Deloitte.

Cyber insurance in India: Navigating risks and opportunities in a digital economy

October 2023

Table of contents

Executive summary 05

The rise of cyber insurance 07

A sneak peek into ground realities 13

Growth drivers of cyber insurance 17

Watch out for the roadblocks 19

Five steps to unleash the potential of cyber insurance 25

Four essential areas that need a push from the government 27

Executive summary

India is going digital. The rising number of mobile phone users, penetration of the internet to the remotest areas of the country, and rapidly expanding digital infrastructure are contributing to India's digital transformation. According to the Ministry of Electronics and Information Technology (MeiTY), India's digital economy is expected to rise to US$ 500 billion by 2025, up from US$ 200 billion in 2019.[1] This is because the digitisation drive is likely to foster a favourable business environment that will attract rapid investment and boost income. Rising income will create stronger demand for goods and services, while younger and price-sensitive demographics are likely to seek high-quality goods and services at affordable prices. These will compel businesses to adopt digital platforms as solutions to meet customer expectations.

With accelerated digitisation comes cyber risks that often deter business growth. Cybercrimes are becoming more rampant and complex; costs associated with such breaches are not only increasing but also becoming more systemic. Organisations are looking at cybersecurity programmes as business enablers to ensure safety and build trust amongst their new-age customers.

While investing in a robust tech-security infrastructure is the obvious solution, cybersecurity programmes also encompass analysing risks for organisations and mitigating them through various strategies. One of the risk-mitigating strategies is that of risk transference through cyber insurance which can help reduce financial risks associated with digitisation.

Conditions are ripe for the cyber insurance market to take off. Rising awareness and hard-hitting experiences over the past few years have brought focus on how to secure against cyber risks. Yet, the decision to trade cyber insurance is not always an easy one. From a purchaser's point of view, the rationale behind the budget allocation for insurance is often not well-defined. Not to mention, the budget required to purchase insurance varies significantly with the nature of the industry and companies' propensity to take risks. On the other hand, sellers remain cautious about writing cyber coverage on a large-scale basis.

We, at Deloitte, tried to understand the potential of cyber insurance as a risk mitigation strategy and the challenges inhibiting the growth prospects of this still-emerging market in India. To substantiate our insights and perspectives, we conducted a survey capturing responses from Chief Information Security Officers (CISOs) from a diverse set of India-based companies. The survey helped us gauge their understanding of cyber insurance and willingness to buy a policy. Issues such as ambiguity associated with technical details, the dilemma of pricing a product, and the buyers' paradox, could explain several of our observations. The reasons behind the responses helped us evaluate the way forward for different stakeholders (the government, buyers, and sellers) to address challenges associated with cyber insurance.

An analogy for cybersecurity today is that of car brakes that enable an organisation to go faster with the confidence that it can stop when required. Cybersecurity risks cannot be treated as mere IT security issues anymore. An organisation embarking on its digitisation journey must prepare itself to fight the escalating cybercrimes. More importantly, we believe boards and CEOs need to deepen their cybersecurity competencies, as cyber risks have become an enterprise-wide risk management issue.

MeiTY report on "India's trillion dollar digital opportunity
[1].https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf

The rise of cyber insurance

After the pandemic, cyber awareness rose significantly as movement restrictions compelled industries, businesses, and citizens to rely on digital options for their daily operations. This also opened up opportunities for cyber criminals to target vulnerable groups. The Russia-Ukraine conflict further aggravated the situation, resulting in a rise in coordinated cyberattacks that affected governments and organisations worldwide. While every industry and sector has seen a spurt in such attacks, the year 2022 saw targeted attacks on the government sector, with India, the US, Indonesia, and China reporting about 40 percent of the total reported incidents in the government sector worldwide.[2] Compared with 2021, global cyberattacks increased by 38 percent in 2022.[3]

Being one of the prominent emerging nations, India is expected to be the most frequent target of cyber criminals. It aspires to be at the forefront of technology-led growth (by adopting cloud, metaverse, and AI) and the rapid transformation in public administrative architecture to become Digital Bharat. That has made the country a lucrative target for cyber criminals. According to the FBI's Internet Crime Report for 2022, India ranks fourth amongst the top five countries by the number of total cybercrime victims.[4] According to the Computer Emergency Response Team of India (CERT-IN), the foremost authority on cyber incidents in India, the country witnessed 1.39 million cybersecurity incidents in 2022.[5] Since September 2022, India reported an average of 1,787 cyberattacks per week against a global average of 983 attacks per week, according to Check Point Research.[6]

These statistics tell us that the cyber threat is critical. More examples are quoted in case study 1. The problem is likely to intensify further as internet users in India are expected to increase by 15.7 percent from 2022 to 900 million by 2025.[7] The widespread adoption of digital infrastructure, such as Unified Payments Interface (UPI), Aadhaar, and Open Network for Digital Commerce (ONDC), is likely to intensify India's critical vulnerabilities.

Cyber warfare does not have geographical boundaries. Both state (government agencies) and non-state actors (scammers, hackers, criminal organisations, private military organisations, media outlets, labour unions, organised ethnic groups, and lobby groups) globally are taking advantage of India's digitisation drive to inflict India's infrastructure and government institutions. Therefore, cybersecurity leaders must respond to the heightened threat environment and build their own warfare capabilities. In addition to securing digital infrastructure, adopting mitigation strategies against losses, primarily financial, is important.

The cyber insurance market has evolved over the years to meet the demand for mitigating losses due to cybercrimes. Cyber insurance offerings help entities that are digitising to cover the costs of recovery and damages in the event of cyberattacks. Globally, the size of the cyber insurance market is about US$ 12.83 billion in 2022.[8] Over the next seven years, the market will grow at a CAGR of 25.7 percent to US$ 63.62 billion in 2029.

[2]Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022 by CloudSek Report - https://uploads-ssl.webflow.com/635e632477408d12d1811a64/63d39e6ee68d87e7d6c799bf_Unprecedented-Increase-in-Cyber-Attacks-Targeting-Government-Entities-in-2022.pdf
[3]2023 Cybersecurity report by Checkpoint https://go.checkpoint.com/2023-cyber-security-report/chapter-04.php#4
[4]FB Internet Crime Report 2022 - https://www.regions.com/-/media/pdfs/treasury-management/2022_IC3Report.pdf
[5]https://economictimes.indiatimes.com/news/how-to/five-cyber-security-tips-to-secure-your-online-shopping-and-memories/articleshow/98313993.cms?from=mdr#:~:text=The%20Ministry%20of%20Electronics%20and,the%20importance%20of%20cyber%20security.
[6]https://thewire.in/tech/india-cyber-attacks-last-6-months
[7]Internet Adoption in India Report 2021 by Kantar - https://images.assettype.com/afaqs/2021-06/b9a3220f-ae2f-43db-a0b4-36a372b243c4/KANTAR_ICUBE_2020_Report_C1.pdf
[8]A study by Fortune, https://www.fortunebusinessinsights.com/cyber-insurance-market-106287

However, corporate spending towards cybersecurity and cyber insurance as a market is in a nascent stage. This is because, in India, the pace of digital adoption and digital maturity differs significantly across industries and organisations. At present, a majority of Indian organisations are going digital not because of choice but for survival. Irrespective of the industry, efficiency and cost are driving digitisation within organisations for them to stay ahead of the competition. They are still early in the digital maturity roadmap.

That said, the cyber insurance market in India shows signs of strong growth. India is one of the fastest-growing regions from the perspective of cyber risk insurance uptake. It is expected to be far more competitive than developed insurance markets.[9]

Our discussions with various industry participants suggest that the current cyber insurance market size in India is US$ 50–60 million. The market has been consistently growing at a CAGR of 27–30 percent over the past three years. It is expected to maintain the growth rate over the next 3–5 years with increasing awareness levels.

The uptake of cyber insurance appears to be lopsided. Industries with a higher degree of digitisation involved in operations (such as IT, pharma, and manufacturing), or those with more integration and exposure to the rest of the economy (such as supply chain, retail, critical industries, and finance) are often the targets of cyber criminals. These industries are expected to be early adopters of cyber insurance.

[9]https://www.forbesindia.com/article/iim-calcutta/how-insurancelinked-securities-can-improve-cybersecurity-in-india/84811/1

Case study 1

Healthcare, infrastructure, and the government were the top three most targeted industries in India. In 2022, the government sector has become a top target for cyber criminals. Futuristic technologies, such as Metaverse and AI, also come with their share of threats.

Healthcare:
A report published by the CyberPeace Foundation and Autobot Infosec, revealed that the Indian healthcare sector experienced 1.9 million cyberattacks until November 2022. However, the cyberattack on the central government's medical research body in November 2022, in which hackers attempted to access the website 6,000 times in a single day, failed.

Government:
According to the information acquired by XVigil, the number of cyberattacks directed at the government sector increased by 95 percent in H2 2022 compared with the same period last year.[10] In another incident, a group of autonomous government-run medical universities (part of the Indian government) was the target of a late-December attack, where about 40 million patient data was exposed.

Infrastructure:
Over the past few years, cyberattacks on India's critical infrastructure have sharply risen; the degradation, destruction, or malfunction of the systems that control such infrastructure could have a significant negative impact on India's national and economic security. In November 2022, one of India's largest depositories was targeted by hackers. In the same month, a state-run oil producer, an Indian airline operator, and a leading power generation company were also attacked by cyber criminals.

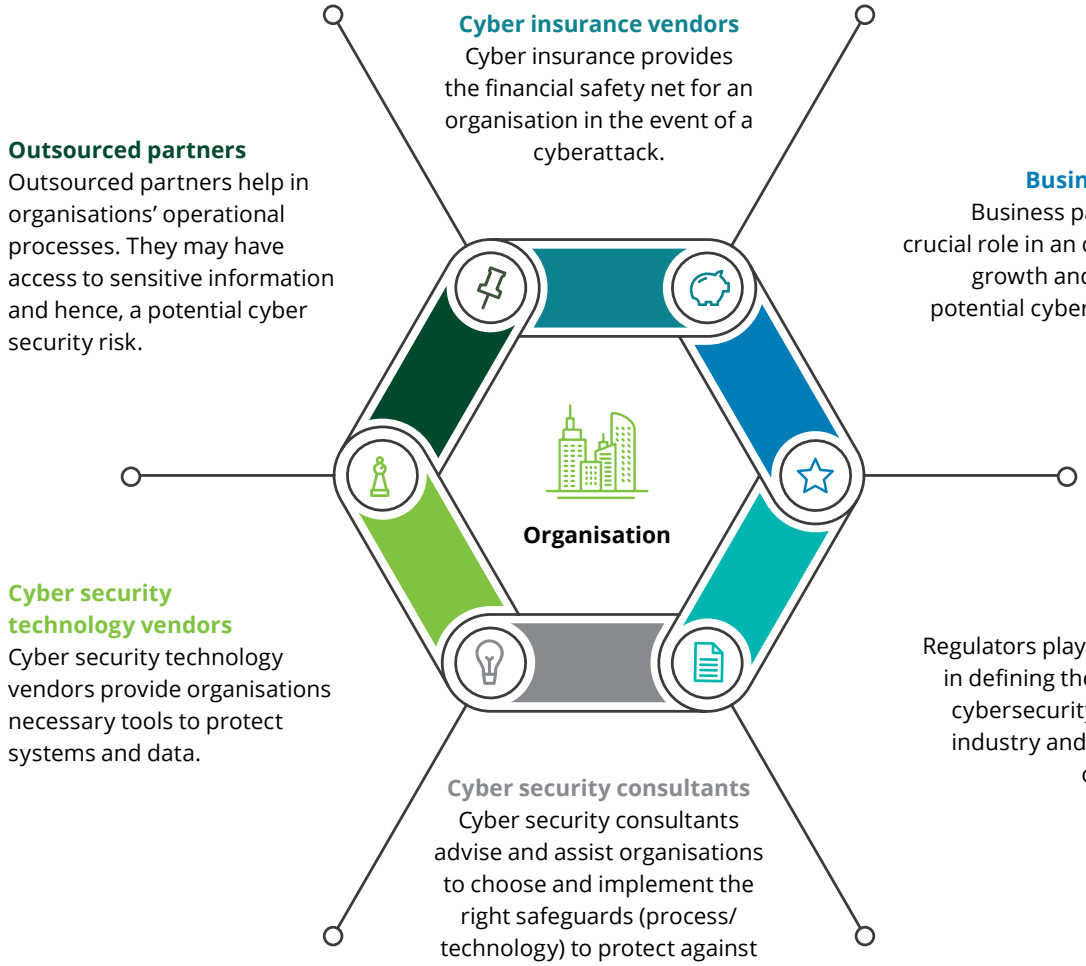
Pharma:
In September 2022, leading pharmaceutical businesses witnessed a cyberattack in which data was stolen from the system. Private information of another public-listed Indian pharmaceutical corporation was disclosed on a dark web forum.[11]

Threats in metaverse and other futuristic technologies:
Metaverse is a platform for virtual communication but requires participants to save critical personal information, such as credit card information and addresses. Even data about people's hand and eye motions and facial traits are collected by the metaverse, raising additional cybersecurity issues. Device vulnerabilities, identification and authentication issues, moderation problems, and decentralisation are a few of the cybersecurity concerns faced by the metaverse.

[10]Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022 by CloudSek Report https://uploads-ssl.webflow.com/635e632477408d12d1811a64/63d39e6ee68d87e7d6c799bf_Unprecedented-Increase-in-Cyber-Attacks-Targeting-Government-Entities-in-2022.pdf
[11]https://etinsights.et-edge.com/cyber-attacks-that-shook-indian-firms-in-2022-critical-infra-healthcare-most-targeted/

Despite grappling with cyberattacks, the Indian industry is digitising at a rapid pace. The cybersecurity ecosystem also has a profound impact on the organisation's ability to safeguard themselves against these cyberattacks. The cybersecurity ecosystem in India has been strengthening and cyber insurance is one of the key players in this ecosystem.

Deloitte survey – methodology



Deloitte survey – methodology

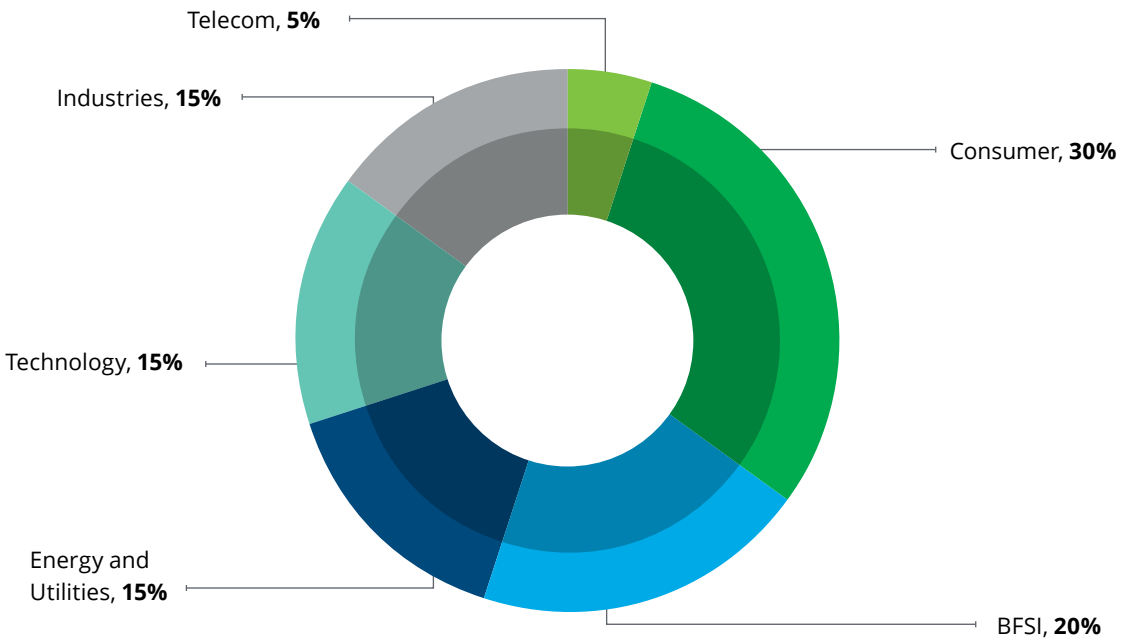
This report shares a top-down view of cybersecurity and the need for insurance in the Indian market. The insights in the report are based on a Deloitte survey. Several CISOs participated in the survey to help us understand the perceived importance of cybersecurity and cyber insurance as a risk mitigation strategy.

The insurance-related questions revolved around the investment in coverage and premiums, and businesses' perception and understanding of both. These gave us insights into India's pace of adoption, how CISOs allocate budgets towards cyber insurance, and their concerns and asks.

We captured responses from select respondents across industries and sectors of different sizes. Respondents were from India-based companies as we wanted to maintain a similar economic and cultural environment.

This report shares our views and insights into the cyber insurance market, backed by the survey findings.

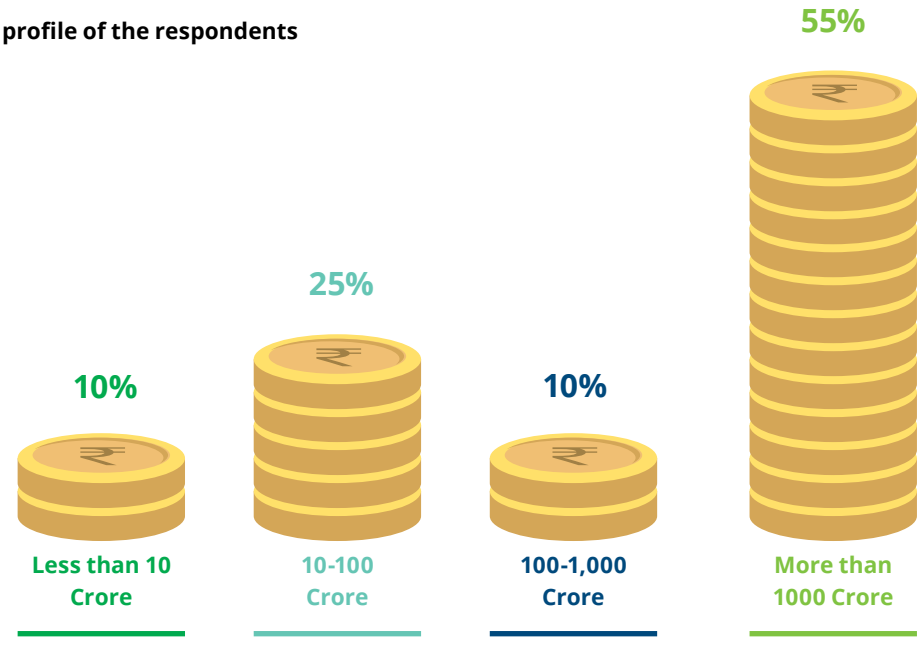
Figure 1. Sector profile of the respondents



Q: Please select the sector of your company.
Source: Deloitte Research

A large segment of the respondents was from the consumer sector followed by the banking and finance sectors. These sectors deal with large consumer databases or are highly technology-intensive in operations, which is where we expect high digitisation and investments in cybersecurity and insurance.

Figure 2. Revenue profile of the respondents



How much is your company's annual turnover (in INR)?

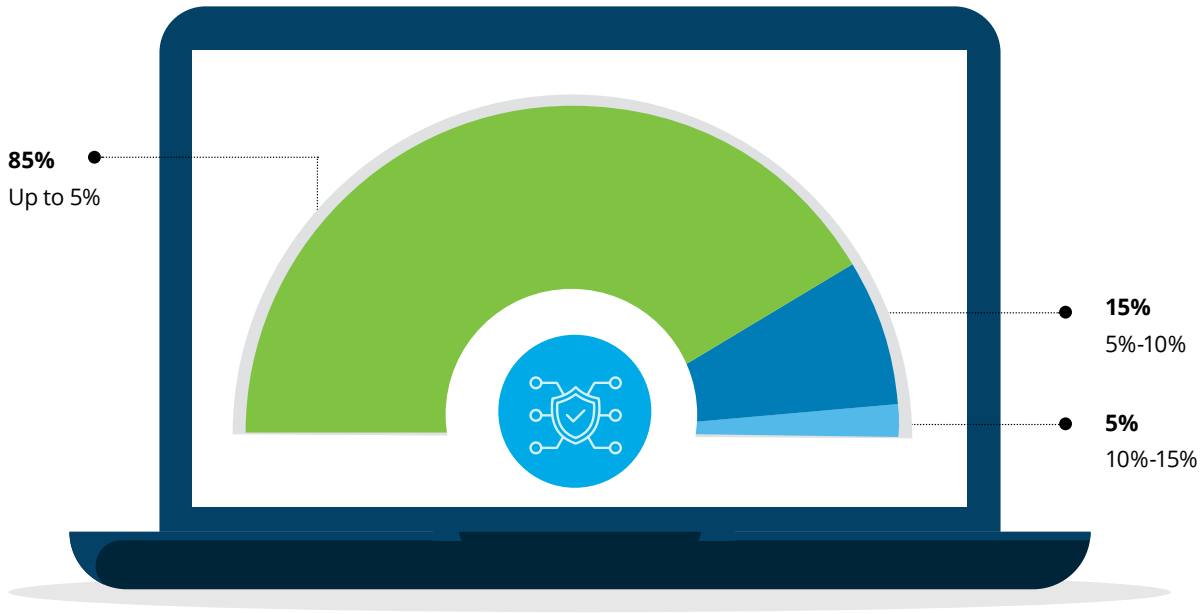
Source: Deloitte Research

The responses received from mid-sized and large firms suggested that most firms' decisions to invest in security and insurance were not contingent on the resources available

A sneak peek into ground realities

The complexity of cybercrimes and the associated losses are on the rise. According to the FBI's Internet Crime Report for 2022, losses due to cybercrime increased to US$ 10.3 billion in 2022, from US$ 6.9 billion in 2021.[12] One would expect that the potential financial and reputational losses would draw more businesses to protect their digital assets against such crimes. However, the survey findings suggest that ground realities are quite contradictory.

Figure 3. The proportion of turnover to cybersecurity budget



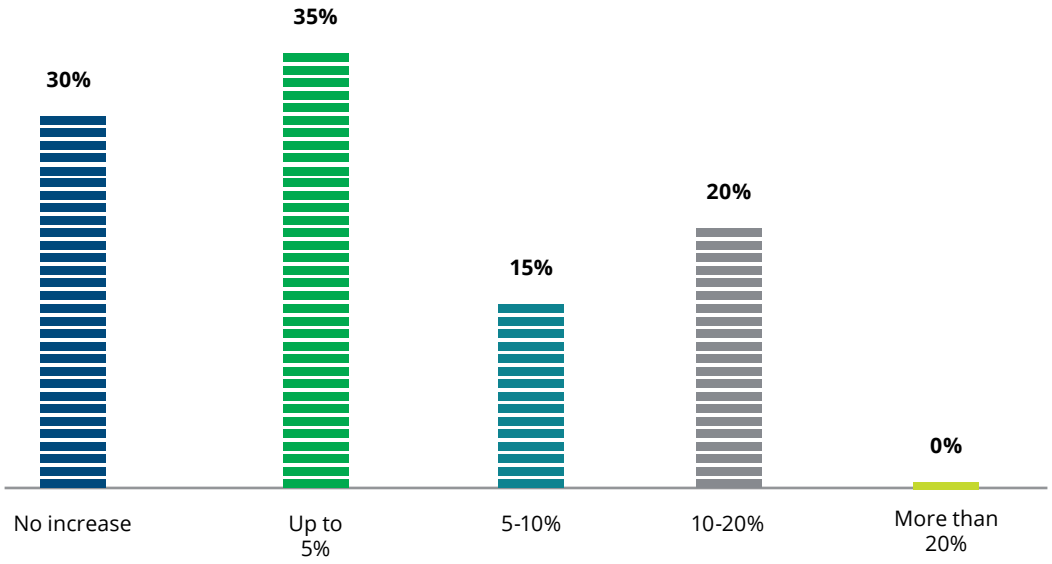
Q: What proportion of your turnover is the cybersecurity budget?

Source: Deloitte Research

The respondents understood the significance of cyber threats and had a dedicated budget for cybersecurity. However, the allocated budget was smaller in proportion to the turnover for most firms. While smaller firms were limited by their ability to spend, most larger firms allocated disproportionately smaller budgets (although in magnitude, it could mean a larger sum). Interestingly, mid-sized firms were amongst the ones with a higher budget for cybersecurity.

[12] FB Internet Crime Report 2022 - https://www.regions.com/-/media/pdfs/treasury-management/2022_IC3Report.pdf

Figure 4. Willingness to spend on cybersecurity in the future



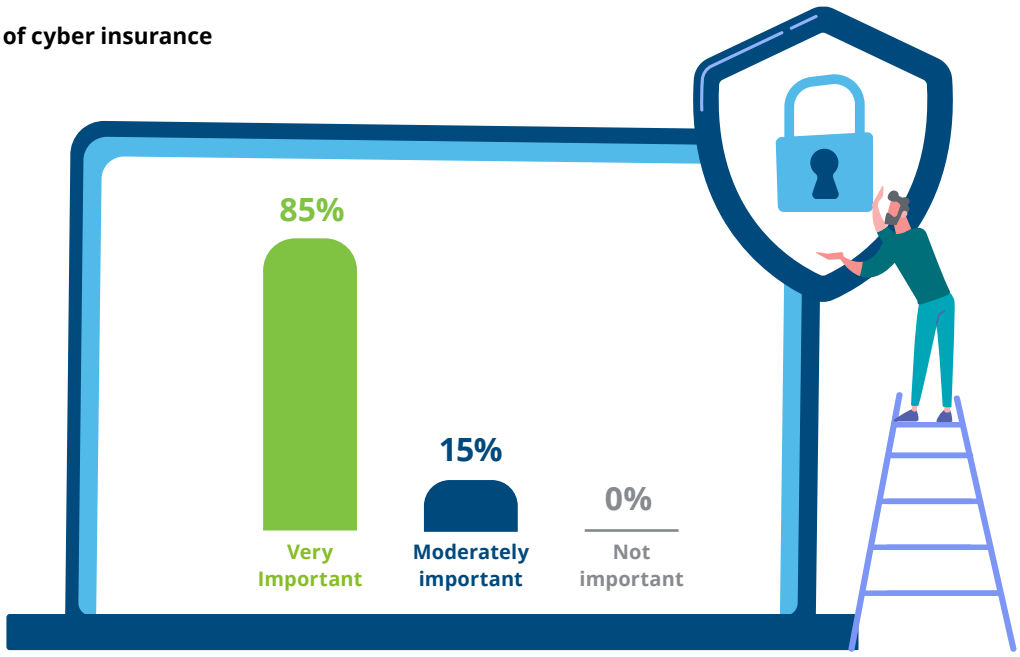
Q: How much more (from your current cybersecurity budget) are you willing to invest in securing your digital infrastructure over the next three years?

Source: Deloitte Research

Two-thirds of the respondents expressed their willingness to spend higher on securing their digital infrastructure over the next three years. The willingness was the highest amongst mid-sized firms. Despite dealing with large consumer databases, several big firms from the consumer sector were not keen on increasing their budget to improve their digital infrastructure. (The survey was done before the Data Protection Act was announced).

The differential needs and appetite are likely to affect the cyber insurance market's growth. As businesses in India are still in the process of prioritising cyber security, the demand for cyber insurance (to mitigate financial losses arising from cyberattacks) is expected to fluctuate.

Figure 5. Importance of cyber insurance

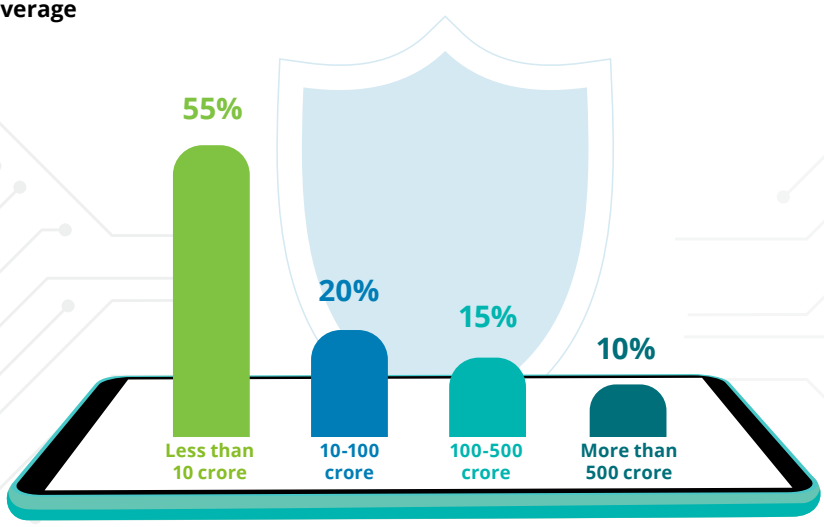


Q: How important is cyber insurance for your organisation?

Source: Deloitte Research

The respondents understood the need to insure against financial losses that may incur because of cyberattacks. However, consumer sector firms with no willingness to increase their cybersecurity budget in the future (discussed above) had moderately prioritised cyber insurance as a risk-mitigation tool.

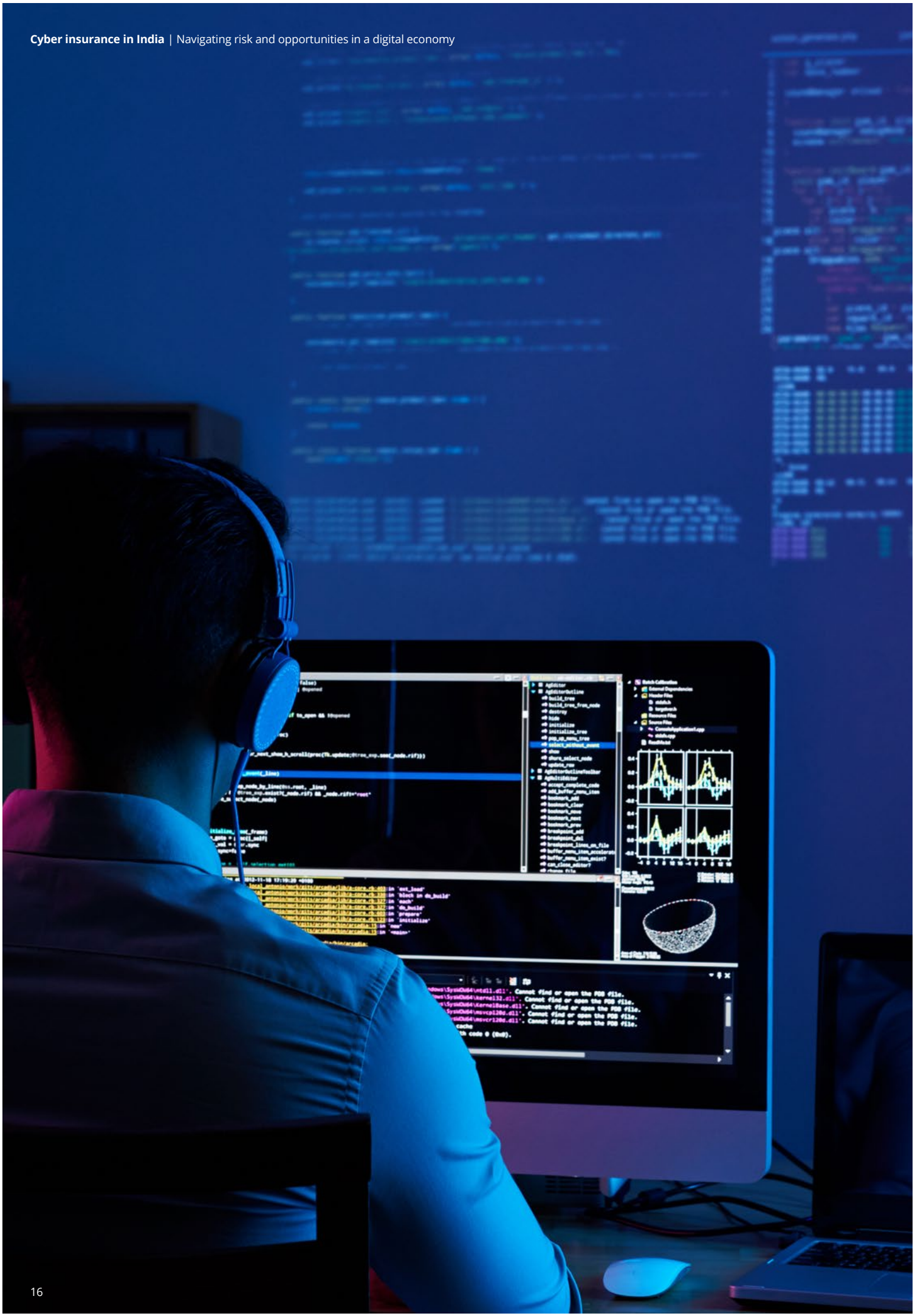
Figure 6. Insurance coverage



Q: How much cyber insurance coverage have you taken (in INR)?

Source: Deloitte Research

There was a clear mismatch between realisation and willingness to act. Three-fourths of the respondents had cyber insurance coverage of INR 100 crore or less (and over 50 percent had less than INR 10 crore of coverage). Financial and banking, and IT firms were the biggest investors (because of the higher risks to attacks), while consumer firms spent the least. The willingness to pay was both a function of lower risk perception by the industry and a mismatch of value they received from the premium, which is highlighted later in the report. A lower priority towards cyber insurance (seen in Figure 5) also translated into lower insurance coverage amongst consumer sector firms. This may change after the Data Protection Act comes into force and the consumer sector, which holds personal information, becomes more vulnerable to attacks in the future. None of the respondents wanted to discontinue their existing policies.



Growth drivers of cyber insurance

Growth of the cyber insurance market will be influenced by the following three factors in India:

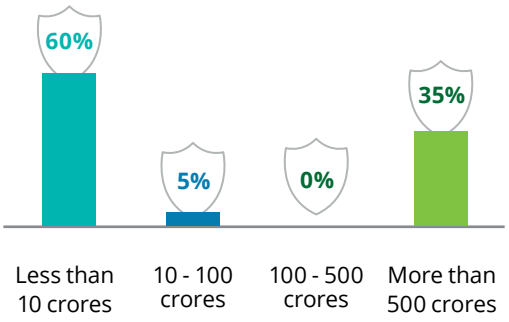
The pace at which firms become digitally mature:
As firms become digitally intensive and mature, threats will no longer be notional. The better realisation of the potential losses will improve firms' willingness to secure and insure their digital infrastructure.

The government's initiative to digitise and form stringent cyber laws:
These will compel firms to opt for cyber insurance. As ministries deal with sensitive citizen data, the government will become the biggest consumer of insurance. This will have a multiplier effect on the private sector as well. Partnerships and collaborations with the government will mandate private firms to insure against cyber losses.

The changing landscape:
Several non-traditional players (technology players, including MNCs) are entering the cyber insurance business, making the entire landscape more competitive. However, new players are also creating opportunities for sellers of insurance policies to invest in technology and partner with insurtech, cloud service providers, and big data start-ups. Technology players have access to troves of data and capital that insurance companies lack. Insurance companies have experience in underwriting.[13] A partnership between the two groups will result in better access to security data and integration of customer cyber risk profiles. This information can be used to design and tailor cyber insurance policies for buyers.[14]

According to the survey, the cyber insurance market is expected to take off modestly in the short run. However, it will see exponential growth once it gains momentum.

Figure 7. Willingness to increase the coverage in the future

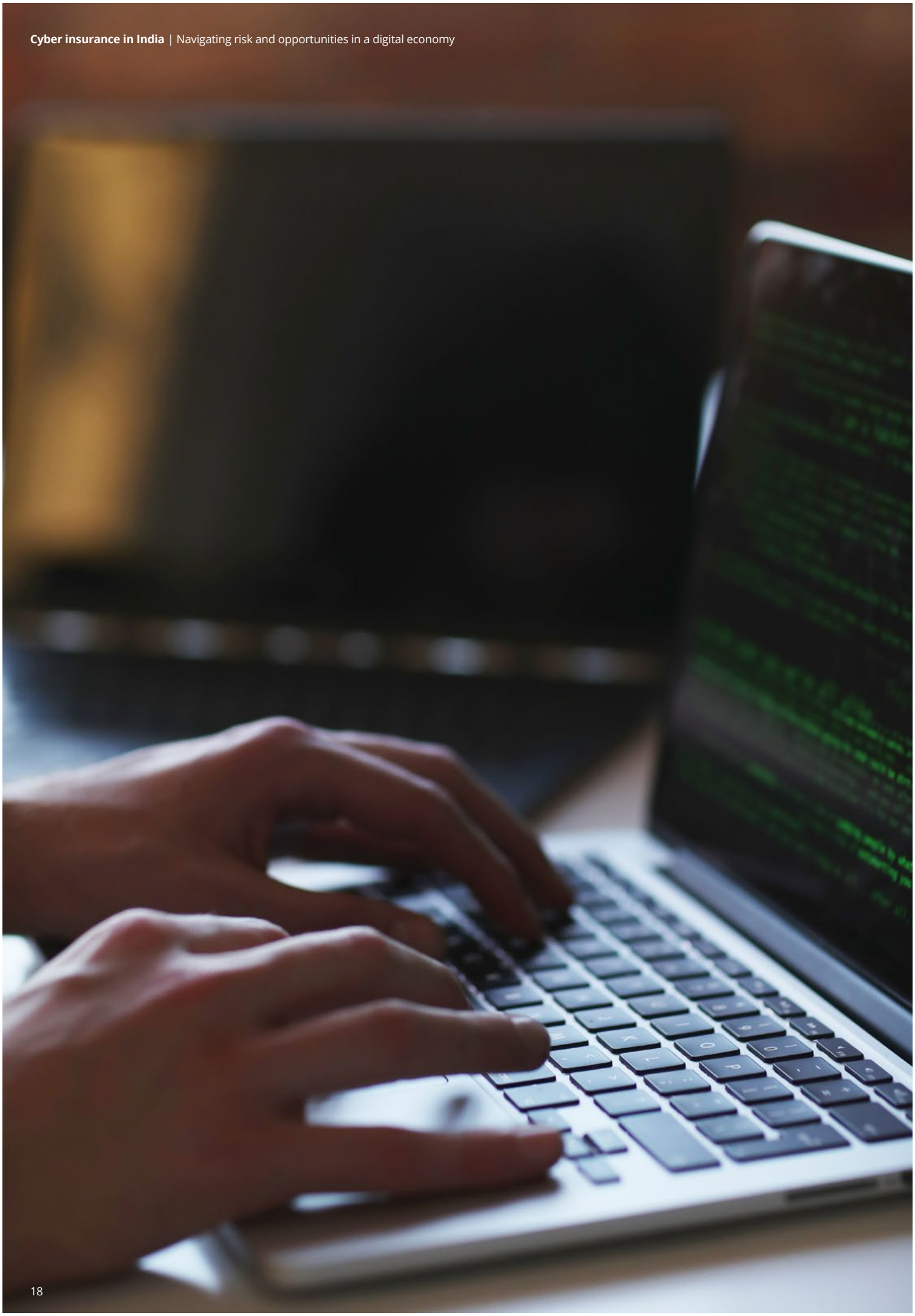


While the survey indicated a smaller appetite towards cyber insurance, there was substantial interest (60 percent) in increasing existing coverage. Firms from cyberattack-prone industries, especially those with more customer information, were keener to opt for cyber insurance.

Q: Against the backdrop of an increasing number of cybercrimes and ransomware attacks, will you be willing to enhance your coverage in the next three years?

Source: Deloitte Research

[13] The future of insurance is happening without insurance firms: https://www.economist.com/finance-and-economics/2019/07/20/the-future-of-insurance-is-happening-without-insurance-firms
[14] https://www.wsj.com/articles/google-working-with-allianz-and-munich-re-on-cyber-insurance-11614688200



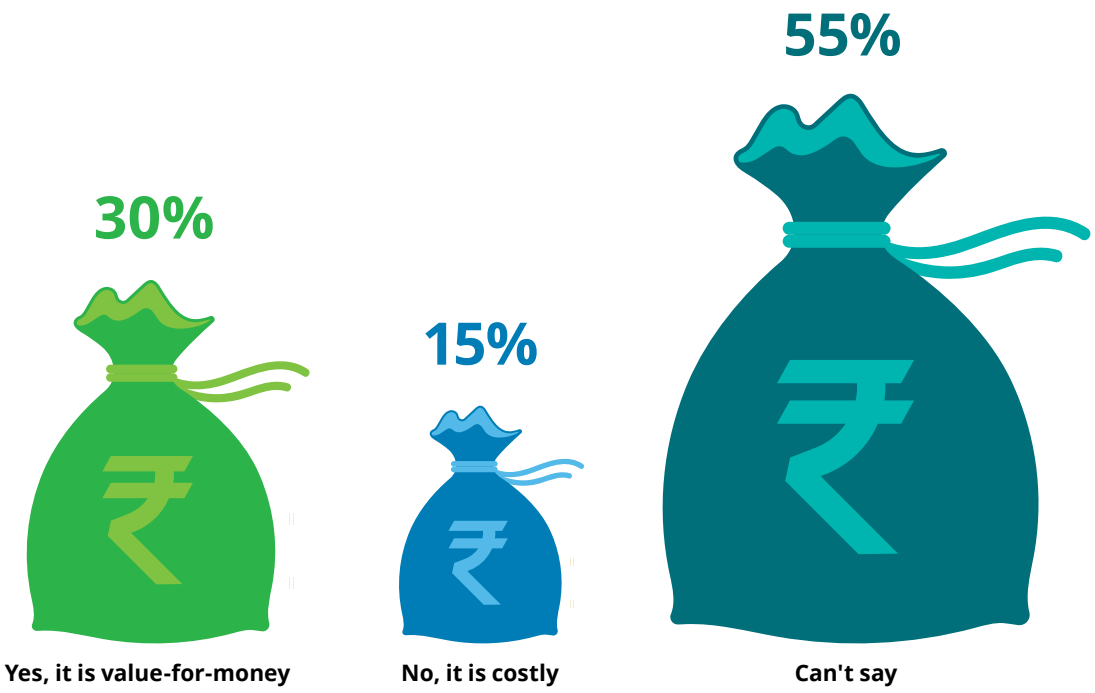
Watch out for the roadblocks

One of the survey findings revealed that several consumer firms that had earlier indicated a lesser desire to spend on digital security, were keener to increase their insurance coverage.

This interesting finding posed a question – why would firms with a lower appetite and willingness to spend on cybersecurity, want to increase cyber insurance coverage in the future? Could this mean that there has been an inclination to pass on risks to the insurance sector without fortifying their own digital security? Were firms worried that forthcoming laws would require them to opt for cyber insurance?

Despite acknowledging the importance of cyber insurance, firms with low insurance coverage were still contemplating whether to increase their insurance coverage. Was it because these respondents were not convinced of the value they would derive from insurance products?

Figure 8. Value for money spent on purchasing insurance



Q: Are you getting value for the money you pay as a cyber insurance premium?

Source: Deloitte Research

Dissatisfaction is likely to be one of the biggest roadblocks to the cyber insurance market's growth. A few factors may contribute to the discontent. Addressing these hurdles will likely help the cyber insurance market reach its inflexion point and growth will be exponential thereafter.

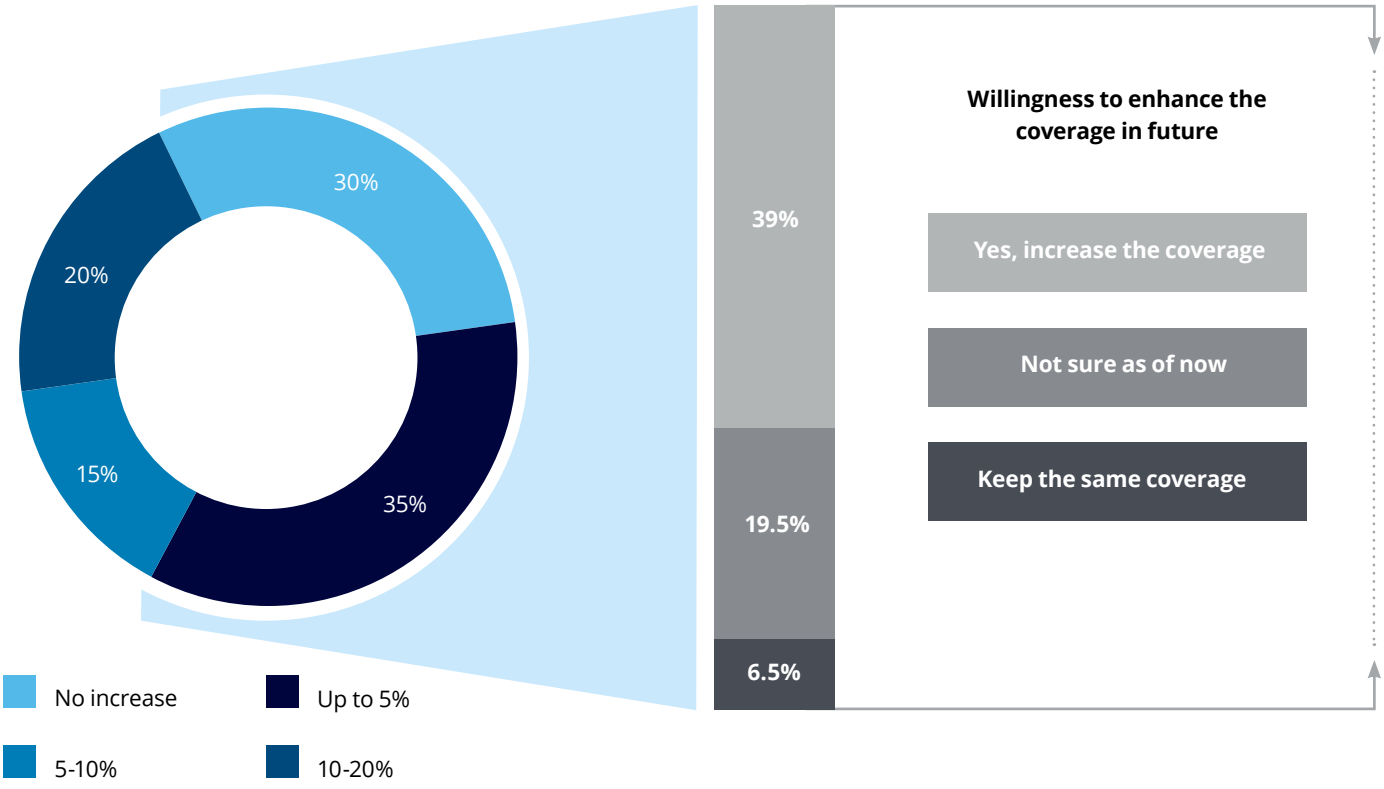
1. Cyber insurance growth paradox

Often, companies perceive cyber insurance as an additional burden if they are already investing in protecting their digital infrastructure. Consequently, purchasing insurance reduces companies' motivation to spend on strengthening their cybersecurity infrastructure. This is a paradoxical situation, where buying insurance policies results in increasing the vulnerability of digital infrastructure, and the inclination to pass on risks to insurers.

Moreover, insurance payouts may encourage hackers to specifically target and attack companies that are insured, adding to insurers' costs (although such a phenomenon has also been seen in non-cyber-related insurances).

In other words, a higher uptake of cyber insurance raises the probability of cyberattacks, leading to higher liability for insurers and premiums for buyers.

Figure 9. Willingness to spend on cybersecurity vs. willingness to increase insurance coverage in the future.



Q. How much more (from your current cyber security budget) are you willing to invest in securing your digital infrastructure over the next three years?

Against the backdrop of an increasing number of cyber-crimes and ransomware attacks, will you be willing to enhance your coverage in the next three years?

Source: Deloitte Research

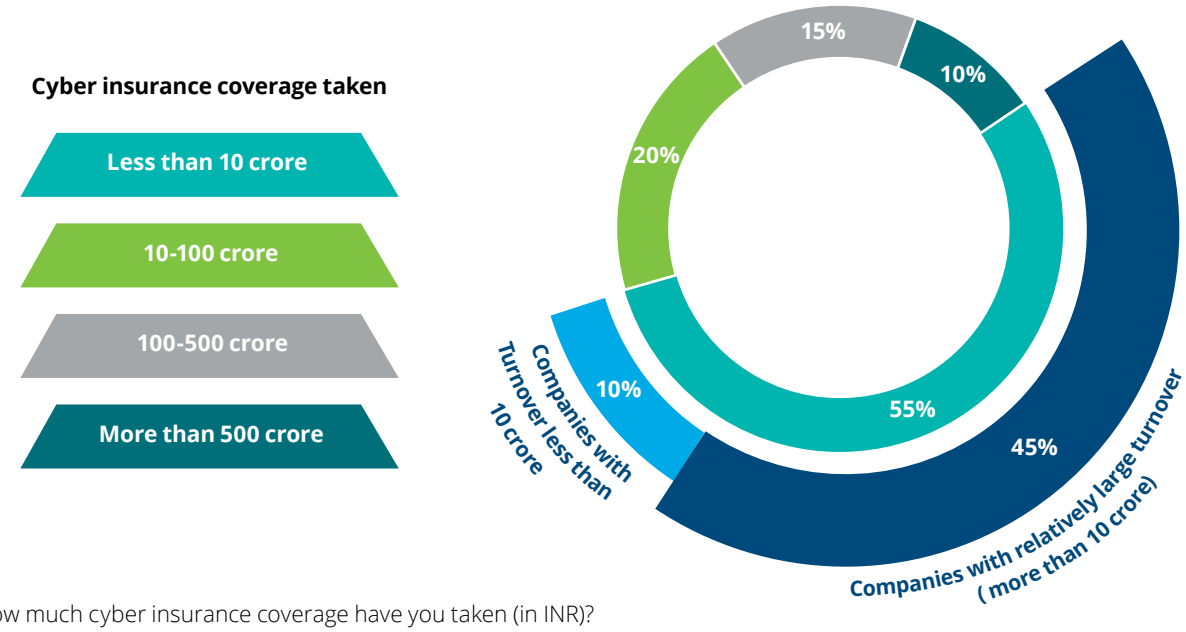
A deeper dive into Figure 7 substantiated the point made above. While a large proportion of the respondents showed a lesser inclination towards increasing the cybersecurity budget, their willingness to increase coverage was quite high. About 60 percent respondents wanted to increase insurance coverage without wanting to invest much in improving their digital infrastructure security

2. Limited understanding of cyber insurance, its coverage, and tax implications

Cyber risks by nature are hard to outline and constantly evolving. Therefore, buyers have limited clarity on the types of cyber risks (including loss of business) covered under cyber insurance and even lesser visibility on the scope and amount of optimum coverage. Besides, unfamiliarity with the claim procedure and resolutions, the ambiguous claim thresholds (stipulated by insurance companies) during settlements, and confusion around exclusions and coverage of regulatory fines and penalties under a purchased scheme further weigh on demand for insurance products. Some indirect incidents of cyberattacks may not be covered by cyber insurance. Due to a lack of understanding of financial exposure, many companies make insurance purchase decisions based on industry benchmarking (i.e., the insurance amount the companies' competitors have bought) rather than assessing actual needs.[15] As insurance is associated with an organisation's cyber risk, the cybersecurity management teams of organisations often get involved in the insurance purchase decision. These management teams often have cost allocation priorities and do not have adequate information about insurance products. Therefore, they do not prioritise such insurance, further driving up the gestation period of cyber insurance deals. However, this global phenomenon has been validated by a study by the Cyberspace Solarium Commission. This federal body was set up in March 2020 to analyse US cybersecurity preparedness.

Another challenge is the associated tax implications when cyber insurance claims are received. Depending on the coverage of the risk and the nature of the attack, whether such claims are taxable for the insured? Is the payer of such ransom money eligible for any tax deduction? As of today, there is less clarity on these questions.

Figure 10. Cyber insurance coverage relative to the company turnover



Q: How much cyber insurance coverage have you taken (in INR)?

Source: Deloitte Research

Only 25 percent respondents, mostly from a select few financial and IT sectors, opted for insurance coverage proportional to their turnover size. While 55 percent of respondents opted for coverage of INR 10 crore or lower, 45 percent of these firms had a larger turnover pointing to a severe mismatch in their operation size and coverage.

In 2022, the average cost of a data breach was estimated at US$ 2.32 million. This number suggests that any single cyber incident involving a data breach could easily affect a firm's bottom line and financial performance, and shareholder confidence. Insurance may not be sufficient to cover these losses.[16]

[15] Unlocking the Value of Cyber Insurance – 2020 Deloitte Report https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-Cyberinsurance-noexp.pdf
[16] https://www.statista.com/statistics/463714/cost-data-breach-by-country-or-region/

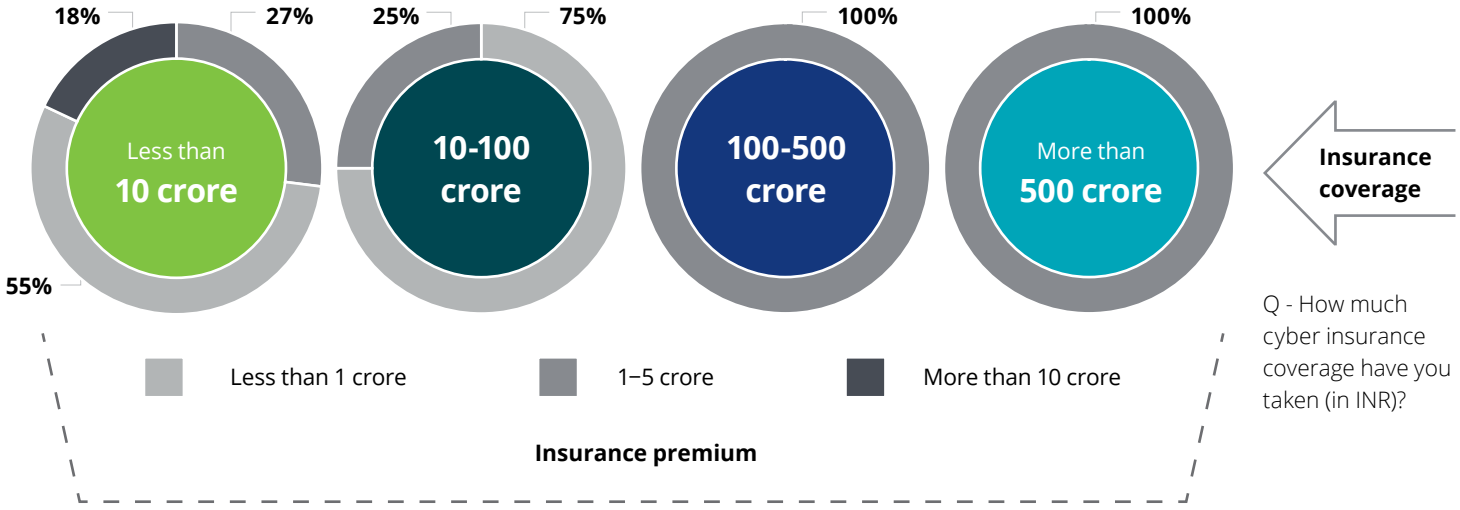
3. Sellers' dilemma of data, pricing, and underwriting cybersecurity insurance

The inability to understand the underlying cyber risks and the quantum of payout in case an incident occurs and the lack of visibility of the possible systemic effect of an attack on various stakeholders make it a challenge for sellers to price cyber risks. For instance, the loss associated with damage to a physical property (such as a vehicle), or a loss of life is estimable because such losses are contained. This visibility of losses disappears in case of cyber threats because of the systemic risks they can cause. Insurers worry that a single big attack could hit many of their clients' systems at once and even beyond. That makes the risk profile of policyholders inconsistent.

Sellers find it quite difficult to stress test buyers' digital tools exhaustively and the possible cyber threats that they could be exposed to. Moreover, due to the rapid pace of technological change and the evolving sophistication of cybercrimes, digitisation is making the traditional underwriting models redundant.

The systemic nature of cyber risk makes it difficult to assess policyholders' risk profiles. Therefore, determining the price associated with a cyber insurance policy, is a big challenge.

Figure 11. The insurance premium paid and the insurance coverage



Q - What is the premium you pay for cyber insurance coverage (in INR)?

Source: Deloitte Research

About 45 percent respondents indicated a strong mismatch between the premium paid and the insurance covered. A majority paid a higher premium for the insurance coverage they received and most of these firms belonged to the consumer sector.

4. Impact on pricing due to stringent monitoring, and terms and conditions by re-insurers

Cybersecurity infrastructure is prone to attacks. Therefore, reinsurers are reluctant to support a yet-to-mature infrastructure in India. Besides, global dynamics of cyber risk insurance markets also affect Indian counterparts as most cyber risk insurance programmes in India are governed by treaty reinsurance guidelines agreed between Indian insurers and their respective global treaty reinsurers. With the rising ransomware and social engineering fraud-related claims, global reinsurers are continuing with a tough underwriting approach and closely monitoring loss ratios in India. These affect risk selections and insurance pricing, driving up treaty reinsurance renewal rates and tightening annual terms and conditions for cyber insurance sellers. Consequently, several Indian insurance companies have witnessed capacity shrinkages in cyber.

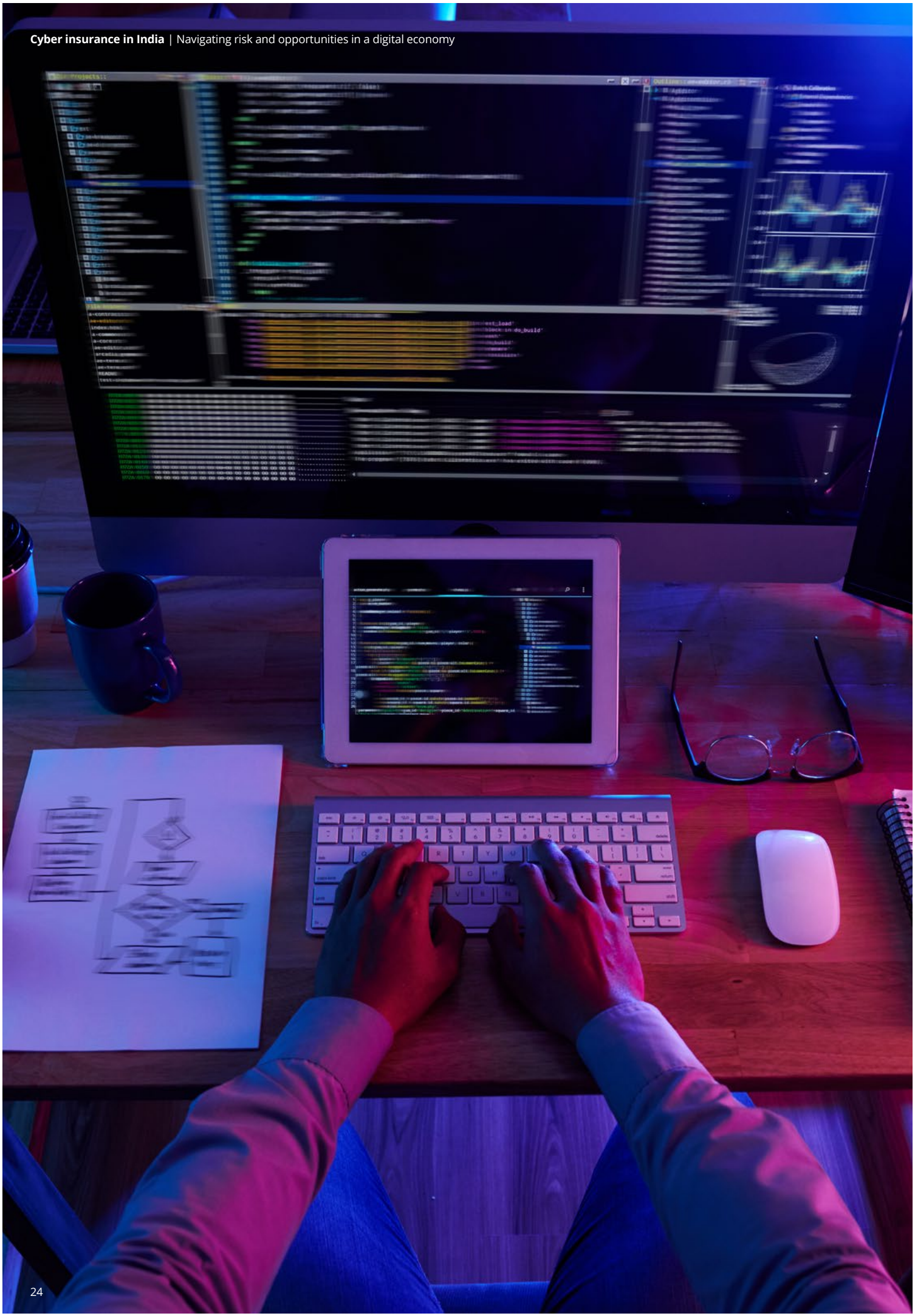
5. Ambiguity on insurance payouts for cyberattacks directed by government agencies

The incident of malware NotPetya brought forward the ambiguity associated with state-sponsored cyberattacks during any geopolitical crisis, making it unclear how to insure against such incidents. At the same time, buyers have an apprehension of denial of claims if such cyberattacks are classified as an 'act of war. The other exclusion is for terrorism, which is more frequent and unpredictable.

Case study 2

Cyber insurance payouts for cyberattacks termed as "an act of war"

In a famous case, a US-based snacking giant, which bought cyber insurance, was refused payment by a Swiss insurance major. The insurance company refused to refund its client for 'NotPetya' ransomware attacks as it considered them to be "an act of war", which was not covered by its policy.



Five steps to unleash the potential of cyber insurance

Cyber insurance is unfortunately still viewed as a "cost" rather than a risk management investment. Most of such insurance is placed on contractual requirements. The uncertainties associated with the classification and scope of cyber risks make it difficult to determine which risks can be insured. Such uncertainties have limited cyber insurance growth. Global markets, such as Singapore, the US, and the UK, cater to more sophisticated buyers from across the globe, while Indian cyber risk insurance placements still largely face pricing pressure. The market is not yet mature enough to reach its potential. Yet, cyber insurance is essential to address and mitigate cyber risks. Although the market will take some time to learn to deal with these uncertainties, some of these measures can help accelerate its progress towards maturity in the order of difficulties to implement.

1. Periodic assessment and guidance
Insurance sellers can offer an independent cybersecurity assessment in partnership with cybersecurity clinics (could be third parties) to evaluate a buyer's risks and exposure; these are quite similar to the preventive health checks done for individuals. These assessments prevent or reduce the probability of the systemic impact affecting several clients, thereby reducing the chances of multiple claims. An assessment helps determine the digital maturity and vulnerabilities, and therefore, decide the optimum premium (keeping into consideration limits and options). In addition, sellers must follow rigorous cyber underwriting, including detailed cyber questionnaires and interviews with buyers' IT security teams.

2. Incentive to invest in securing digital assets
To address the paradox, sellers can incentivise buyers to invest in safeguarding their digital infrastructure. Strong cybersecurity postures are likely to benefit in terms of coverage and pricing. No claim bonuses, extended discounts, and incentives during premium renewal could help reinforce prudent behaviour amongst buyers. Consequently, sellers can cap risk exposures and motivate buyers to continue with the cyber insurance policy longer.

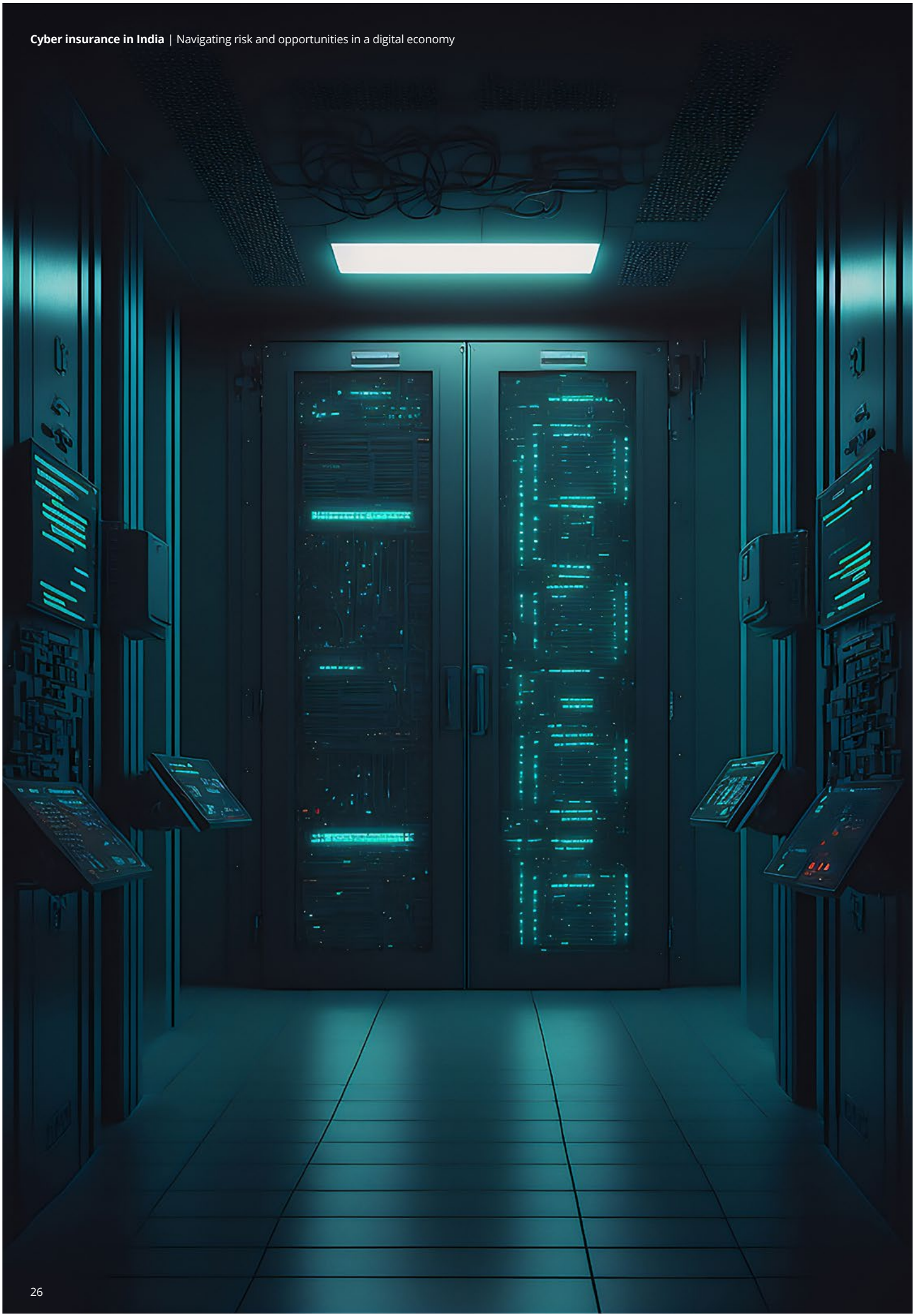
3. Cap coverage for specific threats (such as ransomware)
In India, social engineering cybersecurity breaches are the top loss contributors. The volume of the ransomware threats detected increased with the average ransom paid by Indian enterprises reaching as high as US$ 1.2 million in 2022.[17] More often than not, insurance companies bear such losses, making buyers complacent about risks and relying on policies to payout ransoms. Lately, sellers are reconsidering capping coverage or offering coverages on a sub limited/conservative basis for certain cyber incidents. Several insurers explore tools to quantify their cyber exposure and decide on cyber insurance limits. Such a cap can prompt insurance buyers to not be complacent after purchasing insurance (and address the insurance paradox issue highlighted earlier), but focus on strengthening their cybersecurity measures to avoid ransomware attacks.

4. Data sharing
Buyers working collaboratively with insurance companies and brokers, and sharing data could help insurance companies assess their needs and customise products. Buyers with a cyber incident history must be mandated to provide detailed insights on corrective measures and IT security investments done after the incident. Data availability can also help sellers build their cyber database and can help in pricing and underwriting models. Sellers can determine the vulnerable yet critical assets and the extent of losses buyers might be exposed to.

5. Mindset change
A mindset shift amongst insurance buyers will be necessary. Buyers need to understand that the insurance is to safeguard losses in the event of a cyberattack. It can reduce the liability, costs associated with remediation, and settlement costs arising due to regulatory fines.

This is a cultural aspect and may take a while in India. The realisation that cyber insurance is neither an investment tool nor a substitute for securing digital infrastructure will be critical. It is a risk management tool.

[17] Sophos, https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf



Four essential areas that need a push from the government

The government can play an important role in providing the thrust to the cyber insurance market. Mandating the uptake of cyber insurance, enabling the right infrastructure, and providing a uniform framework will help in this direction.

1. Enable data exchange

» The significant challenge today in the cyber insurance space is to deal with the dearth of data around cyberattacks, threats, and trends. CERT-In has come up with a new directive to report cybersecurity incidents within a stipulated time. Expanding India's cyber intelligence is essential; more such efforts would be needed to deal with the complexity of threats. One of the ways could be a government-backed common platform where organisations, regulators, and government agencies exchange real-time cybersecurity incidents and information on attacks. Such information exchange will help curtail cyber incidents and support cyber insurance sellers to build models to predict and forecast potential losses.

Latest update:

The Master Directions of IT outsourcing for banks, financial institutions, and other regulated businesses were released by the RBI on 10 April 2023. The directive stipulates that financial institutions must ensure that cyber incidents are reported to the RBI within six hours of the incident.[18] One of the prerequisites of cyber insurance policies is to notify insurers of a cyberattack within a certain timeframe, helping in faster and more transparent claim processing. Under the new directions, financial institutions can avoid any coverage disputes that could arise from delayed reporting. This also enables them to work with insurers to determine the extent of the damage caused by the attack and develop a plan to mitigate the damage

2. Ensure a uniform insurance framework

The Insurance Regulatory and Development Authority of India (IRDAI) has offered a framework for cyber insurance products that allow for the coverage of fines and penalties imposed on the insured company. However, more clarity is needed for differentiating payable and non-payable penalties. A better understanding of the scope of coverage and simplification of claim settlement processes, will also help the industry. Even as the industry matures, the government must provide enough information and guidance to standardise variations in cyber risk insurance coverages, simplify policy drafting language and the claims settlement process, and remove the minimum deductions. The insurance coverage should be expanded to different types of known/unknown cyberattacks. cyber risks and protecting against data breaches. The bill will mandate firms dealing with sensitive information, to purchase insurance.

[18]RBIs master direction on outsourcing of information technology services -https://rbidocs.rbi.org.in/rdocs/notification/PDFs/102MDITSERVICES56B33FD530B1433187D75CB7C06C8F70.PDF

3. Need for prompt implementation of the Digital Personal Data Protection (DPDP) Act 2023

India's Digital Personal Data Protection (DPDP) Act, passed in August 2023, aims to regulate how entities process users' personal data. The Act proposes fines of up to INR 250 crore per instance for failing to prevent a personal data breach. Failure to notify the data protection board of a personal data breach and inability to fulfil obligations while processing children's data can result in fines of up to INR 200 crore. Non-compliance with obligations by a significant data fiduciary can result in fines of up to INR 150 crore. These penalties may encourage companies to purchase cyber insurance to mitigate financial risks.

As entities become more accountable for personal data protection and regulatory scrutiny rises, they are likely to be more proactive in mitigating cyber risks and protecting against data breaches. Cyber insurance can help companies demonstrate compliance with the DPDP Act's requirements by providing evidence of financial protection in the event of a data breach or cyberattack. The Act can serve as a catalyst for companies to reassess their cyber risk exposure and consider cyber insurance as part of their overall risk management approach.

The enforcement date of the DPDP Act is yet to be determined. According to the latest update received on 20 September 2023, the Indian government will set up the Data Protection Board (DPB) within the next 30 days and lay down the rules to meet the compliance requirements of the Act.[19] Once in effect, the act will regulate the processing of digital personal data within India. Delays in implementing the new norms of the DPDP Act may expose businesses to data privacy risks. The government needs to implement the Act as soon as possible to secure personal data, ensure compliance with the new requirements, deter violations, and ensure necessary measures to protect personal data kept in India.

Latest update:

The IRDAI released a revised Information and Cyber Security Guidelines on 24 April 2023, to help the insurance industry strengthen its defences against emerging cyber threats and maintain the security and confidentiality of sensitive data.[19] The new guidelines require insurers to implement required security controls, incident response plans, and regular security audits to protect their systems and data from cyber threats. Implementing these guidelines will strengthen the insurance industry's information and cybersecurity posture, safeguard policyholder interests, and increase customer trust and confidence.

4. Create a specialised and dedicated adjudicatory system for online civil and criminal offences

A cyberattack may result in legal issues, such as litigation, regulatory inquiries, or contractual disputes. These legal challenges can be time consuming and expensive; the cost is often borne by cyber insurers. The Indian parliament intends to enact the Digital India Act that proposes to empower organisations such as CERT-In, to create a legal framework for digital governance, data protection, and cybersecurity. These will aid in managing legal conflicts resulting from digital transactions.[20] Creating a dedicated adjudicatory system is a crucial step towards cutting legal and regulatory expenses. This reduces the financial burden on insurers, and they can pass on the benefits to insurance buyers by way of lower premiums.

[19]https://pib.gov.in/PressReleasePage.aspx?PRID=1959161
[20] MEITY's proposed Digital India Act 2023 https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

Summary

Cyber insurance is a niche market and has seen a difficult time lately due to the rising number of breaches and increasing complexities of cybercrimes. These instances have resulted in a sharp rise in premiums and a lower ability amongst sellers to offer flexibility. While sellers faced higher payouts with rising claims, the impact on premiums caused buyers to contemplate the value they derived from the purchase of cyber insurance. Besides, variations in cyber insurance features, coverage, premium, and terms and conditions limit the understanding of buyers and the ability of sellers to assess the risk exposure of assets. In this report, we offered our perspective on the nascent yet highly potent, cyber insurance market in India. Given that there has not been much literature available in the context of the Indian market, we validated a few of our insights using a survey.

There are three things that could determine the future prospects of cyber insurance.

Buyers need to understand their need for cyber insurance and consider appropriate risk assessments to determine the level of protection and coverage they would require.

Sellers must prioritise simplifying insurance policies and educating their customers on various types of coverage to assure buyers of the significance of such risk management tools. At the same time, they must review the defences that buyers are building to safeguard their assets.

The government also has a critical role in determining an effective data protection framework that ensures the privacy of citizens. The government's strict compliance and regulations around data collection, breaches, and reporting may increase the willingness of businesses to purchase insurance and hedge a part of cyber risks. For certain businesses, regulations may require the mandatory purchase of cyber insurance (businesses with high systemic risks, such as banking) Additionally, the government should facilitate data exchange through a central agency on cyberattacks; this can be leveraged to build risk models for cyber insurance and enable better risk evaluation.

We believe the next decade will see the cyber insurance market grow at exponential rates and cyber products become more prevalent. It is going to be an asset for businesses of all sizes. However, its potential will lie in the right products that meet the needs of both buyers and sellers. Advancing technology and government initiatives will play an important role in this regard.

Connect with us

Himanish Chaudhuri
Partner and Financial Services Industry Leader,
Deloitte India
hchaudhuri@deloitte.com

Deepa Seshadri
Partner and CIO Program Leader,
Deloitte India
deseshadri@deloitte.com

Anand Venkatraman
Partner, Risk Advisory,
Deloitte India
anandv@deloitte.com

Debashish Banerjee
Partner and Insurance sector leader
Deloitte India
debashishb@deloitte.com

Contributors

Bahroze Kamdin

Dr. Rumki Majumdar

Meryl Fernandes

Roshan Kule

Acknowledgements

David George

Arti Sharma

Mou Chakravorty

Harsh Trivedi

Swarup Sonar

Deloitte.