with a focus on continuously enhancing security protocols and procedures across the entire network to address both the rapid advancements and emerging complexities in this domain.



Conclusion

This research underscores the critical imperative to address escalating cybersecurity challenges threatening India's digital economic transformation. The increasing sophistication and frequency of cyber threats necessitate collaborative engagement among industries, policymakers, and insurers to develop robust defence mechanisms and comprehensive risk management frameworks. The findings reveal significant disparities between perceived and actual risks across sectors, particularly among SMEs and industries with limited regulatory exposure, creating substantial unaddressed vulnerabilities.

Cyber insurance emerges as a fundamental risk mitigation instrument, yet the Indian market demonstrates significant underdevelopment, with existing policies inadequately addressing advanced and emerging threats including APTs, insider risks, and cloud infrastructure failures. The disparity between Indian and global insurance providers emphasizes the necessity for standardization, modular policy frameworks, and expanded coverage tailored to sector-specific risk profiles. Furthermore, inefficiencies in claims processing, combined with inadequate pre-breach and documentation protocols, exacerbate challenges faced by insured entities, limiting current offering effectiveness.

The insights derived from expert consultations emphasize the value of integrating advanced technologies, particularly AI-driven threat monitoring, in both cyber defence and underwriting practices. These discussions highlight the necessity for dynamic pricing models and modular policy structures aligned with evolving threats and organizational requirements. As digital dependency increases, the significance of proactive risk assessment, third-party evaluation, and employee training becomes increasingly critical.

Ensuring the resilience of India's digital economy amid escalating cyber risks requires a coordinated effort. Insurers must innovate to provide comprehensive, standardized solutions while organizations prioritize awareness and cybersecurity investment. By addressing identified gaps and fostering a resilience culture, India can establish global benchmarks for cyber risk management in emerging economies.



1 Introduction

Cyber Crime and Security Risks have been rated as the 5th top risks by the World Economic Forum, in World Risks Report 2024.



Every Economic and commercial operation in the world has become increasingly reliant on digital technologies, which face a constant threat of disruption or halt because of human error or malicious attacks. Digital adoption is currently being accelerated in all areas of life, health, social media, banking, insurance, manufacturing, and services, and they have become inevitable and highly interdependent. A vast amount of mobile data (79 zettabytes) has been used by nearly

80% of the population in the country today. Over 100 billion networked devices, including Internet of Things (IoT) devices, Mobile Apps, GPS, Radar sensors, connected devices, Cloud, WiFi Routers, etc., are connected to the systems and mobiles, making it highly vulnerable for cyber-attack. India is projected to have over 100 crore Internet users by 2025. Currently, nearly 80% of customers have increased their usage of payments through UPI, G pay, Pay TM, etc. With the increased usage of data and interconnectivity of systems, the cyber vulnerability of organizations increases exponentially. A recent study by KPMG indicates that over 72% of organizations, including service industries, are being hacked or vulnerable to cyber risk. Increasing globalization. As a result, it has become imperative for every organization, including SME Sectors, to be adequately protected from cyber risks.

However, a lack of adequate awareness and sensitivity among the key management personnel (CEO, CFO, CIO, PTO, CRO, etc.) results in cyber insurance still not being perceived as essential. The Indian Cyber Insurance Market is yet to mature, and cyber insurance policy proliferation is very low. However, due to the strict cyber security compliances by various Regulators like RBI, IRDAI, and SEBI, the companies are now increasingly focusing on their Cyber risks more seriously. But, it has not yet led to the development of a mature cyber insurance market. Further, the Digital Personal Data Protection (DPDP) Act 2023 is expected to increase the demand for adequate cyber insurance protection in the Indian Market.

In 2024, India experienced a wave of escalating cyberattacks across multiple sectors, exposing critical vulnerabilities in infrastructure and sensitive data systems. In July 2024, C-Edge Technologies was the target of a ransomware attack, one of the most disruptive attacks to hit the financial services sector.

C-Edge, a service provider for approximately 300 small cooperative and regional banks, experienced a temporary shutdown of banking operations, crippling essential payment systems until cybersecurity protocols were fortified, and services resumed. Government, defense agencies, the educational sector, technological sector all emerged as the primary target, with more than 388 breaches reported in just the first half of 2024. Many of these breaches were orchestrated through messaging platforms like Telegram, where hackers traded sensitive government data and organized attacks, creating serious security risks by exposing critical defense and administrative information. The aviation industry felt the impact as well—in September, two India SATS employees accessed and altered Qantas customer bookings to siphon off frequent flyer points, affecting nearly 1,000 customers. After multiple complaints from customers, authorities launched a formal investigation into the breach.

The education sector emerged as one of the most targeted, recording an average of 2,807 cyberattacks per week in Q1 2024, marking a 33% year-on-year

increase. Educational institutions now face constant security threats, underscoring an urgent need for enhanced digital safeguards. The healthcare industry similarly grappled with a 22% surge in ransomware attacks, where hospitals and medical institutions became prime targets for data breaches, leading to potential service interruptions and compromised patient information. In the technology sector, Hathway, a prominent Indian Internet Service Provider, reported a breach exposing the personal information of over 41.5 million customers, including names, emails, phone numbers, and addresses, following a vulnerability in their content management system. This breach represents one of the largest recent incidents in terms of affected individuals. Additionally, India's defense sector encountered targeted espionage attacks from groups like Transparent Tribe (APT36), which focused on extracting confidential information and undermining national defense security. This surge in incidents emphasizes an urgent need for bolstered cybersecurity measures across all sectors in India to mitigate & counteract these increasing cyber threats.

Cyber insurance, also known as cyber risk insurance or cyber liability insurance, is a specialized insurance product designed to protect businesses and individuals from the financial and other potential consequences of cyberattacks, data breaches, and other digital threats.



In an increasingly digital world, where businesses and individuals rely heavily on technology and data, the risk of cyber incidents has surged, leading to financial, reputational, and operational losses. Cyber insurance provides a financial safety net by covering expenses related to data recovery, legal fees, and crisis management, which can result from incidents like ransomware attacks, hacking, accidental data exposure, and much more. The concept of cyber insurance emerged in the late 1990s and early 2000s

as organizations began to recognize the potential impacts of web-based risks. Initially, coverage was limited, and policies were difficult to underwrite due to a lack of historical data on cyber risks and threats. However, with the exponential rise in cyber incidents, particularly over the last decade, the insurance industry has adapted, developing more comprehensive products to meet the needs of the digital age. The past few years have seen unprecedented growth in cyber insurance policies, driven by the surge in high-profile cyberattacks, regulatory changes, and a growing awareness of cybersecurity risks among organizations of all sizes.



The global cyber insurance market is experiencing rapid growth as organizations increasingly recognize the need to mitigate the financial impact of cyber incidents. In 2023, the global cyber insurance market was valued at approximately USD 13 billion and is projected to grow at a compound annual growth rate (CAGR) of over 25%, potentially reaching USD 84 billion by 2030. This growth is driven by the sharp increase in cyberattacks, including ransomware and data breaches, which have seen a staggering rise over the past decade.

According to a report by Allianz, cyber incidents now rank as the top risk for businesses worldwide, above natural disasters and regulatory changes, highlighting a global shift towards prioritizing cyber security and risk transfer solutions. Increased regulatory requirements, such as the GDPR in Europe and various data protection laws globally, are also driving demand for cyber insurance as companies face penalties for data breaches and non-compliance. Sectors like healthcare, finance, and retail, which handle sensitive customer information, are leading adopters of cyber insurance, with underwriters developing tailored solutions to address the unique risks in these industries. As organizations bolster their cybersecurity defenses,

cyber insurance is becoming an essential component of their risk management strategies, offering both financial security & support for crisis response, thus positioning the global market for sustained growth.

Similarly, the need for cyber insurance in India also has intensified as the country ranks among the top five nations facing cyberattacks, with nearly 1.4 million incidents recorded in 2022 alone, according to the Indian Computer Emergency Response Team (CERT-In). Businesses across sectors, including finance, healthcare, and government, are increasingly vulnerable to cyber threats such as large-scale data breaches and ransomware attacks, underscoring the urgency for robust cyber risk

management. Despite the growing demand for cyber insurance, its penetration remains low, primarily due to limited awareness, the evolving nature of cyber threats, the complexity of risk assessment, and the lack of standardized data on cyber incidents. This is further compounded by India's dynamic regulatory environment and varying levels of cybersecurity maturity across industries.



However, with India's digital economy expanding rapidly, sectors like banking, healthcare, and e-commerce are emerging as early adopters, recognizing the need for comprehensive coverage. A report by the Data Security Council of India (DSCI) notes that the Indian cyber insurance market is growing at a CAGR of around 30%, with the potential to reach USD 100 million by 2027. Furthermore, the Reserve Bank of India (RBI) has issued guidelines urging financial institutions to bolster their cybersecurity frameworks, indirectly boosting the demand for cyber insurance as banks and non-banking financial companies (NBFCs) seek to mitigate liabilities. As insurers invest in advanced risk assessment tools, collaborate with cybersecurity experts, and leverage data analytics to refine underwriting processes, cyber insurance is becoming an inevitable instrument for mitigating financial losses, safeguarding reputations, and building resilience against the evolving cyber threat landscape. The growing market for cyber insurance reflects its immense potential to protect Indian businesses in an increasingly digital world.



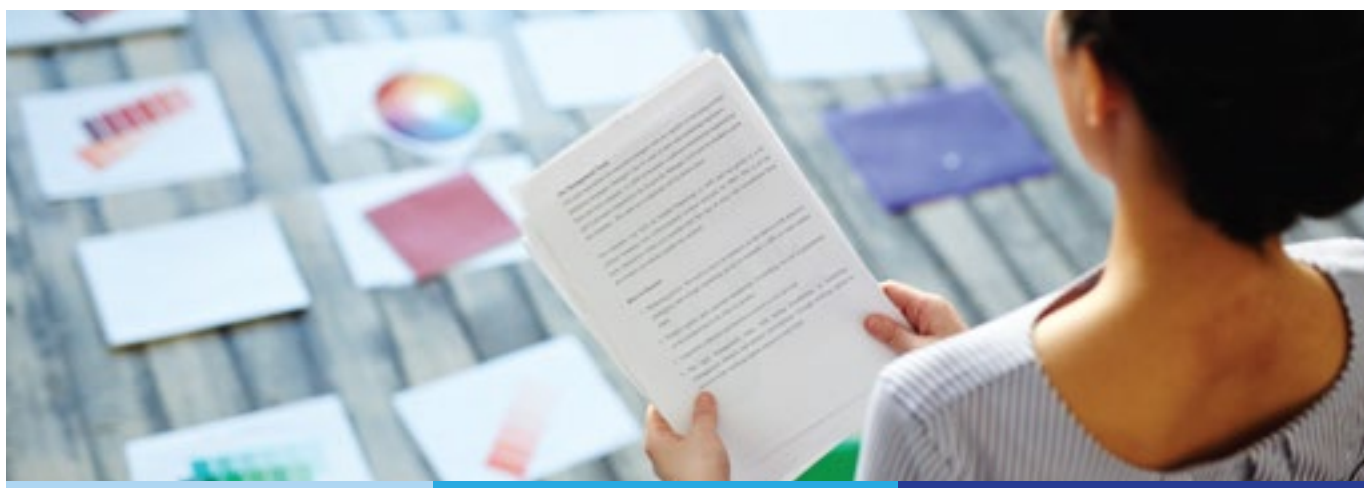
Need and Importance of the Study

2 Need and Importance of the Study

Our preliminary Study of cyber policies available in India indicates that wider perceived gaps exist among Cyber Underwriters. For those companies that purchase Cyber Insurance, coverage limits are usually much lower than what is available for other perils and provided at a much higher premium level. In addition, some of the most critical needs of companies, such as coverage for losses related to property damage, bodily injury or or intellectual property theft, are rarely covered by cyber insurance products.

Overcoming the significant obstacles to developing the cyber insurance market could lead to greater and wider coverage of cyber risk and have a larger impact on risk management. The lack of historical data on cyber incidents also the relevance of the data due to the ever-evolving nature of the risk impede the ability to develop probabilistic pricing and exposure management models. The lack of trusted models reduces the willingness of insurance companies (and reinsurers) to extend significant amounts of coverage. It leads them to apply various exclusions and sub-limits to control their exposure. The limited coverage available in the market and the complexity of the imposed terms and conditions have led policyholders to question the value of cyber insurance coverage in its current form for their business, especially for SMEs.

Some of these challenges and critical issues affecting Cyber Risk Underwriting in the Indian market are discussed in the following section.



Quantification of exposure

The underwriters rely on quantitative data to arrive at exposure values. That presupposes the availability of sufficient data to reduce error margins significantly enough for them to price the risk appropriately. There is only a limited loss history available for the insurers to use when setting the prices for cyber insurance premiums and coverage loss limits.



Rating dilemma – Distribution confusion

Cyber Risk does not fall under the traditional statistical distribution the insurance industry uses, i.e., Poisson or log-normal distribution. The Cyber Risk has more fit with beta or extreme tail distributions, and the Insurance Rating has still not started using these extreme tail distributions for their rating. This leads to misfits, especially in predicting tail losses. This also creates a problem in arriving at a burn layer which is extremely important for acceptance and the rating of a proposal.



Assessment protocol

Underwriters assess the proposals based on the information provided by the organizations that are seeking cover. However, a cursory look at the Proposal Forms reveals much relevant information not captured to rate the risk appropriately. There are four broad areas in which the underwriter needs in-depth information for assessment.



Information regarding social engineering risks

The attackers use highly sophisticated tools like AI&DL to troll the information posted on Social Media. Even Social Media sites provide information for advertisements. These tools can refine that information to create messages specifically targeted to a person or organization, resulting in various loss scenarios, including ransomware. Hence, the underwriter should have clear information about the proposer on the Social Media Threat profile, the kind of resource deployed for monitoring such threat, the quality of the tools used and the frequency with which it is tested for robustness and updated, and whether the organization has clear social media policy for both organization and employees for the use of the social media and how effective is the implementation., etc.



Supply Chain risks

Organizations have started implementing seamless connections with vendors for efficiency and cost management, which poses another threat to them. While organizations have some control over the vulnerability of their systems, often, they have very little information regarding the exposure of the systems used by their vendors. Many attacks have been mounted using the supply chain systems resulting in huge losses. The underwriting information regarding the supply-chain system vulnerability and user awareness need to be captured for proper risk assessment. They include the sensitivity of the information shared by the vendors and the "points of handshakes" of both systems, the mechanisms by which such vendors' risks are assessed, and the appropriate tools and services to control such risks effectively.



IoT and Infrastructure Risks

There is a proliferation of cheap and unsecured devices connected to central systems that create vulnerabilities. It is proven that self-replicating malware can be sent through such devices and is a common way for ransomware demands. The underwriting information should capture the impact of any such IoT device on the risk, the resources used by the organization to manage those threats, and the recovery protocols that could help control the breaches.



Assessing aggregation of exposures

As in biological virus attacks like COVID-19, we are witnessing scalable cyber-attacks as they can infect thousands of systems concurrently. This poses the problem of aggregation of losses for the insurers. The present Asset Liability Management (ALM) system does not possess a valid tool to estimate these aggregations, and, therefore, it will always be challenging to calculate the Solvency Margin based on Estimated Claims.



The Issue of Law and Enforcement

Data Protection Law, similar to GDPR, is being passed through the legislative councils. The current Information Act is found to have a lot of issues in bringing the wrongdoer to book, not to mention the cross-border legal issues. This challenges the underwriter to estimate the Burning Cost Layer on Legal and Defense Costs. Moreover, the policy interpretation also has legal ambiguities as very few cyber cases have been contested in the court till now. While this may be a welcome relief to the insurers, the credibility of the policy is yet to be established.



Breach assessment

As a technical subject operating in real-time, assessing the breach is very difficult. Sometimes the breach is noticed after a long time, and the perpetrator has erased the trace by then. Moreover, most organizations keep their log for a limited period, and the intimation of claims could be made on a date when the log is lost. Such issues pose problems for the assessment of claims.



Documentary nightmare

Unlike other traditional insurances, the documentation process for Cyber Claim Assessments is yet to be clearly laid down. The companies have a board guideline manual but rely primarily on outside experts to provide evidence. There is neither regulatory oversight nor an industry understanding of the documentary requirements. Every claim is dealt with on a case-to-case basis.



Loss estimation

Again, due to the above mentioned factors, the estimation of loss cannot be precise. For example, Business Interruption due to a cyber-attack can be tricky to estimate, and no set procedure exists to assess such losses. This poses Rating issues and can also lead to disputes with the insured.



Resource Expertise

The industry currently relies on outside resources to handle Claims, and those who are technically qualified and able to handle these claims are very expensive. The forensic costs are part of the policy expenses, which are to be adequately factored in while estimating loss and provisioning. However, adding these forensic investigation costs would increase the Premium Rate significantly. However, an optional or add-on cover covering forensic expenses can be explored.

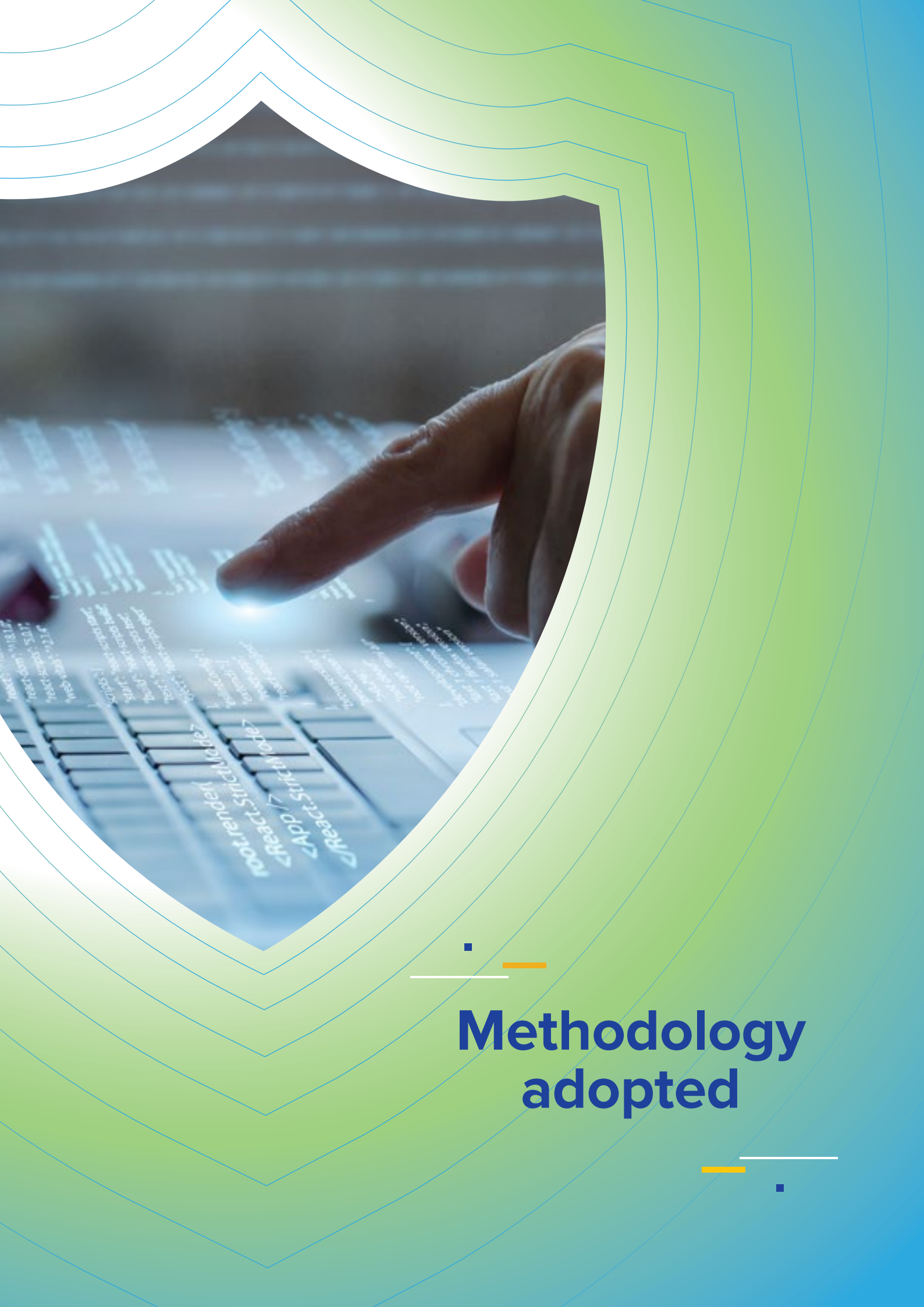
Analyses of these challenges and the product comparison helped us to realize the importance of studying the perceived gaps in cyber insurance products and understand the challenges in cyber risk underwriting in India. Realizing the importance of the subject, the following objectives have been framed for the study.

3. Objectives of the Study

The above challenges and critical issues in Cyber Underwriting motivated us to take up this project to study the following objectives.



- To study the existing Cyber Insurance products available in Indian Market and compare them with those available in the international market, identify the gaps in the product coverages, terms & conditions, exclusions, etc.
- To gauge the perceptions of Corporate customers across different industries or sectors, study their perceived differences and challenges with references to cyber insurance Underwriting.
- To do a Gap Analysis of the Customers' perceptions of Cyber Risk insurance in the Indian Market.
- To offer suggestions and critical recommendations to improve the Cyber Underwriting Standards and enable the development of customized cyber insurance products across different industries / sectors.



■ — ■

**Methodology
adopted**

— ■

4 Methodology adopted

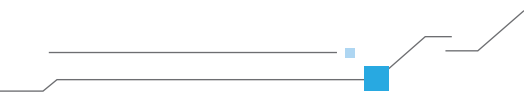
The main objective of this study is to examine some of these underwriting challenges and offer suitable suggestions to improve the underwriting standard of Cyber Insurance and design customized coverages and appropriate rating methodologies for the insurers to adopt. The following para describes the proper methodology adopted for the Study.

As Cyber Risk continues to evolve at a significantly higher speed and become more complex with the availability of little historical data, an attempt has been made to perform a Gap Analysis of Cyber Insurance Coverage available in the Indian Market as against global market differences using the necessary secondary data and the perceived risk responses from the sample of international cyber underwriters and cyber security experts.



Initially, a Delphi method was used with a panel of 30 cyber experts to identify the cyber risk protection and coverage gaps across different organizations. This also further helped us to identify the vulnerabilities and cyber security levels adopted by the corporate clients. Then, the Underwriter's Perception Questionnaire was developed to operationalize the cyber insurance protection and coverage gap. A Risk perception survey incorporating the above-discussed challenges and operational issues was conducted among the system managers,

underwriters/operational heads, Intermediaries, and cyber security auditors. The survey covered around 40 underwriters & Intermediaries and 650 corporate customers across different industries (Energy, including the Power sector, Manufacturing, Service, and Financial Institutions. Thus, the Study covered about 700 sample sizes of respondents selected from the above-mentioned industries. The collected data were analyzed in the following 5 sections of Cyber Underwriting aspects:



1

Gap Analysis of Cyber Insurance Products Available in India and Overseas Markets.

2

Demographic Analysis of the profile of companies selected for the study.

3

Cyber Security Measures and Risk Assessments across different industries / sectors.

4

Cyber Insurance coverages and products terms & conditions and exclusions.

5

Cyber Threat Probability Analysis and Cyber Losses and Claims Analysis.

6

Cyber Risk Mitigation measures and Suggestions to improve cyber risk underwriting.

5 GAP Analysis of Cyber Insurance Products

In order to understand the differences in coverages, types of risks covered, risk limits, and exclusions, among the insurance companies, a critical comparison of their cyber insurance products was carried out. The findings that emerged from the comparison are summarized accordingly.

Table 1 Exhibiting Key Definitions of Cyber Insurance Policies

S.No	Cyber Insurance Terminologies	Market Practices/ Perceived Gaps	Defined under the Cyber Insurance Policy
1	Definition of 'Insured'	The insured person definition is narrow in scope	Broad definition and includes any estates or legal representatives of any Insured
2	Definition of 'Subsidiary'	The subsidiary definition includes the criteria if the policyholder holds more than 50% of issued share capital	Whereas the condition under this policy is more than 50% of either issued share capital or equity capital as well
3	Definition of 'Personal Information' and 'Corporate Information'	The definition of Records is quite narrow in nature and restricts it to a specific list defined under the policy	'Personal Information' and 'Corporate Information' are broadly defined under the policy
4	Data Liability Coverage	Disclosure liability has a restrictive condition that a cyber attack unauthorized access or exceeded authorized access should have impacted the system or system output owned by an organization	Data Liability under the policy offers a very wide coverage in itself and provides covers for claims by third parties/data breaches for which Insured is responsible/liable
5	Cover for Outsourcing Agency	There is no cover for claims by third parties against outsourcing agents/vendors that arise from any actual or alleged breach of duty by the Outsourcer in regard to the processing of Personal Information and/or Corporate Information on behalf of the Company	The policy has a separate section under the Data Liability section which offers cover for a Claim by a Third Party against an Outsourcer (where the Company has a contractual duty to indemnify) and which arises from any actual or alleged breach of duty by the Outsourcer in regards to the processing of Personal Information and/or Corporate Information on behalf of the Company (for which the Company is liable)
6	Network Security	Limited cover is offered under Impaired Access Liability and that too again with a tied-in condition of Fraudulent Access or Transmission	The Network Security section offers very extended and robust coverage including impaired access liability and fraudulent access or transmission
7	Corporate Information	Content Liability is not broad enough to address all aspects of Corporate Data Liability	Coverage under this section is broad enough to address all matters relating to loss of corporate information. However, it does not cover Intellectual Property and or personal information

8	Administrative Obligations	The investigation is tied to the wrongful act	It should not be tied to the wrongful act
9.	PR Trigger	Restricted for listed events	Whereas the policy is extended for any newsworthy event
10.	Notification to Data Subjects and Monitoring	Privacy Notification Expenses are allowed for defined events	Whereas this policy offers both privacy notification cost, incidence risk monitoring & management, and crisis management
11.	Multimedia Liability	Offered under Content liability , however restrictive in nature	A very exhaustive optional extension is provided to cover multimedia liability
12.	Bodily Injury and Property Damage Exclusion	No carve back under property damage exclusion	There is a carve back for Third Party Data , or loss of use thereof, or the physical theft or loss of the Company's Assets under the property damage part
13.	Consequential Loss Exclusion	Yes	Yes, Business interruption and consequential losses are covered under an add-on cover.
14.	Intellectual property Exclusion	Absolute Exclusion	Carve back is there for loss of corporate information
15.	Vendor Exclusion	Exclusion under 1. F Cyber Liability covers Content Liability or Reputational Liability sustained by any person that: (i) creates, designs, develops, or provides any content, material, or services for any Insured ; or (ii) is an assign or heir of any person described in (i) above, provided that this exclusion applies regardless of whether such content, material, or service was jointly created, designed, developed, or provided by any Insured	No such exclusion

The above comparison analysis indicates that largely the above coverages are available under the existing cyber policies sold in the Indian market. Most of these coverages are similar across the leading insurance companies. However, some of these risks like Social Media risks, Loss of IPR, Consequential Loss, Data breach, or cyber risks comprises occur at third-party agencies or vendor companies are not covered under the standard cyber insurance policies. However, some of these risks are covered under the add-on or extended coverages under the cyber policies by the leading insurance companies in the Indian Market.

Figure 5.1 Specific Coverage and Policy Differences across different companies in India:

Table 2 Cyber Threat Coverage of Insurance Companies:

Risk Coverage (Cyber Threats)	Company V	Company W	Company X	Company Y	Company Z
Data Breach	✓	✓	✓	✓	✓
Cyber Extortion/Ransomware	✓	✓	✓	✓	✓
Business Interruption	✓	✓	✓	✓	✓
Network Security Failure	✓	✓	✓	✓	✓
E-Theft (Electronic Theft)	✓	✓	✓	✓	✓
Human Error (Leading to Security Breach)	✗	✓	✓	✓	✗
Reputation Damage/Public Relations Costs	✓	✓	✓	✓	✓
Regulatory Fines & Penalties	✓	✓	✓	✓	✓
PCI Non-Compliance	✓	✓	✗	✓	✗
Outsourced Service Provider Failure	✓	✗	✓	✓	✓
Multimedia Liability (e.g. Defamation)	✓	✓	✓	✓	✓
Cyber Attack (General)	✓	✓	✓	✓	✓
Cloud System Failures	✗	✗	✓	✓	✓
Physical Theft of Digital Assets	✗	✗	✓	✓	✓
Phishing/Social Engineering Attacks	✓	✓	✓	✓	✓
Denial of Service (DDoS) Attacks	✓	✓	✓	✓	✓
Advanced Persistent Threats (APTs)	✗	✗	✗	✗	✗

Keys: ✓ Covered by the insurance policy ✗ Gap present in coverage (Not explicitly covered or not mentioned by the policy)

While analyzing the coverages under cyber insurance products of major Indian insurers (Company V, Company W, Company X, Company Y, and Company Z), the following insights into current trends, coverages, and market directions can be derived. These findings are critical to understanding cyber insurance options available to businesses, the evolving threats addressed, and gaps that may affect consumer decision-making.

Key Observations and Insights:

- All insurers consistently cover critical cyber risks, including data breaches, ransomware, business interruption, network security failures, e-theft, reputational damage, regulatory fines, multimedia liability, phishing, and DDoS attacks, signaling industry alignment on protecting against fundamental cyber threats essential for business continuity.
- Coverage for human error and outsourced service provider failures varies; Company V and Company Z exclude human error, while Company W lacks outsourced provider coverage. This selective approach indicates an insurer's emphasis on direct over third-party risks, potentially leaving gaps in coverage for threats stemming from external entities and human factors.
- None of the insurers cover Advanced Persistent Threats, reflecting a reluctance to underwrite complex, resource-intensive threats. This omission suggests insurers are cautious about including high-cost, unpredictable threats, indicating a gap for policyholders facing sophisticated, evolving cyber-attacks.
- Insurers differ in covering cloud system failures and physical theft of digital assets, with Company V and Company W not covering these areas, unlike Company X, Company Y, and Company Z. This inconsistency highlights that cloud-reliant businesses must carefully select policies to ensure adequate protection, as insurers assess cloud risks differently.
- PCI non-compliance is not universally covered, with Company X and Company Z excluding it, affecting businesses in payment-heavy sectors. The selective approach to PCI and regulatory compliance underscores the need for policyholders to align coverage with specific industry requirements, as insurers may limit coverage based on sector-related risk exposure.

The data highlights that insurers are increasingly recognizing the significance of comprehensive cyber coverage for critical incidents such as ransomware, network failures, and data breaches. However, as insurers exhibit selective coverage in areas such as Human Error and Outsourced Service Provider Failure, Supply chain risks, Data breaches in vendor's system, Social media engineering, Business interruption & consequential losses, and Cloud data breach, etc., which signals a cautious approach to underwriting cyber risks involving indirect or complex dependencies.

Additionally, the complete lack of APT coverage across the board underscores a potential challenge for policyholders facing advanced, evolving cyber threats, potentially leading to demand for custom policies or endorsements in future offerings.

The observed variability, particularly in areas like Cloud System Failures and PCI Non-Compliance, Property Damage & bodily injury, cyber crimes, etc., suggests that cyber insurance products are still evolving. This evolution reflects insurers' responses to different types of consumer demands, sector-specific requirements, and risk exposures, which may further drive market expansion as insurers seek to address these gaps.



Figure 5.2 Cyber Threat Gap in Coverage of Insurance Companies in India:

Table 3 Cyber Threat Gap of Insurance Companies:

Gaps in Coverage	Company V	Company W	Company X	Company Y	Company Z
Advanced Persistent Threats (APTs)	✗	✗	✗	✗	✗
Insider Threats (Malicious Employee Actions)	✗	✗	✗	✗	✗
Coverage for Fines due to GDPR Non-Compliance	✓	✓	✓	✓	✓
Social Engineering/Phishing Coverage	✓	✓	✓	✓	✓
State-Sponsored Cyber Attacks	✗	✗	✗	✗	✗
Third-Party Vendor/System Failures	✓	✓	✓	✓	✓
Exclusion of Certain Geographical Regions	✗	✗	✗	✗	✗
Lack of Pre-Breach Risk Mitigation Services	✗	✗	✗	✗	✗
Criminal Acts by Insured	✗	✗	✗	✗	✗
Cyber Terrorism (Nation-State Attacks)	✗	✗	✗	✗	✗
Cloud Service Provider Breaches	✗	✗	✗	✗	✗
Failure to Cover Intellectual Property Theft	✗	✗	✗	✗	✗
Zero-Day Exploits (Unknown Vulnerabilities)	✓	✓	✓	✓	✓
Reputation Management for Senior Executives	✓	✓	✓	✓	✗

Keys: ✓ Coverage provided or not a gap ✗ Gap present in coverage (Not explicitly covered or not mentioned by the policy)

The analysis of gaps in cyber insurance coverage across five major insurers—Company V, Company W, Company X, Company Y, and Company Z—reveals a few key trends and areas of improvement. These insights are particularly relevant to understanding the current state of cyber insurance underwriting and its alignment with consumer needs and market expansion.

Key Observations and Insights:

- Across all insurers, gaps are consistently present for Advanced Persistent Threats (APTs), coverage for fines due to GDPR non-compliance, insider threats, criminal acts by the insured, cyber terrorism, and pre-breach risk mitigation services. This reflects an industry-wide reluctance to cover these high-risk or hard-to-predict areas. This reflects a potential vulnerability for businesses. As regulatory penalties can be substantial, the absence of coverage may leave organizations exposed to significant financial risks.
- Regarding cloud service provider breaches, Company V and Company W acknowledge the importance of coverage in this area, while Company X, Company Y, and Company Z do not cover such incidents. With increasing cloud adoption, this represents a critical coverage gap that can affect organizations relying heavily on cloud infrastructure.
- None of the insurers offer coverage for zero-day exploits, indicating a broad and significant gap. Zero-day vulnerabilities are highly sophisticated and often the source of major cyber incidents, suggesting a lack of comprehensive support for this advanced threat.
- All insurers show a gap in explicitly covering state-sponsored cyber attacks and cyber terrorism. This reflects hesitancy in covering highly complex and large-scale threats that often have geopolitical implications. Given the increasing frequency of state-backed cyber incidents, this gap is a significant point of concern.
- Every insurer has a gap in offering pre-breach risk mitigation services, signifying a lack of proactive measures to prevent cyber incidents. This reactive approach may impact consumers' perception of the insurance policies' comprehensiveness, leading to market hesitancy in adopting such products.

The analysis reveals that insurers are hesitant to cover fast-evolving risks such as social engineering, zero-day exploits, and cloud provider breaches, indicating a misalignment between existing cyber insurance policies and consumer needs. Additionally, the lack of coverage for GDPR fines and pre-breach risk mitigation services shows that current policies are largely reactive, which could limit market growth as consumers seek more comprehensive options.



There is also inconsistency in covering certain risks like social engineering and cloud breaches, affecting policy competitiveness and market differentiation. Addressing these gaps by offering more standardized and proactive coverage could build consumer confidence and support market expansion by aligning policies more closely with the evolving threat landscape.

Figure 5.3 Overseas Cyber Insurance Gap Analysis in the Market

Table 4: Coverage Offered by Overseas Insurance Companies

Coverage Area	Company A	Company B	Company C	Company D	Company E	Company F
Data Breach & Privacy	✓	✓	✓	✓	✓	✓
Cyber Extortion	✓	✓	✓	✓	✓	✓
Business Interruption	✓	✓	✓	✓	✓	✓
Third-Party Liability	✓	✓	✓	✓	✓	✓
Incident Response Services	✓	✓	✓	✓	✓	✓
Risk Management Tools	✓	✓	✓	✓	✓	✓
Social Engineering Fraud	✗	✗	✗	✓	✗	✓
Regulatory Fines	✗	✗	✗	✗	✗	✗
Supply Chain Risks	✗	✗	✗	✗	✗	✓
Emerging Threats	✗	✗	✗	✗	✗	✗

Keys: ✓ Covered by the insurance policy ✗ Gap present in coverage (Not explicitly covered or not mentioned by the policy)

The cyber insurance landscape reveals notable differences between the coverage offerings of international and Indian insurance companies. International insurers such as Company A, Company B, Company C, Company D, Company E, and Company F generally provide a broader range of standard cyber protections, including comprehensive coverage across areas like data breach, cyber extortion, business interruption, third-party liability, and incident response services. Incident response services are particularly advantageous, as they equip clients with immediate resources for cyber crisis management, often involving a coordinated team of experts to help mitigate damages and restore operations, an asset in high-stakes cyber incidents.



Furthermore, most international insurers offer risk management tools, an additional layer of support that assists policyholders in identifying and managing cyber risks proactively. In contrast, Indian insurance companies, including Company V, Company W, Company X, Company Y, and Company Z, provide coverage for fundamental cyber threats such as data breaches, cyber extortion, and network security failures. However, they have limitations in certain specialized areas.

For example, few Indian insurers cover cloud system failures or physical theft of digital assets, and none offer protections for advanced persistent threats (APTs), which are increasingly sophisticated cyber-attacks often requiring specialized counter measures. Coverage of human error and outsourced service provider failure also varies among Indian providers, which could leave some clients with gaps in their cyber risk management.

Another key difference lies in coverage for regulatory fines; international insurers generally exclude regulatory fines from their policies, while Indian

insurers routinely include them, recognizing the importance of regulatory compliance in India's evolving digital landscape. Despite these efforts, international insurers often hold an advantage in the emerging threat landscape, with Company F covering supply chain risks—a significant area of concern as organizations become more dependent on interconnected networks. Overall, international insurers tend to offer a more robust and nuanced suite of coverages, which can be critical for multinational corporations or high-value targets in need of comprehensive, globally standardized cyber risk solutions.

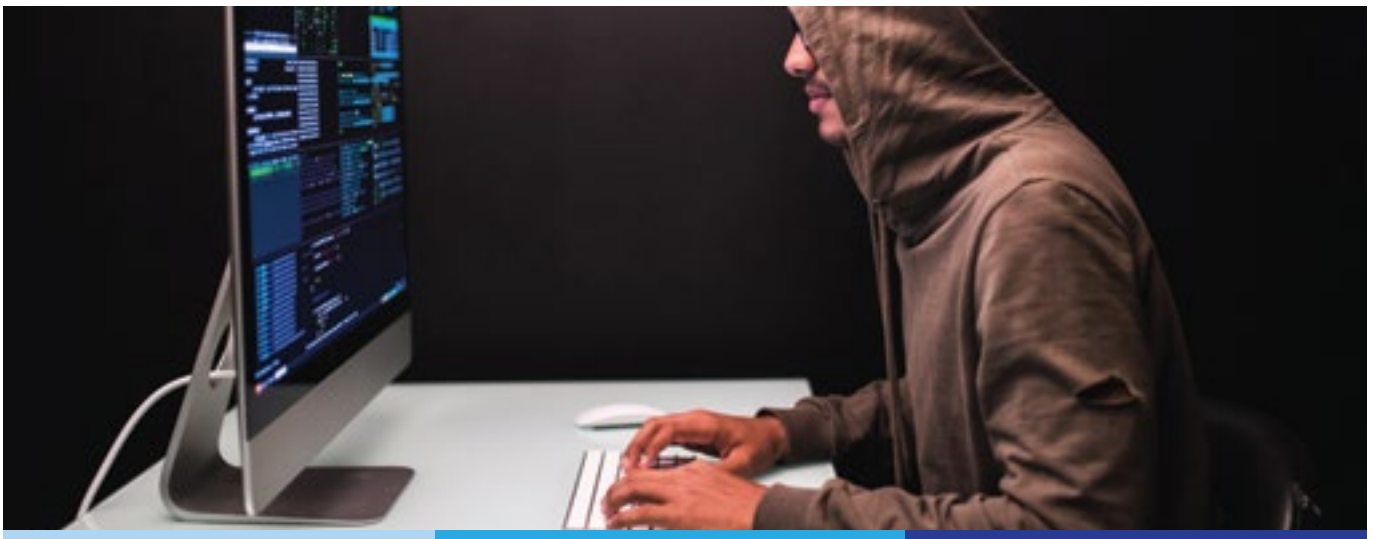
The gaps in cyber insurance coverage between international and Indian companies reveal significant differences in focus and market adaptation, reflecting both the varying needs of their clientele & regional regulatory landscapes.

International insurers such as Company A, Company B, Company C, Company D, Company E, and Company F show notable exclusions in emerging areas, including social engineering fraud, regulatory fines, and coverage for emerging technology risks. While Company F stands out by offering coverage for supply chain and vendor risks, most international insurers lack comprehensive solutions for long-term reputational damage and emerging technology risks. However, the global reach and well-established incident response services of international insurers generally equip them with the expertise to address large-scale cyber threats effectively, providing an advantage in overall preparedness. In comparison, Indian insurers—including Company V, Company W, Company X, Company Y, and Company Z—display significant gaps in coverage, particularly in more specialized and sophisticated threat areas. All Indian



insurers exclude coverage for advanced persistent threats (APTs), insider threats, and state-sponsored cyber-attacks, which can be particularly harmful given the global rise in nation-state and highly organized cyber threats. Additionally, Indian companies generally do not cover pre-breach risk mitigation services, representing a reactive rather than proactive approach to cyber risk. Other gaps, such as exclusions for zero-day exploits, intellectual property theft, and third-party vendor failures, reveal limitations in anticipating or addressing complex and modern cyber threats. Despite these gaps, Indian insurers tend to offer coverage for GDPR non-compliance fines and regulatory penalties more consistently than their international counterparts,

recognizing the importance of regulatory compliance within India's jurisdiction. However, international insurers maintain an advantage in critical areas such as incident response services, supply chain risk coverage, and access to global cybersecurity expertise. This suggests that while Indian insurers provide cost-effective solutions that address regional regulatory requirements, international insurers are better positioned to handle complex, cross-border cyber risks with a more comprehensive and well-resourced approach. In the current cyber landscape, multiple advanced threats continue to evolve, posing significant risks that remain inadequately covered by both international and Indian insurance providers.



Notably, advanced persistent threats (APTs)—prolonged, targeted attacks by sophisticated cyber actors, often state-sponsored—are excluded from the coverage of both international and Indian insurers. APTs exploit system vulnerabilities over extended periods to gain unauthorized access to sensitive data, making them highly destructive for organizations across industries, especially critical infrastructure, financial institutions, & government entities.

Emerging technology risks are another gap across international policies, indicating an absence of coverage for vulnerabilities in rapidly advancing areas like artificial intelligence (AI), machine learning, and Internet of Things (IoT) devices. These technologies, while transformative, introduce complex security challenges, as they often collect extensive data, interact across unregulated networks, and may lack standardized security

measures. The absence of coverage for these risks suggests that organizations relying on emerging technologies remain vulnerable to attacks targeting these platforms. Additionally, long-term reputational damage is not covered by any international insurer, leaving companies without support for managing the prolonged impacts of a data breach or cyber incident on public perception and brand trust.

For businesses heavily dependent on customer trust and reputation, such as those in e-commerce, finance, and healthcare, this coverage gap can result in sustained financial losses and customer attrition that insurance does not mitigate.

In India, further gaps exist in insider threats and state-sponsored cyber-attacks, reflecting a lack of protection against malicious actions by employees or nation-state attacks specifically targeting private sector entities. Insider threats—actions from employees or trusted partners that compromise internal systems—are increasingly prevalent and difficult to detect, often leading to significant data breaches or intellectual property theft. State-sponsored cyber-attacks are sophisticated threats commonly directed at critical sectors like finance, defense, and technology, where attackers seek to disrupt operations, steal sensitive information, or damage national security interests. The lack of coverage in these areas indicates a vulnerability for Indian companies in scenarios where cyber espionage or sabotage might affect business continuity. Finally, zero-day exploits represent a

universal gap, as no insurers provide coverage for this category. Zero-day exploits target previously unknown vulnerabilities within software or hardware, often making defenses ineffective as patches or security updates are not immediately available. Given the potentially devastating impact of zero-day exploits on sensitive systems, the absence of coverage for these threats underscores a critical shortfall in both international and Indian cyber insurance offerings. This gap is particularly concerning in an environment where attackers actively search for unpatched vulnerabilities and execute attacks with minimal opportunity for defense. Addressing these evolving and high-impact threats remains crucial for organizations navigating today's complex cyber risk landscape, but the current insurance offerings lack comprehensive support in these high-risk areas.



Figure 5.4 Other Significant Insights on the Cyber Insurance Market

The rapid expansion of the cyber insurance market is being driven by the increasing complexity of cyber threats and the rising cost of cyber incidents. Insurers are responding by offering more comprehensive policies that cover both traditional risks (data breaches, business interruptions) and newer risks (cyber extortion, multimedia liability). However, as the market continues to evolve, insurers will need to address several emerging areas of risk:



■ Advanced Persistent Threats (APTs):

As cybercriminals become more sophisticated, insurance policies will need to expand their coverage to include more advanced threats, such as state-sponsored attacks or AI-driven malware.

■ Regulatory Compliance:

With the proliferation of data protection laws worldwide, insurers will need to offer more comprehensive coverage for regulatory penalties and the legal costs associated with non-compliance.

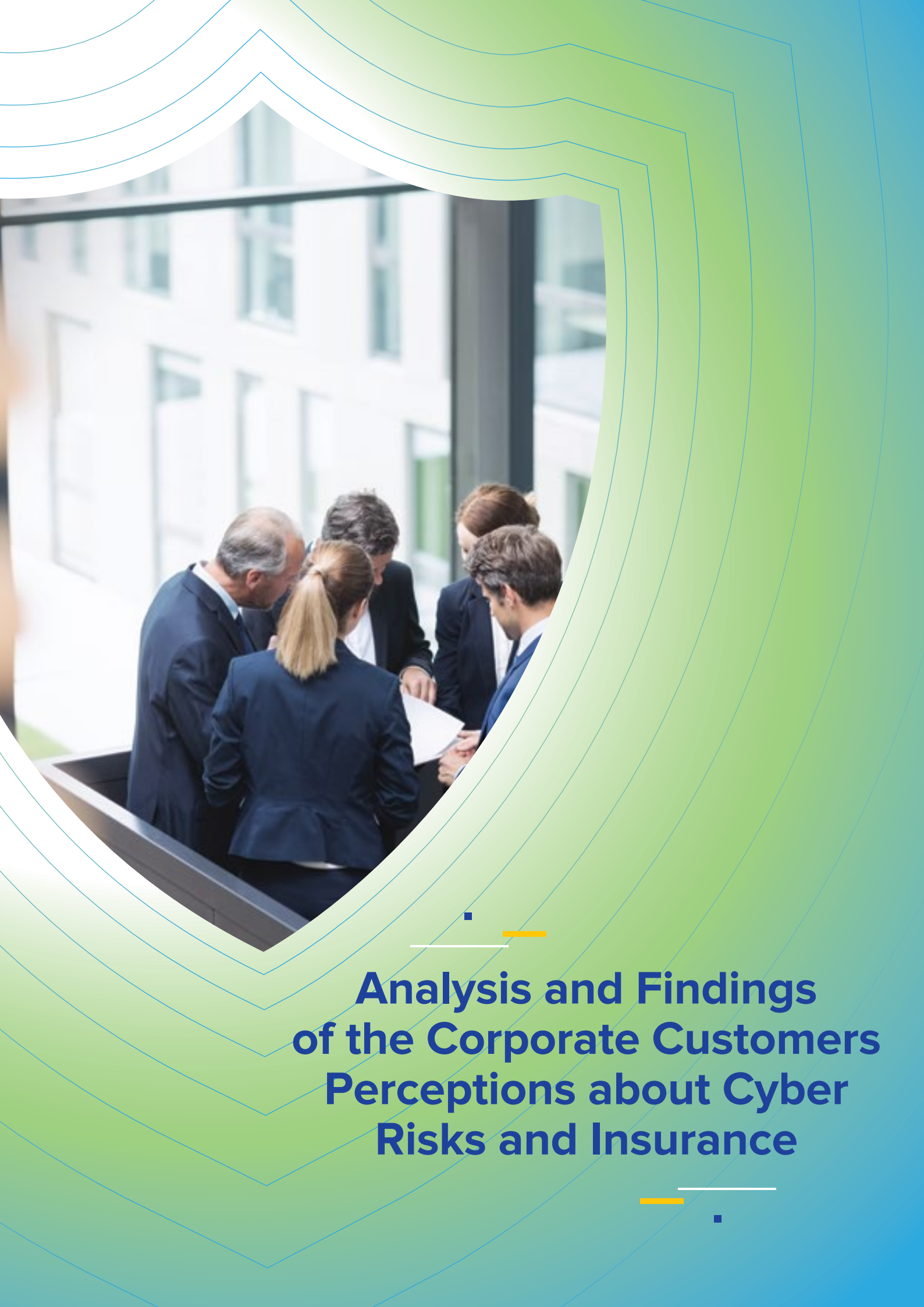
■ Cloud and Outsourced Systems:

As businesses increasingly rely on cloud services and third-party providers, there is a growing need for insurance policies that cover losses resulting from failures or breaches in these outsourced systems.

■ Cybersecurity as a Service:

The future of cyber insurance may lie in offering not just financial protection but also proactive cybersecurity services, such as continuous threat monitoring and vulnerability assessments, helping businesses reduce the likelihood of a breach before it happens.

Cyber insurance is becoming an essential part of risk management for organizations of all sizes. Insurers that can adapt to the rapidly changing cyber threat landscape and provide comprehensive, forward-looking coverage will be well-positioned to capture the growing demand in this sector.



■ ——— ———

Analysis and Findings of the Corporate Customers Perceptions about Cyber Risks and Insurance

————— ■

6 Analysis and Findings of the Corporate Customers Perceptions about Cyber Risks and Insurance:

The questionnaire for the data and survey conducted was designed using the perception about cyber products, cyber security measures and risk assessment carried out, cyber insurance and coverages, cyber loss claim settlement process, and finally cyber security risk mitigation.

Descriptive analysis of these responses using frequency distribution and measures of central tendency and dispersion analysis were carried out to understand the overall perception and also identify the difference between customer segments and industries and sectors.

The analysis and interpretation derived from the analysis have been discussed in the following 5 different sections.

1

Demographic Analysis of the companies selected for the Study.

2

Cyber Risk Assessments and Security analysis of the different sectors/ industries.

3

Cyber Insurance and Coverages.

4

Cyber Risk Threat Probability, Cyber Losses and Claims Analysis.

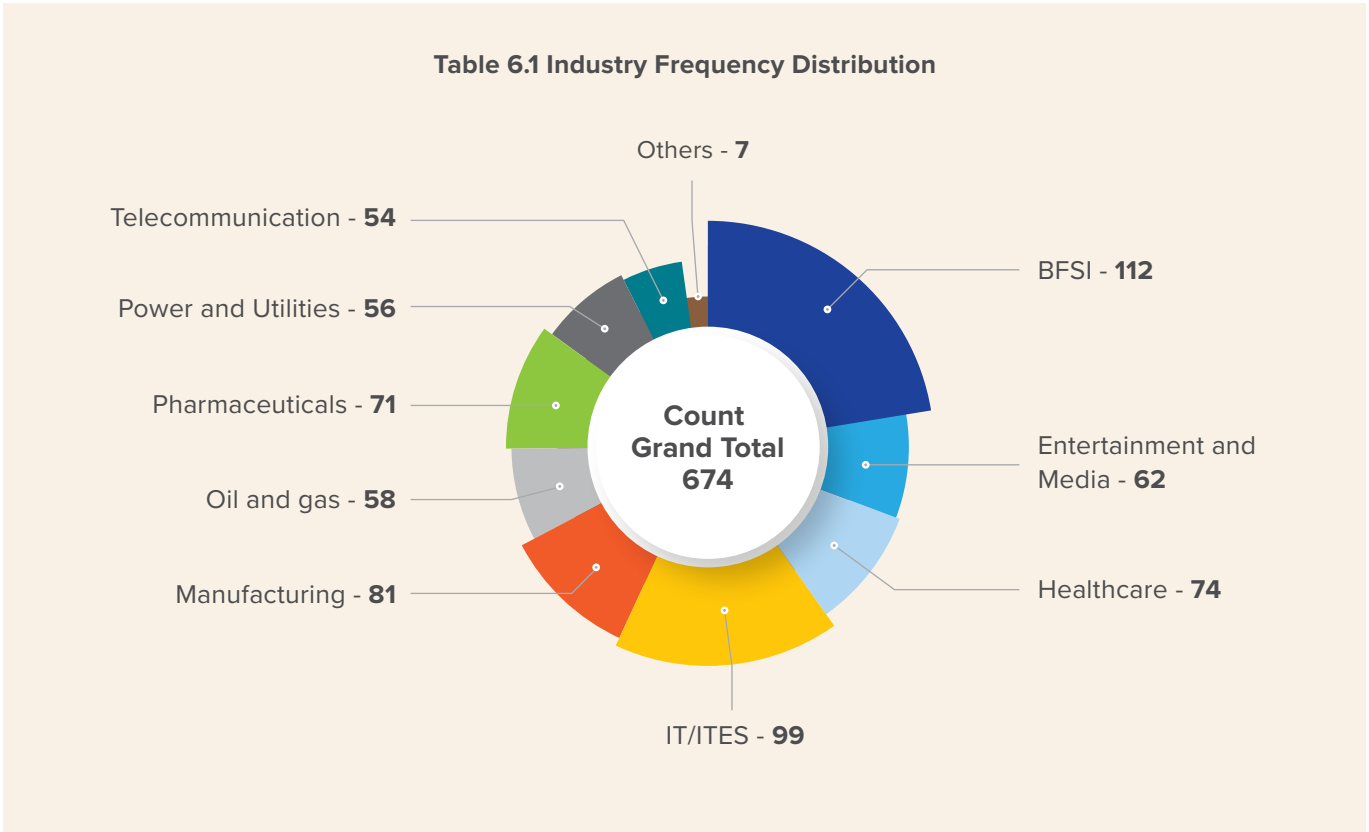
5

Cyber Risk Mitigation Measures.

6.1. Demographic Analysis of Companies Selected for the Study

The Demographic Analysis of the selected companies of the study provides an overview of the diverse range of businesses analyzed, categorized by industry type and turnover levels. This demographic breakdown offers a foundation for understanding how company size and sector impact cybersecurity needs and risk exposure, key factors in shaping appropriate cyber insurance solutions.

By examining these characteristics, the study gains insights into the varying levels of cyber preparedness and insurance needs across the corporate landscape.



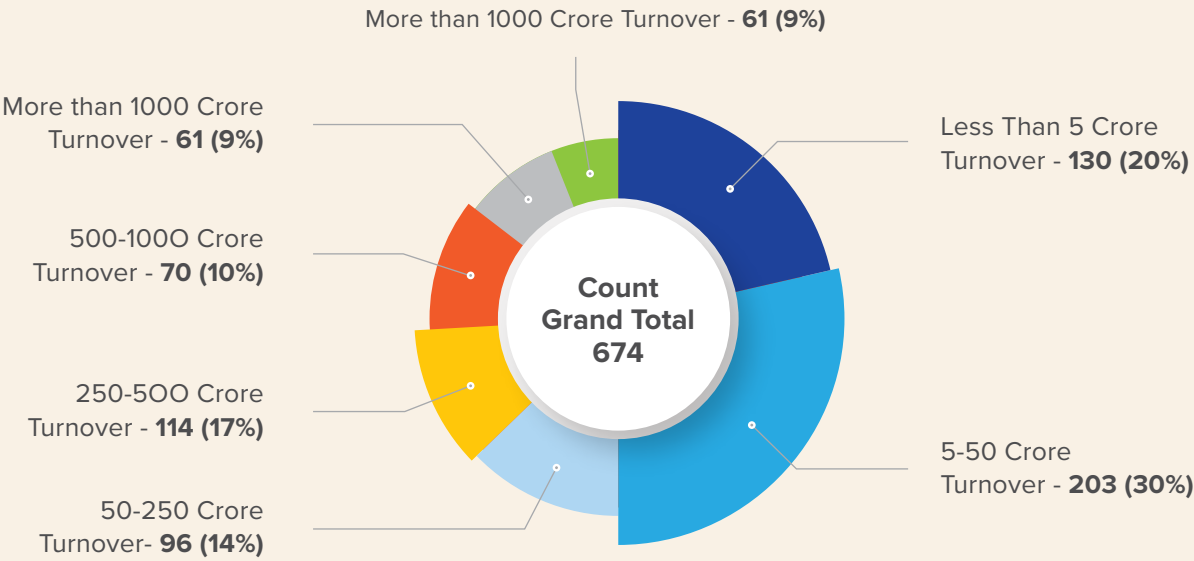
- The BFSI sector leads with 112 responses (17%), underscoring its critical need for cyber insurance due to high regulatory scrutiny and vulnerability to cyber threats. Similarly, IT/ITES (99 responses - 15%) and Healthcare (74 responses-11%) also represent significant sectors where tailored cyber insurance solutions can mitigate risks.
- Understanding sector-specific risks allows for the creation of tailored insurance products. Industries like Manufacturing (81 responses-12%) and Entertainment and Media (62 responses-9%) face unique vulnerabilities that necessitate specialized coverage, making targeted product offerings essential for effective market penetration.

Industries such as BFSI and Healthcare have stringent regulatory requirements. Cyber insurance can help these organizations meet compliance standards while protecting against potential financial losses from cyber incidents, emphasizing the necessity of integrating risk management strategies with insurance products.

Classifying organizations by sector facilitates strategic marketing and targeted educational initiatives. By raising awareness of cyber risks and the importance of insurance in sectors with lower engagement, such as Oil and Gas (58 responses) and Telecommunication (54 responses), insurers can expand their reach and strengthen overall cybersecurity across the market.

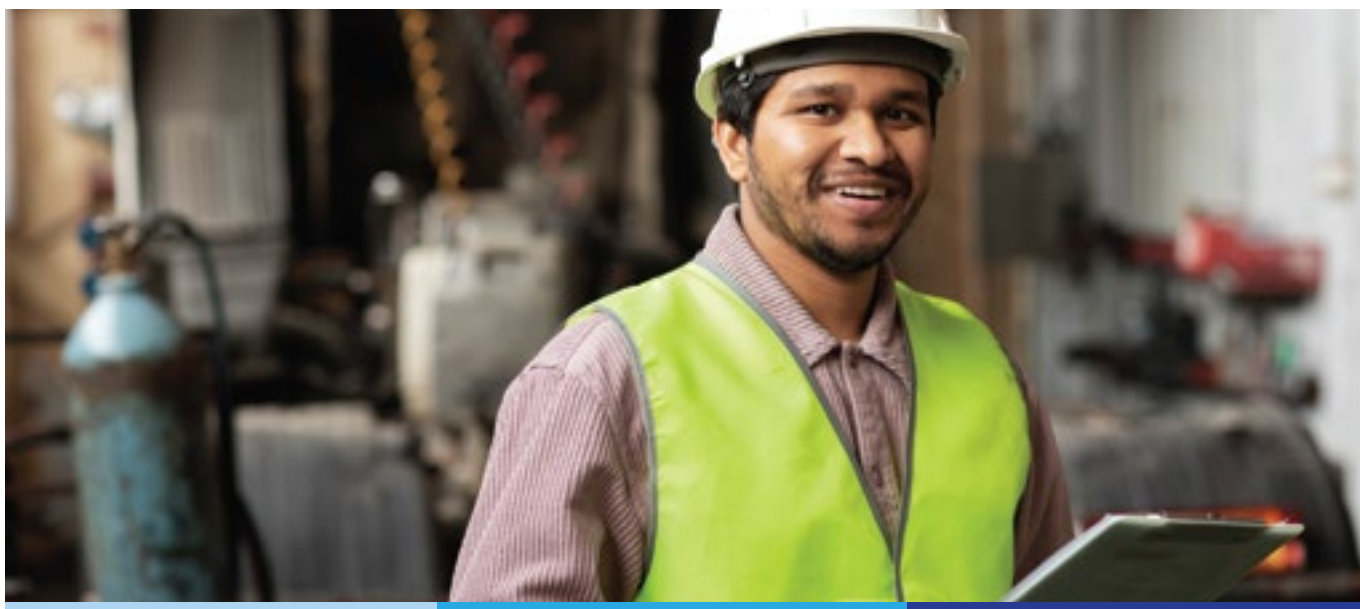


Table 6.2 Turnover Frequency Distribution



The Turnover classification reveals a diverse distribution among respondents, with 203 organizations (30%) in the 5-50 Crore range and 130 (20%) in the Less Than 5 Crore category. This segmentation indicates a significant opportunity to tailor insurance products to different turnover brackets, ensuring coverage is relevant and accessible for organizations of varying sizes.

- Although the number of organizations with 500-1000 Crore (10%) and More than 1000 Crore (9%) turnover is smaller in the selected sample, these large enterprises typically have higher budgets for cyber risk management and may be more inclined to invest in sophisticated cyber insurance products. Targeting this segment can yield substantial revenue opportunities due to their significant risk exposure.
- The 50-250 Crore (14%) and 250-500 Crore (17%) segments highlight a robust market of mid-sized businesses that may require comprehensive cyber insurance solutions. These organizations often have more complex operations and assets, making them attractive targets for cyber threats, thus necessitating tailored coverage options.
- Organizations in the Less Than 5 Crore and 5-50 Crore categories, particularly MSMEs and medium-sized companies, have limited cyber risk awareness and low demand for cyber insurance. However, increasing cyber risk exposures among small and medium-sized organizations and cyber vulnerability, they need to be made aware of the importance of cyber insurance coverage through educational initiatives and tailored marketing campaigns which can bridge this knowledge gap, enhancing the understanding of the importance of cyber insurance as part of their overall risk management strategy.

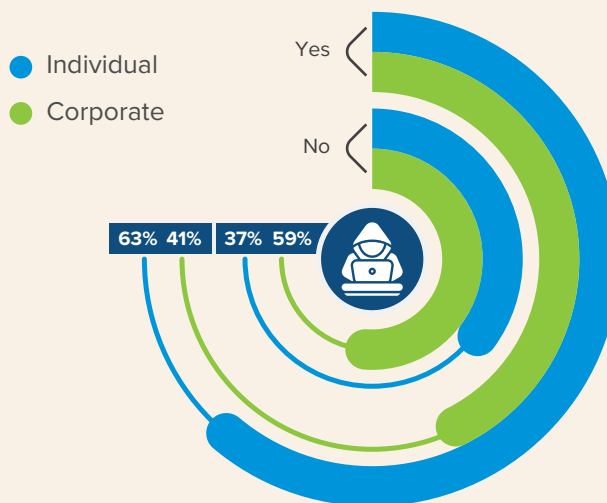


6.2. Increasing Cyber Risk Incidences:

A recent study by KPMG indicates that over 72% of organizations, including service industries, are being hacked or are vulnerable to cyber risks. Increasing globalizations, the use of clouds and IoT, AI, and connected devices exponentially increase system vulnerability.

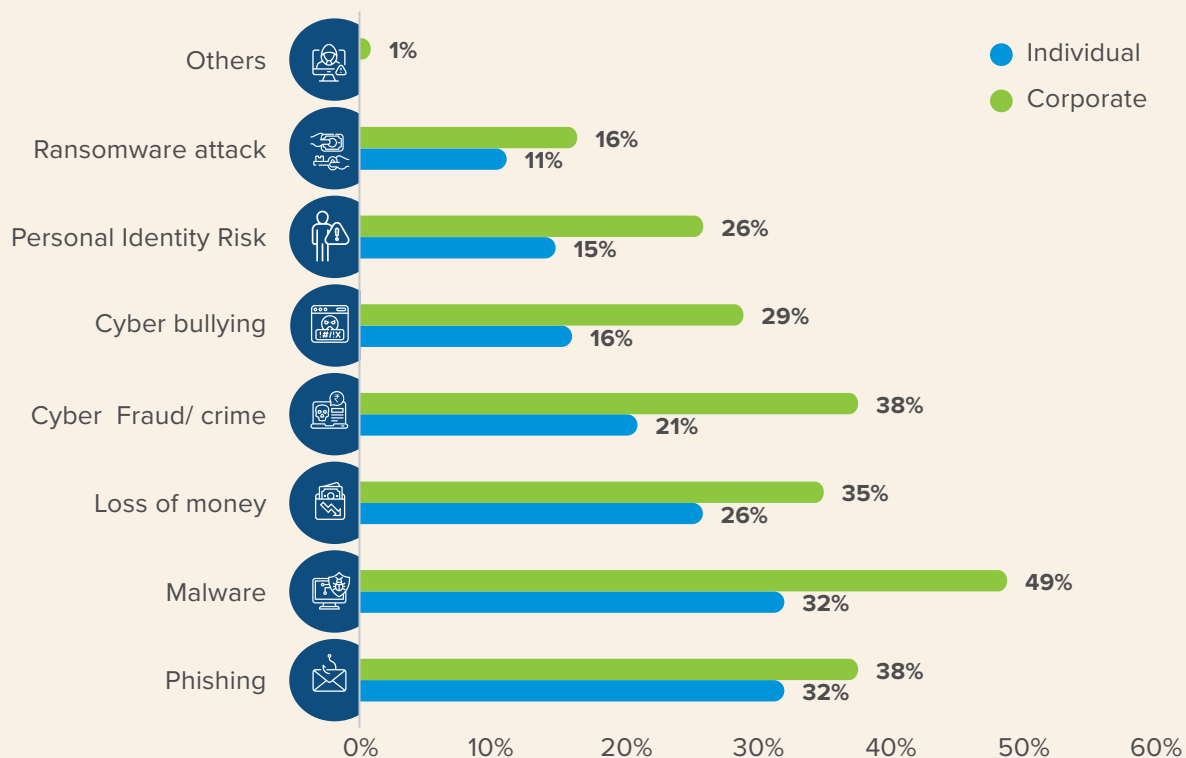


Figure 6.2.1 Cyber-attack Incidences



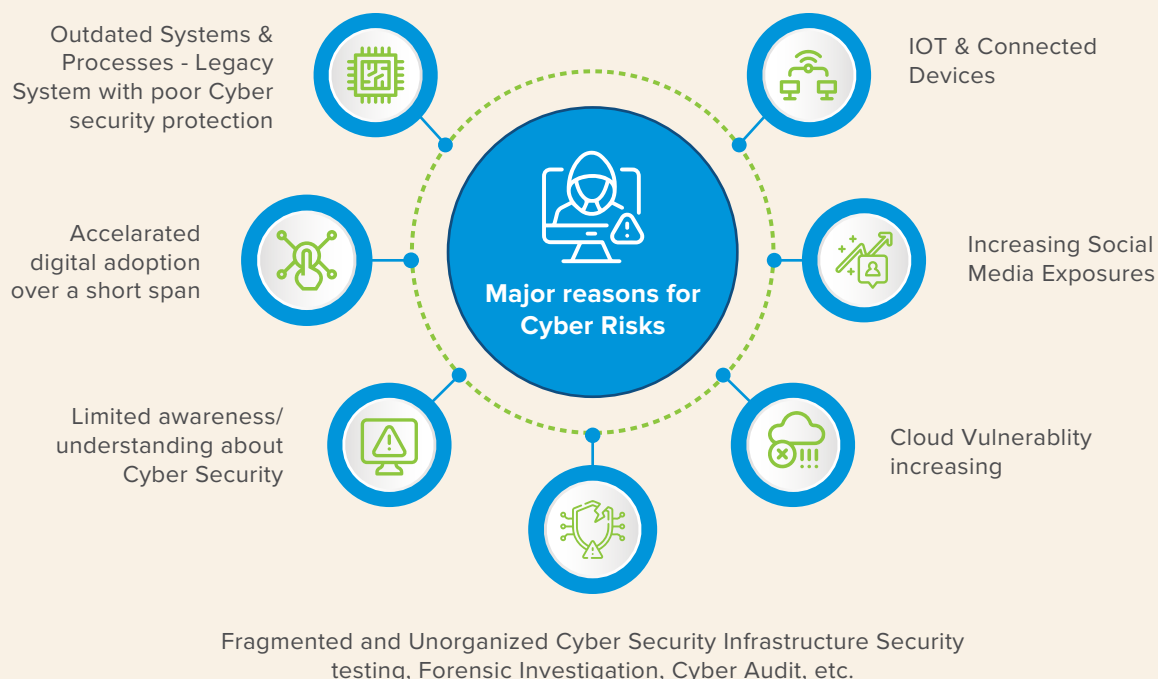
Our study highlights that nearly 63% of individual customers and 41% of corporate customers perceive increased cyber incidents in their daily lives. The majority of customers experienced cyber-attacks in the form of phishing, spoofing emails, malware, ransomware, as illustrated in Figure 6.2.2

Figure 6.2.2 Cyber Risk Incidences - Individuals & Corporates



Social media & Personal Identity Risks are also increasing in recent times. A significant number of corporate customers have also experienced malware-related system bugs (49%), phishing emails (38%), and 39% cyber frauds or crimes in their organizations. It has been observed that the types of cyber attacks vary significantly across different organizations. For instance, banking and insurance companies receive a large number of phishing emails or malware, while manufacturing companies experience major threats from their vendor or supply chain-related vulnerabilities.

The major reasons contributing to the increasing cyber vulnerability in organizations are as follows:



1) Use of Outdated Systems & Processes:

The main vulnerability, as seen in the diagram above, is the use of outdated systems and processes—legacy systems with a lack of regular updating of cybersecurity. Most public sector organizations and government sectors face such vulnerabilities more often.

2) Accelerated Digital Adoption:

The accelerated digital adoption, particularly during the COVID-19 pandemic, by almost all industries within a short span, has contributed to increased vulnerability.

3) Fragmented Cyber Security Infrastructure and System Vulnerability:

Many organisations have fragmented cyber security infrastructure and examine the cyber security lapses in tandem/ solos. They do not perform regular security testing, forensic investigations, updation of filters and firewalls etc.

4) Cloud Storage, IoT, & Connected Devices:

A large number of organizations opting for cloud storage, use of IoT and connected devices, and increasing social media exposures have all contributed to enhanced exposure.

However, lack of awareness among organizations, particularly key management personnel (CEO, CFO, CIO, PTO, CRO, etc.), results in cyber insurance still not being perceived as essential. As a result, there is an immense need for every organization, including SME sectors, to obtain adequate cyber risk protection.

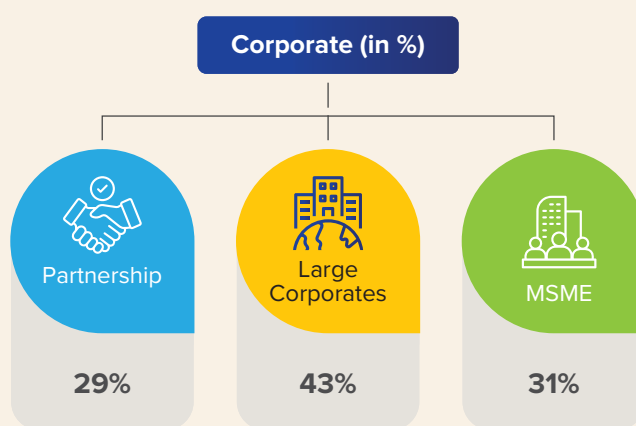
6.3. Cyber Insurance Penetration amongst Corporate Customers:

According to insurance company statistics, less than 10% of corporations have opted for cyber insurance policies. The majority of these are large companies that have done so to meet the requirements of SEBI and RBI, ensuring the security of customer deposits and investments.

One of the main reasons for the low adoption of cyber insurance is the lack of awareness and a perceived need for such coverage. Our analysis indicates a low level of awareness across different types of organizations. While corporate customers recognize the importance of protecting their network security and core functions of their IT systems, their awareness of known risks such as network security, identity theft, data loss, and financial loss is reasonably good.

However, they do not perceive the importance of emerging risks associated with increased usage of Artificial Intelligence, IoT, and connected devices. Web servers are currently being increasingly exposed to higher cyber vulnerabilities, and there is a need for comprehensive protection in these areas.

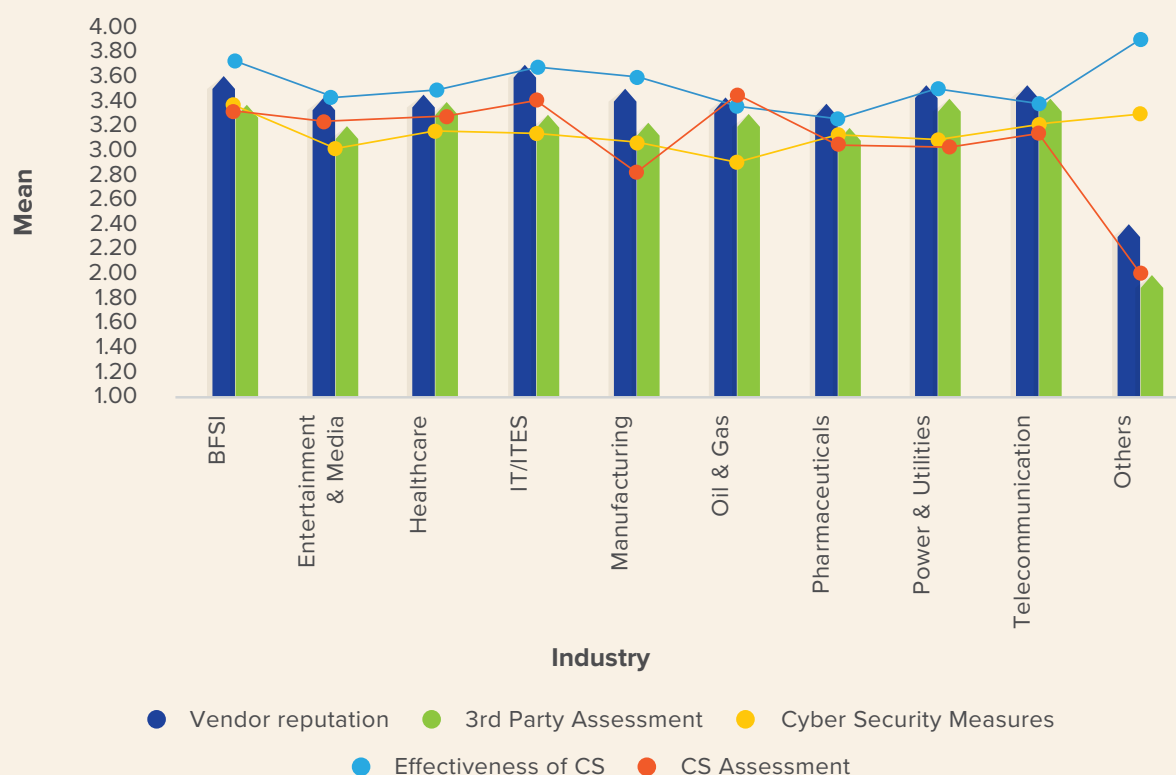
Figure 6.3 Cyber Insurance Penetration- Corporates



6.4. Cyber Security Measures and Risk Assessments across different sectors

The section provides a comparative overview of how different industries/sectors adopt cybersecurity risk assessments and various mitigation measures. This analysis exhibits the major cyber security practices adopted in managing cyber risks. These insights strongly emphasize a better understanding of sector-specific vulnerabilities and industry preparedness in mitigating cyber risk threats. Further, it also necessitates the need for assessing cyber insurance needs across different business types and turnovers.

Figure 6.4.1 Cyber Security Assessment by Industry
Cyber Security Measures & Assessment across Different Industries

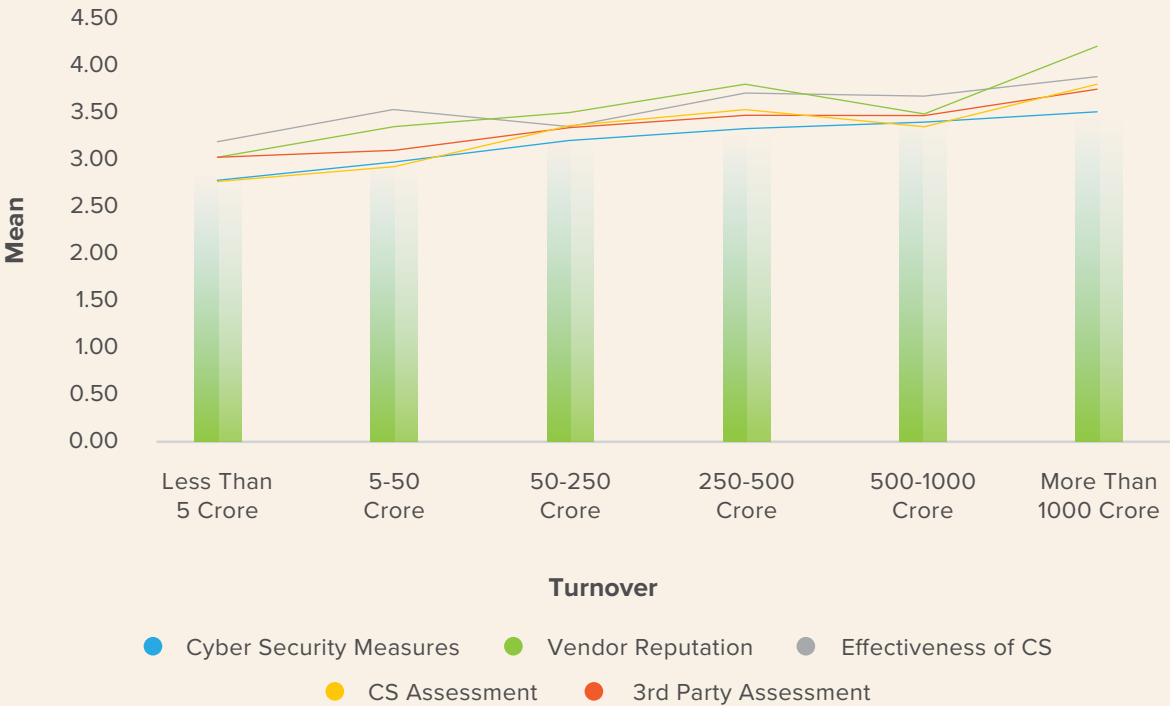


- The Cyber Security assessment among various industries, in short, ends in a moderate value. To elaborate, the Cyber Security assessment including vendor reputation, cyber security frequency, and third-party assessment, was performed with low to medium frequency intervals across all industries. This inevitably draws the inference, that the cyber security of the industries is in much dire need of improvement and growth. The companies need to conduct these assessments at regular intervals as any lapse intervals, can trigger cyber risk threat vulnerability at any time as the cybercriminals are always on the lookout for any system vulnerability.

The graphical data implies that the major industries like IT/ITES, Power and Utilities, etc, do perform regular cyber security assessments, but the overall rating of their risk assessment quality doesn't imply confidence at all. Data and information are handled every second by all these industries, which indeed inflicts the need for better cyber assessment secondly, cyber risks are evolving fast, and any gaps in the system vulnerability need to be plugged in immediately.

The cyber security and its assessments are the first step to evaluating the security measures of an industry. Evidently, these same variables are the face of evaluating the Cyber Insurance policy coverages and their adequacy. Thus, the need for improvement of these assessments across industries is inevitable, as all of them are part of the cyber dynamics and consumers of cyber infrastructure and facilities.

Figure 6.4.2 Cyber Security Assessment by Turnover
Cyber Security Assessment across Turnover



As company turnover increases, the average scores across all cybersecurity assessment metrics show an upward trend. This indicates that larger organizations with higher turnover generally invest more in cybersecurity measures and assessments, likely due to increased resources and awareness of cyber risks.

Vendor reputation consistently ranks higher across turnover levels compared to other metrics, indicating its perceived importance in the assessment framework. In contrast, cybersecurity measures and Cybersecurity assessments have lower scores, suggesting potential gaps in active security practices that might not be prioritized as highly despite their critical role in cybersecurity.

■ A robust cybersecurity posture (particularly in higher turnover organizations) directly correlates with a stronger eligibility profile for cyber insurance, as insurers prefer clients with established cyber defenses. This trend highlights the critical role that effective cybersecurity assessments and vendor management play in shaping the cyber insurance market.

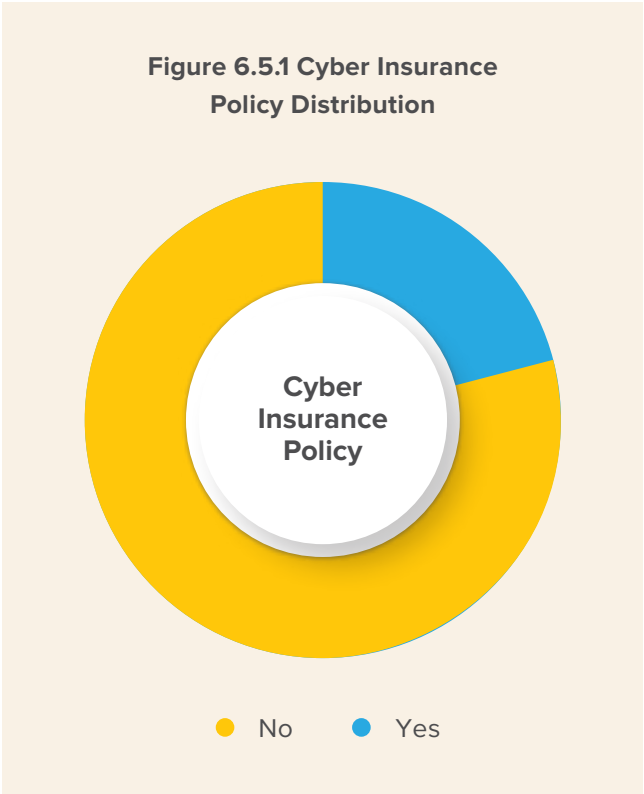
■ Given the steady increase in mean cybersecurity assessment scores with turnover, the market for cyber insurance can leverage this data to tailor policies for mid- and high-turnover companies that show readiness. However, for smaller organizations, there remains a market need for affordable and scalable cybersecurity solutions to help them reach maturity levels that meet insurance criteria.



6.5. Cyber Insurance and Coverages

This section of the analysis discusses the cyber insurance products that are available in India and overseas markets. Further, it dwells into number of people under different sectors/industries covered under cyber insurance. The insurance penetration across different sectors and industries and the reasons for low penetration of cyber insurance in certain industries. This also further delves into the key criteria determining the adequacy of cyber insurance (sum insured) and coverage limits across various industries and turnover categories. By examining how coverage amounts are allocated based on specific industry needs and organizational scale, this section provides a comprehensive view of risk-based insurance underwriting. These insights help clarify the alignment between industry risks and insurance provisions, offering a benchmark for businesses to evaluate their own coverage requirements in the evolving landscape of cyber threats.

- The figure 6.5.1 showcases the distribution of adoption of cyber insurance. Only about 24% have adopted a cyber insurance, inspite of increasing recognition of cyber threats. This low uptake suggests a need to create awareness on the importance of cyber risk management across industries.
- A significant portion of organizations 76% remain uninsured. This disparity could stem from factors such as limited budgets, perceived low risk, or lack of understanding of cyber insurance benefits, signaling a gap in market penetration.
- Understanding why a portion of organizations opt out of cyber insurance is critical for this project. Targeted outreach and tailored products could help bridge this gap, making cyber insurance more accessible and appealing to all types of organizations.

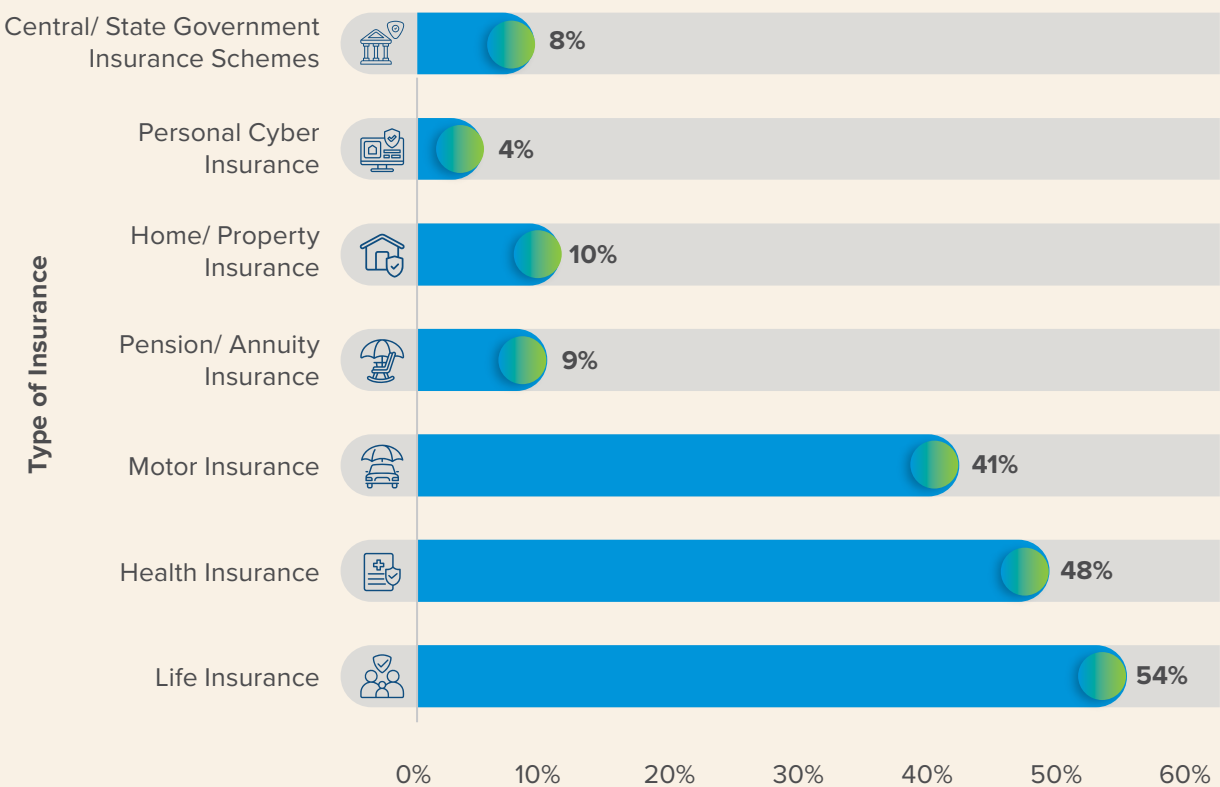


The presence of uninsured entities indicates substantial growth opportunities within the cyber insurance market. Expanding coverage through education, cost-effective options, and targeted solutions can help increase adoption rates, supporting market expansion and resilience against cyber risks.

6.6. Cyber Insurance Penetration - Individuals

The Indian cyber insurance market is still in the process of maturation, and the prevalence of cyber insurance policies remains very low. Presently, only 1200 to 1400 corporate cyber policies are being sold to corporates, indicating a significantly low penetration rate.

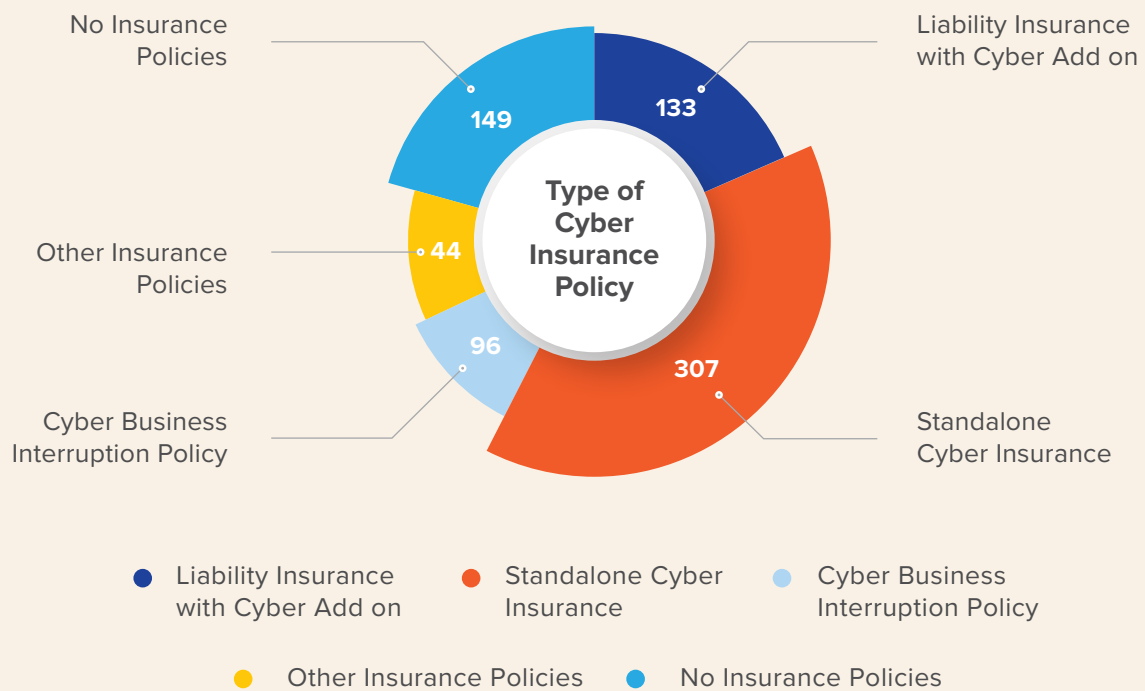
Figure 6.6.1 Cyber Insurance Penetration - Individual Customers



The analysis above reveals that less than 5% of individual customers currently possess cyber insurance, leaving ample room for business expansion in the retail sector.



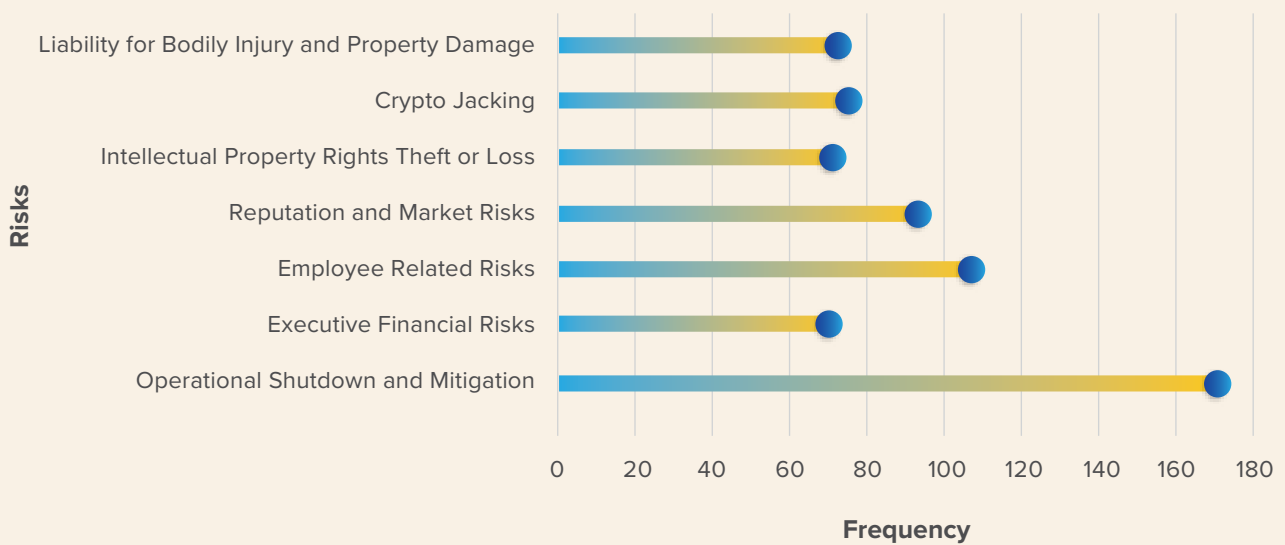
Figure 6.6.2 Types of Cyber Insurance Policy



- The above analysis (figure-4) exhibits the different types of Cyber Insurance purchased by the companies. Nearly 42% of companies have taken the standalone cyber policy, suggesting that organizations require more dedicated and specialized protection. This trend aligns with the growing complexity of cyber threats, where standalone policies offer comprehensive and focused coverage.
- A substantial portion of organizations opt for cyber add-ons to their liability insurance, indicating a cost-effective approach to cyber protection. This option might be attractive to smaller organizations with limited budgets, though it often lacks the full scope of protection offered by standalone policies.
- Despite increase in cyber risks, a small segment remains uninsured. This gap reveals potential barriers, such as cost or lack of awareness, highlighting areas where the cyber insurance market can expand by addressing these hurdles and promoting broader adoption.
- The variety in policy types showcases the market's flexibility but also underlines a need for more tailored solutions. Understanding this distribution is crucial for the insurance industry, as it reflects both the current demand and future growth potential within the cyber insurance sector, especially as organizations seek policies that address evolving threats comprehensively.



Figure 6.6.3 Additional Risks Sought by the customer



- The above analysis (figure-3) reflects the demand for certain specialized coverages and additional risks that the respondents seek to cover under the Cyber Insurance Policy, indicating the scope of business potential for the existing cyber insurance business.

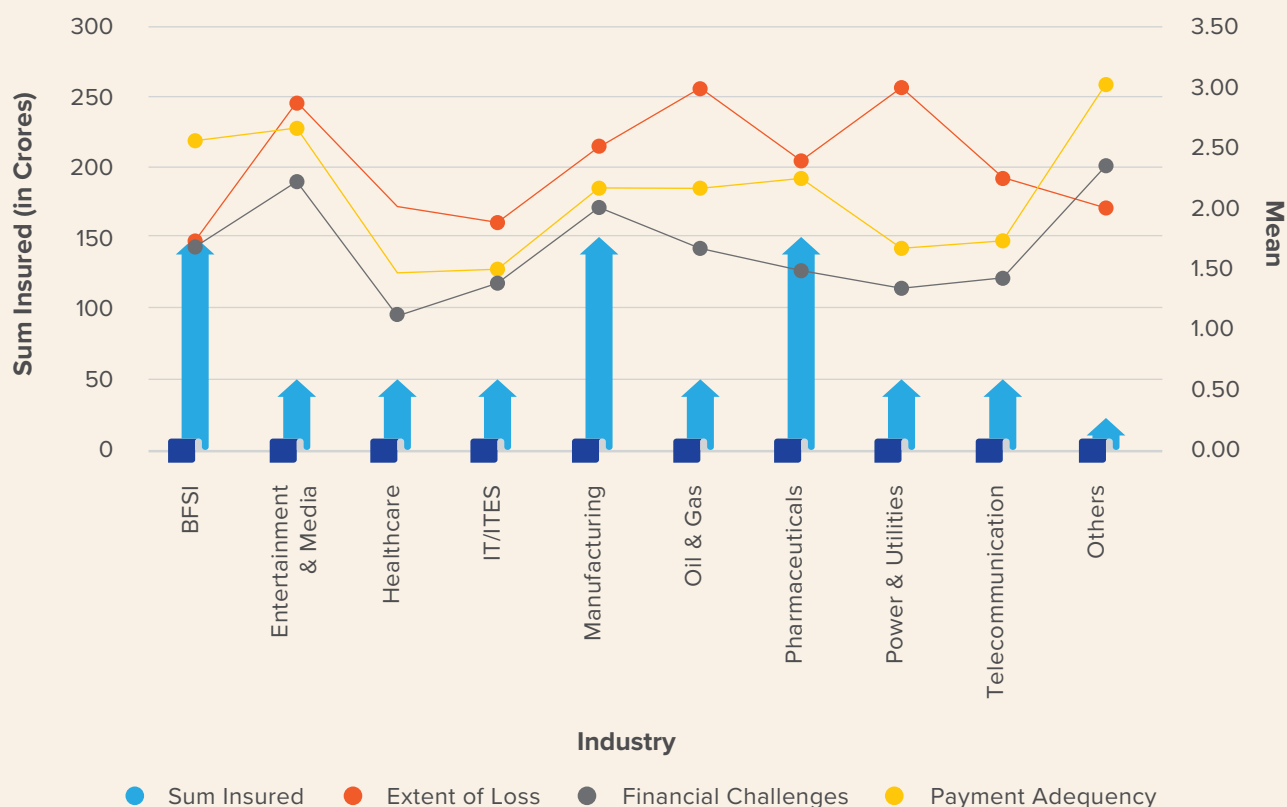
The analysis highlights that operational shutdown and mitigation risks are the most sought-after coverage in cyber insurance policies. This emphasis reflects real-world concerns over the financial and operational impact of prolonged downtime due to cyber incidents. However, many of the existing cyber policies do not cover this risk, but the operation shutdown of the system as part of cyber risk mitigation needs to be covered and nearly 35% of the existing customers require this coverage.

- Employee-related risks and reputation/market risks exposures are also increasing with higher severity of losses. These preferences underline the reality that internal threats and reputational damage are pressing concerns for organizations, as cyber incidents increasingly involve human factors and can lead to lasting brand damage and reputational risks for the company. Nearly 25% of the insured customers prefer to cover these risks.
- The diversity in desired coverage points to significant growth potential in the cyber insurance market. Insurers that can offer comprehensive, tailored policies addressing these specific risks will be better positioned to attract clients and meet the evolving needs of a broadening customer base.

- The range of additional risks sought—spanning intellectual property, bodily injury, and financial risks—demonstrates the need for flexible, customizable insurance solutions. Though property damage and bodily injury are covered under property insurance, companies like MSME or medium-sized enterprises desiring to take exclusive cyber policy may need to protect against these risks as the number of exclusive cyber-driven bodily injuries and property damages is increasing and the increasing number of manufacturing and service industries are adopting to generative AI and automation. This insight is crucial for the insurance industry, as it highlights the importance of developing customized policies that can cater to the varied risk profiles of different organizations.

Figure 6.6.4 Perception about Coverage of Loss, Payment Adequacy, and Sum Insured

Average Sum Insured of Cyber Insurance across different Industries



- The respective graph above reflects the distribution of the total sum insured under the cyber insurance policy adopted and Coverage of Loss & Payment Adequacy.
- The highest frequency of policies falls within the 50–150 crore sum insured range, followed closely by other categories, indicating significant demand in high coverage tiers. Lower and very high ranges (up to 1 crore and above 250 crore) have similar frequencies, suggesting a more moderate uptake for these levels.

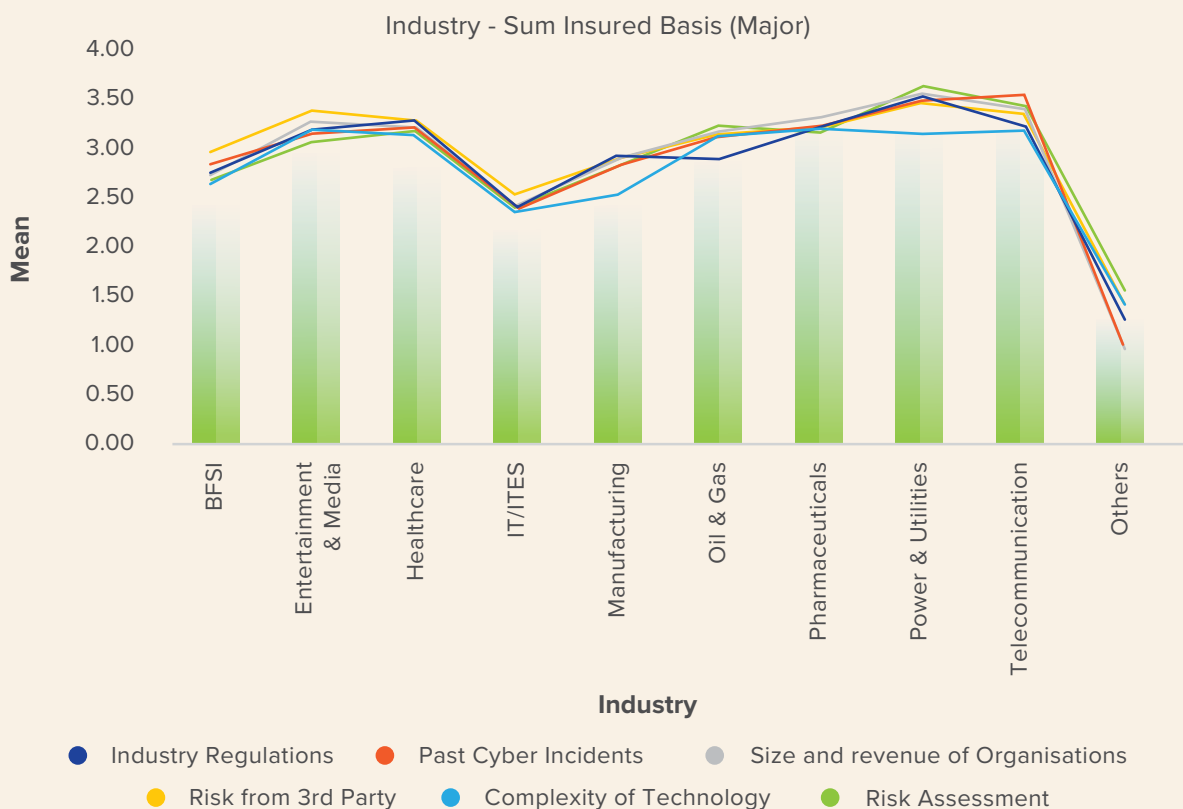
■ As it can be observed from the above analysis many companies, particularly, Health Care, Media companies, IT/ITES, and Manufacturing sectors have taken low coverage (Sum Insured), which is much lower than the actual loss limits. Consequently, perceive that their policy coverages are much lower than the actual loss experienced and opined that their cyber loss payouts are much lower resulting in huge financial challenges at the time of cyber loss incidents.

■ The mid-to-high demand suggests that product offerings could be optimized by focusing on these sum-insured ranges. It also highlights an opportunity to educate smaller businesses on the importance of cyber insurance, as they may be underestimating their risk exposure.

■ This distribution reflects a strong market need for mid-to-high-level cyber insurance, potentially aligning with the increasing cyber risks faced by businesses with considerable operational losses and assets at stake. The limited demand for very low or very high sum insured levels may hint at smaller companies' hesitancy to invest heavily in cyber insurance, or larger entities possibly having alternative risk mitigation measures.

With cyber threats escalating globally, this data underscores a growth potential in the cyber insurance sector. Encouraging adoption in currently underserved segments (low and very high sum insured categories) could further expand the market, meeting diverse needs and increasing overall resilience against cyber threats.

Figure 6.6.5 Major Basis for Sum Insured by Industry



Key industries such as BFSI, Healthcare, IT/ITES, and Manufacturing show relatively higher average scores for factors like Industry Regulations and Size and Revenue of Organization compared to others, indicating a stronger awareness of cyber risks, although only moderate at the entire mean.



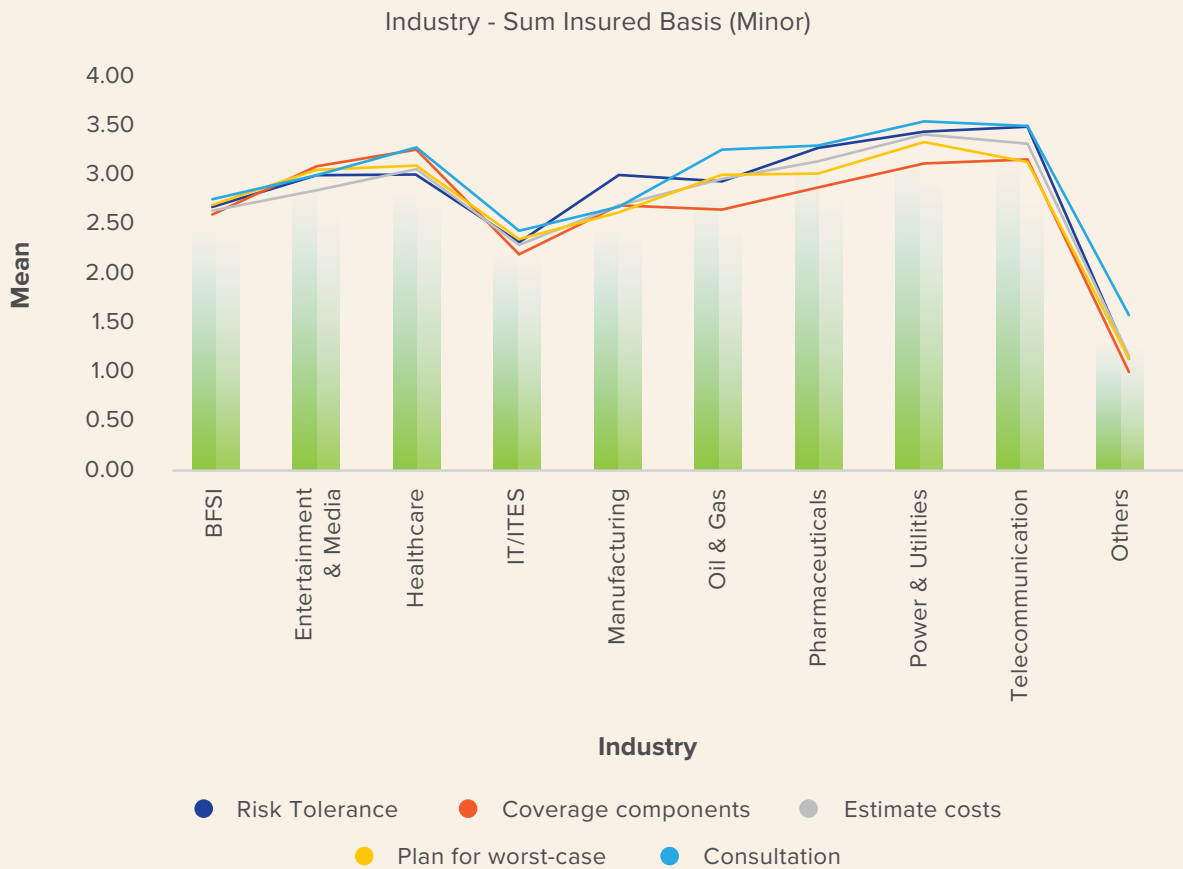
■ The graph highlights significant variance in perceived threat probabilities due to Third-Party Risks and Technology Complexity, particularly in sectors like Pharmaceuticals and Oil & Gas. This disparity suggests that although awareness exists, the adoption of comprehensive cyber coverage in these industries may lag due to challenges in addressing complex, industry-specific risks.

■ The analysis suggests that one-size-fits-all policies may not cater effectively to the distinct risk profiles across industries. Cyber insurers could expand market penetration by customizing policies to address industry-specific factors such as Size of Organization and Plan for Worst-Case Scenarios, providing comprehensive coverage for high-risk sectors such as Oil & Gas, and Pharmaceutical.

■ Industries scoring higher on Risk Assessment and Past Cyber Incidents have shown an increasing interest in cyber insurance, driven by regulatory compliance and historical incidents. This trend points to potential growth areas for cyber insurers, who can tailor offerings to address these recurring concerns, especially for industries like BFSI and IT/ITES.



Figure 6.6.6 Minor Basis for Sum Insured by Industry

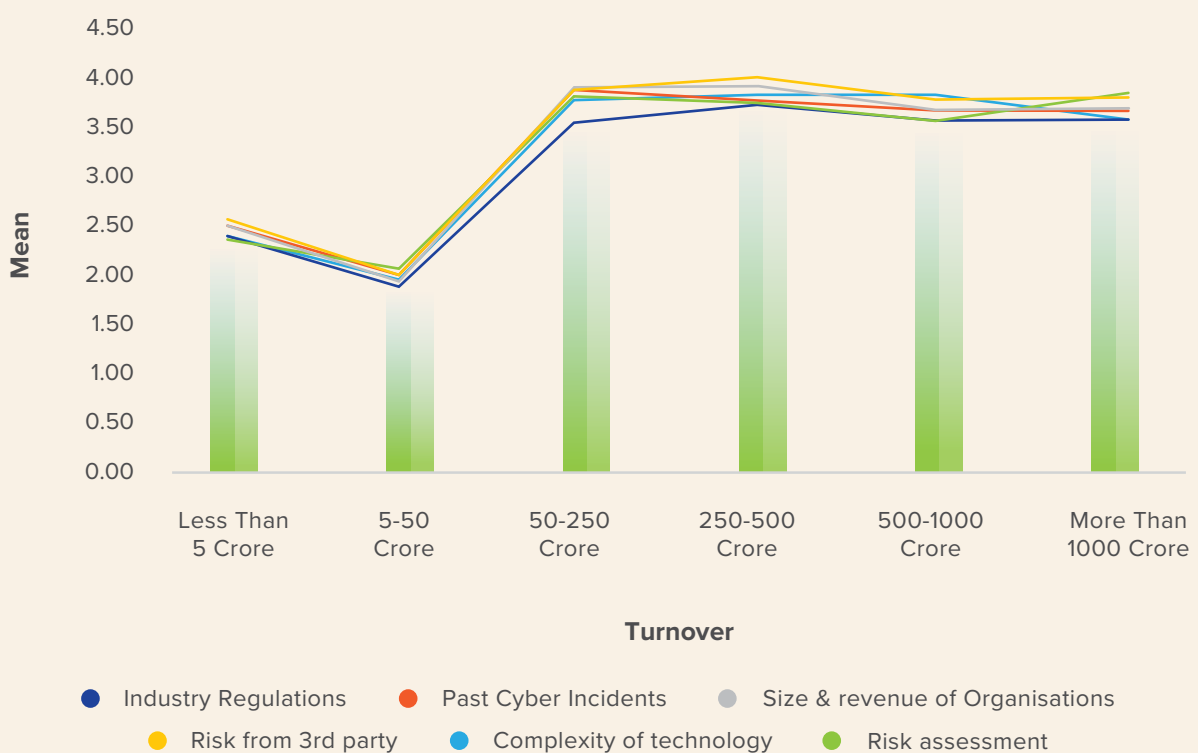


- Key sectors like BFSI, IT/ITES, and Telecommunications display higher average adoption scores for cyber insurance criteria such as Risk Tolerance and Coverage Components. This reflects real-world trends where these industries, due to high data sensitivity and regulatory pressures, prioritize comprehensive cyber coverage, while other sectors are more cautious or selective in adopting full coverage components.
- The graph shows that industries with complex operational needs, such as Pharmaceuticals and Manufacturing, exhibit lower scores for planning for Worst-Case Scenarios. This discrepancy points to an underestimation of the potential financial impact of cyber incidents, highlighting a need for insurers to raise awareness of comprehensive protection, especially for sectors with critical infrastructure dependencies.
- The differences in Risk Tolerance and Estimated Cost adoption across industries indicate that standardized policies may not fit all sectors effectively. Insurers could expand market reach by offering customized cyber insurance policies tailored to specific risk profiles and cost constraints, addressing the unique needs of high-risk and heavily regulated industries like BFSI and Healthcare.

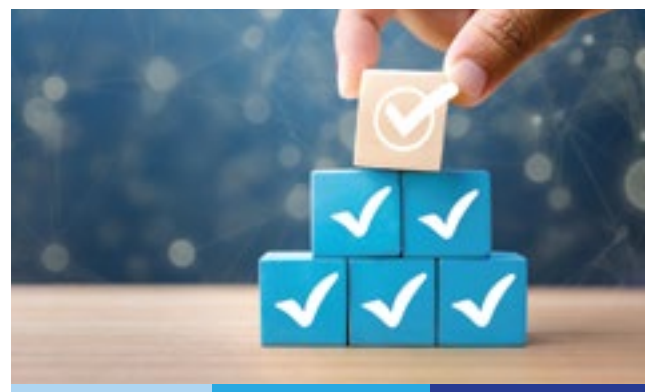
Lower scores for some industries in Consultation and Worst-Case Planning suggest a gap in understanding the full scope of cyber risks. This presents an opportunity for the project to focus on educating these industries about the importance of comprehensive coverage, ultimately aiding market expansion by helping companies better recognize the value of cyber insurance in protecting their assets and reputation.

Figure 6.6.7 Major Basis for Sum Insured by Turnover

Turnover - Sum Insured Basis (Major)



As turnover increases, the mean score for each sum insured criterion also rises, indicating that larger organizations tend to adopt more comprehensive cyber insurance criteria. This pattern suggests that higher turnover firms have both the resources and the risk awareness to prioritize a more robust cyber insurance framework.



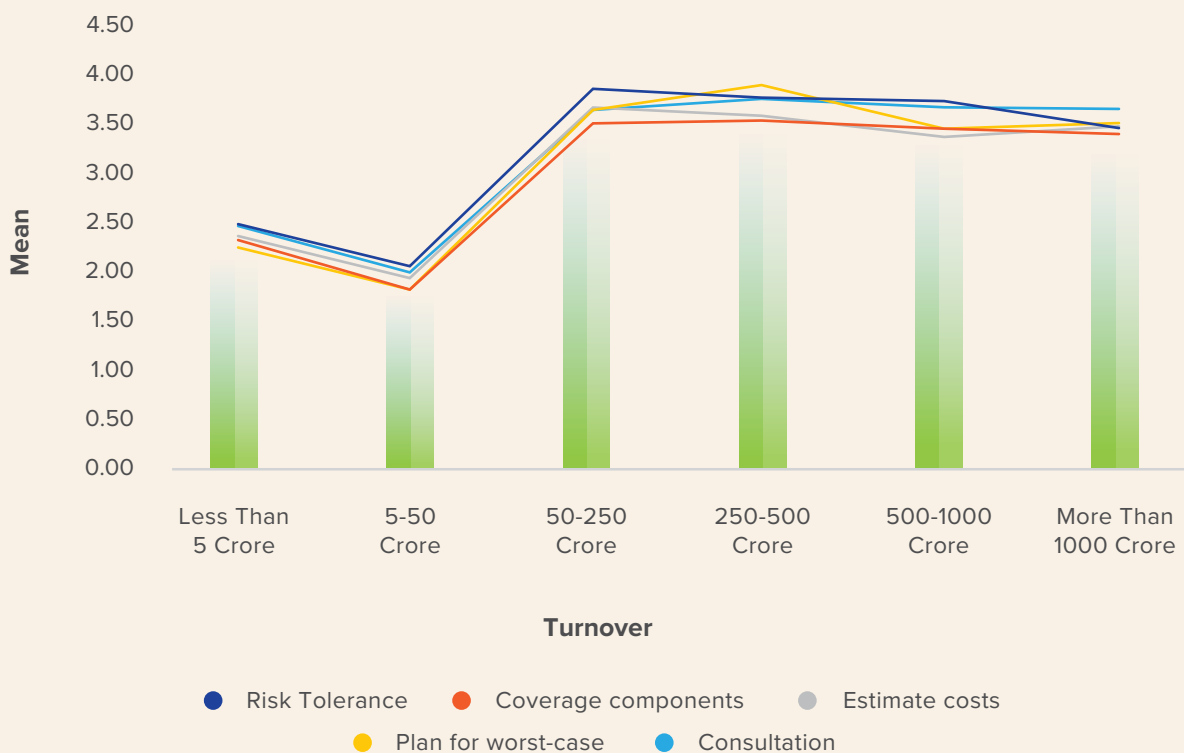
- After the 50-crore turnover mark, the mean scores for all insurance criteria converge closely, suggesting that beyond a certain size, organizations adopt similar levels of coverage, risk tolerance, and security assessments. This uniformity highlights a potential industry standard for cyber insurance adoption in medium to large organizations, driven by a combination of regulatory expectations and internal risk management practices.

High scores in criteria like "Industry Regulations" & "Risk from Third Parties" across turnover categories suggest that regulatory requirements and external dependencies are key drivers of cyber insurance adoption. Organizations recognize that compliance and third-party risks require structured insurance coverage to mitigate liability and ensure business continuity.

- The lower scores in organizations with less than 50 crore turnover indicate an opportunity to expand the cyber insurance market among smaller firms. These organizations may lack the perceived need or resources to meet higher insurance criteria. Offering simplified and cost-effective insurance solutions could increase adoption, enabling these firms to mitigate cyber risks effectively.

Figure 6.6.8 Minor Basis for Sum Insured by Turnover

Turnover - Sum Insured Basis (Minor)



- 
- There's a clear trend across turnover ranges, with lowest points in the 5-50 Crore segment (around 2.0) and highest peaks in the 250-500 Crore range (nearly 4.0), suggesting optimal risk-return balance is achieved in mid-to-high sum insured brackets.
 - All measured parameters (risk tolerance, coverage components, costs, worst-case scenarios, and consultation) show remarkable convergence in higher turnover brackets (>250 Crore), indicating that larger organizations have more standardized cyber insurance needs and assessment frameworks.
 - The sharp increase in all metrics from the 50-250 Crore bracket onwards aligns with current market dynamics where mid-sized companies are rapidly digitalizing, making them prime targets for cyber attacks and consequently driving higher insurance adoption and comprehensive coverage requirements.
 - The consistent high values (3.5-4.0 range) across all parameters in higher turnover segments, coupled with relatively lower values in sub-50 Crore segments, highlights an untapped market opportunity in the small-business segment where customized, scalable cyber insurance solutions could drive significant market expansion.

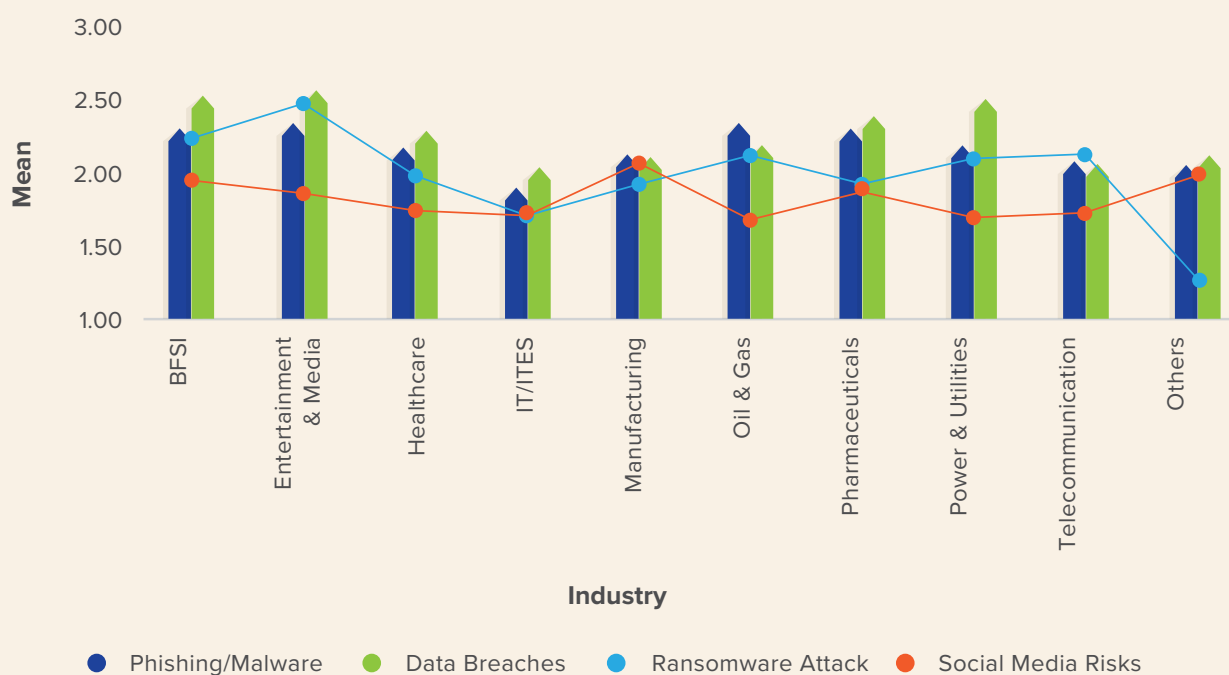
6.7. Cyber Risk Threat Probability, Cyber Losses, and Claims Analysis:

The Cyber Incidents / Threat Perceived Probability and Cyber Loss and Claim section explores the likelihood of cyber threats alongside actual losses and claims filed across industries and turnover brackets. This analysis reveals patterns in perceived versus actual risk, highlighting the frequency and impact of cyber incidents that influence insurance claims. By understanding these factors, businesses and insurers gain a clearer picture of industry-specific vulnerabilities, supporting informed decisions on coverage levels and risk mitigation strategies essential for effective cyber insurance planning.

Perception about Cyber Incidents / Threat Probability:

Figure 6.7.1 Threat Perception Probability by Industry

Cyber Risk Threat Perception Across Different Industries



- The graph shows significant variability in threat perception among industries, with certain sectors perceiving a moderate likelihood of cyber threats. This suggests that industries with more sensitive data or critical infrastructure (such as BFSI, healthcare, and telecommunications) recognize a moderate exposure to cyber risks, aligning with their reality of being frequent targets of cyberattacks.

Some industries may underestimate cyber threat probabilities relative to their actual risk. For example, manufacturing or oil & gas may perceive a lower threat probability, despite recent real-world attacks targeting operational technologies in these sectors. Addressing this gap could improve risk assessment accuracy, aligning perception with emerging cyber threat landscapes.

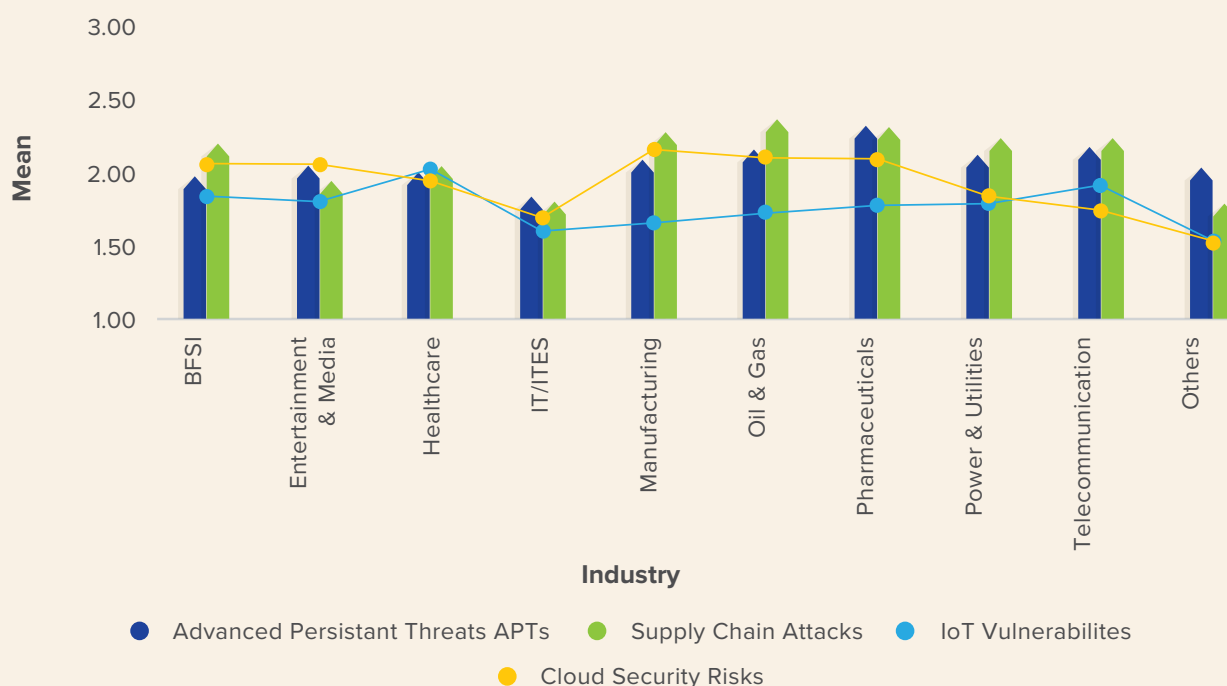


This varied perception of threat probability emphasizes the need for industry-specific cyber insurance products. Industries with higher threats might require coverage with broader protections, while those with lower risks could benefit from basic policies. This understanding enables insurers to create targeted solutions, meeting diverse needs and encouraging adoption across all sectors. However, it doesn't mean that the perceived low probability of the threats is accurate, instead, the entire perception of the industries is incorrect to the reality.

Industries with low perceived threat probabilities may be underestimating the necessity for cyber insurance, creating a market expansion opportunity. By educating these industries on emerging risks and the importance of proactive coverage, insurers can increase demand and improve overall cyber resilience. This strategy aligns with the broader goal of enhancing cyber insurance adoption to address evolving cyber threats across the economy.

Figure 6.7.2 Threat Perception Probability by Industry

Cyber Risk Threat Perception Across Different Industries



■ The graph depicts a diverse range of cyber threat probabilities across multiple industries, highlighting the pervasive nature of cybersecurity challenges facing organizations. This underscores the importance of a comprehensive, cross-industry approach to cyber risk management and insurance coverage.

■ The analysis reveals heightened threat probabilities in the Power & Utilities, Telecommunications, compared to the other industries. Although the overall threat probability of various threats to various industries is only at a moderate level, which is dangerous in the reality of the cyber world.

The real-world trends indicate that these industries are prime targets for malicious acts of cyber threats. However, the overall data doesn't align with real-world trends, where disruptions to critical infrastructure and financial systems can have cascading societal and economic consequences.

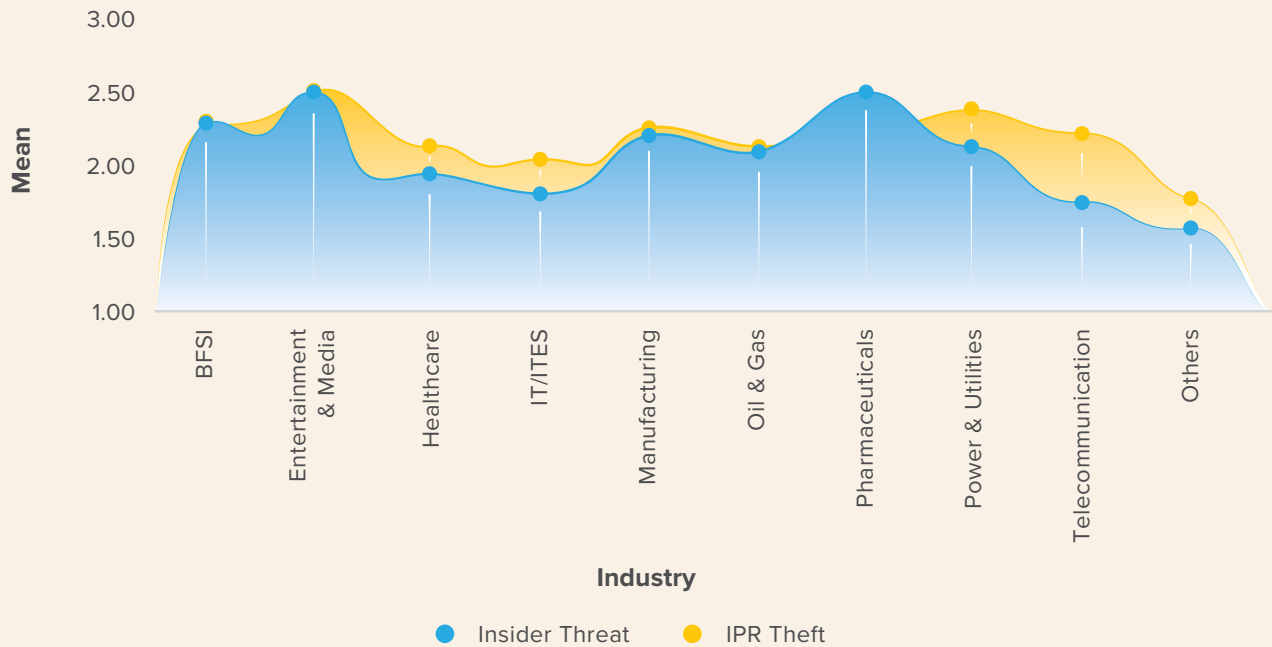
■ The study highlights parallel threat patterns between the Healthcare and Manufacturing sectors, particularly in the areas of Cloud Security Risks and Insider Threats. This suggests that the ongoing digital transformation of these industries has introduced new avenues for cyber attacks, requiring tailored risk management solutions.



■ While the analysis indicates some industries perceive lower cyber threat probabilities, cyber insurers should proactively address this gap. By educating organizations on the evolving nature of cyber risks and the importance of comprehensive insurance coverage, the marketing or educational campaign should drive broader market adoption and position cyber insurance as an essential risk management tool, regardless of industry-specific threat perceptions.

Figure 6.7.3 Threat Perception Probability on Insider Threats and IPR Theft

Perception about Insider Threats and IPR Theft

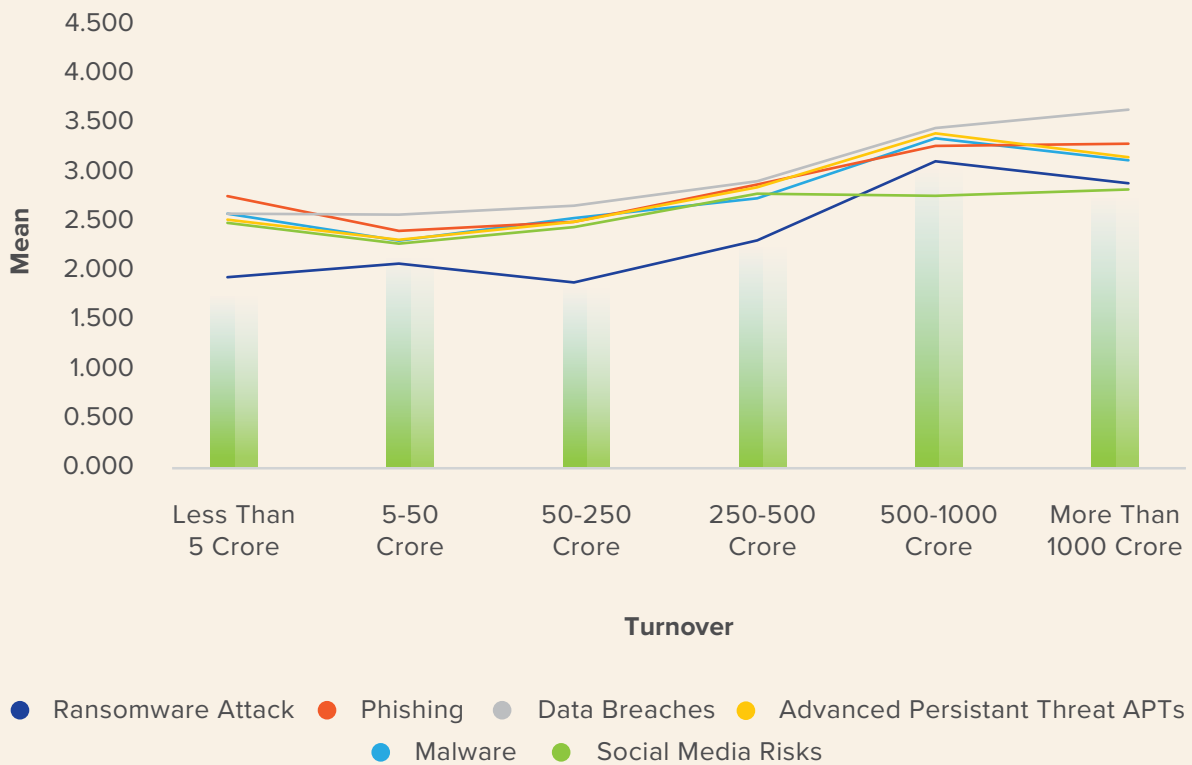


As indicated in the above chart (figure-3), a large number of respondents perceive the Intellectual Property Rights (IPR) and Insider Threats by the employees of the companies as low to moderate risk. However, the recent cyber intelligence report highlights that Media companies, pharma and manufacturing companies, the IPR breach, and insider threats are increasing and the companies need to take cognizance of these risks and develop appropriate mitigation measures to minimize them.



Figure 6.7.4 Major Perceived Threat Probability by Turnover

Turnover - Threat Probability (Major)



- The analysis indicates a general trend where the perceived probability of threats such as ransomware, phishing, and data breaches increases with a rise in turnover. Organizations with larger turnovers (over ₹250 crore) see these threats as more probable. This suggests that larger firms recognize their heightened vulnerability due to greater digital footprints, data sensitivity, and potentially larger attack surfaces.

Despite an overall increasing trend, it is evident that the threats are perceived as only moderate across all turnover brackets. Besides, specific threats like ransomware and advanced persistent threats (APTs) demonstrate more marked increases compared to others. The sharp rise in the perception of ransomware threats suggests that businesses of all sizes increasingly consider ransomware as a significant and potentially devastating threat, reflecting the real-world scenario where ransomware incidents have skyrocketed in the past years, causing operational disruptions and financial losses.

- Although the rise in perception of certain threats is not adequate to counteract the cyber risks associated with any organization, the average value suggests a moderate perception only.

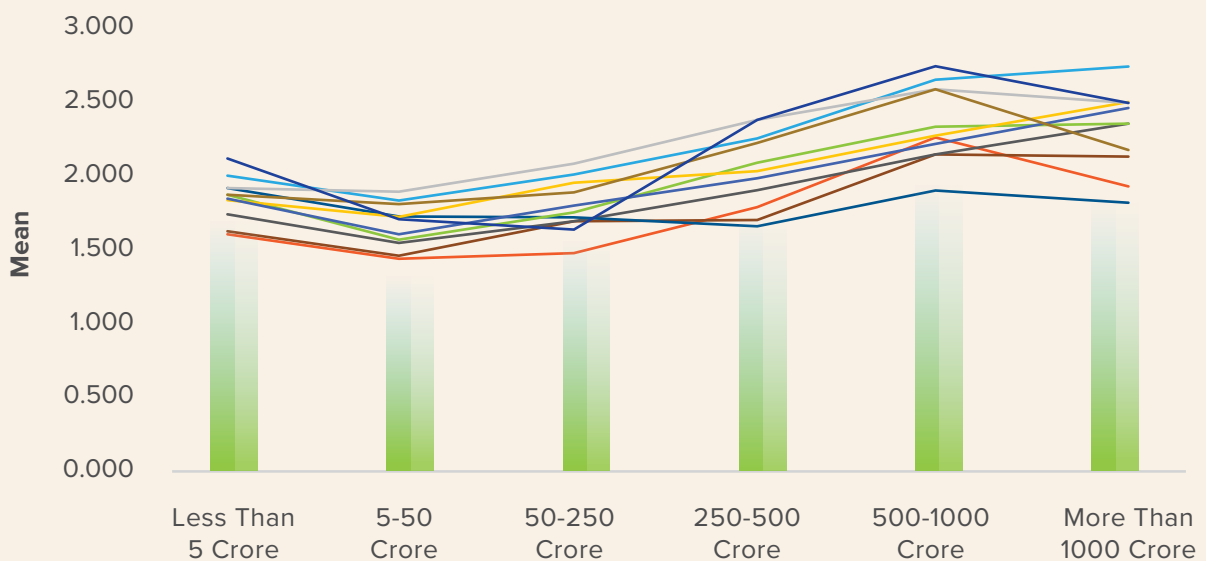
Understanding the variance in perceived threat probabilities across firms of different turnovers provides crucial insights for the cyber insurance project. It suggests that firms with higher turnovers require more specialized and targeted insurance solutions, given their heightened concerns for specific threats like ransomware and phishing. This can guide product development and policy structuring in the cyber insurance market.

The correlation between increasing turnover and perceived threat probability emphasizes the opportunity for expansion in the cyber insurance market, particularly targeting larger firms. It reveals the necessity for tailored insurance packages that address the needs of large-scale firms, which could serve as a lucrative entry point for insurers. Furthermore, the disparity in perceived threats indicates the need for a dynamic risk assessment model that adapts to evolving digital threat landscapes.



Figure 6.7.5 Minor Perceived Threat Probability by Turnover

Turnover - Threat Probability (Minor)



- The study shows a clear positive correlation between turnover and the mean threat probability perception scores across various insurance criteria. This indicates that larger organizations with higher turnovers tend to adopt more comprehensive cyber insurance coverage. This pattern suggests that higher-turnover firms have the resources, risk awareness, and incentive to prioritize a robust cyber insurance framework to manage their heightened cyber risk exposure.

- Although, the analysis depicts only a moderate rise in cyber threat probabilities across organizations of all turnover sizes, indicating that businesses, regardless of their scale, are facing an increasingly complex array of cyber risks. This trend suggests a widespread vulnerability to threats ranging from supply chain attacks and insider breaches to financial and intellectual property theft.

While the analysis indicates that organizations may perceive lower cyber threat probabilities, the cyber insurance project should proactively address this gap. By educating businesses on the evolving nature of cyber risks and the importance of comprehensive insurance coverage, the project can drive broader market adoption and position cyber insurance as an essential risk management tool, regardless of an organization's specific threat perceptions. This approach will ensure the project's long-term success and the continued expansion of the cyber insurance market.

Perception about Cyber Incidents, and Cyber Loss Experience:

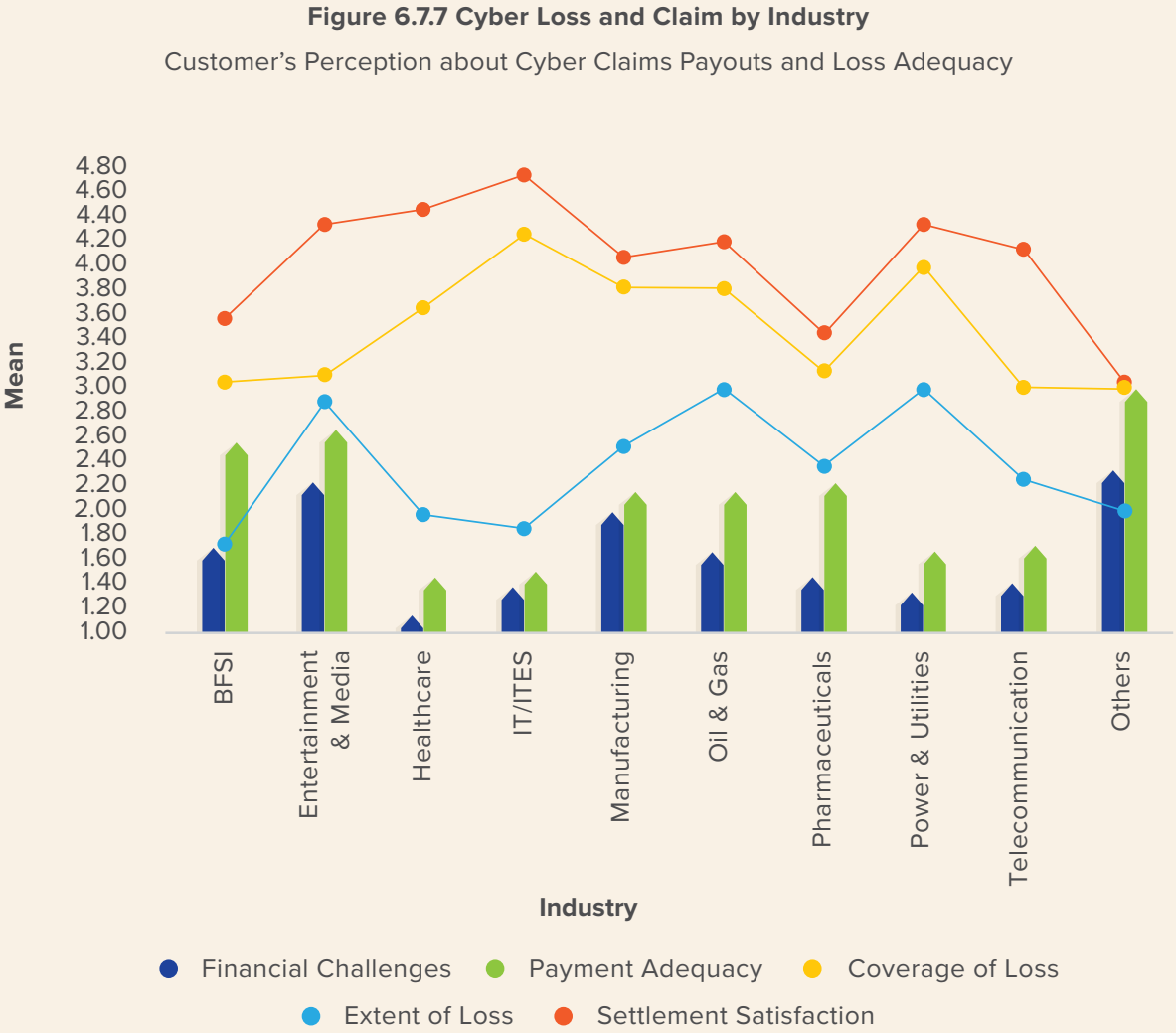
- This specific graph reflects the distribution of the cyber incidents among the respondents.
- The majority of respondents (70%) reported no occurrence of cyber incidents, while a smaller but significant portion did report incidents. This suggests that while cyber incidents are not universally experienced, they are prevalent enough to warrant attention, particularly in certain sectors or among specific types of businesses.
- This trend may reflect an underestimation of cyber risks, as many businesses may lack sufficient detection systems or reporting standards, resulting in an apparent low incident rate. In reality, the frequency of unreported or undetected cyber threats could be much higher, hinting at a gap in cyber threat awareness and risk perception.

Figure 6.7.6 Cyber Incident Distribution



The data highlights an opportunity to position cyber insurance as a critical safety net, especially for companies that may believe they are not at risk. By addressing misconceptions about cyber threat prevalence, the project can raise awareness of hidden vulnerabilities and promote cyber insurance as a proactive measure.

This distribution indicates a significant market opportunity. Educating businesses about the latent risks and potential financial impacts of cyber incidents can drive the expansion of cyber insurance adoption, encouraging more companies to protect themselves before experiencing an attack.



The line representing "Extent of Loss" shows significant variation across different industries, indicating that the impact of cyber incidents varies widely. For example, industries like IT/ITES and Pharmaceuticals experience higher losses, pointing toward greater exposure to cyber risks. This disparity underlines the need for customized cyber insurance policies that account for the sector-specific risk exposure.

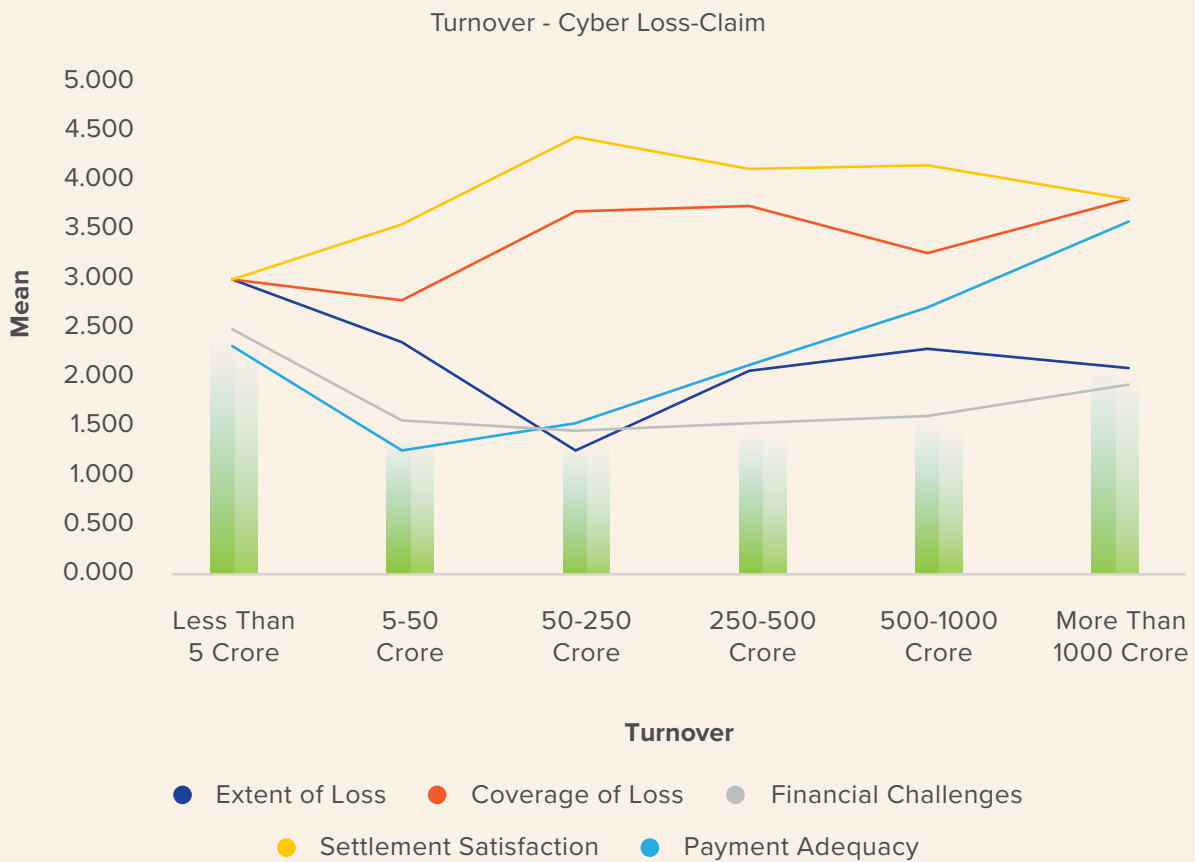
■ The lines for "Coverage of Loss" and "Settlement Satisfaction" indicate that industries like Healthcare and Telecommunications have relatively higher satisfaction with the settlement but experience inconsistent loss coverage adequacy. This suggests that while claim processes may be efficient, policyholders could still be facing financial gaps in cyber incident coverage, highlighting a mismatch between perceived satisfaction and actual risk coverage.

■ The "Financial Challenges" metric shows consistent trends across industries, indicating that the cost burden following cyber incidents remains a critical challenge. The relatively lower mean values here reveal the financial struggles industries face despite having insurance coverage, which emphasizes the need for re-evaluating policy structures and coverages to better support businesses in mitigating financial hardships.

The trends highlighted in the graph reveal an underlying inconsistency in the adoption and effectiveness of cyber insurance across industries. This suggests that while cyber insurance policies are being adopted, there is a need for strategic alignment with industry-specific requirements and a push towards tailored offerings. Focusing on sectors with high loss exposure, like IT and Pharmaceuticals, and addressing the gaps in coverage and financial support can help foster market expansion and strengthen trust in the value of cyber insurance.



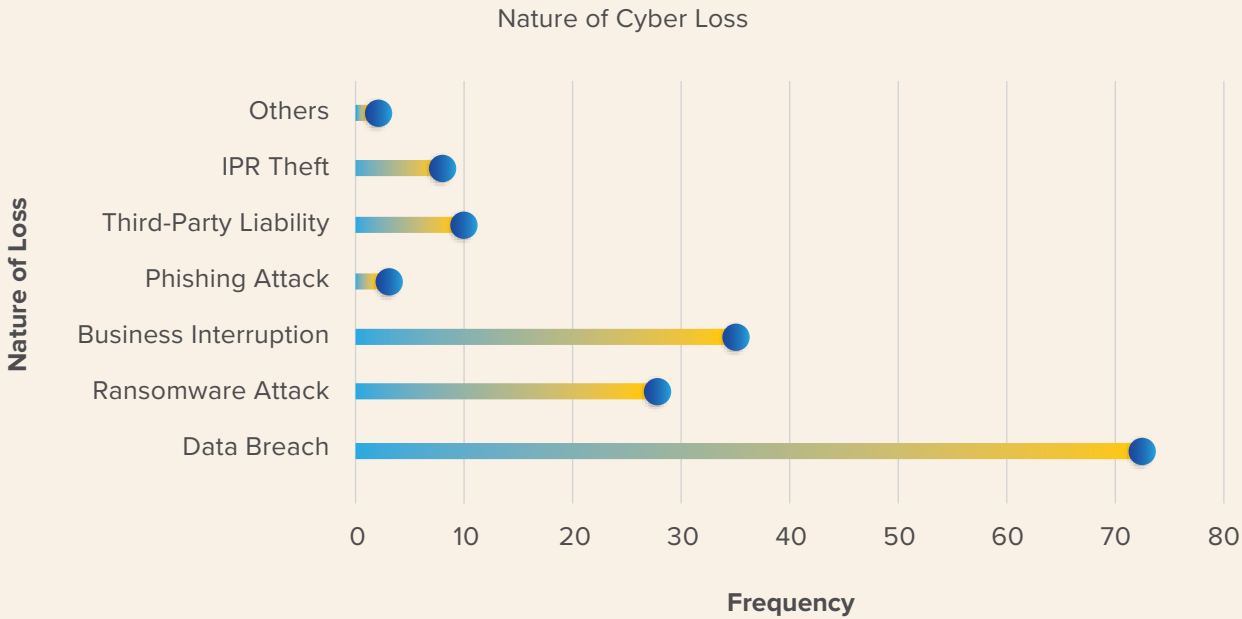
Figure 6.7.8 Cyber Loss and Claim by Turnover



- The analysis indicates that as turnover increases, there is an upward trend in "Coverage of Loss" and "Settlement Satisfaction" metrics. This suggests that larger organizations with higher turnovers are better equipped or more proactive in securing comprehensive cyber insurance policies. It points towards a disparity where smaller businesses may face challenges in acquiring adequate coverage due to limited resources or negotiation leverage.
- Both "Financial Challenges" and "Payment Adequacy" lines show relatively flat trends across turnover levels, indicating that even larger organizations are not immune to financial burdens despite seemingly comprehensive coverage. This disconnect reflects that insurance policy structures may not be fully addressing the actual financial impact of cyber incidents, leaving companies exposed regardless of their size.
- The "Extent of Loss" metric remains relatively higher for firms with moderate turnovers (50–250 Crore) but dips towards the higher turnover end. This might indicate that mid-sized companies face proportionally higher losses compared to smaller or larger firms, possibly due to their limited cybersecurity resources combined with significant digital footprints. This pattern highlights the necessity for scalable cyber insurance models that accommodate the diverse threat landscapes and resilience levels of businesses of different sizes.

The varying trends across turnover levels underscore the need for differentiation in cyber insurance offerings. For instance, targeting mid-sized firms with tailored policies and enhanced support structures could address their disproportionate loss levels, thereby boosting their confidence in adopting cyber insurance. Additionally, efforts to bridge the financial gap and improve payment adequacy for all turnover categories can help establish a more resilient market presence and drive expansion in sectors previously hesitant to invest in cyber insurance.

Figure 6.7.9 Nature of Cyber Loss and its frequency



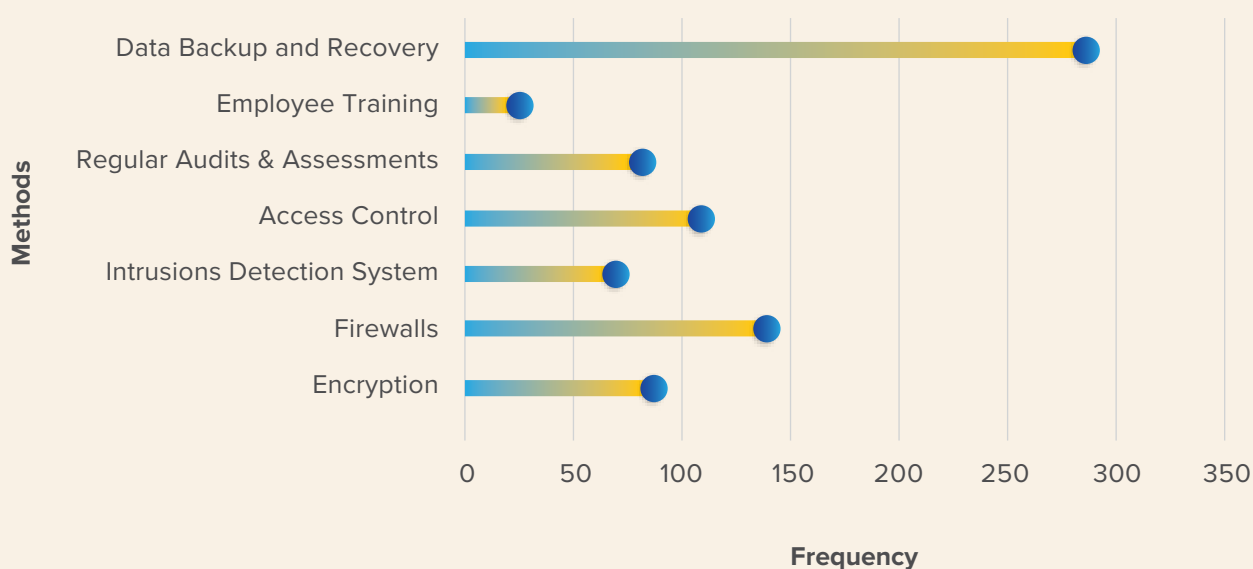
- The respective graph illustrates the distribution of the nature of cyber loss during the cyber incident, a cyber attack faced by the organization.
- The most common type of loss reported is Data Breach, followed closely by Business Interruption and Ransomware Attacks. This distribution suggests that cyber incidents often lead to significant operational and data-related disruptions, which can severely impact business continuity and reputation.
- Understanding the types of losses most commonly experienced helps tailor the cyber insurance product to cover high-impact incidents. Prioritizing coverage for data breach recovery, business interruption costs, and ransomware response can enhance the product's appeal and ensure it meets the critical needs of potential customers.
- The prevalence of data breaches and business interruptions aligns with current global cyber risk trends, where data theft and downtime are increasingly common due to sophisticated attacks. The high frequency of ransomware attacks further reflects the growing threat landscape, where attackers often target companies for quick financial gains, leveraging stolen or encrypted data.



- The variety in loss types suggests an opportunity for the cyber insurance market to grow by offering comprehensive policies that address specific risks like data breaches, ransomware, and operational disruptions. By addressing these diverse loss types, the market can appeal to a wider range of businesses, promoting the importance of cyber resilience across sectors.

Figure 6.7.10 Methods of Data Storage and Protection

Data Storage and Protection Methods Distribution

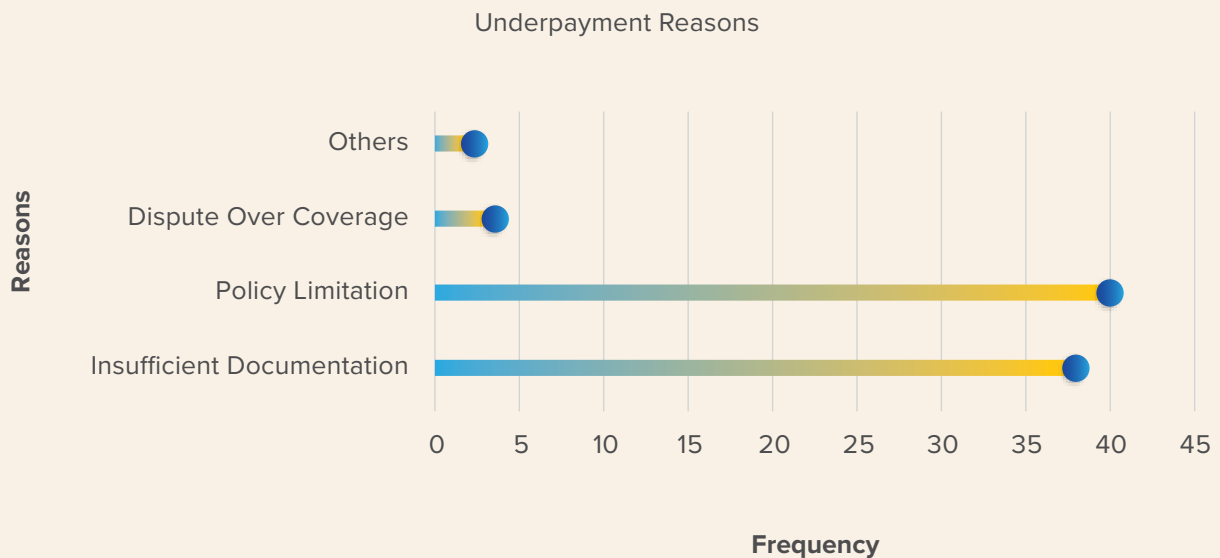


- This respective graph above reflects the distribution of the methods of how data is monitored, stored, and protected.
- Among that, the graph highlights Data Backup and Recovery as the most frequently used method for data protection, surpassing all other measures. This underscores the heavy emphasis organizations place on recovery solutions to mitigate data loss. However, it indicates a potential gap in proactive defense, as reliance on recovery alone does not prevent breaches but only mitigates their impact.
- Firewalls, Access Control, and Regular Audits and Assessments show a low moderate adoption, indicating that though organizations are utilizing some level of multi-layered security, initial threat detection through auto-intrusion testing, regular conduct of cyber auditing and penetration testing are not frequently done. This reflects about lack of awareness of diverse risk mitigation.

- Employee Training shows a notably low frequency, revealing a significant gap in focusing on human elements of cybersecurity. This is concerning as studies consistently highlight that human error is a primary cause of breaches.

For the project and the broader cyber insurance market, these findings suggest that insurers can play a crucial advisory role by encouraging comprehensive protection strategies that include proactive, human-centric measures. By addressing the disparity in protection practices, cyber insurers can enhance policy structures, promote better risk management, and support market growth through targeted recommendations that bolster an organization's defense posture.

Figure 6.7.11 Reasons for the Underpayment of Cyber Insurance



- This graphical distribution illustrates the reasons for the underpayment or insufficient payment of the cyber insurance amount in the occurrence of a cyber attack and cyber loss.
- Evidently, the policy limitation is the major reason across the data for the insufficient payment of cyber insurance. This remarkably indicates the limitation of the existing policies, which are clearly inadequate to the growing world of cyber threats. The existing policies have to be altered and subjected to changes to match the growing cyber threats so that they can be covered adequately in case of an event.
- Insufficient documentation is in close proximity to the policy limitation. The lack of awareness of organizations regarding the threats and risks in the cyber world leads to the inefficiency of not filing sufficient documents regarding the same. This clearly marks the need for better knowledge regarding the existing threats and risks.

- The expansion of the cyber insurance market within the organizations can only be progressed with better practices regarding cyber insurance and better tailored cyber insurance products that overcome the policy limitations and cover the growing threats of the cyber world.

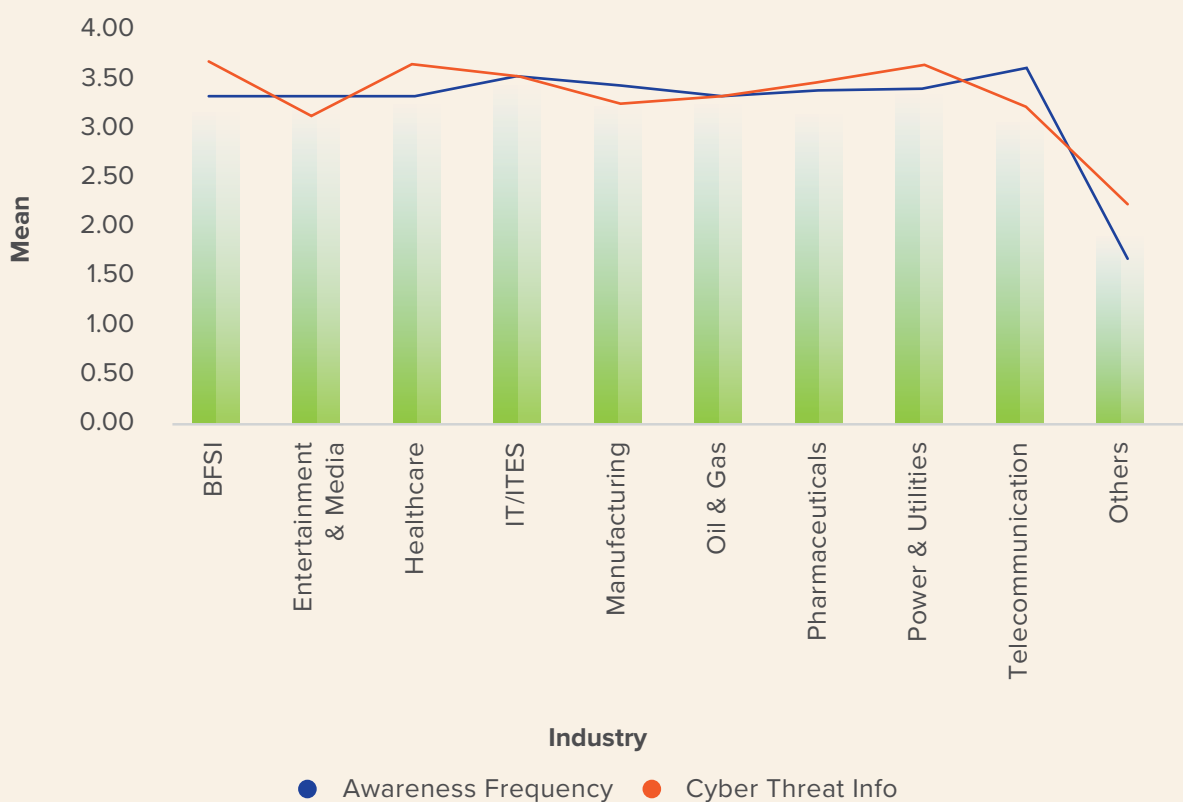


6.8. Cyber Risk Mitigation Measures

The Cyber Security Risk Mitigations section examines the range of proactive measures industries adopt to minimize cyber risks, tailored by industry type and business turnover. This section highlights the alignment of specific mitigation strategies with perceived risk levels, showcasing how businesses prioritize and implement safeguards to protect against cyber threats. These insights are essential for understanding the preventative approaches that reduce the likelihood of incidents, directly influencing the structure and requirements of effective cyber insurance policies.

Figure 6.8.1 Cyber Security Awareness by Industry

Industry – Cyber Security Awareness



- The graph reveals a generally high level of awareness in industries like BFSI, IT/ITES, and Telecommunications regarding both general cybersecurity awareness and specific cyber threat intelligence. This trend aligns with real-world conditions where these sectors are prime targets for cyber threats due to sensitive data handling, prompting higher awareness levels and a proactive stance toward cyber defense.

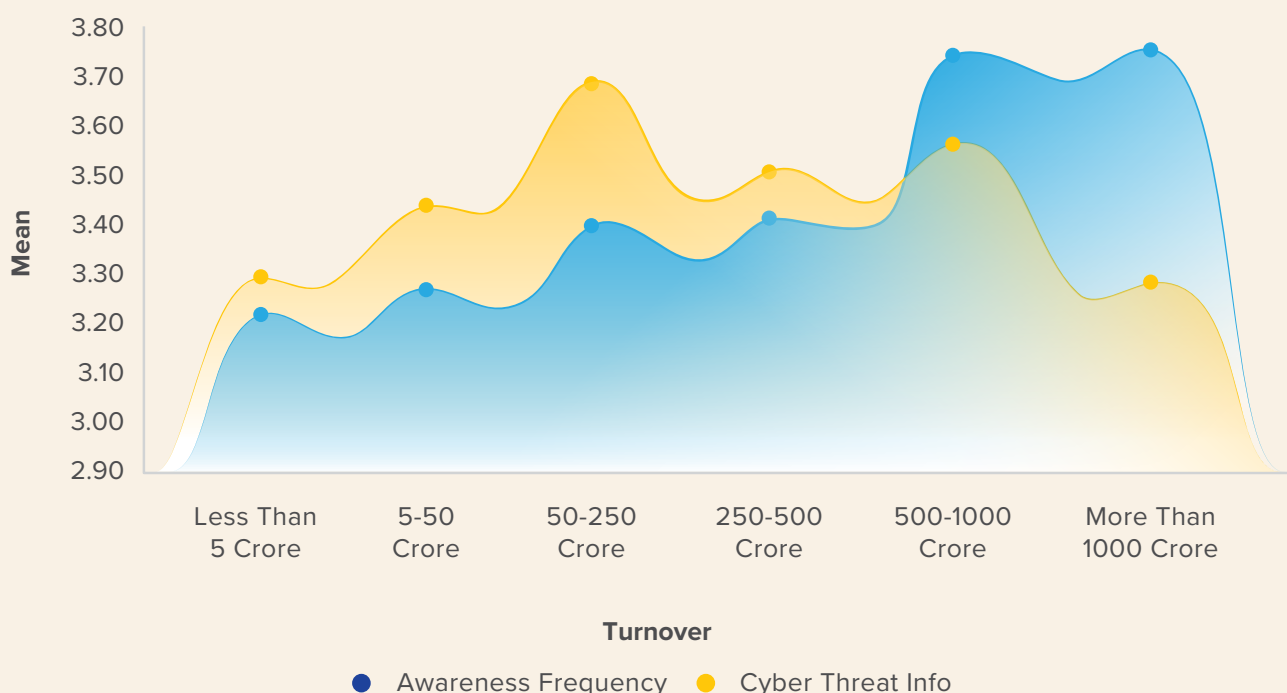
- In industries like Healthcare and Manufacturing, there is a noticeable dip in awareness frequency and cyber threat information, highlighting a potential vulnerability. This disparity between awareness and threat levels in these critical sectors reflects real-world challenges, as they often prioritize operational continuity over cybersecurity investments, potentially exposing gaps that cyber insurance can help mitigate.
- Identifying sectors with lower awareness and cyber threat intelligence, such as Pharmaceuticals and Oil & Gas, offers a strategic avenue for cyber insurance providers. These sectors present opportunities to educate and promote customized insurance products, addressing industry-specific risks while highlighting the necessity of insurance as a risk mitigation tool.



- As awareness grows across diverse industries, there is a clear opportunity for the cyber insurance market to expand by developing targeted products that cater to sectors with both high and moderate awareness levels. Emphasizing comprehensive coverage for industries with higher threat perceptions (like BFSI and Telecommunications) alongside awareness-raising efforts in lagging sectors can foster market growth and increase overall cyber resilience across industries.

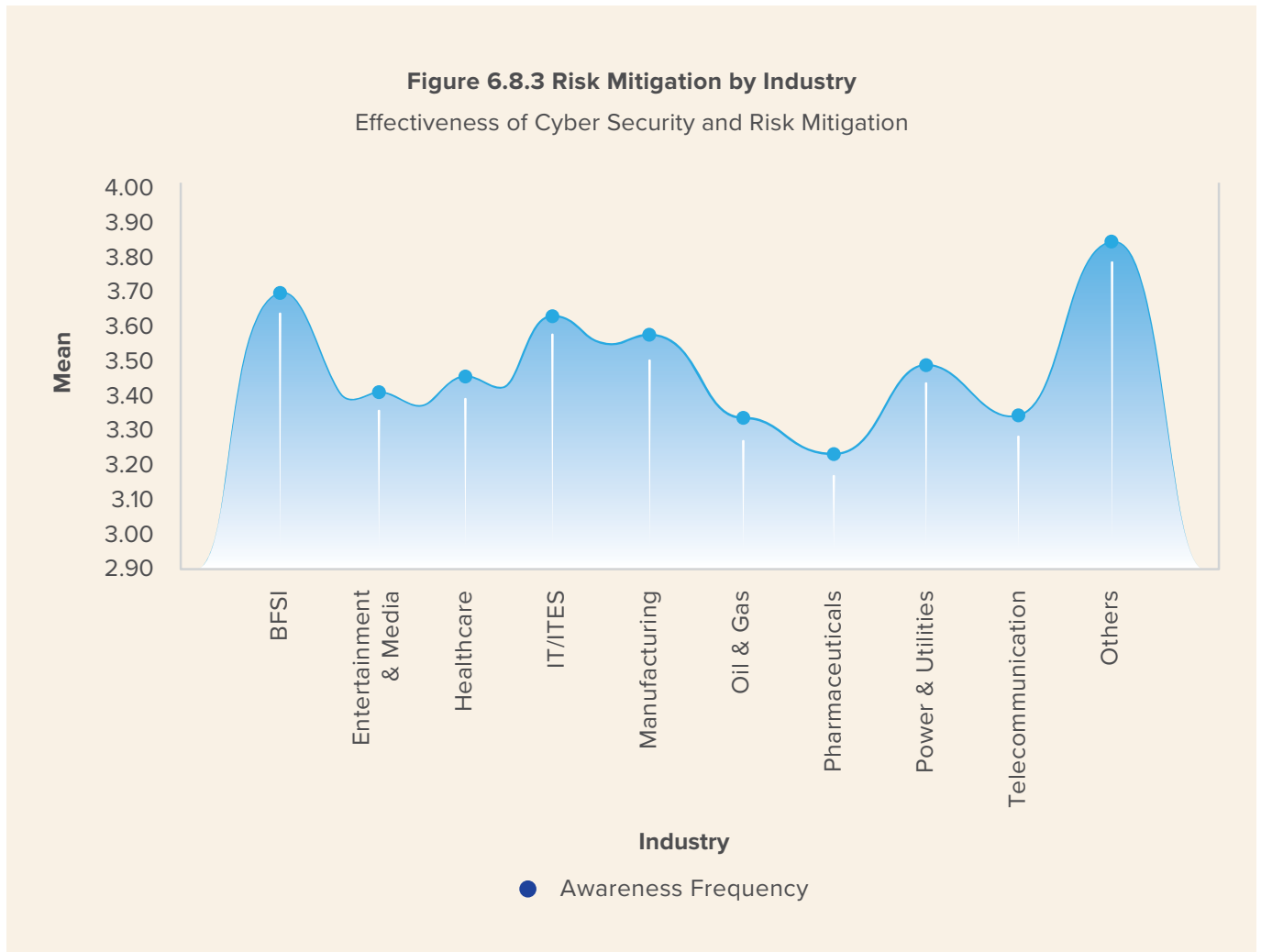
Figure 6.8.2 Cyber Security Awareness by Turnover

Turnover – Cyber Security Awareness



- The “Awareness Frequency” line shows a consistent upward trend as turnover increases, reflecting a correlation between larger financial capabilities and more frequent cybersecurity awareness initiatives. This trend suggests that larger organizations invest more in raising awareness, possibly due to greater regulatory pressures or higher stakes in mitigating cyber risks.
- The “Cyber Threat Information” line peaks in the 250–500 Crore turnover range and then declines. This implies that businesses in this turnover category might have more active information-sharing practices or greater emphasis on threat intelligence. However, the decline at higher turnover levels might indicate a potential overconfidence in existing defenses or a shift towards in-house security measures rather than external threat-sharing.
- Despite the rising trend of awareness frequency with turnover, the graph shows a disparity where smaller firms (with less than 50 Crore turnover) lag in both awareness and threat information. This gap underscores the persistent challenge of accessibility to resources and expertise for smaller businesses, posing a significant vulnerability in the broader cybersecurity landscape.

The observed trends pointing to the need for cyber insurance products that are tailored not only to financial capacity but also to cybersecurity maturity. Insurers could leverage these insights to offer bundled services that enhance threat information sharing for larger firms while supporting awareness-building initiatives for smaller firms. This approach would not only strengthen risk mitigation but also expand the market’s appeal to a broader range of businesses, fostering a more resilient and proactive client base.



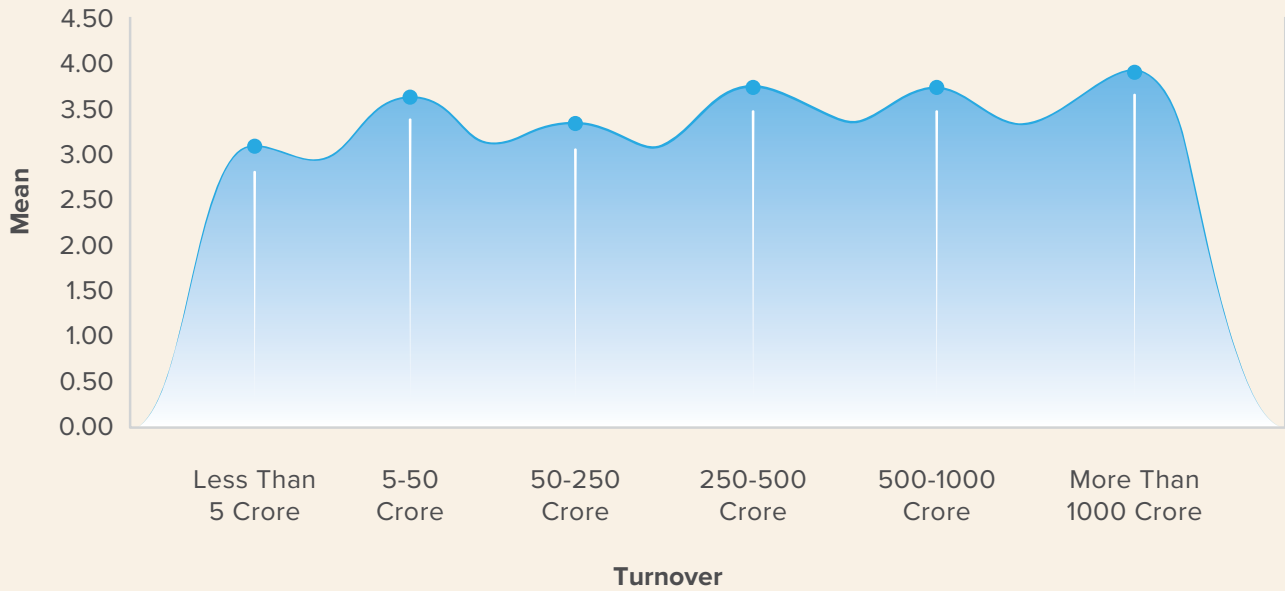
- The effectiveness scores across industries mainly hover between 3.5 and 4.3, indicating a generally positive assessment of cybersecurity and risk mitigation measures. However, there are variations, with certain sectors like Pharmaceuticals and Oil & Gas scoring slightly lower compared to others such as Power & Utilities, which reflects varying levels of cyber preparedness across industries.

Industries with high infrastructure vulnerability, such as Oil & Gas, show lower effectiveness in cybersecurity and risk mitigation. This aligns with real-world challenges, as these sectors often face complex, legacy systems and have historically been more vulnerable to cyber threats, compared to more tech-integrated sectors like IT/ITES. The variability in effectiveness highlights the opportunity for cyber insurance providers to tailor solutions based on specific industry needs. For instance, sectors like Pharmaceuticals and Oil & Gas may benefit from more comprehensive or specialized cyber insurance policies, focusing on mitigating their unique cyber risks and bolstering their security gaps.

With industries like Power & Utilities showing better cybersecurity scores, insurers might target sectors with lower scores to expand the cyber insurance market. Providing risk mitigation insights and financial protection can be pivotal in gaining trust and increasing cyber insurance adoption across sectors that may currently underestimate or underfund cybersecurity.



Figure 6.8.4 Risk Mitigation by Turnover
Effectiveness of Cyber Security and Risk Mitigation



The effectiveness scores generally increase with revenue size, starting from around 3.3 for companies with less than 5 Crore to about 4.0 for those with more than 1000 Crore. This pattern suggests that larger companies tend to invest more in cybersecurity and risk mitigation, likely due to greater resources and awareness of cyber risks.

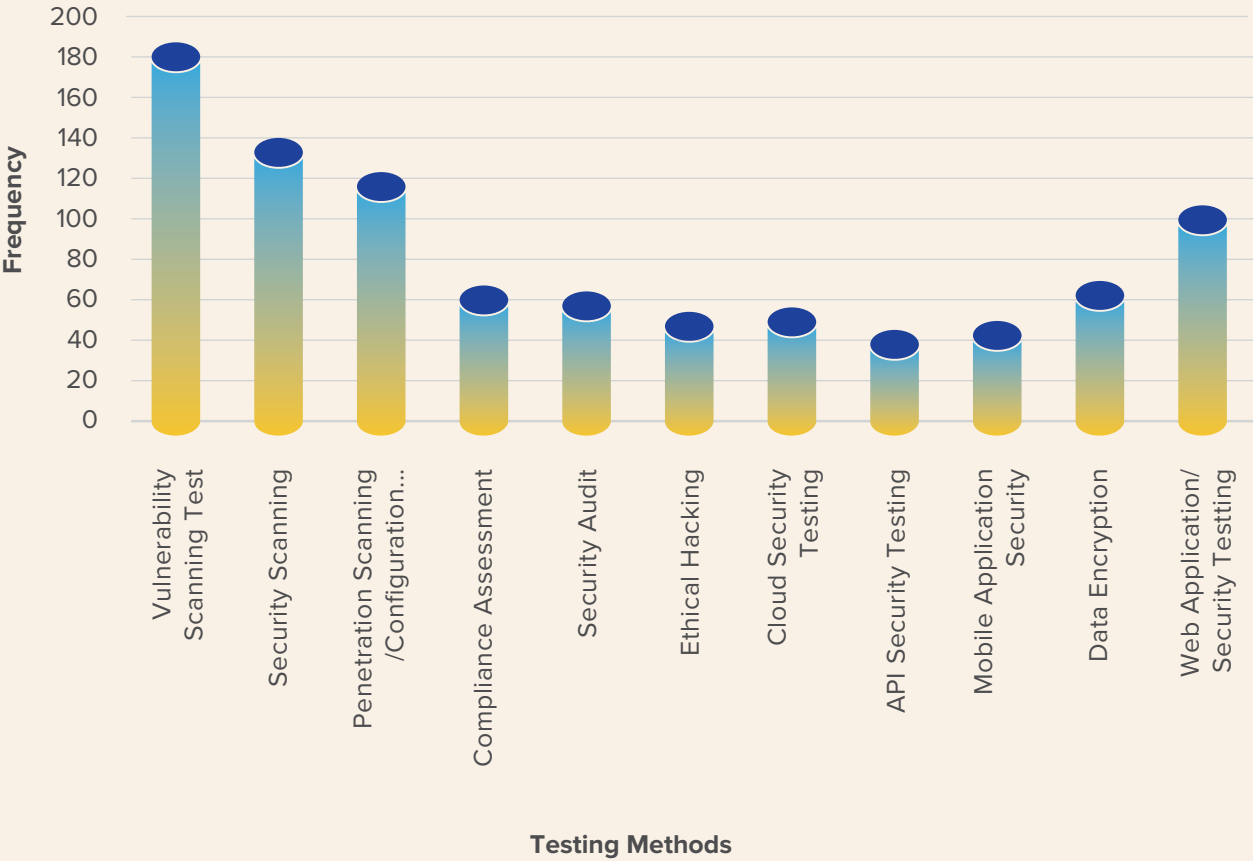
This trend reflects a real-world scenario where high-revenue organizations are often better equipped to handle cyber threats due to bigger budgets, more sophisticated systems, and dedicated cybersecurity teams. Smaller companies, with limited resources, may struggle to implement advanced security measures, leaving them more vulnerable to cyber risks.

Understanding the disparity in cybersecurity effectiveness by revenue size is crucial for cyber insurance projects. Insurers can target smaller and mid-sized companies with tailored insurance solutions and cybersecurity resources to address their specific vulnerabilities. This targeted approach would address a gap in the market, as smaller businesses may need more support in risk mitigation.

As smaller companies show lower cybersecurity effectiveness, there is a growth opportunity for the cyber insurance market to expand into this segment. Cyber insurance products designed to support cybersecurity improvement can drive market adoption in lower-revenue brackets, fostering resilience and encouraging more widespread use of cyber insurance.

Figure 6.8.5 Testing Methods for Assessing Cyber Risks

Testing Methods Distribution



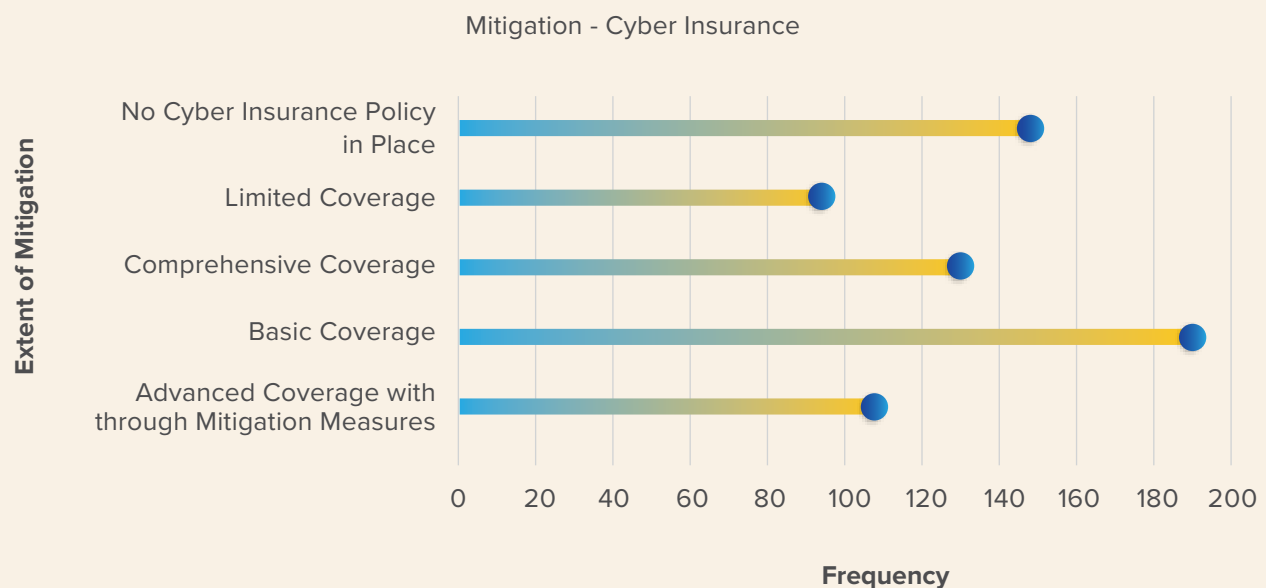
This particular graphical distribution illustrates the testing methods adopted by the organizations to mitigate their cyber risks.

The Vulnerability Scanning Test is the most commonly adopted method, standing out with the highest frequency among all testing approaches. This highlights that organizations prioritize identifying weaknesses in their systems but may not equally focus on deeper, more targeted testing like penetration tests. This reliance on surface-level assessments can leave critical security gaps unaddressed.



- Penetration Scanning/Configuration Assessment and Security Scanning are utilized at moderate levels, suggesting organizations acknowledge the need for more comprehensive checks. However, this moderate adoption may not suffice in the current cyber threat landscape.
- Techniques such as Web Application/Security Testing and Mobile Application Security have relatively lower frequencies, pointing to potential vulnerabilities in securing application-specific risks. This reflects a possible underestimation of the specialized nature of cyber threats that target specific layers, which may leave these areas insufficiently protected.
- The variation in the use of different testing methods underscores an opportunity for cyber insurers to emphasize the importance of adopting a full spectrum of risk assessments. By promoting a broader implementation of diverse testing methods, insurers can help clients mitigate risks more effectively, fostering trust and driving market growth.

Figure 6.8.6 Types of mitigation through Cyber Insurance

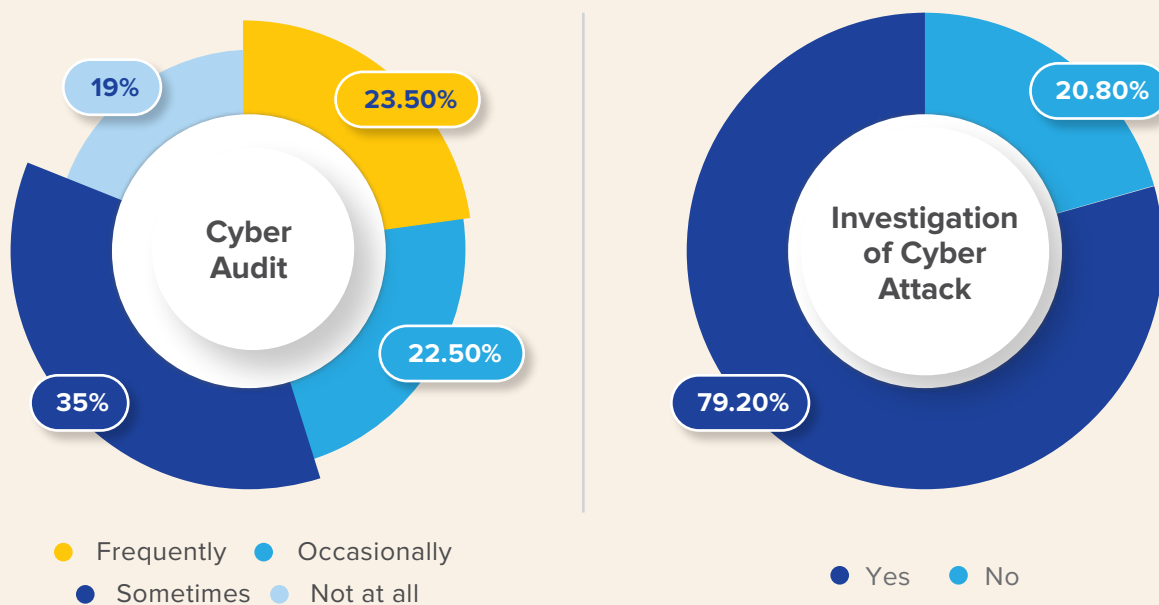


- This specific graph displays the distribution of the extent of mitigation of cyber loss and liabilities with the purchase and existence of a cyber insurance policy.
- The graph shows that Basic Coverage is the most common extent of cyber insurance among organizations. While this indicates an acknowledgment of the need for insurance, it also suggests a lack of comprehensive protection. Basic coverage may only partially mitigate liabilities and losses, potentially leaving organizations vulnerable to substantial financial impacts from severe incidents.
- Advanced Coverage with Thorough Mitigation Measures has a notably lower frequency, highlighting that few organizations opt for policies that provide extensive protection. This disparity may reflect cost considerations or a lack of awareness about the benefits of advanced coverage. As cyber threats continue to evolve, this gap points to an area of potential risk where firms may face greater exposure to sophisticated cyber-attacks.

A considerable number of organizations report having No Cyber Insurance Policy in Place, revealing a substantial vulnerability within the industry. This aligns with real-world reports where businesses, especially smaller ones, often underestimate the risk or lack the resources to invest in insurance. This gap represents an opportunity for targeted education and tailored policy solutions to expand market penetration.

- The findings emphasize the importance of educating potential clients on the value of Comprehensive Coverage and encouraging more robust risk management strategies. For the project and the cyber insurance market, addressing the disparity in the adoption of thorough coverage can drive growth and foster a more resilient customer base.

Figure 6.8.7 : Frequency of Cyber Audit and Investigation of Cyber Attack for Loss Recovery



- As it can be seen from the above chart only 20% of the companies carry out cyber forensic investigations post cyber attacks. Similarly, only about 23% of organizations conduct frequent security drills or cyber intrusion tests.



- As a result, there has been considerable delay in data recovery, the meantime of data recovery is 3-7 days post-attack, and nearly 60% of the organizations, ' data recovery time is above 7 days. Even for the critical infrastructure-related data also the delay is more than 2 days.

Figure 6.8.8: Frequency of Security Drill/ Mock Exercise

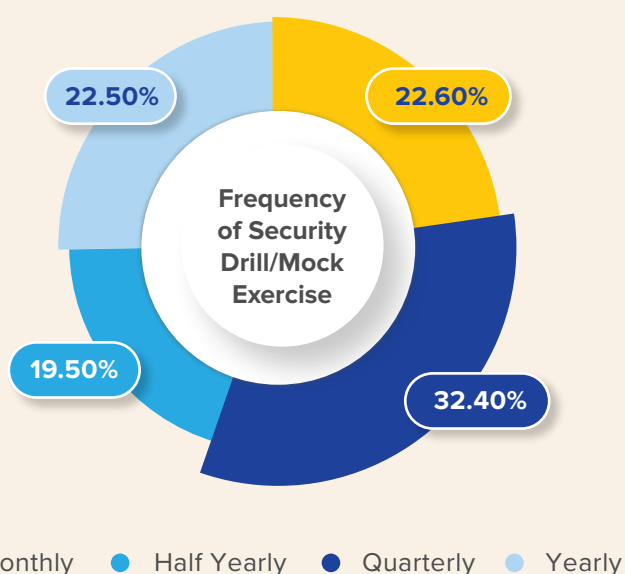
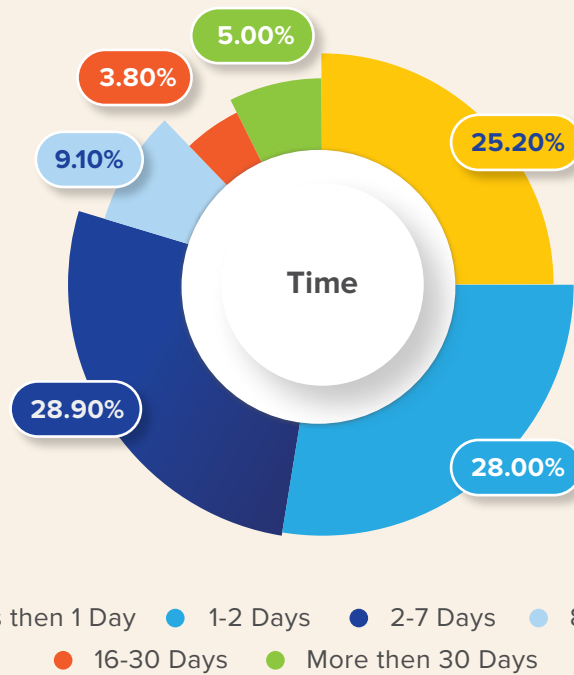


Figure 6.8.9 Time taken to Restore the Damage of Cyber Attack



As indicated in the above chart (figure-9), in nearly 50% of the cases, the time taken to restore the system and the data recovery is almost more than a week. This suggests that the regular monitoring of system compromise or cyber risk threats is not there in many companies. There is a need for regular monitoring and sensitivity testing and secondly, the periodical security analysis by third-party agencies is essential.

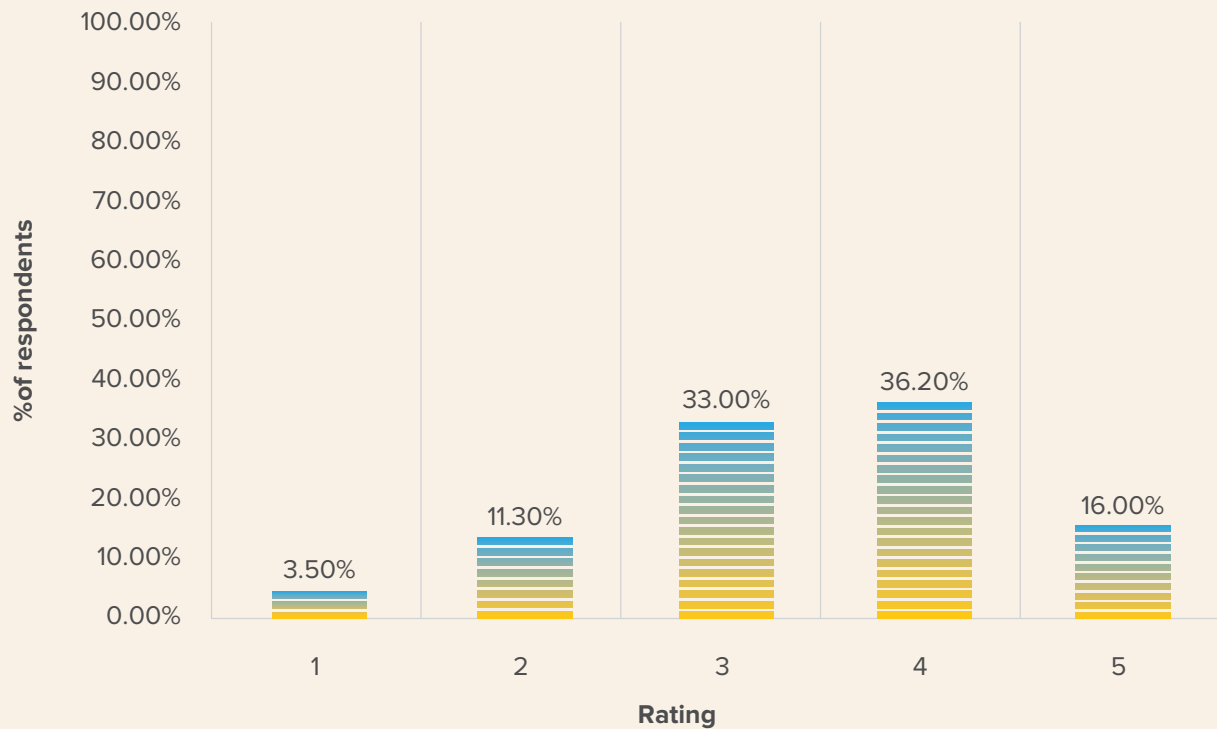
A considerable number of organizations report having No Cyber Insurance Policy in Place, revealing a substantial vulnerability within the industry. This aligns with real-world reports where businesses, especially smaller ones, often underestimate the risk or lack the resources to invest in insurance. This gap represents an opportunity for targeted education and tailored policy solutions to expand market penetration.

The findings emphasize the importance of educating potential clients on the value of Comprehensive Coverage and encouraging more robust risk management strategies. For the project and the cyber insurance market, addressing the disparity in the adoption of thorough coverage can drive growth and foster a more resilient customer base.

Perception of Cyber Risk Reporting System:

Organizations need to have a good cyber risk reporting system that can help them quickly detect when a cyberattack happens in their system or network breach.

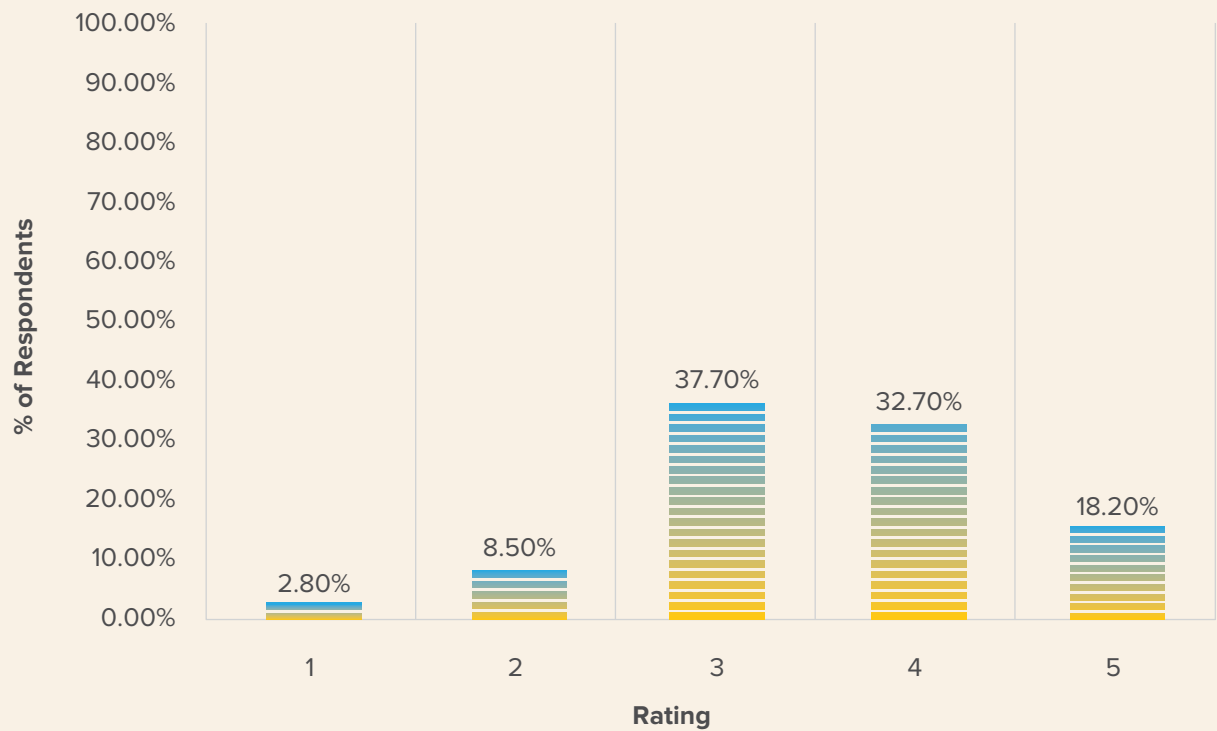
Figure 6.8.10 Evaluation of Cyber Reporting System



As can be seen from the above chart nearly 52% of the customers perceive that their cyber risk reporting system is good while 33% perceive that it is moderate and needs to be improved and 15% perceive that the reporting system is poor. Though nearly 52% perceive that their cyber risk reporting system is good at present, their perception appears to be highly optimistic, but since many do not perform the cyber risk intrusion or fishing test often to detect the cyber network breach or data breach in their organization, and secondly, the present cyber attacks are highly sophisticated and the actors are one level higher and type of tools and techniques used are highly advanced and the nature of cyber-attacks are continuously evolving and difficult to detect in quick time.



Figure 6.8.11 Evaluation of Disaster Recovery System



Their perception of the disaster recovery system is also similar to the cyber reporting system. Nearly 51% perceive that their disaster risk recovery (DRR) system is good, while 38% opine that it is only moderate and needs to be improved. 11% of the people perceived that the system was poor.

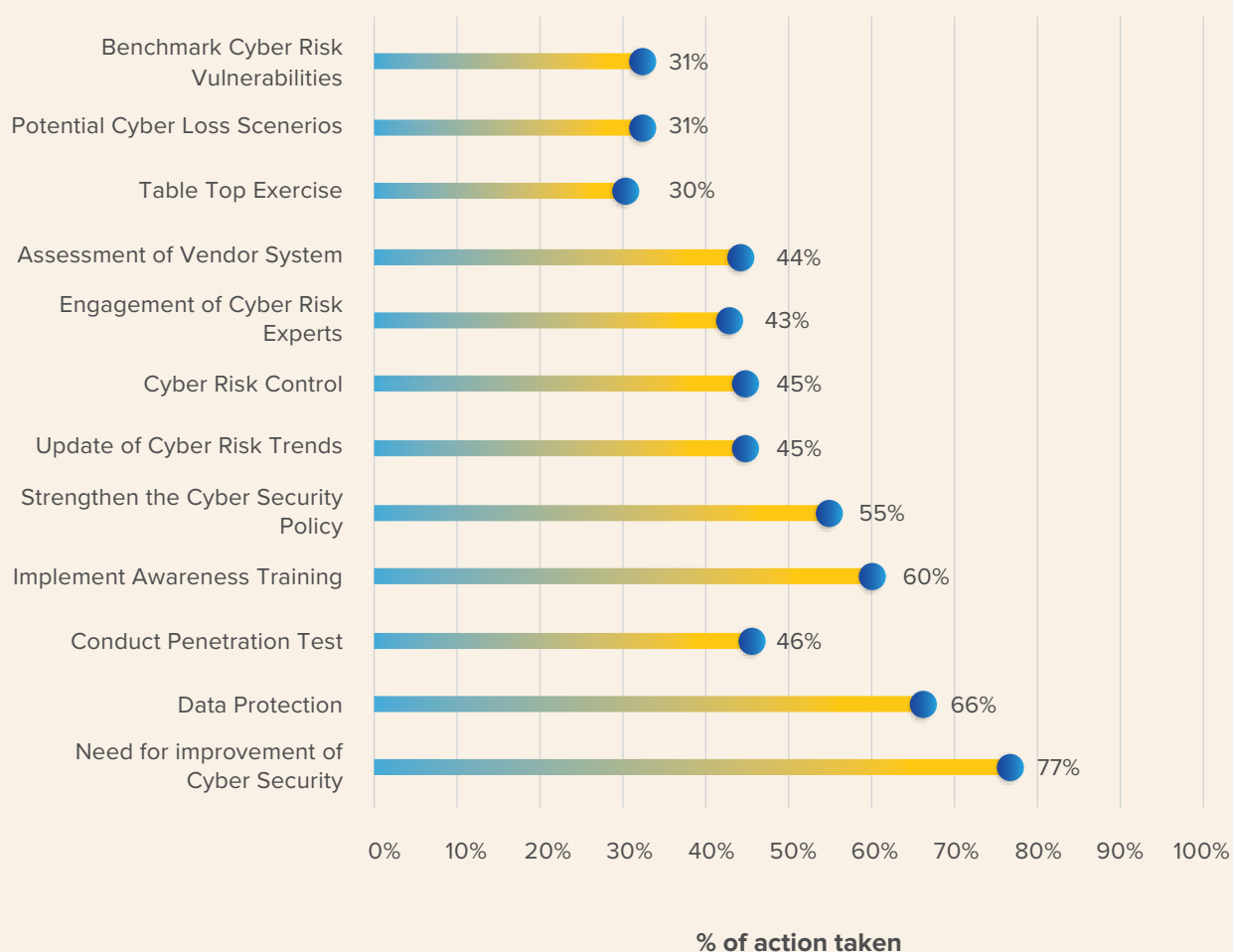
However, when a real pandemic like Covid-19 happened, many organization's DRR systems were put to the test and only very few organizations were able to recover back to normal life and many organizations were not prepared to mitigate such pandemic situations.



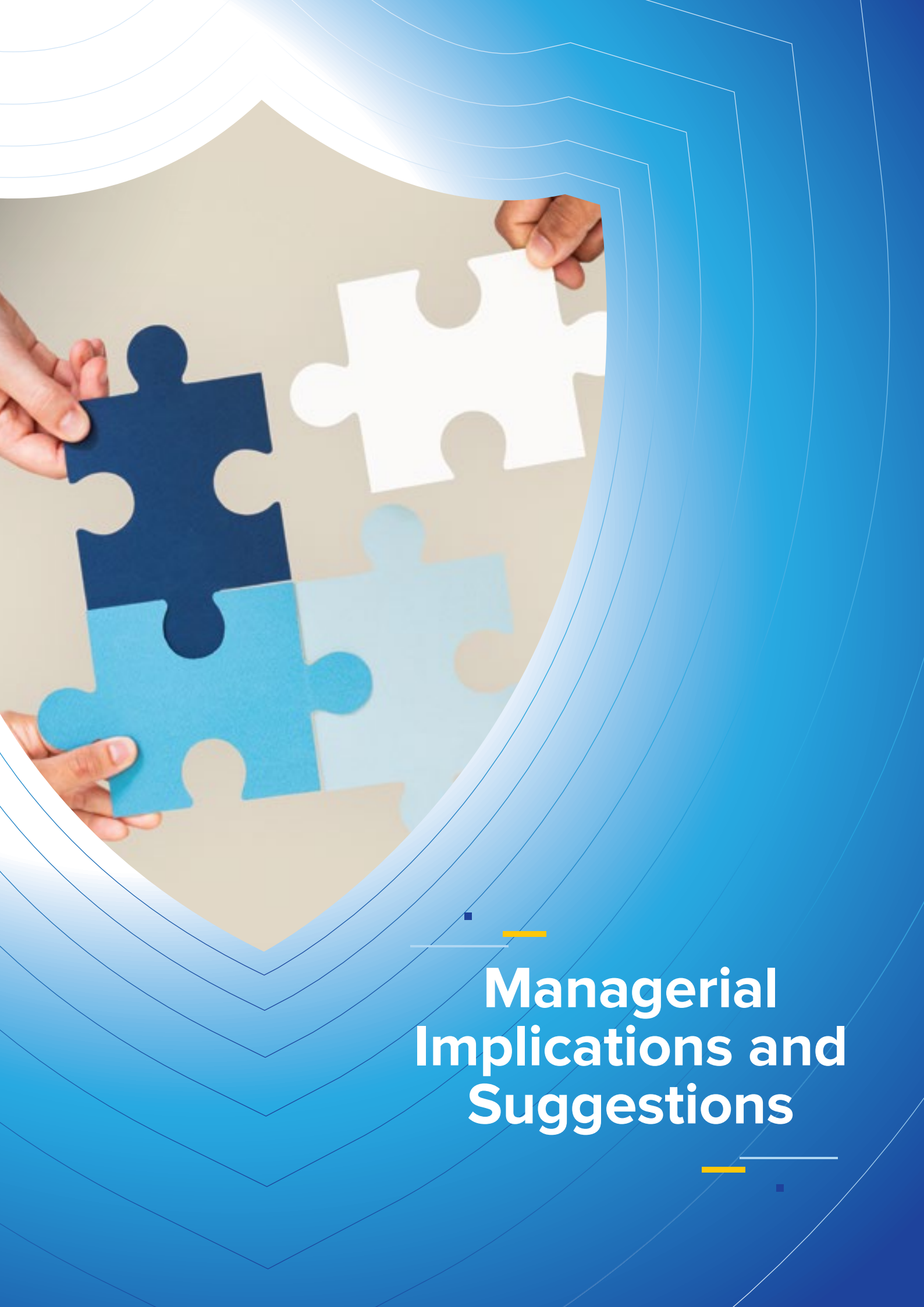
Hence, most of the customers suggested that they need to improve their cybersecurity protections and develop risk mitigation measures to combat natural disasters and pandemics.

Figure 6.8.12 Measures by the Organisation to Improve Cybersecurity

Actions taken by the Organisation to improve cybersecurity



Nearly 77% of the customers have stressed the importance of improving their cybersecurity system and 66% to improve data protection and cloud security protections. Many of them accepted that the current level of cyber awareness among their employees is quite low and they want to invest heavily in cybersecurity training for their staff (60%). About 55% suggest that they need to strengthen their cybersecurity policy and update their guidelines in light of the current cyber risk trends.



Managerial Implications and Suggestions

7 Managerial Implications and Suggestions

The insurance buyers while proposing insurance provide information based on their perception of the risk which is by nature very biased, while the underwriters accept, reject, or accept with conditions based on their perception of the client's risk. This information asymmetry is more pronounced in cyber portfolios due to the lack of availability of large data on claims experience. Proper scientific underwriting requires highly technical computer simulation models which are currently not much in use. This leaves the underwriter with large exposure gaps and can result in ruinous losses in case of a major virus pandemic. The present modeling techniques that are used in the conventional product portfolios are found to deviate largely from "low probability –high impact" claims.

1 . Implications for the Corporates:

- We find from the results that the effects of cyber threats differ from industry to industry. Also the type and motivation of the threat actors differ with the different segments. Hence corporations need to rank and prioritize their risks individually. Industry data can only give a big picture but that may have limited use for individual organizations to identify their critical assets under cyber threat and their exposure values. The present practices of organizations in assessing cyber threats need to be made more robust. There is a need to create a standard framework to assess the threats for each industry.
- The corporation needs to deploy tools to efficiently capture residual risks due to cyber influence. Measuring the underlying cyber impacts on the operational risk like people, processes, etc. is extremely important in identifying exposures which some of the tools attempt to do.
- Most insurance decisions are taken on the basis of price discovery. In a market where there is no industry standard, this process can be very detrimental as different coverage may carry different rating mechanisms. Those coverage gaps are learned only at the time of claim which is very late to do anything about.
- From our study we can conclude that some of the Corporates give superfluous priority to cyber risk mitigation plans. Most of the respondents have agreed that though there may be a plan on paper its efficacy has never been tested. Added to this is the weak link originating from employee devices, other supply chains, outsourcing, or cloud partners. Nearly 45% of corporations do not conduct auto intrusion tests or cyber audits periodically. The sensitization training on the seriousness, skillsets, and tenacity of the adversaries is lacking.
- The cyber mitigation plan can only be full-bodied if the planners have an depth understanding of risk and likelihood levels. This requires a dedicated detection engineering and threat-hunting resource which most of the corporate do not budget for.

- The risk engineering process of most organizations still deploys heuristics or peer group references to decide on the exposure levels. There is very little attempt to use valid scientific models to measure their exposure. The result so derived is way off from the actual exposure if an event occurs, as proved in most affected cases. There is also a tendency to procure cyber insurance for a lower value.
- Most of the top executives and boards still believe cyber risk does not fall within their purview. It is assigned to a much lower rung in the corporate hierarchy. As a consequence, the evaluation process is not as staid as it should be. While there are compliance requirements for taking cyber exposure earnestly, it has still not gained impetus.
- Most insurance decisions are taken on the basis of price discovery. In a market where there is no industry standard, this process can be very detrimental as different coverage may carry different rating mechanisms. Those coverage gaps are learned only at the time of claim which is very late to do anything about.

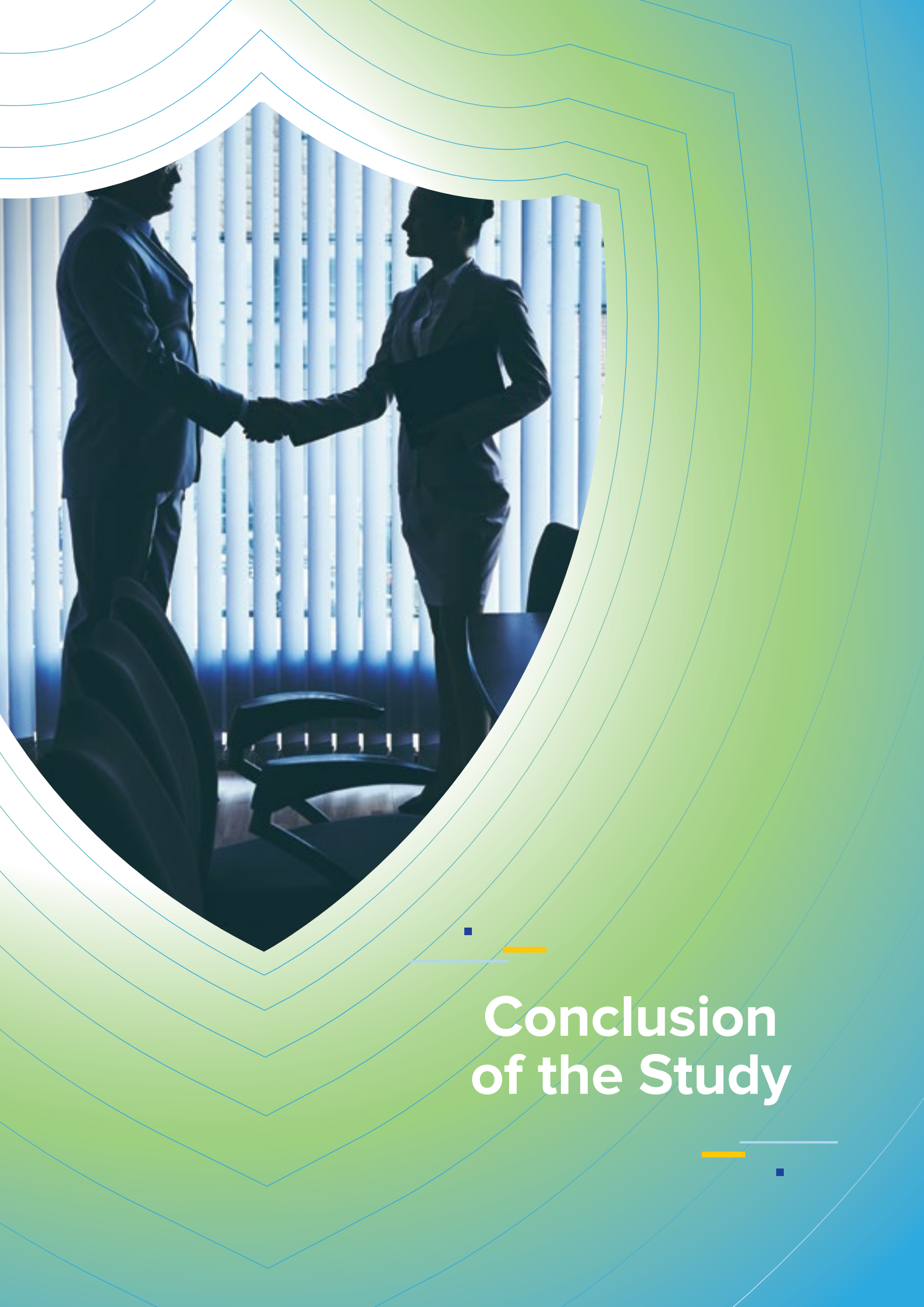
2 . Implications to the Underwriters:

- The purpose of estimated loss equations is to determine and simulate “closer to reality” fat tails. The use of non-linear models will emphasize the significance of understanding the interdependencies of the risk variables and their final bearing on the outcome to reduce the error margin. The objective is to arrive at a walk-away price for the risk.
- As noticed in the study nearly 77% of the clients do not seriously undertake forensic investigation post a breach incident. If anything, only to the extent of documenting for insurance claims the exercise is undertaken. No prominence is given to this exercise nor were any budget creation considered necessary. The insurers can encourage their customers to mature their cyber response and recovery processes and stress on building cyber resilience.
- A 360-degree view approach to risk assessment helps to ascertain the exposure more accurately. This enables the underwriter to estimate the burn layer of the portfolio decorously and hence rate appropriately. Even if the client organizations request a lower sum insured the insurer can avoid the mistake of erroneous premium rating calculation.
- The corporate concentrates on technology - related vulnerabilities as a matter of rule. The other long-term impacts are relegated to the not-so-serious category, which the experience from cyber attacks has shown as the wrong decision. However, a focus on the economic aspects of cyber risk, especially digital asset valuation and risk ranking based on the financial impact of individual risk will improve the risk posture of the organization. The underwriter can correct this abnormality by policy terms and warranties.
- A robust modeling too will enable the insurer to deeply understand the response behavior of the client organizations and in turn tune in their policy construct to impose cyber discipline which will help both.
- The process of documenting exposure and mitigation policies is mostly not comprehensive. Also, the measure is done at a discrete time period without understanding the effect of residual risk over time. The insurers need to address this gap.
- The underwriters need to identify and structure their aggregation of risk which is essential for determining residual risk and their risk transfer strategies. This will be the last stand between survival and bankruptcy.

- 
- Currently, there is no industry-accepted standard of policy term definitions. While there is no serious litigation at present on interpretations there could be some serious legal problems in the future. As the knowledge of risk proliferates and mitigation plans are widespread, the lack of a standard term is likely to play havoc at the time of claims. This will in turn have a huge impact on the actuarial pricing of the risk.
 - The actuaries are used to rate the risk based on large quantitative data that are not available at present. While near-reality simulations are available there is a lack of confidence in using them for their pricing policies. Even more is the difficulty in ascertaining IBNR claims, especially in the third-party liability area.
 - The regulatory requirements on actuary certification on pricing of a portfolio recommends only a limited number of methodologies. These types of new modeling techniques need to be presented to the regulator to impress upon the efficacy of their use.
 - To streamline the claims process and reduce any potential conflicts, it is recommended that clients be provided with a clear and concise claim document checklist. This checklist should explicitly outline all necessary documents that need to be prepared, and submitted. This would ensure that clients are well-informed about the required documentation in advance, minimizing delays and improving the efficiency of the claims process.
 - It is recommended that individuals and organizations purchasing insurance products proactively address breach response preparedness. The breach response measures should include forensic readiness to analyze breaches, a technology recovery plan to restore systems, a crisis management plan for effective communication, and legal readiness to meet compliance requirements. Integrating these elements helps mitigate risks, minimize downtime, and ensure a structured and smooth response to cybersecurity incidents, enhancing overall resilience.

3 . Implication for the Intermediaries:

- There is a skill and knowledge gap in the industry among the distribution channels. While there is no entry barrier for distribution, it will be in the interest of the intermediaries to build skill sets for specializing in cyber risk and insurance.
- The intermediaries by virtue of their understanding and closeness to the customer base will be able to provide more insights and data to structure the contract terms of the cyber insurance policies. There is a possibility of customized policy wording for different industry segments.
- There is a need for the intermediaries to work on the documentation process for managing claims in cyber insurance.



Conclusion of the Study

The Study examined the current Cyber Insurance covers available in India and overseas markets to study the protection gaps in Cyber Insurance products. The results highlight that though many of the risks are covered under the existing products, there are variations observed, particularly, in Advanced Persistent Threats (APT) by the State Actors, and insider threats. Cloud Breaches, and third-party vendor failures. The policy terms & conditions should clearly specify the silent risks under the exclusions. The study analyses cyber risk insurance through Gap Analysis across the selected industries, which indicates that the risk profiles of each major industry/sector vary significantly. Regular industry-specific intelligence can help the insurers with proper risk assessment and pricing of Cyber Risks. The Study Results would help improve underwriting standards and enable the design of customized cyber risk coverage across different industries and sectors. It would also help them understand the significant underwriting challenges and operational issues in cyber insurance.



The Study analyses cyber risk awareness among Key Management Personnel (CEO, CFO, CIO, CRO, etc.), including Board level, and examines the effectiveness of Cyber security measures taken by the organizations. The study results highlight that cyber risk awareness among senior executives is comparatively higher in large industries with higher turnovers (More than Rs.500 crores), particularly, in BFSI, IT/ITES, Energy & Communication sectors, while the cyber risk awareness level is quite low among the users and department heads, suggesting a need for a regular training and need to enhance the cyber security capabilities across the industries.

The Study analyses Underwriters' perceptions and key challenges, which would help them understand their perceptions of cyber risk threats and vulnerabilities. The study highlights that the cyber threat perceptions have been highly underestimated with the assumption that their cyber security and safety measures are being updated regularly.

However, their ratings about cyber risk mitigations, including cyber risk audits, auto-penetration testing, cloud risk security, web application (API), and mobile security measures, were quite low. This suggests that insurers need to get regular cyber risk assessment reports, including pre-breach risk mitigation, vulnerability assessment, and incidence response reports. The insurers can offer these services in collaboration with the cyber security vendors as value additions. Further, they can take the support of CERTIN and other cyber risk & security institutes to provide regular technical

training on cyber risk trends and security assessments to their clients.

The Study provides Cyber Risk Response Behaviors of the people within the selected companies. Also, it offers necessary suggestions for effective Cyber Risk underwriting and appropriate pricing to the clients and Insurers. It has been observed that many of the cyber risk underwriters and brokers need to be updated about the latest cyber risk trends, particularly the vulnerability assessment details of social media, cloud security, IoT & AI-related technological updates.

The Project Team Members



Mr. Renjit Gangadharan

Retired Chair Professor (Non-Life)
- National Insurance Academy



Dr. Steward Doss

Professor -
National Insurance Academy
gdoss@niapune.org.in



Mrs. Jayashree Sridhar

Chief Administrator -
National Insurance Academy
sridharjayashree@niapune.org.in



Mr. Indraneel Roy

Faculty Member -
National Insurance Academy
iroy@niapune.org.in



**NATIONAL
INSURANCE
ACADEMY**

National Insurance Academy

25, Balewadi, Baner Road, NIA P.O.,
Pune 411 045, India

Phone: +91-20-27204000 / 27204444

Fax: +91-20-27204555 / 29515710