Cybersecurity: how do you rise above the waves of a perfect storm?

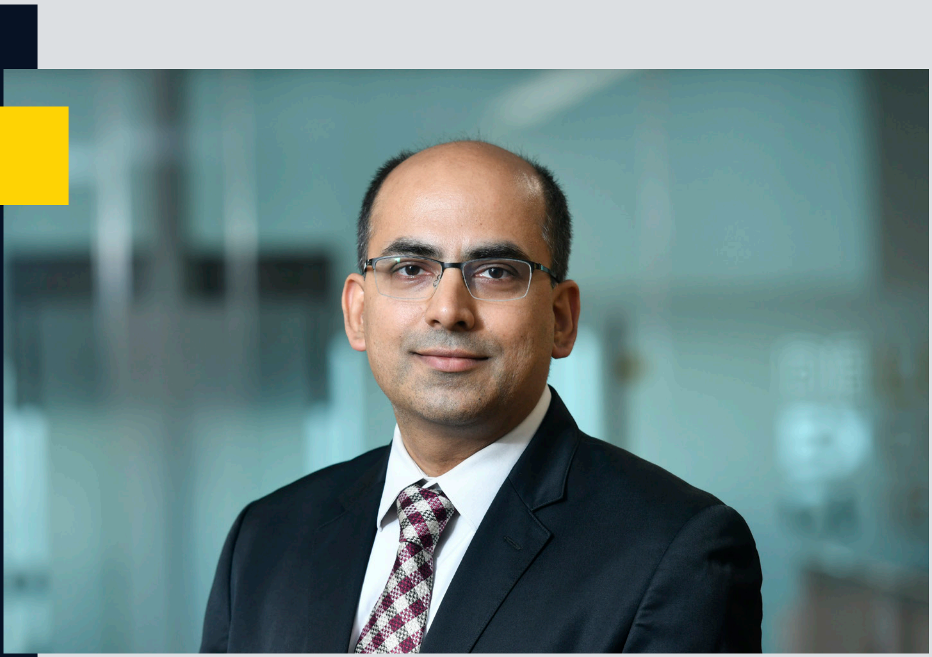
EY Global Information Security Survey 2021: India Edition

The better the question. The better the answer.
The better the world works.

EY
Building a better
working world

Table of Contents

Foreword



Rohit Mathur

EY EMEIA Consulting Risk Leader

Welcome to the 23rd annual EY Global Information Security Survey (GISS) 2021 India edition, which explores the most important cybersecurity issues organizations face today. We are grateful to the more than 120 respondents (Chief Information Security Officers (CISO) or equivalent) across multiple sectors for participating in this invitation only survey.

It is encouraging to see CISOs increasingly advocating the adoption of Security and Privacy by Design amid the challenges posed by the global pandemic. India has also made it to the top 10 in the Global Cybersecurity Index (GCI) 2020 by the International Telecommunications Union (ITU), moving up 37 places . Whilst the CISOs are on the right track, a complete transition is yet to be witnessed in organizations.

To ensure this transition successfully, it is critical to implant cybersecurity as a part of a firm's strategy, technology transformation initiatives and now increasingly in the broader Environmental, Social and Governance (ESG) framework. The need of the hour is to include cybersecurity across the entire business value chain even as much attention is being given to privacy owing to the upcoming Personal Data Protection Bill.

This year's GISS illustrates the devastating and disproportionate impact that the COVID crisis has had on a function that is striving to position itself as an enabler of growth and a strategic partner to the business. Notably, the report also outlines what cybersecurity leaders need to know about their current operating environment and what they need to do to transform it. Organizations need to hit refresh, adopt radical change and spearhead this revolution to lay a strong foundation for the future.

[1] Source: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

What has changed from pre-pandemic era?

Murali Rao

EY India Consulting Cyber Leader

The pandemic posed a variety of challenges and disruptions to most of the firms across industries. The Chief Executive Officers (CEO) grappled with multiple novel challenges to sustain their businesses and then thrive. They took a phenomenal leap of faith to embrace the inevitable change, come up with innovative, and cost–effective solutions and enable the entire business value chain to go digital.

In fact, many CISOs invested in secure systems in a sudden frenzy. But even as the firms transformed themselves, they were not completely prepared for the looming attacks by threat actors. A major challenge has been to onboard senior stakeholders to the cybersecurity value proposition. With a fast–evolving regulatory environment, cybersecurity has become a part of the board meetings.

The recent release of cybersecurity guidelines in the power sector to create a secure cyber ecosystem is a great example. The guidelines aim to promote research and development in cybersecurity and open the market for setting up cyber testing infrastructure in public and private sectors in the country. Ultimately, cybersecurity in the power sector will not only address potential threats from disgruntled employees, terrorists, and espionage operations but will also take care of vulnerabilities arising from user errors, equipment failures, and natural disasters and reduce risk significantly for itself.

Active participation by each stakeholder has now become pivotal. The business transformation would not just require investments, but also the creation of a cyber aware culture and embedding cybersecurity as a core business strategy. Our report outlines what leaders need to know now about their current operating environment and how they can transform it.

Besides senior stakeholder buy–in, our global survey of more than 1,000 senior cybersecurity leaders finds CISOs grappling with inadequate budgets, struggling with regulatory fragmentation, and failing to find common ground with the functions that need them the most. Leaders across organizations and government departments expressed their concern on how to become cyber resilient, adopt security and privacy by design, and so on.

As a prelude to the survey results, we present to you a summary of the key focus areas of security professionals as the pandemic wanes. The survey highlights how the CISO's relationship with the business is under more stress than before, and the fallout is greater exposure to cyber risk coupled with budget restrictions. The survey clearly establishes the urgent need for inclusion of cybersecurity as part of business strategies to enable the business transformation.

Executive summary

Survey results

India is aspiring and consciously moving towards becoming a digital economy. However, heightened cyber security attacks and challenges are posing a threat to India's growing digital society. The cyber threat to organizations with extended supply chains and broad ecosystems is truly global but regulation is becoming more fragmented. The COVID–19 pandemic has further stretched the potential attack surface for bad actors, and the responsibilities of CISOs as well as the government have never been so critical and core. They must counter the global risk and manage local compliance whilst supporting their organizations' efforts to focus on technology - enabled rebound and growth.

Many CISOs across India are feeling the strain. GISS reveals the emerging and increasing stresses of the global–versus–local balancing act. As CISOs work to transform their organizations to create long–term value, the stakes are high. This year's GISS also points to the mechanisms and solutions to create that long–term value and accelerated growth.

EY recommendations in brief

Based on the findings from this year's GISS 2020–21: India edition, there is now a real opportunity to position cybersecurity at the heart of business transformation and innovation. This will require boards, senior management teams, CISOs and leaders throughout businesses and the government to work together to:

1. Envision a paradigm shift for cybersecurity
2. Strategically approach the cyber funding
3. Enhance the communication and inclusion through the business value chain

The situation is likely to get worse before it gets better. Organizations want to invest in technology and innovation for the post–COVID era, and they need to ensure resilience for the next significant disruption. Still, many are yet to address the deferred risks and potential vulnerabilities introduced during their transition efforts at the height of the pandemic.

CISOs are at crossroads. To contend with the complex and draining issues they face, they must act fast. Our report deduces what cybersecurity leaders need to know now about their current operating environment and what they need to do to transform it.

1

CISO at the crossroads

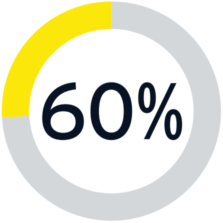
Current cybersecurity landscape in India

The COVID–19 pandemic has bulldozed every business to adapt to disruptions within timeframes that would have otherwise been considered as a herculean task just a short time ago. Agile and progressive organizations rolled out new customer–facing technologies and cloud–based tools that supported remote working and kept the channel to market open. We further saw many government departments accelerating technology adoption for citizen services as well as for inter–departmental coordination.

This forced us to rapidly adopt a digital lifestyle making internet the backbone today for all services, giving rise to rapid proliferation of Social Media, Online Shopping, Digital Payments, e–Education, e–Health, etc. But the speed of change came with a heavy price. We saw cyber–attacks increasing in exponential manner towards various Critical Information Infrastructure (CII) entities specifically across power and other utilities. Many businesses did not involve cybersecurity in the decision–making process, whether through oversight or an urgency to move as quickly as possible. In today's world, everyone – organizations, cybersecurity professionals, hackers, and activists – is a next–door neighbour in the cyberspace and hence, it has escalated the potential attack surface for bad actors, thereby increasing the importance of cybersecurity manifold. It is no more a matter for security experts and web admins to take care of. Hackers and cyber attackers are no longer restricting to companies and government but targeting individuals too. India reported 1.16 million cyber security cases in 2020, that's 3–fold more than 2019, as per government data presented in the parliament of India. Over 3,000 cybersecurity related issues were reported daily during the year[2].

'Financial services sector is a hub for cyberattacks' is a statement of bygone days. Today, no industry is safe or spared from attacks. Each sector such as manufacturing, energy, retail, professional services, government, healthcare, media, transport, education, etc. has been a victim of cyber–attacks.

The Indian Computer Emergency Response Team (CERT–In) observed over 0.6 million cyber security incidents in the first six months of 2021[3]. The responsibility of managing such incidents has been thrust upon CISOs, leaving them in deep waters.



To further strengthen this, based on the survey, 60% of the respondents believed that there has been increase in cyber–attacks in the last 12 months.

> Driven by the hyper disruptive landscape over the last few months, there is a complete transformation of how organizations work and collaborate with their partners and reach out to customers. With the exponential increase in data usage, the new way of working has led to whole new sets of diverse risks that are associated with managing operational continuity, compliance and security.
>
> Tiffy Isaac, EY Cyber Partner

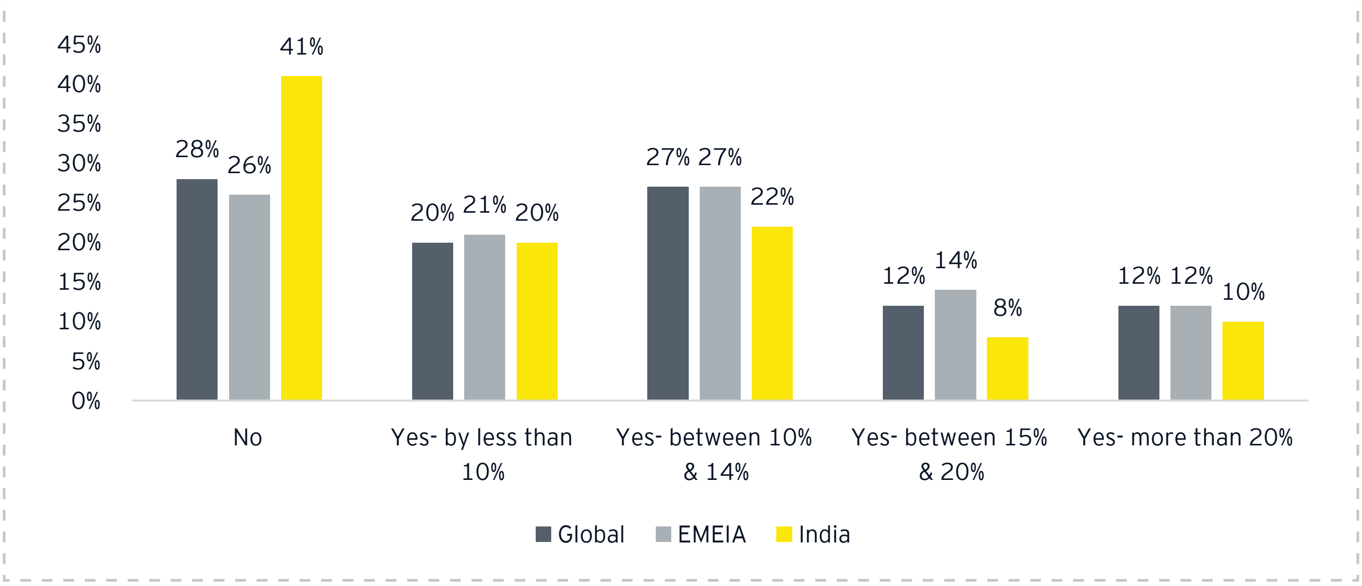
[2] https://economictimes.indiatimes.com/news/company/corporate-trends/3x-increase-in-cyber-attacks-results-in-increased-budgets-and-attention-on-cyber-security-issues-etilc-members/articleshow/83949181.cms?from=mdr

[3] https://economictimes.indiatimes.com/news/india/over-6-07-lakh-cyber-security-incidents-during-first-half-of-2021-govt/articleshow/84832168.cms?from=mdr

Yet, CISOs are struggling to make themselves heard. Almost half of the respondents **(46%)** admit that cybersecurity teams are not consulted, or are consulted too late, when leadership makes urgent strategic decisions. Whilst some maintain that this happens 'not very often', it only needs to happen once for a flaw in the defences to be exploited by threat actors.

85% respondents either believe that hackers are using new strategies, such as exploiting vulnerabilities in procurement and the supply chain, and do not know whether their defences are strong enough to stop the attacks to be successful, or do not know at all.

Fig: 1.1 – Have you seen an increase in the number of disruptive attacks over the last 12 months?



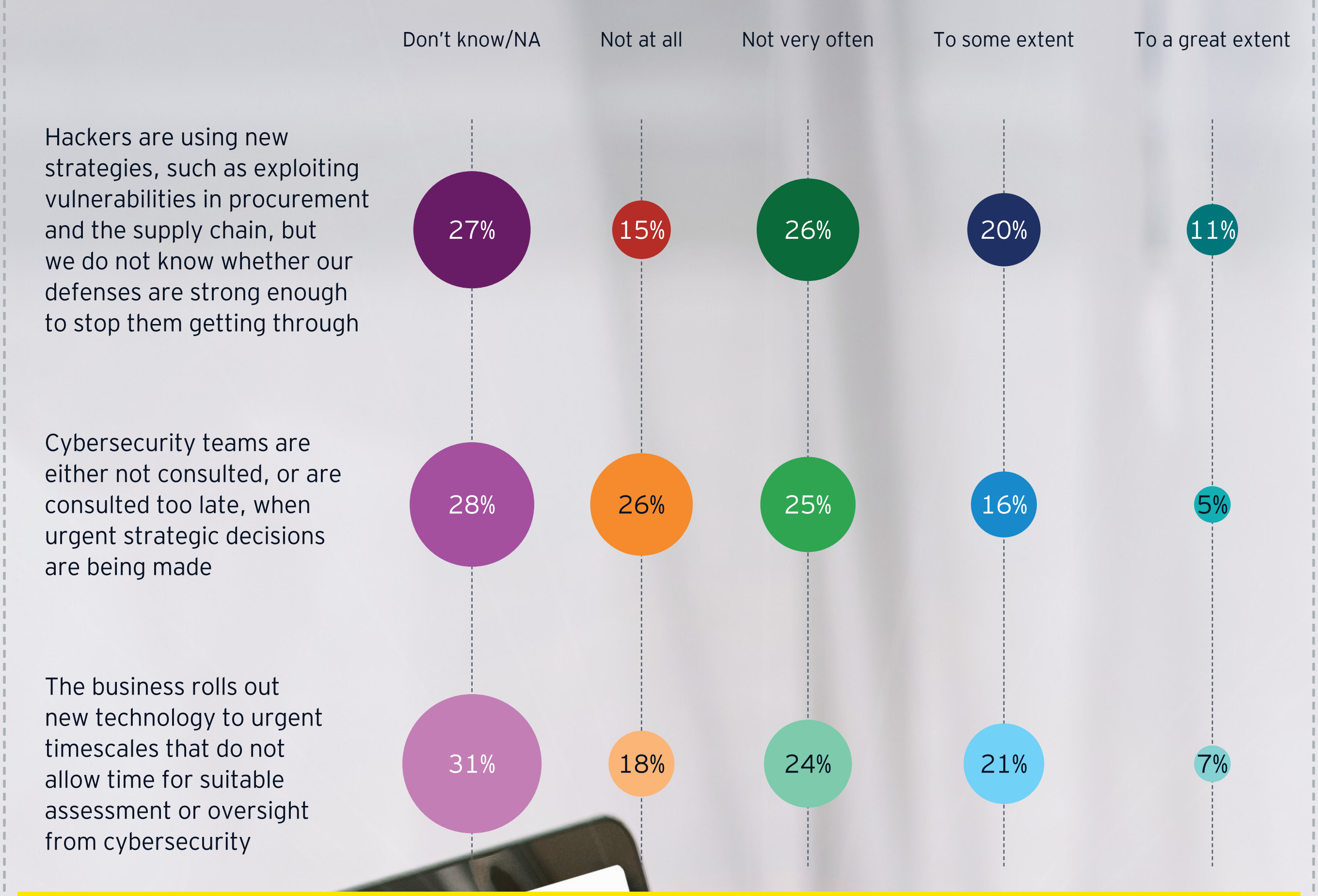
In this year's GISS, **over three - quarters (76%)** of Indian CISOs agreed that they have never been as concerned before about their ability to manage cyber threats for the business.

Over the last year, threat actors have increasingly adopted new strategies, whether by targeting businesses with phishing campaigns, by embedding backdoor codes that enable exploiting commercial software, targeting newer vulnerabilities in the areas of procurement or exploiting the ever–evolving Supply Chain which has very quickly moved from the Physical Supply Chain to Software Supply Chain and now to the Digital Supply Chain. Attackers are targeting a growing attack surface area and their tactics are increasingly getting more and more unpredictable. Alarmingly, 60% of the respondents either do not know or are not confident in their ability to make the supply chain suitably robust or water - tight, highlighting the importance of working closely with colleagues in procurement and operations. **Less than half (44%) the respondents** say they understand and anticipate the strategies attackers use; an issue that has been illustrated by the increase in cyber incidents.

> The need of the hour is for the organizations to revaluate the defences, where the trust factor associated with the cybersecurity tools and technologies are to be regularly reassessed as the threat actors and hackers are increasingly targeting the same tools that are used for detecting and defending the enterprise.
>
> Krishna P Sastry, EY Cyber Partner

To what extent do the following take place in your business?

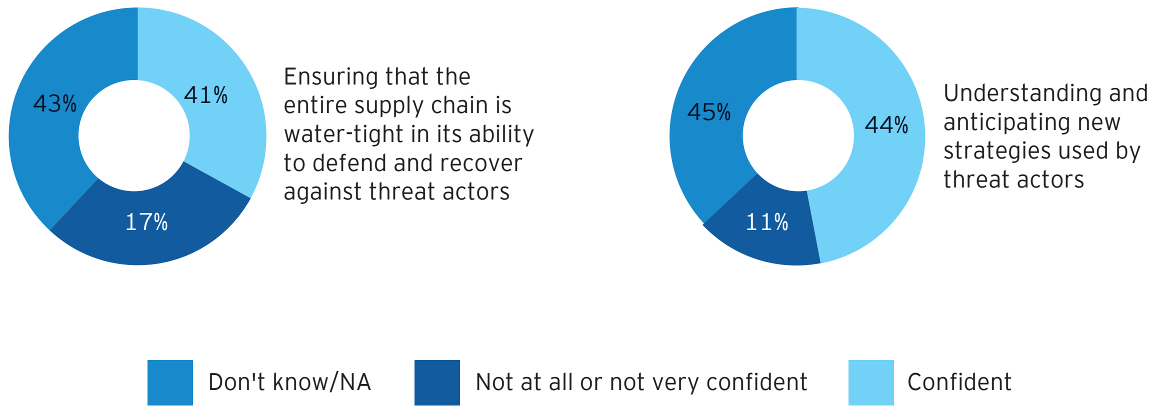
Fig: 1.2 – Cybersecurity teams are excluded from decision - making in businesses



More than half **(56%)** of the respondents agreed that either they are not confident, or they are not aware about their team's abilities to understand and anticipate new strategies used by bad actors.

How confident are you in your team's abilities across the following areas

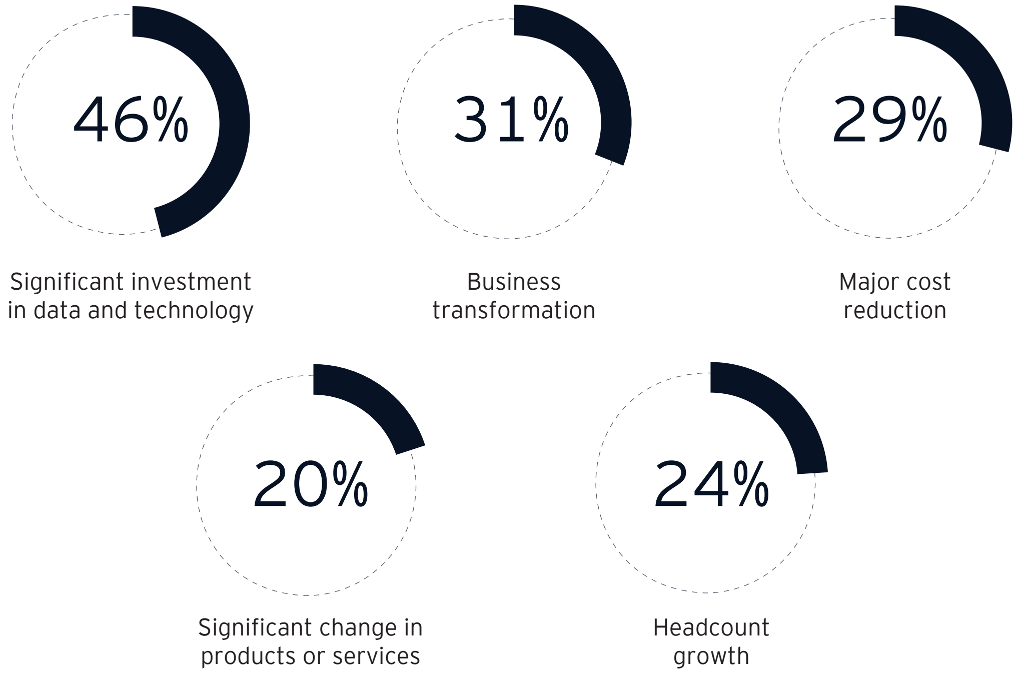
Fig: 1.3 - CISOs are lacking in confidence when faced with threat actors



As CISOs work to transform their organizations to create long–term value, the stakes are high. As companies become more and more digital, cyber security plays an important role in their journeys. CISOs are struggling to turn these digital risks into any kind of competitive advantage to create long–term value. Businesses are witnessing a renewed focus of customers for a differentiated experience, responsive cybersecurity posture, digital, sustainability, etc.

Which of the following actions do you anticipate your organization will take in the next 12 months?

Fig: 1.4 – Businesses' top 5 strategic priorities suggest an ongoing focus on transformation



2

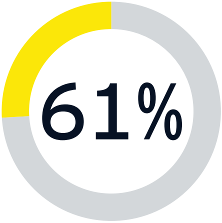
Three challenges holding back the CISO

Are today's cybersecurity organisations severely underfunded? – Turning the tide on cybersecurity

The sudden thrust towards digitization involving the new internet users particularly from rural and semi-urban population has made organizations more susceptible to data breaches and frauds like phishing and ransomware.

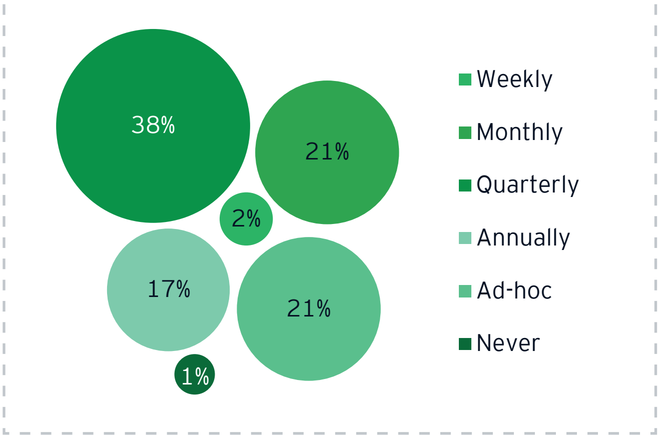
A malware attacked the power utility systems of Mumbai in 2020 which caused a massive power outage. The power disruption halted trains and shut down stock exchanges and hospitals for hours. In recent months, supply chain attack incidents such as the hacking attempt of IBM vaccine supply chains, the breach of file security at Singtel, the hacking of 570 ecommerce sites including those in India and the data breach of companies like Upstox, Mobikwik resulting in exposure of sensitive customer data has alarmed companies around the globe. The impact of these attacks is witnessed not only at an individual, an organization, a sector, or a specific geographic level but something that has to be dealt by unified allies at the Global or national levels. In the wake of these crisis, cybersecurity professionals have the chance to advance their reputation in the cybersecurity field.

The discipline of cybersecurity is under greater scrutiny today than it has been in the past. The Board has acknowledged the need to discuss security issues more frequently than ever before considering the sudden spike of cybersecurity incidents in India.

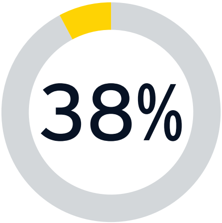


of those surveyed said cybersecurity was discussed in a Board meeting at least once in a quarter.

Fig: 2.1 How often is cybersecurity on the agenda of the Board?



Despite the need for agility given the volatility of the pandemic era and the possibility of future disruptions, survey data indicate that budget allocation processes remain largely rigid.



of the respondents agree that is only a matter of time before they suffer a breach that could have been avoided through investment'

Whilst **almost half (41%)** of the respondents say that the cybersecurity budget is a part of larger expense and is defined dynamically, the cybersecurity budget has been considerably low to manage the challenges organizations have been facing since the pandemic started. Not surprisingly, **2 out 3 (67%)** believe that their cybersecurity budget is either lower to what is needed to manage the cyber-related challenges that have emerged in the last 12 months or could not conclude.

We observed that about **69%** of the respondents were of the opinion that their annual spend on cybersecurity is below US$500,000. Nearly 7 out of 10 (67%) CISOs believe that their budget is lower than what they needed to manage the cyber-related challenges that have emerged in the last 12 months.

To mitigate the challenges of a weak and undefined cybersecurity budget, focus has been on the following activities (Kindly note the list below is not mutually exclusive):

14% reviewed their legacy architecture for cost-reduction opportunities

13% realigned cybersecurity requirements to better meet changing business needs

7% reduced the employee headcount

10% scaled back innovation activity to focus on core, non-strategic tasks

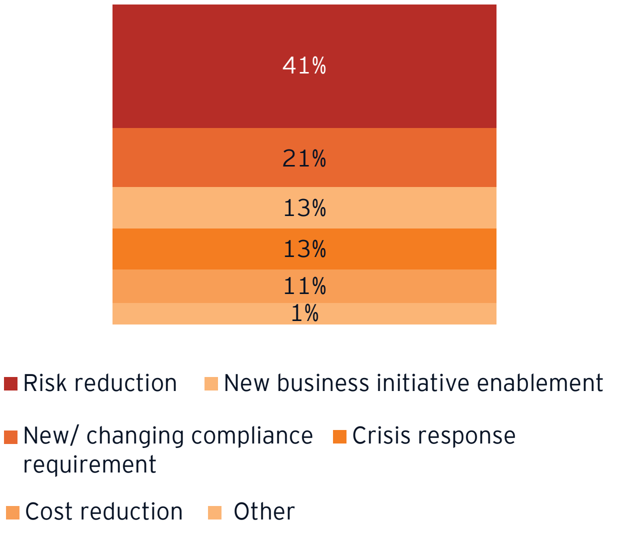
16% increased reliance on third-party providers

[4] Supply Chain Attacks - The new danger, https://ccoe.dsci.in/2021/06/21/supply-chain-attacks-the-new-danger/

> Through an iterative and data driven approach, CISOs need to work out a cohesive narrative that establishes security investments as a value add over time with a realistic payoff period, and a clear vision of demonstrating performance against committed parameters
>
> **Prashant Choudhary, EY Cyber Partner**

Below are the primary drivers for cybersecurity budget allocation:

Fig: 2.2 – What is the primary driver for new or increased spending (i.e., the easiest way to justify new funds)?

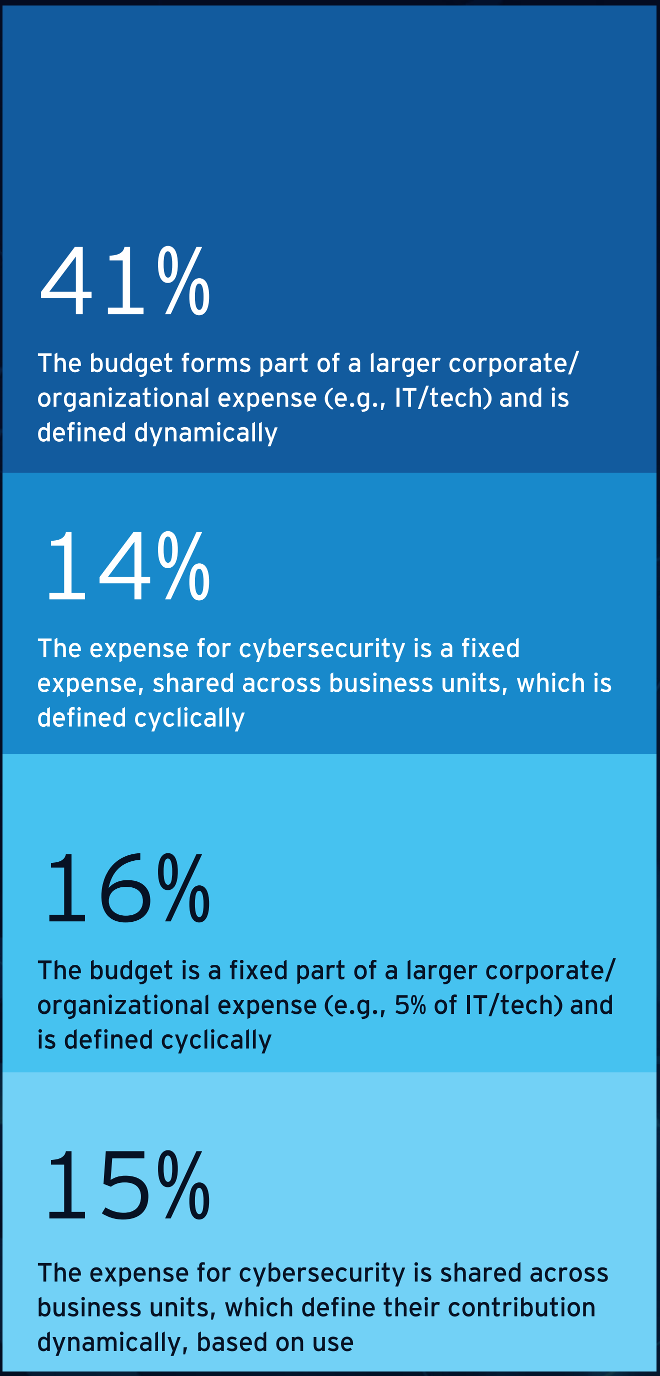


41% of the respondents agree that risk reduction is one of the key drivers for increased spending'

5 'India Cybersecurity Services Landscape – A Global Hub in the Making' report - Data Security Council of India (DSCI)

Strategic alignment of expenditure

Fig: 2.3 - How do you define your cybersecurity budget?



41%

The budget forms part of a larger corporate/organizational expense (e.g., IT/tech) and is defined dynamically

14%

The expense for cybersecurity is a fixed expense, shared across business units, which is defined cyclically

16%

The budget is a fixed part of a larger corporate/organizational expense (e.g., 5% of IT/tech) and is defined cyclically

15%

The expense for cybersecurity is shared across business units, which define their contribution dynamically, based on use

Most of the respondents throughout India believe that cybersecurity expenses are not factored adequately into the cost of strategic investments and most Indian respondents agree with this scenario. As a result, even though the amount of cybersecurity investment in India is higher, there is still a need for organizations to strategically invest in the cybersecurity function.

In a pandemic year, security leaders had to cut spending due to budget restraints, but that trend is reversing in 2021.

According to market analysts, India's cybersecurity services industry is projected to grow from US$4.3 billion in 2020 to US$7.6 billion in 2022. It is estimated that the market size for data security in India will be US$13.6 billion by 2025, and it will grow at 21% per year5.

The increasingly widespread use of technology by employees across various layers of an organization, has exposed numerous entry points for attackers, placing a heavy strain on legacy systems. For example, the IT architecture of banks consists of on–premises core legacy systems and a wide range of bespoke and ancillary applications. Legacy systems perform critical functions but may not be able to scale up to ‘speed and mobile banking’ requirements. As part of the changing paradigm, core applications are being integrated with new ones (mobile, SaaS, etc.), exposing them to new, frequent, and ever–evolving cybersecurity threats. Only a few firms relied on third–party providers. They mainly relied for security operations, vulnerability management, physical security and awareness and training.

5 ‘India Cybersecurity Services Landscape – A Global Hub in the Making’ report - Data Security Council of India (DSCI)

Is regulatory fragmentation presenting bigger challenges for CISOs?

Privacy and security regulations demand more from CISOs than ever before. Global businesses operating in multiple jurisdictions are under additional pressure due to fragmentation of regulation.

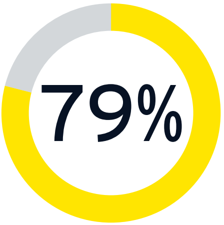
Compliance is one of the most stressful aspects of their jobs for approximately three out of five (60%) respondents, and approximately 61% expect regulations to become even more fragmented and time–consuming in the future.

> The Indian compliance environment is becoming more complex, with organizations operating at National and International levels, with silos, overlaps and massive amount of data being generated by Indian citizens. The regulatory and legal requirements are bound to get more explicit and stringent basis various industry/sector.
>
> **Vidur Gupta, EY Cyber Partner**

Is it the time to strengthen the relationship between cybersecurity and other leaders?

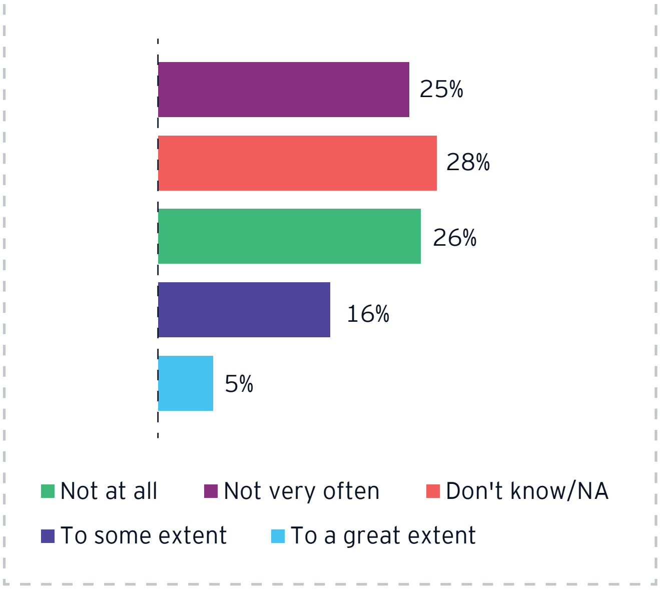
Cybersecurity teams are most effective when they are involved from the planning stage of a new business initiative. The early involvement helps CISOs to analyze the security impact of an initiative and establish appropriate security checks. However, the relationship between cybersecurity and other functions sometime lacks mutual trust and frequent consultations.

CISOs have always worried about weak relationships, but the GISS suggests the problem is becoming more pronounced. According to the study, business leaders are not considering cybersecurity during important conversations.

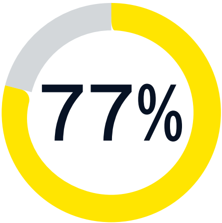


Most organizations (79%) are not able to assess or oversee cybersecurity risks by analyzing technologies and performing security assessments and implementing checks due to their late involvement in projects.

Fig: 2.4 – Cybersecurity teams are either not consulted, or consulted too late, when urgent strategic decisions are made



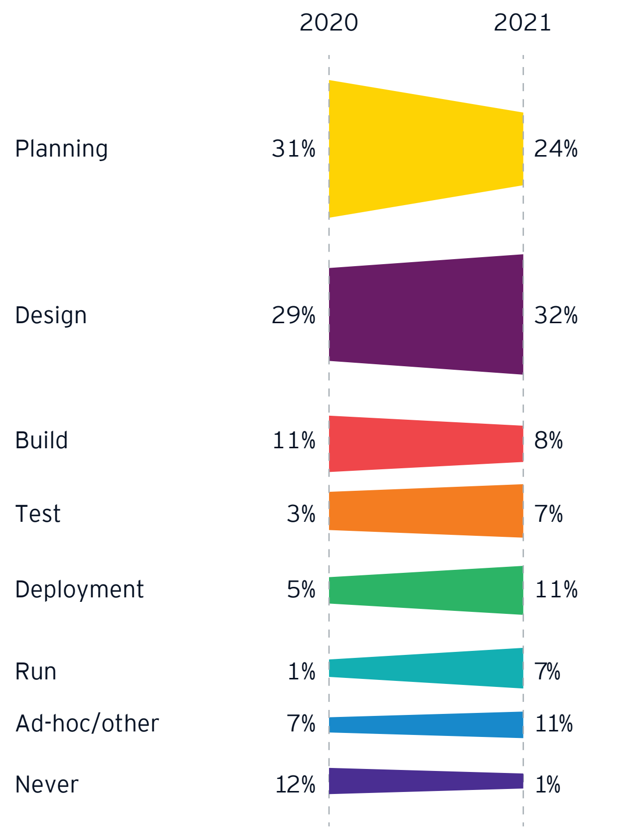
> In addition to the role for protection and recovery, the CISO is required to be perceived as an internal business partner and a trusted enabler for transformation in alignment with the strategic goals of the organization. The additional focus of a CISO needs to be around business value creation, including enhancing customer experience.
>
> **Mini Gupta, EY Cyber Partner**



In the wake of the pandemic, 77% of the organizations sidestepped cyber processes and failed to consult security teams during the planning phase.

CISOs will need to strengthen relationships with other managers. Amongst respondents, 29% perceive their relationship with the marketing department as unfavourable, whereas 20% believe their relationship with business owners is weak. Compared to 2020, when more than a third of respondents (36%) believed that cybersecurity teams were consulted when planning new business initiatives, that number plunged to 23% in 2021. This could be due to the fact that the business and cybersecurity teams are finding it challenging to co-ordinate and communicate frequently in remote working model.

Fig: 2.5 - At what stage in a new business initiative's journey is the cybersecurity team brought in?



> Cybersecurity has been evolving from a technical discipline to a strategic concept and it is imperative for businesses to have the Cybersecurity function as a strategic contributor starting at the Board
>
> **Burgess Cooper, EY Cyber Partner**

3

Next steps for the organizations and CISOs

Building a bridge together

It is difficult to progress when teams do not communicate well.

CISOs often find it difficult to get their people to articulate the commercial need for cyber consultation. Although cybersecurity has traditionally aided businesses in reducing risk, the business does not see the security function as a strategic partner. Based on the GISS survey only **15% CISOs** think senior business leaders would describe cybersecurity as commercially minded.

> It is of paramount importance that the cybersecurity function is supported by the Board as a trusted enabler for transformation and growth. The rapidly growing rise in cyberattacks worldwide comes at a hefty cost for businesses, with the increase in frequency and increase in associated financial losses
>
> Karthik Shinde
> EY Cyber Partner

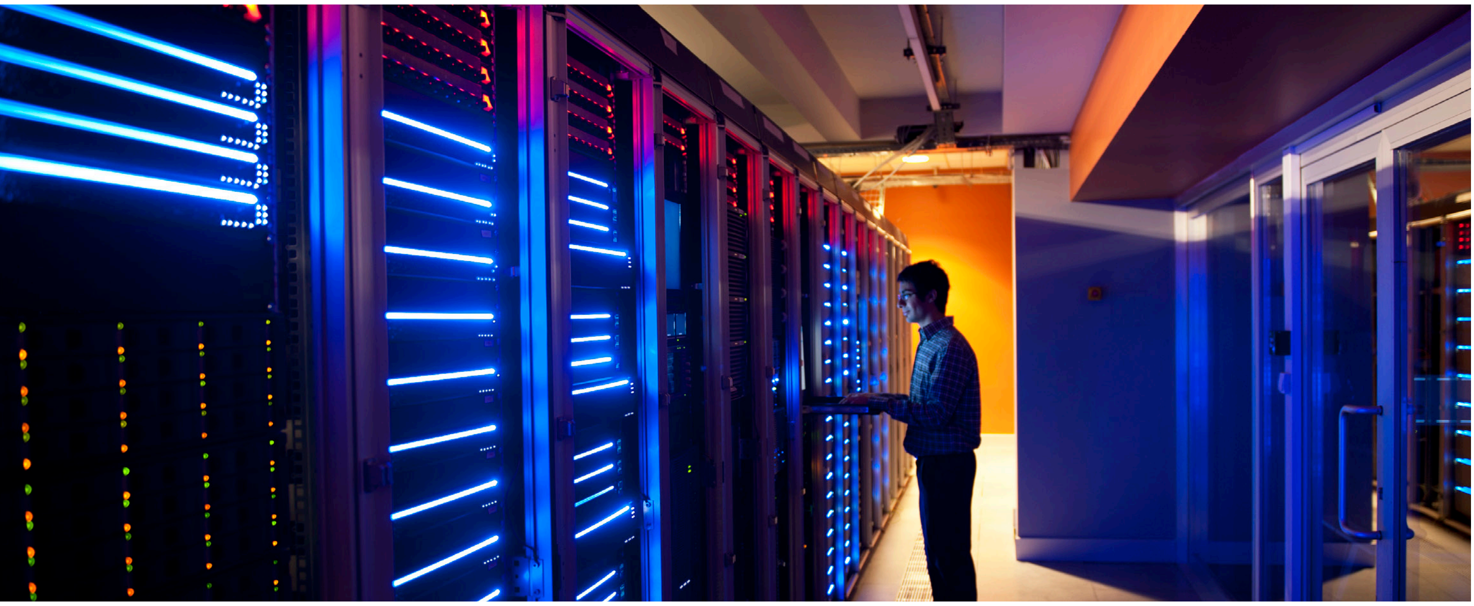
This is where the Executive Management, the Board and the CEOs should foster and contribute with the CISOs to bring cybersecurity to the forefront as the trusted enabler for the transformation and growth. The Executive Group should enable CISOs to incorporate the following activities into cybersecurity ecosystems to deal with the issues mentioned above:

Establish a partnership between business functions and cybersecurity specialists in order to change their culture of division and enable stronger relationship with the cybersecurity team.

Ensure communication and collaboration early on by working together from the very beginning, at application ideation and architecture design and review stages, IT and security teams can work more effectively together and avoid conflicts arising at the later stages.

Ensure that cybersecurity becomes a strategic business operation by letting the CISOs become a risk management leader.

The CISO to shed the image that cybersecurity is not commercially minded, and translate the commercial advantage it brings by securing the organization effectively.



Conclusion

CISO to envision a paradigm shift for cybersecurity

The onset of the pandemic has thrown normalcy out of gear. The synapse between the COVID–19 pandemic and cybersecurity imperatives can be addressed with a call to execute new cybersecurity strategies.

There must be a sync with these modern realities and adaptation along with willingness of organizations to innovate for future disruptions which will in turn reinvigorate trust and boost our digital immunity.

CISOs must be available to different departments and remain ahead of the curve in an ever–changing threat landscape, across all areas of cyber security. CISO’s relationship with the Board must shift from ‘informing the Board’ to ‘educating the Board’ and eventually ‘leading the Board‘ on cyber risk program, its maturity and way ahead.

> “
>
> Successful digital transformation is not possible without successful data transformation. Redesigning and integrating the approach to data from siloed to a pan–enterprise one, managed and protected consistently and systematically throughout the entire lifecycle, would determine the success of digital transformation.
>
> **Lalit Kalra, EY Cyber Partner**

Strategic approach to cyber funding

To respond to organizational challenges pertaining to rapidly proliferating cyber threats, most Indian CISOs have undergone tremendous stress in order to strike a balance between increasing cyber threats and appropriate cybersecurity budgets.

Whilst organizations are realising the importance of cybersecurity, their budgets need to be restructured to reinforce their cyber defence. Additionally, cybersecurity budgets should be factored adequately into the cost of strategic investment and should drive business objectives.

Communication and inclusion is the key

For organizations to manage the cybersecurity risks, the cybersecurity group should build good relationships with the C–Suite leaders and relevant business functions.

When cybersecurity is embedded in the business, CISOs will be in a strong position to help drive innovation and become better informed of threats faced by the organization. Cybersecurity leaders must have the ability to communicate in a language the business understands, and a willingness to find solutions to security problems.

With the regulatory landscape getting stringent and complex, organizations are in the need of experienced cybersecurity professionals with advanced technical skills, passion for cybersecurity initiatives and the ability to build relationships across business functions. This will enable the organization to develop a resilient cybersecurity defence strategy.

Beyond the storm

While organizations are recovering from the COVID–19 crisis and threat actors are hitting a new level of maturity, cybersecurity in India has seen a substantial change in horizon. Cybersecurity has gained priority within the C–suite leadership and the business has looked to the cybersecurity function to protect the organization from evolving cyber threats, whilst enabling urgent technology transformation and new growth avenues. The government has also been working towards tackling this new age threat. A conscious effort is being provided by central governmental agencies to provide guidelines on managing cyber security across CII entities.

Whilst CISOs have risen to the challenge and can today demonstrate the growing strategic importance of their role, the crisis has certainly provided an opportunity. CISOs can leverage this opportunity to accelerate their efforts to address new age constructs like:

Security by default as a concept which has been evolving ever since where security is no more by choice but by default right from the inception of a program, planning a strategic implementation, etc.

The evolving regulatory framework across the globe has triggered the need for body corporates to align their business and have Privacy by design and technology solutions as the ethos to ensure seamless data flows and sustain compliance requirements.

Remote working which has become the new normal and borderless workspaces is transforming how companies can securely operate in a hyper - distributed and exceptionally remote model.

Zero trust architecture which is rooted in the principle of 'never trust, always verify' which should be designed to protect modern digital environments by leveraging network segmentation, preventing lateral movements and simplifying granular access control.

Quantifying cyber risks based on factual data can provide the Board, senior management and the CISO function near real time insights into the true cyber maturity posture and corresponding risk exposure that can also help strike the right balance between cyber risks and cyber insurance.

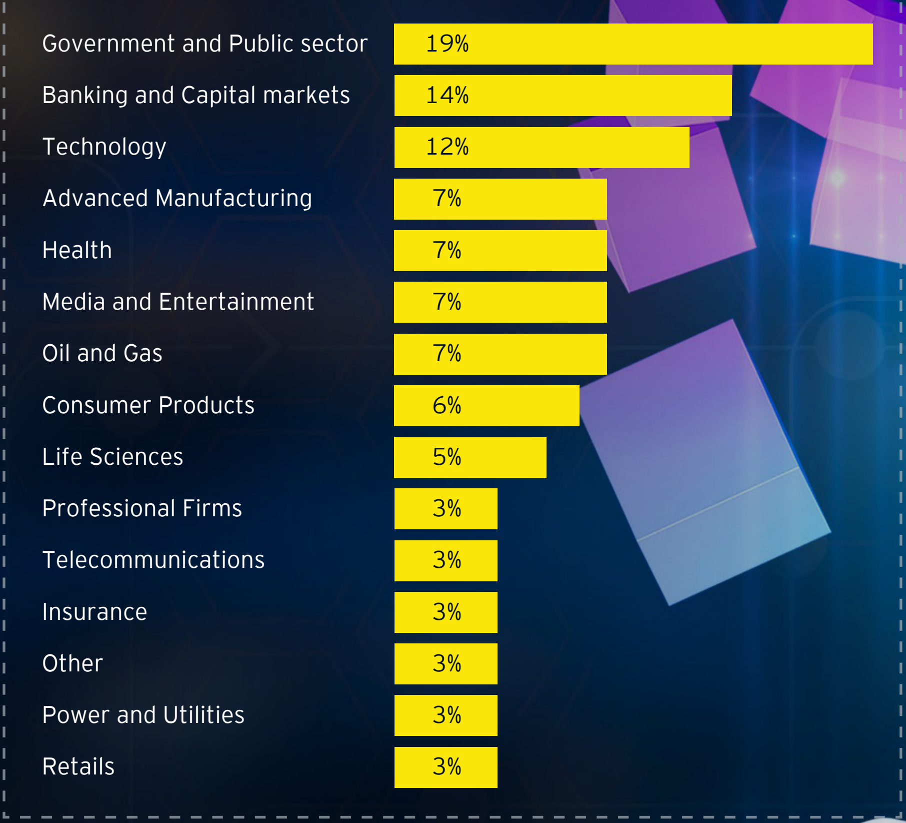
The oncoming roll out of Fifth–generation wireless (5G) in India just around the corner, shall bring about a transformation in the telecom industry in terms of speed, better response, lower power usage, however with the possibilities of uncertainties around the handshake of legacy and new network, heightened requirements around security monitoring, safeguarding information etc.

Although it is not a direct or straightforward initiative, it is an ambitious objective that can be reached within a year, and this is the time when cybersecurity has been given prominence like never before, especially in India. For strategies, investments, and priorities, CISOs must be involved with the business. It is the time for them to secure a seat at the table, whilst continuing to build stronger, trust–based relationships with their C–suite peers.

Appendix

In this year's GISS, 123 Indian companies (19% from the government and public sector, 14% from financial services sector, 12% from technology,14% from health & life sciences, 9% from consumer products and retail, 7% from advanced manufacturing, and 25% from varied industry sectors such as insurance, power utilities, telecommunications, oil & gas, media & entertainment, others) have actively participated and shared their situation and challenges regarding cyber risks and cybersecurity.

Fig: 3.1 – Industry–wise breakup of GISS respondents (survey demographics)



Management team

Rohan Sachdev
India Consulting Leader
Email: rohan.sachdev@in.ey.com

Rohit Mathur
India Consulting Risk Leader
Email: rohit.mathur@in.ey.com

Murali Rao
India Consulting Cyber Leader
murali.rao@in.ey.com

Burgess Cooper
India Partner - Cybersecurity
Email: burgess.cooper@in.ey.com

Lalit Kalra
India Partner - Cybersecurity
Email: lalit.kalra@in.ey.com

Kartik Shinde
India Partner - Cybersecurity
Email: kartik.shinde@in.ey.com

Vidur Gupta
India Partner - Cybersecurity
Email: vidur.gupta@in.ey.com

Kunal Bhatia
India Partner - Cybersecurity
Email: kunal.bhatia@in.ey.com

Mini Gupta
India Partner - Cybersecurity
Email: mini.gupta@in.ey.com

Prashant Choudhary
India Partner - Cybersecurity
Email: prashant.choudhary@in.ey.com

Tiffy Isaac
India Partner - Cybersecurity
Email: tiffy.isaac@in.ey.com

Sambit Sinha
India Partner - Cybersecurity
Email: sambit.sinha@in.ey.com

Akshay Tiku
India Partner - Cybersecurity
Email: akshay.tiku@in.ey.com

Sameer Paradia
India Partner - Cybersecurity
Email: sameer.paradia@in.ey.com

Prashant Gupta
India Partner - Cybersecurity
Email: prashant.gupta2@in.ey.com

EY offices

Ahmedabad
22nd Floor, B Wing, Privilon
Ambli BRT Road, Behind Iskcon
Temple, Off SG Highway
Ahmedabad - 380 059
Tel: + 91 79 6608 3800

Bengaluru
12th & 13th floor
"UB City", Canberra Block
No. 24, Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 6727 5000

Ground Floor, 'A' wing
Divyasree Chambers
# 11, O'Shaughnessy Road
Langford Gardens
Bengaluru - 560 025
Tel: + 91 80 6727 5000

Chandigarh
Elante offices, Unit No. B-613 & 614
6th Floor, Plot No- 178-178A
Industrial & Business Park, Phase-I
Chandigarh - 160 002
Tel: + 91 172 6717800

Chennai
Tidel Park, 6th & 7th Floor
A Block, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100

Delhi NCR
Golf View Corporate Tower B
Sector 42, Sector Road
Gurugram - 122 002
Tel: + 91 124 443 4000

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Gautam Budh Nagar, U.P.
Noida - 201 304
Tel: + 91 120 671 7000

Hyderabad
THE SKYVIEW 10
18th Floor, "SOUTH LOBBY"
Survey No 83/1, Raidurgam
Hyderabad - 500 032
Tel: + 91 40 6736 2000

Jamshedpur
1st Floor, Shantiniketan Building
Holding No. 1, SB Shop Area
Bistupur, Jamshedpur – 831 001
Tel: + 91 657 663 1000

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 433 4000

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000

Pune
C-401, 4th floor
Panchshil Tech Park, Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

Ernst & Young LLP

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

EYIN2103-XXXX
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

RS1

ey.com/en_in

@EY_India in EY YouTube EY India f EY Careers India @ey_indiacareers