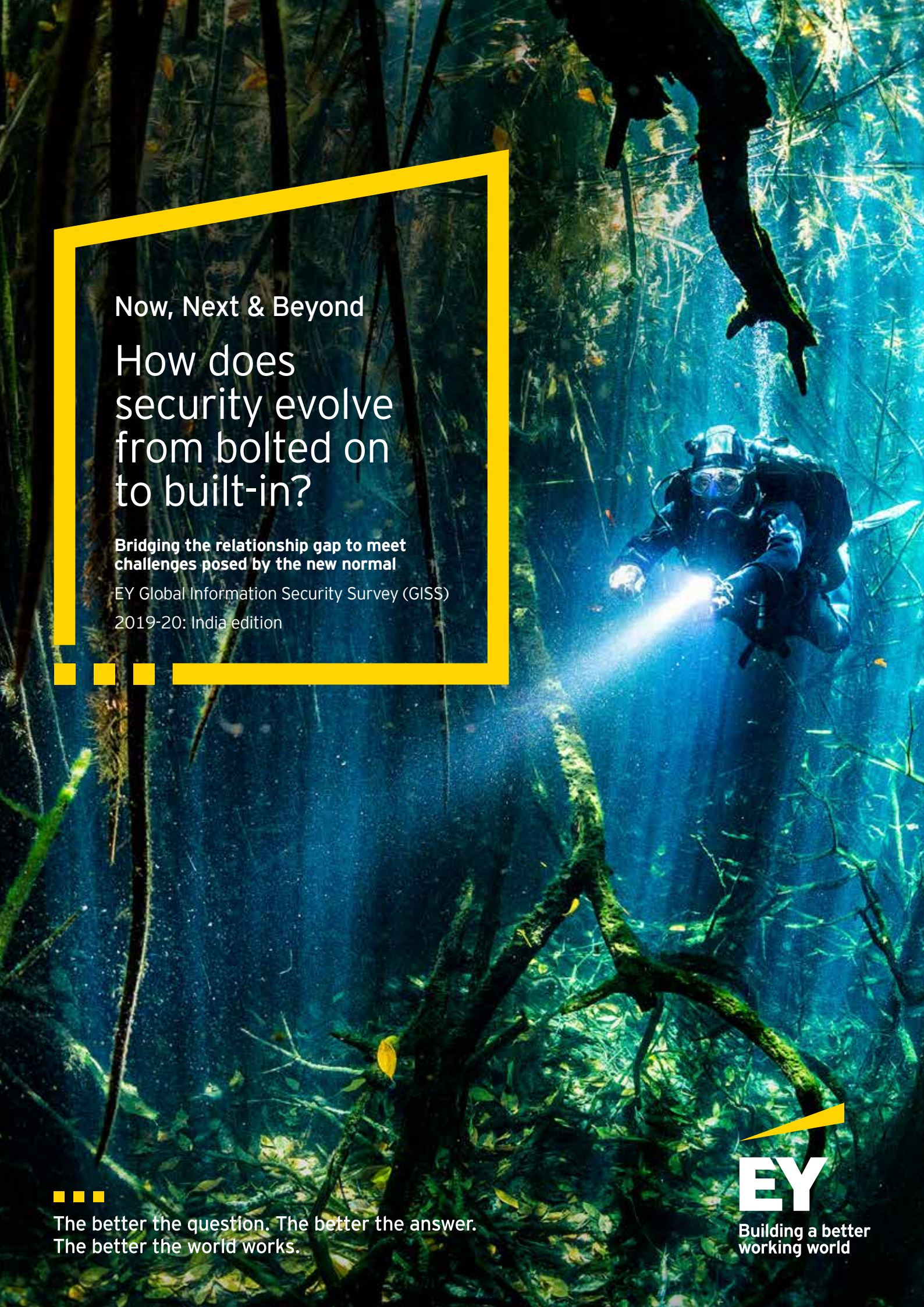


Now, Next & Beyond

How does security evolve from bolted on to built-in?

Bridging the relationship gap to meet challenges posed by the new normal

EY Global Information Security Survey (GISS)

2019-20: India edition

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

EY
Building a better working world

Contents

Foreword

Rohit Mathur
EY India Advisory Risk Leader

Welcome to the 22nd annual EY Global Information Security Survey (GISS) 2019-20 India edition, which explores the most important cybersecurity issues facing organizations today.

We are grateful to more than 190 respondents from multiple sectors in India for participating in the survey. It's an invitation only survey and most of the data was collected by EY during on-site meetings between August and October 2019. Respondents include CISOs or their equivalents across every industry sector.

More than two decades since EY started reporting on organizations' efforts to safeguard their cybersecurity, the threat continues to both increase and transform. We face more attacks than ever before and from a wider range of increasingly creative bad actors — often with very different motivations.

The good news is that boards and senior management are engaging more intimately with cybersecurity and privacy matters. In this era of transformation, senior leaders are acutely conscious of their organizations' vulnerabilities and the potentially existential dangers posed by attackers. But there is work to do. Not only is cybersecurity an evolving risk, it also has to be confronted in the context of innovation and change.

COVID-19 has shaken up the entire world and as businesses evolve to operate in the new-normal, it is evident that accelerated adoption of technology to swiftly move to a touchless, digital world is no longer a choice but a key business enabler. As organizations are rapidly moving towards adopting new age technologies, their risk landscape is also changing.

Considering that cyber security risks materialize at digital speed, security can no longer be an afterthought. It is time now for business and cybersecurity stakeholders to work together and make the definitive leap towards Security and Privacy by Design.

Security and Privacy by Design should be the aim of every organization. This year's GISS explores these ideas in more detail.

What just changed?

Murali Rao
EY India Advisory Cyber Leader

In recent times, we have witnessed great changes in the cybersecurity function. However, in 2020, organizations across the world are witnessing a new array of cybersecurity challenges in the wake of the COVID-19 outbreak. The pandemic is proving to be not only a health, economic, political or social scare but also a cybersecurity one. Organizations are particularly vulnerable during this time from opportunists, threat actors and even insider threats.

Rapid adoption of scaled up remote connectivity combined with the inherent need to sustain and scale the infrastructure, has led to implicit demand for adaptable controls to monitor, secure and respond adequately to de-risk the infrastructure.

Mitigating risks with a remote workforce requires adaptation to various use cases driven by regulatory constraints, business needs and privacy demands. We need to identify and understand the risks exposed due to this scenario, adapting a risk-based approach to identify, defend and secure the various user journey(s) of access to enterprise assets is the need of the hour. Enterprises need to revisit and create appropriate controls to enforce 'Security & Privacy by Design' with the intent to build and establish trust driven handshakes in the technology ecosystem.

Digital hygiene is the need of the hour and CISOs need to protect organizations from disruptive network and application level attacks, web application attacks and cloud related attacks. They also need to plan to ensure that remote working infrastructure (e.g., bring your own device) is stable and secure and there is enhanced focus to educate and train users on cybersecurity best practices.

The COVID crisis has also brought in several other challenges for CIOs and CISOs like business continuity, remote collaboration and communication. In our endeavor to support our clients in these uncertain and complex times, we interacted with more than 750 industry leaders and CXOs in the last six weeks across sectors via the medium of fireside chats wherein we brainstormed on the Now, Next and Beyond in cyber for a secure and resilient enterprise.

Leaders across organizations discussed the increased susceptibility to technology disruptions and potential service degradation due to increased network traffic, reduced capacity and so on.

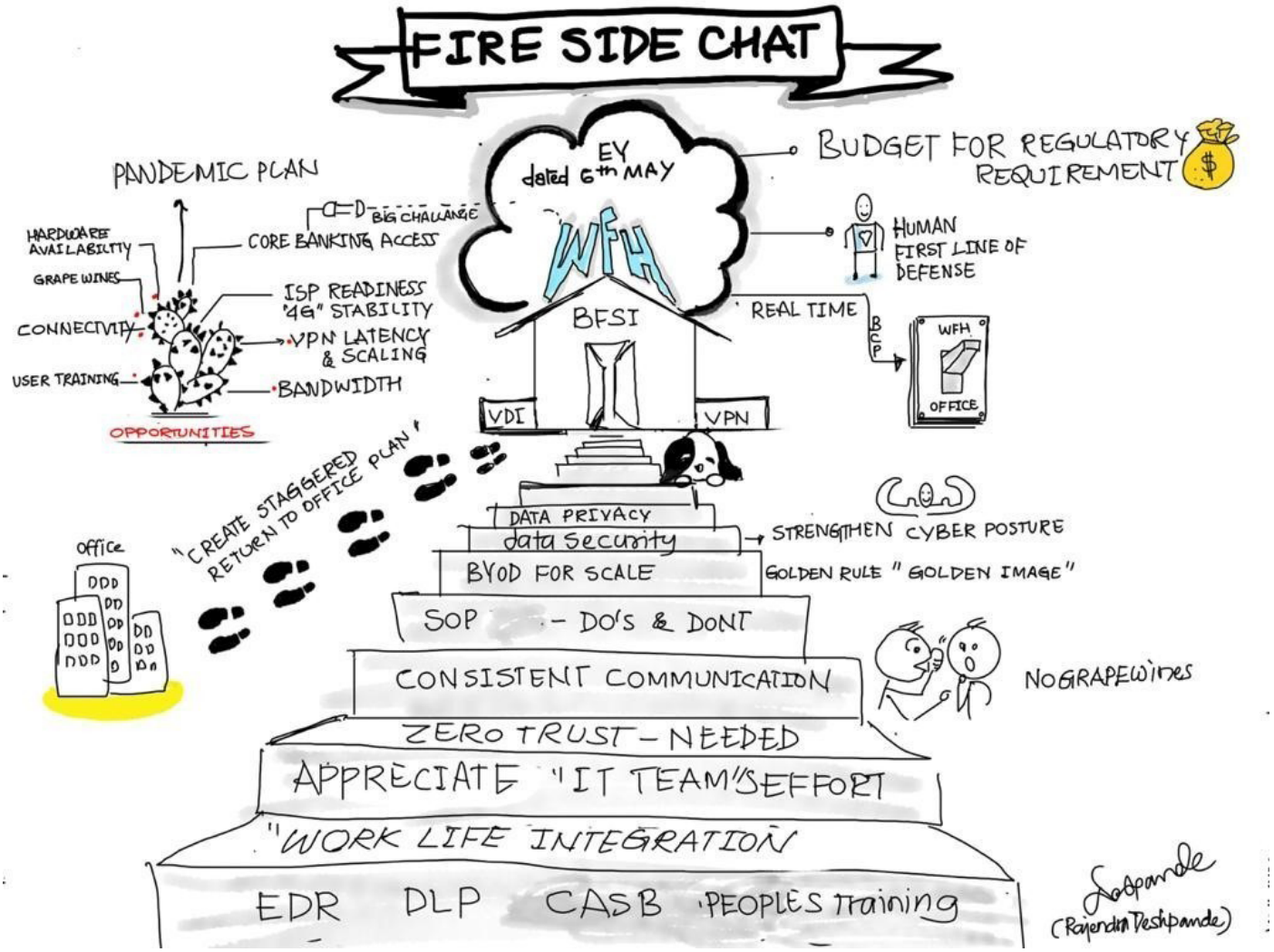
As a prelude to the survey results, we present to you a brief summary of the key focus areas of security professionals in the times of COVID-19 and beyond.

The survey also points to the need of CISOs to take a pause to rethink in these times of great turbulence and change how will they function as a change agent to transform the cybersecurity function to reach its own new normal.

As the business models evolve to adjust to the new normal, CISOs have a great opportunity to enable the business transformation.

Prelude

Best practices from the fireside chats for a secure and resilient enterprise



Now

Focus on business continuity and crisis planning

- Segregate devices for distribution to enable WFH and prioritize employees as per roles and responsibilities in the organization
- Extend existing bring your own device (BYOD) policies and enhance back-end infrastructure with security measures
- Demand for sensible investment on technology with reasons of cost-benefit, ROI (Return on Investment) and TCO (Total cost of ownership)
- Enable remote access only to a specific group so that the bandwidth does not become a challenge and bottleneck
- Classify role-based training, to appropriately deliver the required security related do's and don'ts
- Focus on how to sustain and manage the risk, networks and other infrastructure

Next

Manage a restricted business, lead through ongoing disruption

- Revisit new security challenges and make it a continuous process of innovation
- Update BYOD policies with learnings from the past after processes return to business as usual (BAU)
- Continuously perform risk assessments to evaluate data theft/ privileges/leakages
- Enhance on-ground support once WFH reduces/ceases and operations normalize
- Data Loss Protection (DLP) to be made a mandatory requirement
- Strike a balance between people, technology and processes for efficient capacity utilization
- Focus on relationship management with people from other functions, learn and empathize with them
- Prepare a Business Continuity Plan (BCP) plan in people management and be wise in doing it right

Beyond

Bounce back from the challenges, build a resilient enterprise and reframe the future

- Audit the security control measures implemented during the new normal for risks, threats, and vulnerabilities
- Leverage ML and AI to measure WFH productivity and its efficiency
- Third-party due diligence to be done on priority once the new normal ceases for any new vulnerabilities and hurried implementations of controls
- Implement proactive bug bounty programs as it is fruitful for the security of the organization
- Upgrade BCP plans

Executive summary

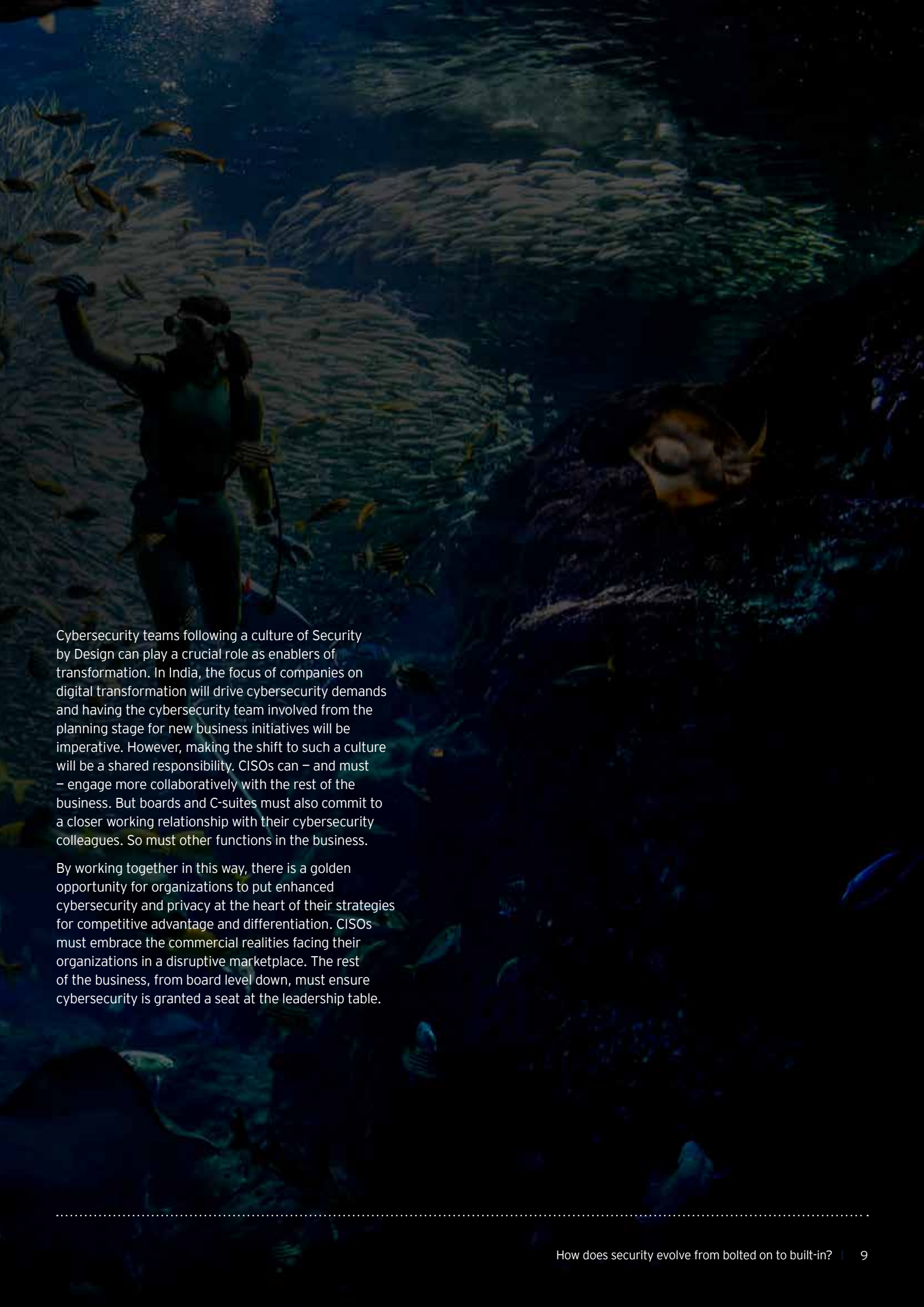
Survey results

Against the backdrop of mounting threats in an era of disruption, the most forward-thinking cybersecurity functions can be critical agents of change. But this will require organizations to foster new relationships between CISOs, the board and C-suite, and every function of the business.

EY recommendations in brief

Based on the findings from this year's EY Global Information Security Survey (GISS) 2019-20: 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 the business to work together to:

1. **Establish cybersecurity as a key value enabler in digital transformation –** bring cybersecurity into the planning stage of every new initiative. Take advantage of a Security by Design approach to navigate risks in transformation, product or service design at the onset (instead of as an afterthought).
2. **Build relationships of trust with every function of the organization –** analyze key business processes with cybersecurity teams to understand how they may be impacted by cyber risks and how the cybersecurity team can help enhance the business function around them.
3. **Implement governance structures that are fit for purpose –** develop a set of key performance indicators and key risk indicators that can be used to communicate a risk-centric view in executive and board reporting.
4. **Focus on board engagement –** communicate in a language the board can understand; consider a risk quantification program to more effectively communicate cyber risks.
5. **Evaluate the effectiveness of the cybersecurity function to equip the CISO with new competencies –** determine the strengths and weaknesses of the cybersecurity function to understand what the CISO should be equipped with and how.



Cybersecurity teams following a culture of Security by Design can play a crucial role as enablers of transformation. In India, the focus of companies on digital transformation will drive cybersecurity demands and having the cybersecurity team involved from the planning stage for new business initiatives will be imperative. However, making the shift to such a culture will be a shared responsibility. CISOs can — and must — engage more collaboratively with the rest of the business. But boards and C-suites must also commit to a closer working relationship with their cybersecurity colleagues. So must other functions in the business.

By working together in this way, there is a golden opportunity for organizations to put enhanced cybersecurity and privacy at the heart of their strategies for competitive advantage and differentiation. CISOs must embrace the commercial realities facing their organizations in a disruptive marketplace. The rest of the business, from board level down, must ensure cybersecurity is granted a seat at the leadership table.

This year's GISS focuses on this evolving role of the cybersecurity function and is divided into three sections:

1

A systemic failure in communication

The increase in hacktivists, who this report shows were the most common source of material or significant breaches, underlines how the cybersecurity function needs a much deeper understanding of its organization's business environment. CISOs who do not work collaboratively with colleagues across the business may inevitably be side-stepped by other functions and lines of business which could, for example, launch new products or services that expose the organization to new threats.

Majority of Indian companies are on the path of digital transformation and this technological disruption is identified as the greatest strategic opportunity for organizations. However, the risk of cyberattacks is a major impediment in digitalization progress. Hence, the role of CISOs becomes more important as they need to work more closely with the board and C-suite so that they can embed cybersecurity solutions at a much earlier stage of new business initiatives – a culture of Security by Design.

- The cyber and privacy threat is increasing and expanding. About 5 in 10 organizations (53%) have faced a material or significant incident in the past 12 months. Close to more than one-fourth of these attacks (28%) came from hacktivists – tech-enabled, political and social activists – just ahead of organized crime groups (25%)
- Cybersecurity spending is driven by defensive priorities rather than innovation and transformation: 82% of new initiative spending focused on risk or compliance rather than opportunity
- 15% respondents spend 5% or less of their cybersecurity budget on supporting new initiatives

Only

31%

of organizations say cybersecurity is involved right from the planning stage of a new business initiative.

2

Increase trust with a relationships reboot

69%

of organizations say that the relationship between cybersecurity and the lines of business is at best neutral, to mistrustful or non-existent.

With Security by Design as the goal, CISOs and their colleagues across the organization – including functions such as marketing, R&D and sales – need to form much closer relationships in order to improve overall business understanding of cybersecurity and meet the mark of Security by Design.

Increased collaboration with other functions must be a priority, but cybersecurity leaders also need to form much more productive relationships with the board, the C-suite and senior leaders.

73%

of boards/executive management teams perceive cyber risk as a significant risk to the organization.

3

The CISO becomes the agent of transformation

- 83% of organizations say that the relationship between cybersecurity and marketing is at best neutral, to mistrustful or non-existent; 75% say the same of the research and development team; 69% for the lines of business. Cybersecurity teams even score poorly on their relationship with finance on whom they are dependent for budget authorization, where 71% of companies say they fall short
- More than half of respondents (68%) say that the board has a full understanding of cybersecurity risk; 67%, meanwhile, say that the board fully understands the value and needs of the cybersecurity team
- 39% of organizations schedule cybersecurity as a board agenda item quarterly
- 5 in 10 organizations say that they cannot quantify the effectiveness of their cybersecurity spending to their boards

Only

7%

of organizations would describe cybersecurity as enabling innovation.

With stronger relationships at business and board levels, a better understanding of the organization's commercial imperatives and the ability to anticipate the evolving cyber threats, CISOs can become central to their organizations'transformation.

CISOs are required to become powerful agents who instead of denying new initiatives should drive them. They need a new mindset and skills in the areas of communication, negotiation, and collaboration to work more effectively.

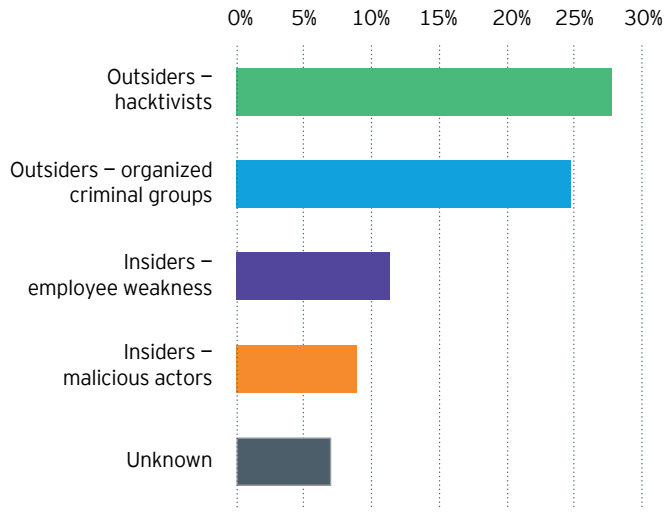
- 30% of organizations would describe cybersecurity as "protects the enterprise" and 26% as "enables the organization to understand cybersecurity risk" compared to describing it as an innovation enabler (7%)
- About half the organizations (45%) say that the primary driver for new spending is risk reduction and 37% cite compliance requirements. Just 5% point to new business initiative enablement
- 7 in 10 organizations have a head of cybersecurity who sits on the board or at executive management level

68%

of organizations have a head of cybersecurity who sits on the board or at executive management level.

1 A systemic failure in communication

Figure 1: Attacks come from multiple sources, including hacktivists
Threat actors behind confirmed breaches



> It is critical for a CISO to embed cyber security into the very cultural fabric of an organization. People, the most valuable and vulnerable assets of an organization, are the threads of this fabric and they should be able to see cyber security as an enabler rather than a roadblock.

Tiffy Isaac
Partner Cybersecurity, EY India

India is facing growing concerns from attacks on critical infrastructure which could cripple its developing economy. In September 2019, a government-run nuclear power plant which is the newest and largest such power station in India admitted the presence of malware in one of the systems deployed at Tamil Nadu[1]. The growth in digital transformation brings in rise of digital data inventory which is exposed to cyber-attacks. An India-based healthcare website was attacked in 2019 as a result of which medical records and information of 68 million patients and doctors were stolen.

This year's GISS 2019-20 – India edition too underlines the significant increases in the number of destructive attacks respondents face (in fact this is serious enough – 72% say such attacks have become more frequent over the past 12 months, including 38% who report an increase of more than 10%); also, the change in the types of perpetrators. According to respondents, hacktivists have launched more attacks than any group, other than organized criminal gangs.

The activist threat illustrates one of the challenges facing CISOs. After years spent combatting threats posed by traditional bad actors – data or intellectual property theft and fraud, for instance – and adapting to the techniques of those attackers – ransomware and business e-mail compromise, as prime examples – cybersecurity functions now have to protect the organization from attackers with much more diverse motivations. But, consider a CISO who does not realize that their organization's investments in coal mining, for example, or its record on human rights, or revelations about one of its executives, puts it in the sights of hacktivists. Unless they collaborate with their colleagues beyond the cybersecurity function, CISOs are likely to be blind to these weaknesses – and therefore to the threat.

Cybersecurity teams face a perfect storm. Amid a rise in destructive attacks, including attacks by angry and well-organized activists, CISOs who are not close to the businesses they serve, who lack the trust of colleagues across the organization, have less and less hope of providing the protection required.

[1] India confirms malware attack at Kudankulam nuclear power plant, Livemint.com, November 2019. https://www.livemint.com/news/india/india-confirms-malware-attack-at-kudankulam-nuclear-power-plant-11574262777163.html

Only

31%

say that their cybersecurity team is involved right from the start of a new business initiative.

> "You're in an environment where technology is evolving so quickly. Business initiatives are being rolled out with these new technology-enabling capabilities so that companies can maintain their competitiveness. If security continues as an afterthought, we will always be behind the threat."

Kartik Shinde
Partner Cybersecurity, EY India

What is Security by Design?

Security by Design is a new approach that builds cybersecurity into any initiative from the onset, rather than as an afterthought, enabling innovation with confidence. It is a strategic and pragmatic approach that works across all parts of the organization. Security by Design remains in the initiative's lifecycle to help with the ongoing management and mitigation of security risks.

Cybersecurity is still an afterthought

The deduction of this year's GISS 2019-20: India edition is that this evolution – from "introverted technologists to outgoing business partners" – has yet to take place at many organizations. Crucially, just 31% say that their cybersecurity team is involved right from the start of a new business initiative – taking part in the planning process for new projects rather than being brought in only as part of the design team or even later.

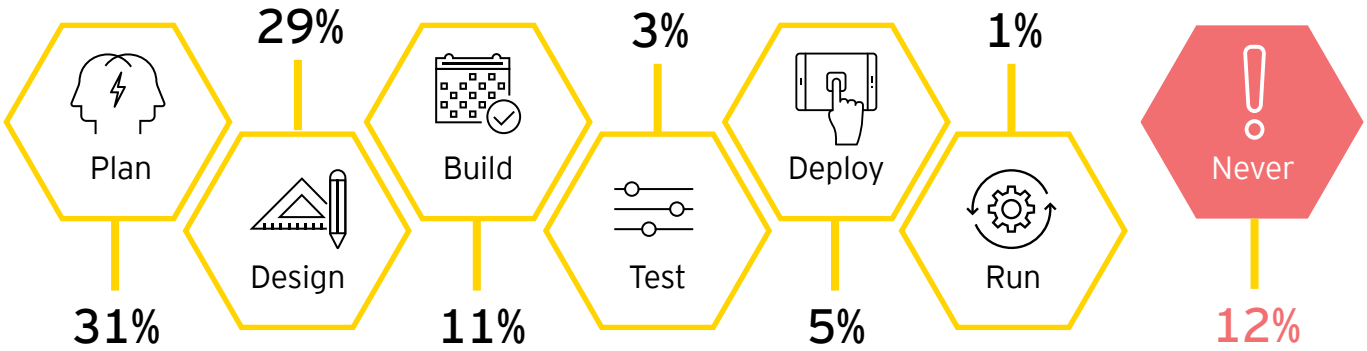
In other words, many cybersecurity teams are working for the business, rather than in the business. The result is that instead of Security by Design, whereby cybersecurity is a central consideration right from the start of each new project, the function finds itself constantly retrofitting protection, which will often lead to imperfect and costly solutions or impractical workarounds.

In this era of digital transformation, where every organization is constantly revamping its products, services, operational processes and organizational structures, this is not good enough.

Now that activists are using cyberattacks and business transformation is driving the corporate agenda, cybersecurity teams have to move beyond the defensive, reactive role they might have played in the past. Only by embedding themselves within the organization will they be able to integrate the security agenda into digital transformation programs from the beginning and anticipate the full range of bad actors that might target the business.

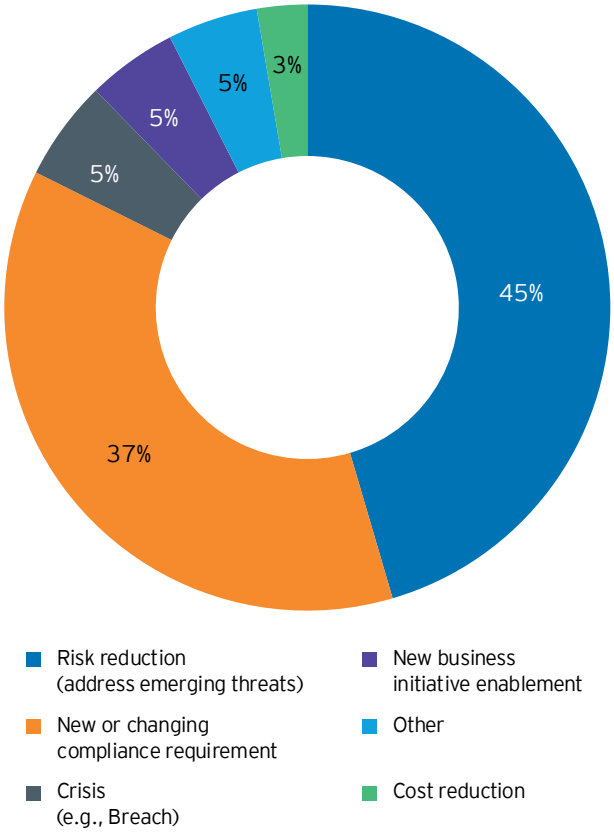
"Where we see companies winning, there has been a true, dedicated focus to drive programs that focus on integration, speed and consistency," says Sameer Paradia, Partner Cybersecurity, EY India. "Where we see failure, there is a lack of integration, simplification and focus."

Figure 2:
When are cybersecurity teams joining new business initiatives?



82% of organizations say that crisis prevention and compliance remain the top drivers of new or increased security spending.

Figure 3: New business initiatives miss out on extra spending
Justification for new or increased cybersecurity funds



Organizations are spending on business as usual, not on new initiatives

The spending priorities of many cybersecurity functions today show that there is significant work to do to embed a culture of Security by Design. Right now, the majority (45%) of organizations say that where there is additional focus and spending on cybersecurity, it is driven by concern about risk.

When asked to identify the new business or technology initiatives that are driving new spending, artificial intelligence/cognitive adoption ranked highest in India. Risk and controls optimization will be on the radar for 14% of organizations. For example, despite highly publicized concerns in the media about the exposures that connected devices could bring, just 7% point to Internet of Things-related initiatives as driving new spending on cybersecurity.

Figure 3 suggests that the spending of many cybersecurity functions is heavily weighted toward business as usual instead of new initiatives. Some 15% of organizations spend 5% or less of their organization's cybersecurity budget on new initiatives.

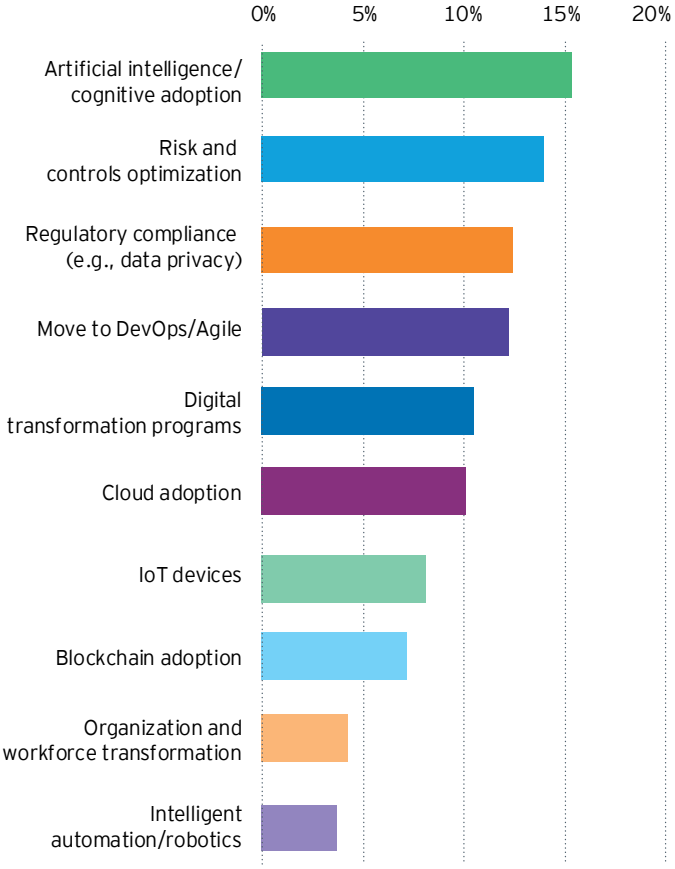
Nor are CISOs necessarily preparing and equipping their functions for future challenges. Organizations are only spending 21% of their cybersecurity budgets on operations; almost one third (32%) currently dedicate less than a quarter of their spend to capital projects and long-term investment.

"CISOs need to partner with business teams and other functions to ensure a cogent security approach of the enterprise. Business transformation led technology deployments without consulting the CISO, add to the attack surface thereby enhancing the vulnerability quotient of the organization." says Sambit Sinha, Partner Cybersecurity, EY India.

53% of organizations experienced a significant or material breach in the last 12 months.

Figure 4: How new or increased cybersecurity funds are spent

Use of net new funds for cybersecurity



Only

14%

of new or increased cybersecurity funds are used on digital transformation programs.

CISOs need to get ready for a new proactive role

A complete transformation will not be easy. After all, cybersecurity functions continue to face significant workloads that require commitment to operations. And alongside the new need to confront a broader range of attackers and support innovation and transformation, the more familiar challenges have not gone away – attackers continue to target organizations' data – and particularly their customer data, which carries reputational and regulatory risks.

Many organizations are still struggling to detect and repel breaches. In India, only 43% of survey respondents detected their most significant breach of the past 12 months within a month, while 25% indicated the problem took longer to uncover. And they are more vulnerable in some areas than others – 59% of organizations say that they would be unlikely to detect a file-less malware attack, for instance.

CISOs will therefore be all too aware that they must not neglect business as usual; defending the organization will naturally remain their priority. However, to perform this role effectively, the function will need to adapt. As their organizations transform around them and the external threat landscape evolves, CISOs must be ready for a more proactive role.

Defending the organization and enabling change are not mutually exclusive. Organizations that embrace the idea of Security by Design will be more resilient – and will therefore find themselves spending less time detecting, repelling or resolving breaches. Cybersecurity teams with a deep-rooted understanding of their businesses will be better placed to anticipate new threats and to recognize potential new aggressors, and to respond ahead of time.

So, in taking on the role of business partner and change-enabler, CISOs will not only provide greater value to their organizations but will also become more effective in their traditional areas of operation.

58% of boards are fully involved in cybersecurity direction and strategy

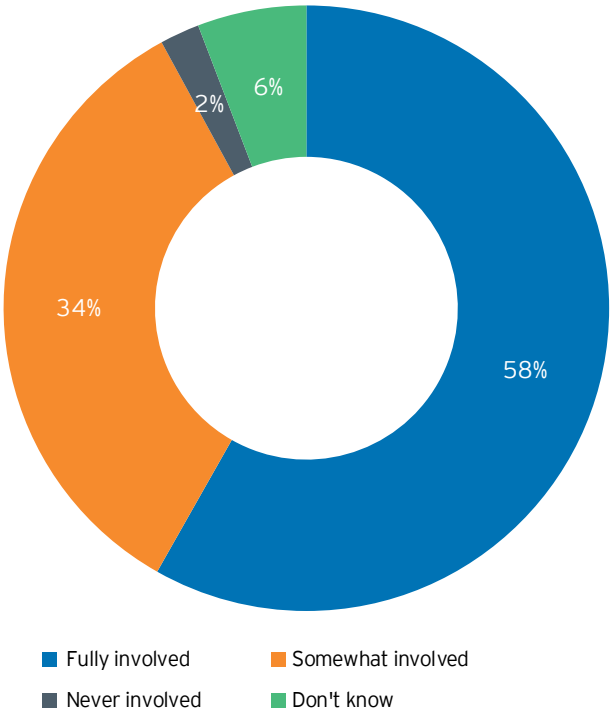
"Just when we had started to think that we will overcome the cybersecurity challenges; COVID-19 changed the entire landscape.

While the need of the hour is to focus on enabling crisis response and on imminent cyber threats posed by remote working infrastructure; in the medium-term cybersecurity professionals have another opportunity to build the trust by partnering in the accelerated digital transformation businesses will undergo.

Prashant Choudhary
Partner, Cybersecurity, EY India

Figure 5: Boards play a large role in approving the cybersecurity strategy, direction and budget

How CISOs perceive the level of board involvement in establishing and/or approving the strategy, direction, and budget of cybersecurity program measures.



2 Increase trust with a reboot of relationships

Figure 6: A trust deficit
Cybersecurity's business relationships

69% of organizations say that the relationship between cybersecurity and the lines of business is at best neutral, to mistrustful or non-existent.

As we have seen, many organizations feel that their cybersecurity functions are stuck in defensive mode – not yet ready to play a central role in enabling the business to transform. What is it that is preventing CISOs from making the leap?

The answer lies in the relationships between the cybersecurity function and other parts of the business – both at a functional level with other departments and with senior management and the board. Rebooting these relationships, establishing trust and proving cybersecurity's full value to the organization, is now essential.

Why is collaboration so crucial?

One imperative is to reach out to functions across the business in order to work more closely than ever before. As Figure 6 shows, the cybersecurity team at many organizations currently has little or no relationship with other key functions – and especially those involved in innovation, product development and customer facing activities.

More than three-quarters of organizations (83%) say that the relationship between cybersecurity and marketing is no better than neutral – and in many cases they describe it as mistrustful or non-existent. Some 75% say the same of the function's relationship with the product development and R&D teams. It is only when it comes to functions such as IT, risk and legal, where cybersecurity's traditionally defensive, compliance-driven role is a more comfortable fit, that significant numbers of businesses describe the relationship as trusting and cooperative (see Figure 6). In many organizations, even the relationship with finance is difficult, with almost half of respondents describing it as non-existent or mistrustful.

The CISOs who find themselves on the lower end of these trust statistics will find it almost impossible to play the role their businesses increasingly expect of them. Without strong relationships of mutual trust with the rest of the organization, cybersecurity will struggle to get involved in the early stages of new business initiatives, which undermines the concept of Security of Design. Nor will the function pick up the market intelligence it needs to anticipate threats such as the danger posed by hacktivists.

So stronger relationships are vital. "It's time for executive management to drive home the need for a 'Trusted' relationship between various stakeholders in the enterprise and the CISOs, it is critical to consciously develop this." says Prashant Gupta, Partner Cybersecurity, EY India.

In part, it is a simple case of investing time and effort in relationships with other functions. But the nature of the interaction will be important too. Today, cybersecurity is respected for its work in keeping the organization safe, but it is not seen as a key ally in the transformation process. While 30% of executive management says that they associate the function with the idea of protecting the enterprise, only 7% agree that the function "enables innovation with confidence."

Changing that perception will be key. If cybersecurity is seen as an obstacle to innovation and transformation — as a function that says no to new initiatives on security grounds — the rest of the organization will inevitably try to sidestep it. But if it can provide workable solutions to any problem, it will be more likely to become a trusted partner.

Build board engagement with better communication. These cross-functional relationships are not the only links for the cybersecurity team to work on: many organizations also report a disconnect between their boards and the cybersecurity function. This is a concern, because those disconnects will undermine the ability of cybersecurity to connect more fully with other departments: if the board does not afford the function status, nor will other parts of the business. They will also threaten the CISO's ability to secure the resources they need.

"

Stronger relationships are vital to the success of the CISO.

The best CISOs have taken time to connect with the business deeply, in a trusted way. What they're trying to do is to make sure that they're automatically brought into the business, into its strategy and planning and thinking.

Burgess Cooper
Partner Cybersecurity, EY India

39% of organizations quarterly schedule cybersecurity as a board agenda item.

Figure 7: Cybersecurity is not a regular agenda item for the board
How often is cybersecurity on the agenda of the fullboard?

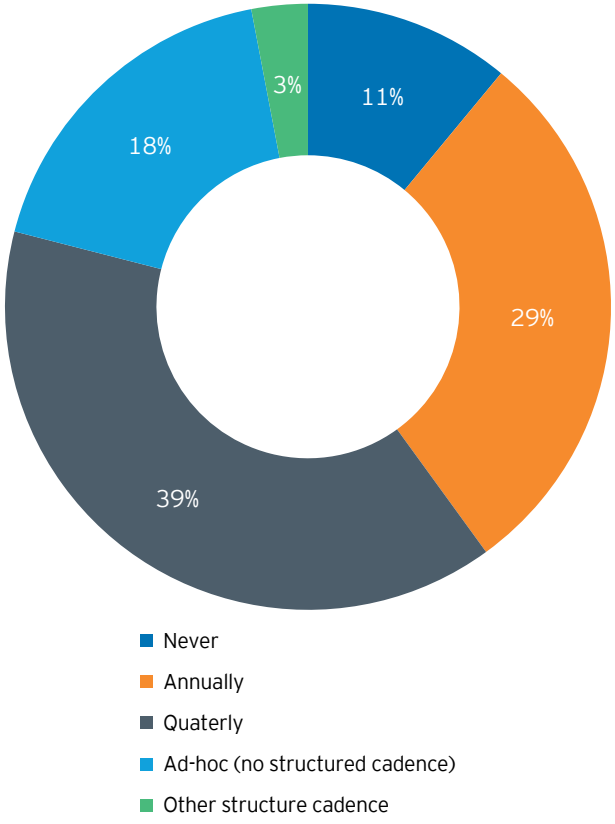
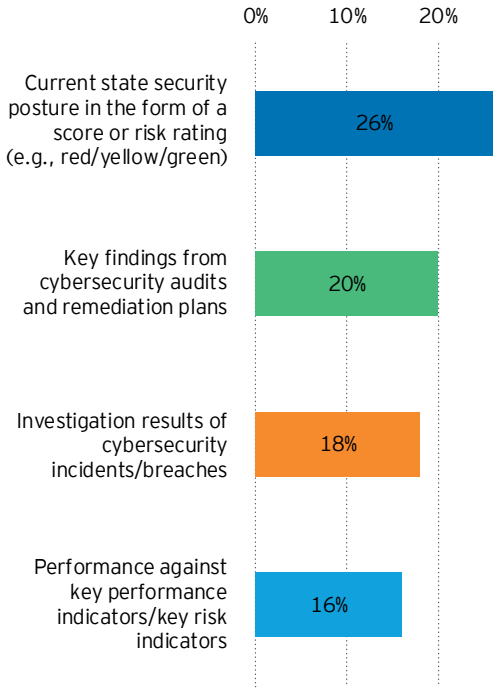


Figure 8: Time for a new conversation with the board
What are CISOs reporting to the board?



61% of organizations are able to quantify in financial terms the effectiveness of their cyber spend.

The problem is not that boards do not recognize the importance of committing to cybersecurity. In fact, EY research reveals that CEOs now believe that national and corporate cyber-attack is the greatest threat facing the world economy over the next 10 years. And in this year's GISS 2019-20 – India edition, 73% of organizations agree that the board sees cyber risk as significant.

67% of respondents say that their board and executive management team have the understanding they need to fully evaluate cyber risk and the measures it is taking to defend itself and 33% complain that their boards do not fully understand the value of the cybersecurity team and its needs.

If the CISOs focus on communication with their boards appropriately the effectiveness can be increased multifold. For example, 61% of respondents say they can quantify, in financial terms, the effectiveness of their cybersecurity spending in addressing the risks faced by the business. The survey suggests 67% of the Indian boards are highly confident that the cybersecurity team is effective.

Many CISOs are concerned that their boards do not have a structured way to review cyber risk. Just 39% of organizations quarterly schedule cybersecurity as a board agenda item and just 43% regularly put the issue on the agenda of a board subcommittee. This could be a symptom of the way the function chooses to communicate with the board — the emphasis is on current state security, audit results and so on, rather than performance or innovation (see Figure 8).

"Senior leadership in most organizations do fundamentally recognize the cybersecurity threat. As a result, they are increasingly supportive of cybersecurity.

Where they find cybersecurity function lacking is in its ability to articulate the issues in business context and to execute.

Mini Gupta
Partner Cybersecurity, EY India

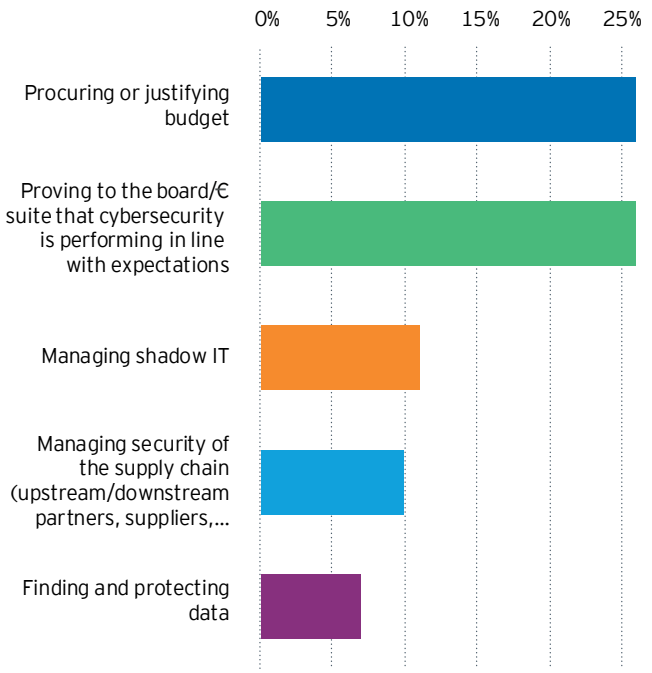
In the absence of a richer conversation with boards and management teams about the value of cybersecurity to the business, greater engagement is likely to prove elusive.

Many CISOs already say that the most challenging aspect of their role is proving the value of what they do and securing the budget they believe they require (see Figure 9). For many, this is more difficult than managing security — even when it comes to evolving technologies and new threats.

Kris Lovejoy, EY Global Advisory Cybersecurity Leader, believes that this is another reason to reset the mindset of the cybersecurity function. "Where are cybersecurity functions spending their money? They're spending it on risk and controls optimization. Where are they reporting? Often, into the audit committee. What are they giving to the audit committee? They're giving it benchmark results on their status on risk and controls optimization," she says.

"The way we've organized cybersecurity is as a backward-looking function, when it is capable of being a forward-looking, value-added function. When cybersecurity speaks the language of business, it takes that critical first step of both hearing and being understood. It starts to demonstrate value because it can directly tie business drivers to what cybersecurity is doing to enable them, justifying its spend and effectiveness. It gets closer to cementing positive relationships outside of traditional lines, and it changes the conversation from 'Why we can't' to 'How can we?' It moves the debate from risk reduction to innovation."

Figure 9: Fighting to be heard
Pressing challenges for cybersecurity



“

There is a need to ramp up security budget given the rising number of cyber-attacks and data breaches in India.

It is equally important to consciously select the cyber spend strategy and judiciously allocate budgets for optimization of the risks.

Jaspreet Singh
Partner, Cybersecurity, EY India

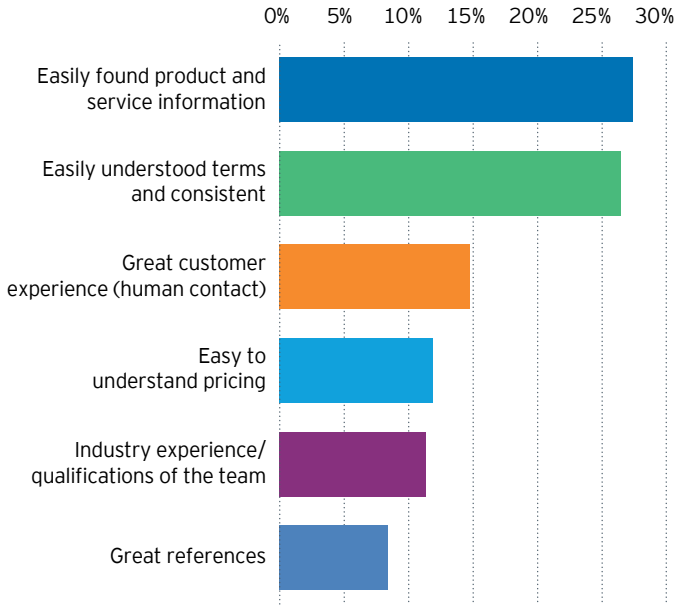
What is the role of third-parties?

Can third-party vendors help CISOs improve the performance of cybersecurity and move it closer to the business? Right now, there is some skepticism about the value vendors in the industry genuinely add. Only 32% of respondents to this survey say they trust the marketing claims of cybersecurity vendors, though a further 57% say it depends on the vendor in question. Almost a quarter say vendors fall short on inconsistent delivery (32%) or their confusing products and services (20%).

However, with 84% of organizations using up to 30 cybersecurity products or tools (and some using even more), there is scope to drive performance through closer collaboration with a select group of the most trusted vendors. CISOs focus on easily found product and service information and easily understood terms and consistent as key qualities.

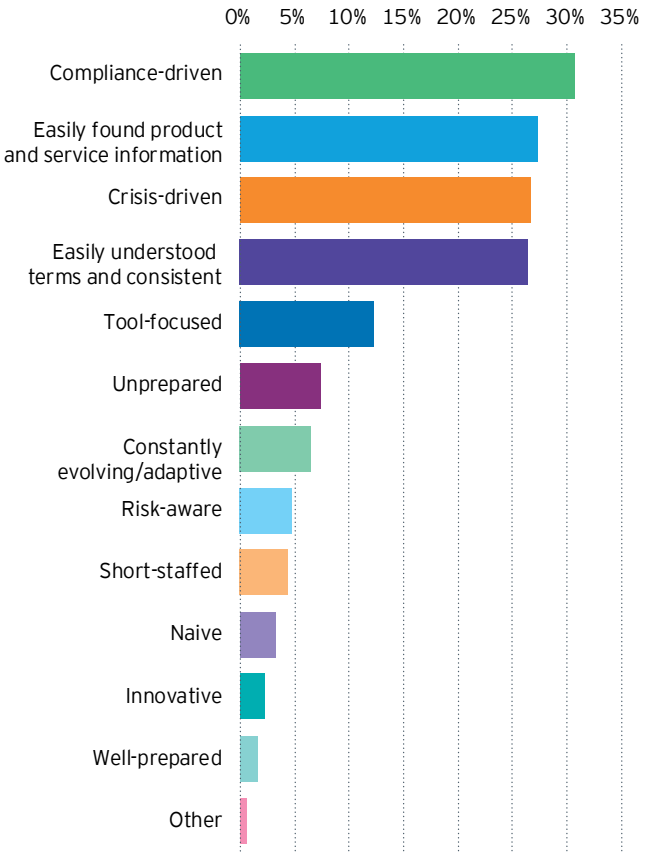
"CISOs are saying, 'how do I optimize and simplify?'," says Mike Maddison, EY EMEIA Cybersecurity Leader. "One option is to reduce the number of point solutions they have, or to bring in a particular flavor of software provider to reduce management overheads, moving towards broader enterprise agreements to get maximum consumption from one vendor."

Figure 10: Industry experience and qualifications of the team is the number one factor cited to help increase levels of trust with a cybersecurity provider



3 The CISO becomes the agent of transformation

Figure 11: Perceptions have a long way to go
How CISOs are perceived



Many CISOs now find themselves at crossroads. So far, they have focused on improving their organization's defenses and protecting it from cyber attackers. That challenge remains, but there is now an opportunity for CISOs to move on to the front foot – to become agents of change who are crucial figures in their organizations' efforts to transform their businesses. CISOs in India are now committing to evolve their role especially the mindset of the IT department to become a trusted ally of business leadership in driving business model change.

These CISOs will build cybersecurity functions that operate as enablers of innovation. They will collaborate more closely with other functions than ever before. And they will leverage these relationships to anticipate emerging and changing disruptive threats from bad actors with a range of motivations.

"As digital transformation is increasingly inevitable in organizations, these connected systems also pose a significant cyber risk. The CISO function needs to be well integrated across the lifecycle of digital transformation such that each key milestone of the lifecycle has guidance and required validation by the security team." says Binu Chacko, Partner Cybersecurity, EY India.

The role of CISO will evolve and will require the cybersecurity function as a whole to adapt to new ways of working. But the upheaval will be worth it: this is a chance for cybersecurity to become a trusted business partner at the center of the organization's value chain, driving transformation and proving its worth.

The cybersecurity industry in India today is widely regarded as compliance-driven, set up to respond to crisis and focused on the tools it has at its disposal (see Figure 11).

Just 6% of respondents describe the sector as constantly evolving and adaptive; even fewer use the word "innovative."

"

Cyber is increasingly being acknowledged as an enabler to business operations and for delivering widespread citizen services. The recent Covid-19 crisis led newer work environments and remote operations for enterprises, was vastly dependent on agility of CISO's/ Cyber team to enable continued and secure processes.

Vidur Gupta
Partner, Cybersecurity, EY India

61% of security leaders have the ability to financially quantify the impact of breaches.

The future CISO: New skills, new structures, new status

One important question for CISOs is whether they currently have the right skills and experience to work in this new way, and to lead a function that is more proactive and forward-thinking. Their considerable technical skills, earned during careers moving up through cybersecurity functions, will not be enough. The new CISO role will require commercial expertise, strong communication skills and an ability to work collaboratively. The CISOs in India are committed to acquire new skills, approaches and methodologies in IT to understand internal and external customer needs and address them effectively.

Recognizing this, senior leadership in some organizations are onboarding CISOs from beyond the cybersecurity function, says Rohan Sachdev, EY India Advisory Leader. These executives have served in other areas of the business – particularly the more commercial roles. "Organizations are realizing that you don't need to be a technologist to be a CISO," he says. "At the end of the day, the objective is to manage the risk, hence in my view the best CISOs are the ones who understand the language of risk."

Other organizations will prefer to stick with CISOs who have more conventional backgrounds, while also trying to build the organizational processes that will enhance relationships between cybersecurity, the board/C-suite, and the rest of the business. "We've got to both mentor the function, as well as create more formal management and governance structures that enable cybersecurity to communicate within a business context," says Rohit Mathur, EY India Risk Advisory Leader. "Essentially, we need the language and mechanisms to interpret between that function and the board/C-suite and other functions."

The change can be summed up succinctly, continues Rohit Mathur, "we need to go from a CISO who says 'no,' to one who says 'yes, but …'" In other words, CISOs cannot afford to be seen as blockers of innovation; they must be problem-solvers – enablers who promote Security by Design and allow their organizations to transform safely and securely."

However, as CISOs contemplate this different type of role, are today's reporting structures fit for purpose? Currently in India, the role of CISOs is expanding, which is apparent from the fact that currently 68% of CISOs sit on their organization's board or operate as a member of the executive management team. This is a positive change and will help CISOs to have broader and closer relationships with senior leaders and other business functions become more vital; more organizations may need to elevate the role's status.

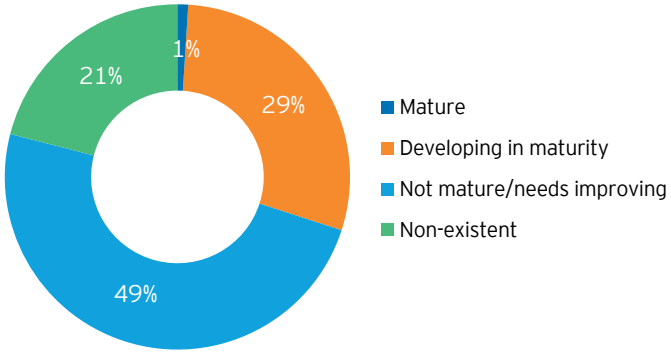
Take reporting structures: respondents tell us that CISOs are most likely to report into the organization's CIO. This could leave cybersecurity one step removed from the rest of the business, with the CIO required to act as a conduit.

That will have to change if cybersecurity is going to play an enabling role in business transformation, with these organizations following the example of the 14% whose CISO reports directly to the CEO. The small minority of organizations whose CISOs report into risk, finance or legal may find that these structures no longer work.

> "CISOs play a vital role in today's digital landscape, acting as business enablers rather than mere risk managers promoting Security by Design and business resilience embedded in the organization's transformation journey.
>
> **Murali Rao**
> EY India Advisory Cyber Leader

Figure 12: Shortfall in ability to quantify the financial impact of breaches

Security leaders' ability to quantify the financial impact of cybersecurity breaches



Case studies

1 3 pillars: People, process and technology

A global financial services corporation enhanced their overall security posture through a convergent cybersecurity program focusing on the three pillars: people, process and technology with an emphasis on solutions such as information security management system, infrastructure and application security, cyber threat management and identity and access management. This has helped the organization to manage security holistically and identify pertinent gaps and security exposures in IT and network systems.

The global information security team thus works in a hub and spoke model wherein they coordinate for multiple security programs and initiatives for all locations focusing on improving the security posture of each location of operation. Further, each program focuses to integrate security in the DNA of the organization through well defined, continuously improved and managed initiatives.

2 Better coordination and decision making – a baseline for today and a starting point to improve tomorrow

A global management consulting firm restructured their entire information security and risk management vertical by aligning the key activities of all verticals of their security function with the plan, design, implement, operate, improve and innovate (PDIOII) model. This model helped them in enhancing the overall security posture through clear segregation of responsibilities. Further, they also focused on key security solutions such as threat and malware protection, data protection, vulnerability management and business continuity. This helped the organization in improving their business agility, performance and risk management year on year.

The program aimed at enforcing Security by Design and operational level along with availability assurance, ensured smooth business operations across global locations. Additionally, centralization including automation and streamlining of security processes helped improve the overall security maturity of the organization.

3 Centralizing cybersecurity

A multinational ITES company after a cyber incident embarked on a major transformational journey to revamp its overall cybersecurity program. As part of this transformation they brought together security functions across all regions globally, which were operating and running their own cybersecurity programs.

Further as part of this exercise they performed a cyber benchmarking assessment to understand their cyber maturity and compared it with industry benchmarks. The security team now has a deeper understanding of the cybersecurity risks across the enterprise. They defined a list of organization wide cybersecurity initiatives and converged their resources to establish and run an enterprise wide cyber program.

The CEO has taken cyber maturity improvement as a key performance KPI in his scorecard. Cybersecurity is a key agenda item in board updates. The security transformation program is now demonstrated as key differentiator during its investor summit and earnings call.

4 CISO as a service program

A large organization with many group companies is managing their cybersecurity program by establishing central systems and processed and enabling group companies leverage these solutions thereby enabling consistent and uniform security implementation.

They have established CISO as a service program for group companies who leverage security expertise as a service model. This allows group companies flexibility in leveraging multiple security skill sets from a central pool and manage the program as per their schedule and timelines.

A centralized SOC performs 24x7 monitoring of threats across organization infrastructure landscape and provides protection against attacks, data leakages and other vulnerabilities. A centralized security helpdesk allows users a single point to address queries on security related requests/ incidents.

5 Cross-functional teams for holistic view

EY is assisting a government organization in India for assessing their business and IT controls, cybersecurity posture, IT service management and business resilience. This three-and half-year initiative is focused to ensure compliance with applicable acts, leading standards, rules and dynamic regulatory environment across the vast spectrum of the tax ecosystem. EY is also supporting with an overall governance, risk and compliance framework to facilitate creation of a robust, comprehensive and secure environment for the indirect tax ecosystem. This also entails implementation of a GRC solution that would provide an integrated view of compliance and help in deriving deep insights thus enabling a coordinated and responsive digital governance.

The project team being an amalgamation of multiple cross functional teams, has given EY a holistic view and in-depth understanding of the indirect tax ecosystem and its intricacies. Hence bringing forth critical insights on revenue leakages and gaps in cyber security posture for their ecosystem. This is further enabled by the deep relationship between the project operations team and senior leadership of the organization.

6 Centralizing cybersecurity

EY is assisting a major UAE based bank in its efforts to enhance its information security governance function through renewal of a cyber strategy, upliftment of the cybersecurity posture, digital transformation, policies, procedures, baseline standards and enhancement of the cyber security governance framework. It is imperative for the bank execute to a systematic, measured plan of action to address some of the common denominators and enhance security group-wide.

The initiative and roadmap span a three-year period, consist of technology, governance and program management initiatives and have been sequenced to limit risk and realize early value.

Designing the program through cyber initiatives, enabled the cyber/information security function to consolidate the complete strategy on theme of cyber resilience, compliance, digital transformation, data centricity, proactive risk management and cyber culture and governance. Cyber and information risk has gotten embedded at the forefront of the bank's business strategy and real-time cyber/information risk intelligence has enabled the strategic decision-making

#1 spending category in cybersecurity budgets is the SOC.

Encouraging signs but barriers still exist

Cybersecurity cannot fulfil its potential to add value if it is kept at arm's length from the rest of the organization.

There are some encouraging signs. For example, 45% of organizations say they are articulating cyber risk – and their tolerance of risk – in the context of business or operational risk. And more than half (56%) of organizations expect the security function to provide governance as new intellectual property is developed; only slightly fewer (46%) say the same of operational technologies.

This is promising, but organizations will encounter obstacles as they seek to integrate cybersecurity with other functions.

Budget allocation, in particular, may represent a challenge. In many organizations, the budget for cybersecurity is already derived from several sources, including monies from other lines of business and business functions. Less than a third of respondents (17%) say that their budget comes from more than one source, and this is likely to increase as collaboration rises. Who should be responsible for controlling those funds? More than three-quarters (83%) of organizations say that there is one centralized "owner" of sourcing and disbursement, but this will be an increasingly open question.

These are structural and operational issues to be weighed up rather than significant barriers to a new way of working. The benefits of greater integration to both the business and to cybersecurity outweigh these obstacles, and should persuade organizations to do all they can to resolve them.

Only 6% of breaches in the last 12 months were detected by the SOC.

Are Security Operations Centers (SOCs) fit for purpose?

This year's GISS 2019-20 – India edition finds that the performance of many organizations' SOCs has been disappointing. Respondents report spending 21.5% of their cybersecurity budgets on their SOCs and allocating 21.3% of employee time to operating them; however, only 6% say that their SOC identified their most significant breach over the past 12 months.

This might be because many organizations continue to operate with first-generation SOCs that require significant amounts of manual intervention – particularly given the reluctance (or inability) to invest in future-proofing. Only 17.8% of budget is currently going towards architecture and engineering. Are SOCs holding cybersecurity functions back?

Upgrading the SOC could now generate significant dividends. Not only will it improve the organization's ability to identify threats and breaches, but it will also free up resources through increased automation. Organizations that can reduce the amount of employee time required for operating SOCs can then redeploy cybersecurity staff into business-facing activities.

EY Cognitive Cyber Centre

Upgrading a SOC to a Next-Gen SOC would mean a single platform for security monitoring, incidence response and threat intelligence. EY launched its Cognitive Cyber Centre which has built-in automation for Incident and forensics life cycle management to protect, detect, respond, remediate and investigate evolving threats.

The SOC utilizes advanced behavioural analytics and threat hunting capabilities to provide near real-time and in-line reporting in various form factors.

Conclusions and next steps

This year's EY GISS 2019-20: India edition looks at the progress made by organizations as they attempt to position cybersecurity at the heart of business transformation, built on the foundation of Security by Design.

There is a significant opportunity here for CISOs, board and C-suites and the rest of the business to work together to reposition the cybersecurity function. Organizations that succeed in this endeavor can ensure that the cybersecurity function becomes a key agent of change, enabling the transformation their businesses must undergo to remain competitive. Organizations will also find that cybersecurity becomes more effective in its traditional defensive role, able to anticipate new threats as they evolve with a wider understanding of the potential risks posed by hacktivists, for example. And with stronger relationships between boards and CISOs courtesy of a new style of reporting and communication, old battles over resources and value will fall away.

Making this transition is not straightforward, nor is it the same for everyone. What organizations do next – their CISOs, board and C-suites, and individual functions – will depend on the current state of their cybersecurity functions and the characteristics and objectives of their organizations.

There are, however, five actions that every organization can prioritize to make the most of the opportunity:

1

Establish cybersecurity as a key value enabler in digital transformation

Integrate cybersecurity into business processes using a Security by Design approach. Bringing cybersecurity into the planning stage of every new business initiative is the optimal model as it reduces the energy and expense of triaging issues after-the-fact and builds trust into a product or service from the start. It requires cybersecurity to become far more integrated and collaborative.

2

Build relationships of trust with every function of the organization

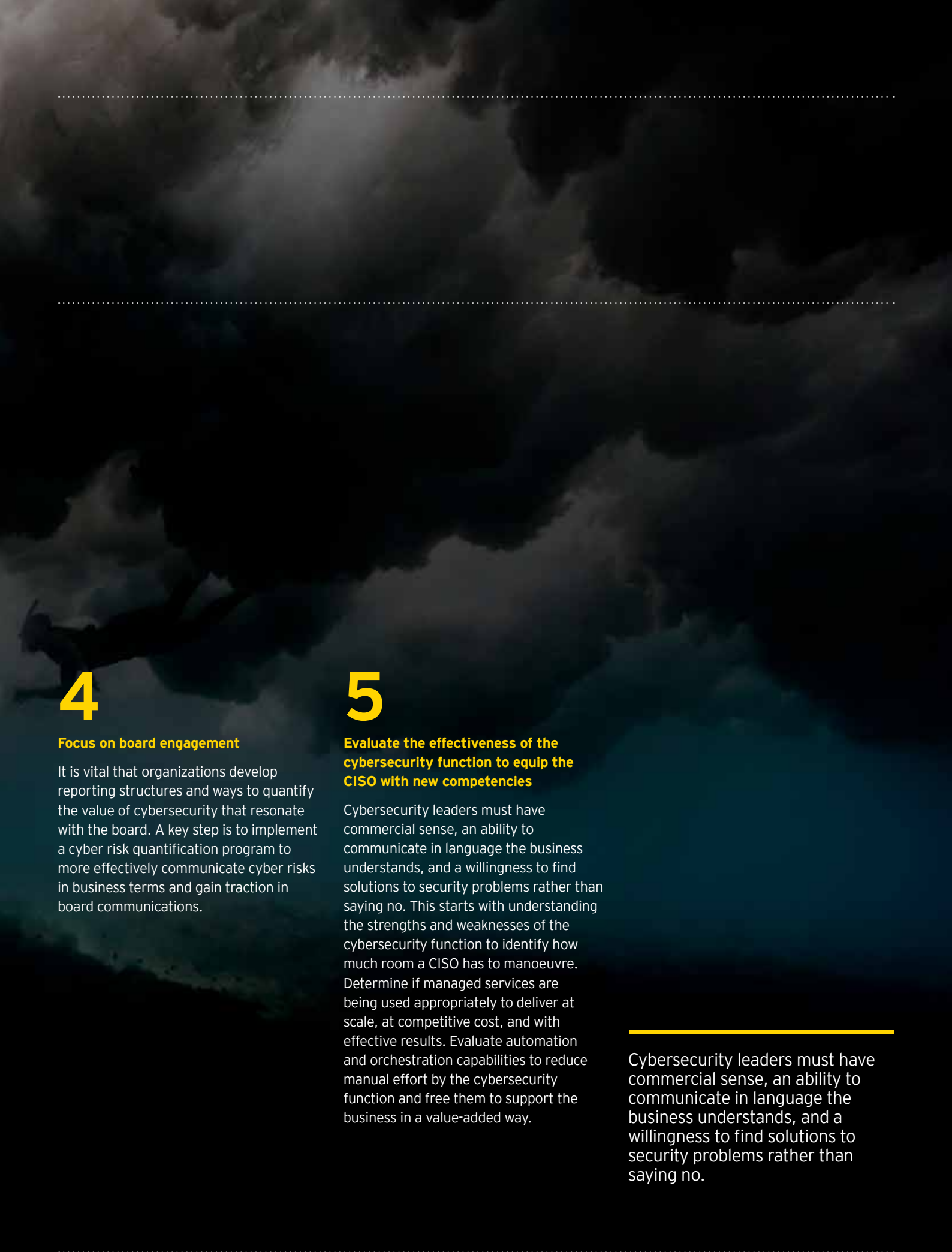
When cybersecurity is embedded in the business, CISOs will be in a strong position to help drive innovation and become better informed of threats faced by the organization. A key way of doing this is using existing data to model business processes and associated controls and collaborating with CISOs to understand the true cybersecurity impacts to these business processes.

As the evidence becomes clear to all, business functions gain real-time insight to the security of their processes and build trust; CISOs gain visibility on potential additional risks and threats and how to help the business control or innovate around them.

3

Implement governance structures that are fit for purpose

Boards and C-suite leaders should reconsider lines of reporting, budget control and accountability to reflect the new role for cybersecurity at the heart of innovation. Once these are set, develop a set of key performance indicators and key risk indicators that are used to communicate a risk-centric view in executive and board reporting.



4

Focus on board engagement

It is vital that organizations develop reporting structures and ways to quantify the value of cybersecurity that resonate with the board. A key step is to implement a cyber risk quantification program to more effectively communicate cyber risks in business terms and gain traction in board communications.

5

Evaluate the effectiveness of the cybersecurity function to equip the CISO with new competencies

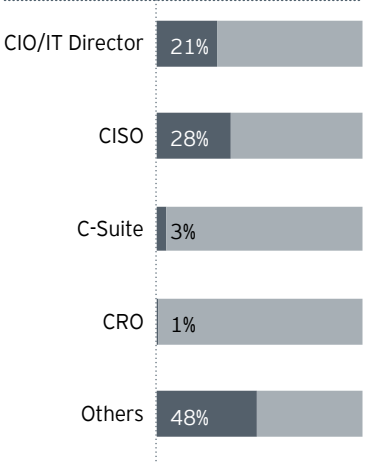
Cybersecurity leaders must have commercial sense, an ability to communicate in language the business understands, and a willingness to find solutions to security problems rather than saying no. This starts with understanding the strengths and weaknesses of the cybersecurity function to identify how much room a CISO has to manoeuvre. Determine if managed services are being used appropriately to deliver at scale, at competitive cost, and with effective results. Evaluate automation and orchestration capabilities to reduce manual effort by the cybersecurity function and free them to support the business in a value-added way.

Cybersecurity leaders must have commercial sense, an ability to communicate in language the business understands, and a willingness to find solutions to security problems rather than saying no.

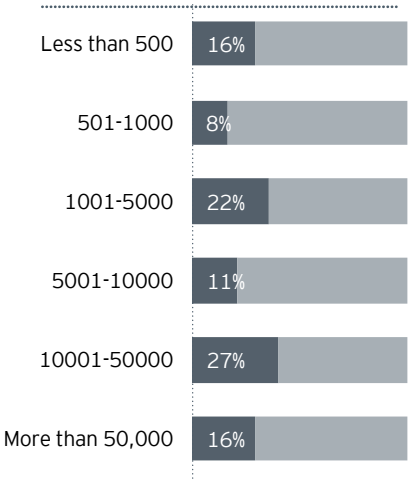
Survey methodology

The 22nd edition of EY Global Information Security Survey 2019-20 – India edition, captures the responses of over 190 C-suite leaders and information security and IT executives/ managers, representing many of the world's largest and most recognized global organizations.

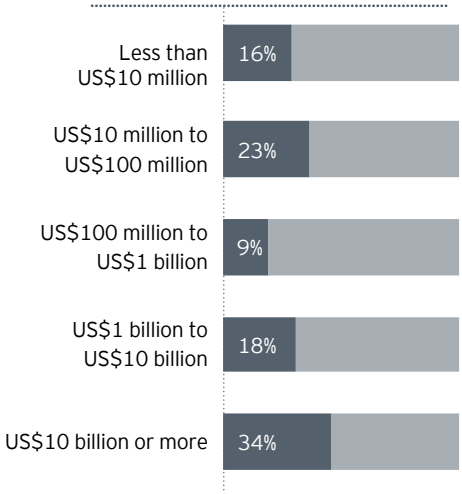
Respondents by position



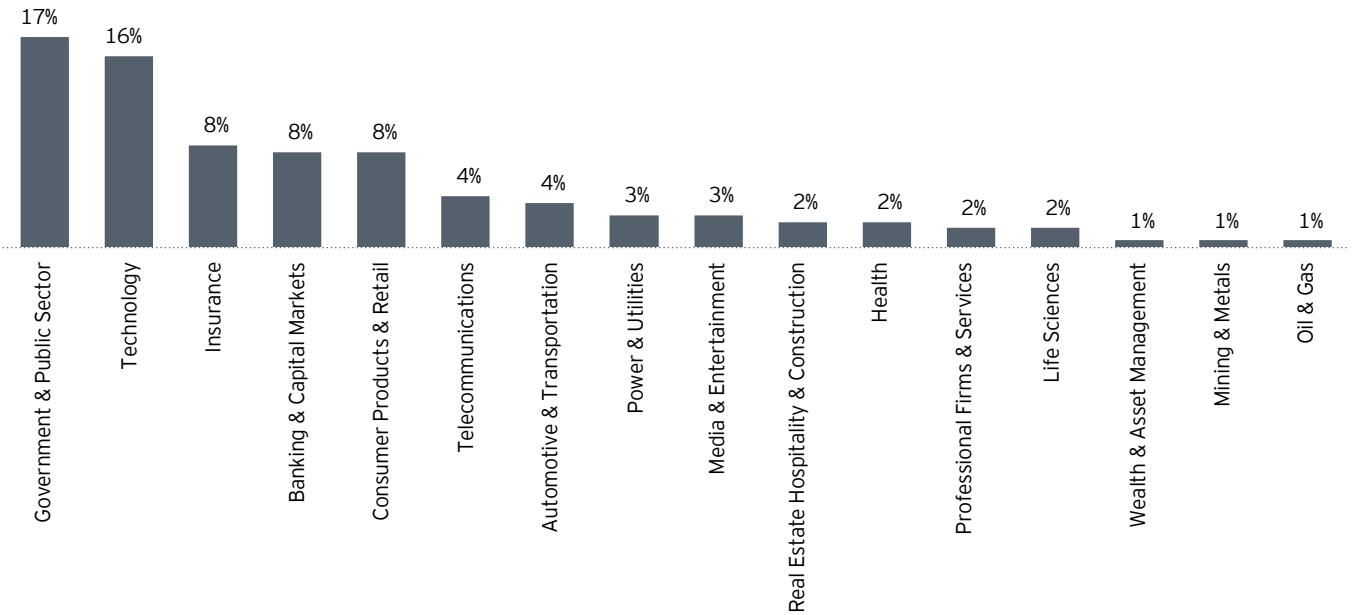
Respondents by number of employees



Respondents by total annual revenue (in US$)



Respondents by primary industry



Management Team

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

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

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

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

Jaspreet Singh
India Partner – Cybersecurity
Email: jaspreet.singh@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

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

Binu Chacko
India Partner – Cybersecurity
Email: binu.chacko1@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

Notes:

EY offices

Ahmedabad
22nd Floor, B Wing, Privilon,
Ambli BRT Road,
Behind Iskcon Temple,
Off SG Highway,
Ahmedabad - 380 015
Tel: + 91 79 6608 3800

Bengaluru
6th, 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 - 160002
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
Gurgaon - 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
Noida - 201 304
Gautam Budh Nagar, U.P.
Tel: + 91 120 671 7000

Hyderabad
THE SKYVIEW 10
18th Floor, "Zone A"
Survey No 83/1, Raidurgam
Hyderabad - 500032
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 | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

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. 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

EYIN2006-033
ED None

JS

ey.com/en_in

 @EY_India  EY  EY India  EY Careers India  @ey_indiacareers