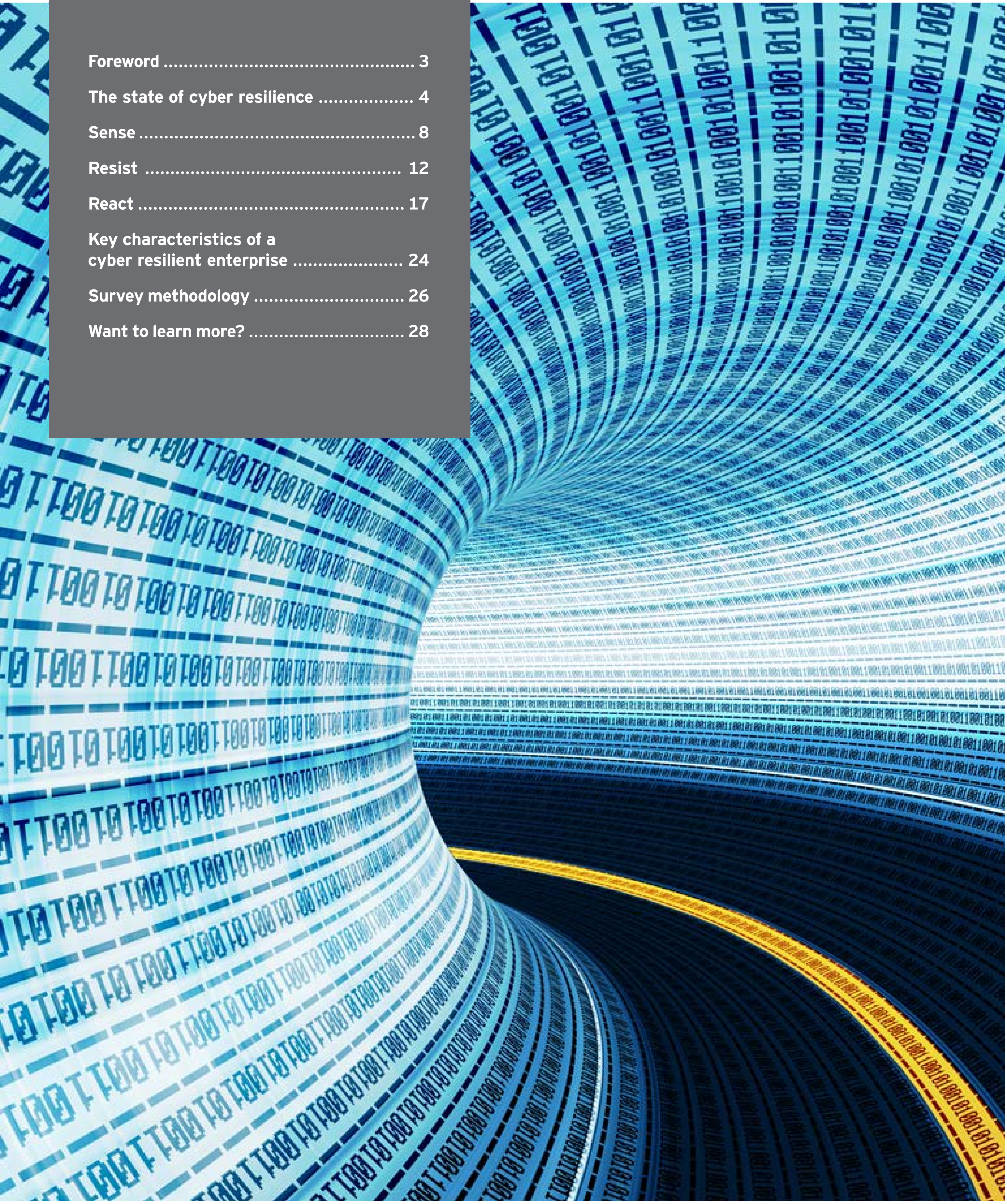
Path to cyber resilience: Sense, Resist, React

Global Information Security Survey 2016-17

India Report

Building a better working world

Contents



Foreword

As disruptive innovations and new business models transform organizations and communities around the world, their sustainability is threatened by a plethora of cyber risks. Indeed, criminals and nation states are increasingly attacking the technology assets of individuals, organizations and governments, stealing and selling valuable information, and in an alarming trend, paralyzing critical infrastructure.

With governments and enterprises increasingly leveraging the internet for mission-critical applications – from managing smart cities and operating power grids to conducting banking transactions and manufacturing connected vehicles – cybersecurity continues to remain a top imperative across the world. Unfortunately, India Inc.'s response to cyber risks has not been robust. India ranks third globally as a source of malicious activities and its enterprises are the sixth-most targeted by cybercriminals. Despite investments in high-end security products, the cyber-breach prevention, detection and incident-response capabilities of most organizations are yet to mature.

The key challenge for Indian companies is that most view cybersecurity as an "IT issue". Consequently, cyber risks do not get appropriate top management attention. This needs to change. Cyber resilience is a critical boardroom imperative. The likelihood of operational, financial and reputational damage is growing as criminals exploit organizations' enhanced attack surface as a result of their online presence, automated operations, and use of social media, mobile devices and cloud services. In many cases, the enemy lies within the organization's perimeter. Research indicates that malicious or negligent insiders, including employees and business partners, are responsible for over half of the cyber-breaches. At risk is intellectual property, customer, vendor and employee data, strategic plans, financial statements, legal positions and indeed, business continuity itself.

What can organizations do to enhance their cyber resilience? The results of our latest global survey of 1,735 CXOs, out of whom 124 were from India, suggest the following:

First, sharpen your senses. Can you see the cyberattacker approaching your perimeter? Does your perimeter even exist anymore? Would you know if someone is beginning to launch an attack on your defences? Can you spot an attacker hiding in a remote part of your network?

Second, upgrade your resistance to attacks. What if the attack is carried out with a new, more sophisticated technique that you haven't experienced before? Would your defences be able to resist something new and more powerful?

Third, react better. In the event of a cyberattack, what is the organization's plan and what is your role in it? What would be your first step? When do you get to know about it and when it is remediated? At what point will you disclose the attack?

As the popular saying goes, there are two kinds of organizations: the ones that have been hacked and those that will be hacked. Indeed, the digital age and the increasing connectivity of people, devices and enterprises are presenting new playing fields of vulnerabilities. Fortifying the enterprise for cyber resilience is therefore an urgent imperative for organizations.

Nitin Bhatt

National Head and Partner – Risk Advisory | India

The state of cyber resilience

Cyber resilience or cyber agility?

In today's time, the government and private sector understand the need to enhance cyber security posture and resilience in the Information Technology infrastructure. However, for the overall national security we need to join hands to share, evaluate and acquire threat intelligence and develop robust operational framework to use this with security technologies. Also, our country's focus needs to continue on encouragement of technological innovations in cyber security to secure national critical infrastructure from cyber criminals.

Dr. Gulshan Rai,
National Cyber Security Coordinator,
National Security Council,
Prime Minister's Office

The cyber threat landscape continues to evolve and presents new challenges to organizations every day. In response, organizations have learned over decades to defend themselves and respond better, moving from basic measures and ad hoc responses to sophisticated, robust and formal processes. While the regulatory landscape in India evolved since the introduction of the Information Technology Act 2000 (IT Act); organizations have been compelled to transform their cybersecurity measures on account of recent events such as the demonetization drive coupled with the corresponding push to adopt digital technology, heightened focus on e-governance and digital governance, breach of sensitive defense data and the outburst of cybercrime. Similarly, organizations are realizing that threats originating from the digital world require dedicated resources and efforts. Here is a short overview of the evolution of the threat landscape:

1970s	1980s	1990s	2000	Recent times
‣ Ready for natural hazards ‣ Physical response measures in place, e.g., evacuation and first aid ‣ Call for external assistance	‣ Reliance on a few new technologies ‣ Basic disaster recovery in response to system failures ‣ Virus protection developed ‣ Identity and access management	‣ Enterprise-wide risk management introduced ‣ Regulatory compliance commonplace ‣ Business continuity a focus	‣ Advances in information & ‣ Switch to online ‣ Third-party outsourcing, e.g., cloud ‣ Connectivity of devices	‣ Global shocks (terrorist, climate, political) ‣ Business resilience ‣ Internet of Things (IoT) ‣ Critical Infrastructure (utilities & energy) ‣ State-sponsored cyber espionage and cyber attacks
Mainframes	**Client/Server**	**Internet**	**E-Commerce**	**Digital**

Cyber resilience focuses on how resilient an organization is to cyber threats. Before going into the details, let us first look at the three high-level components of cyber resilience and how well – in general – organizations are performing in these three areas:

Sense

Sense is the ability of organizations to predict and detect cyber threats.

Organizations need to use cyber threat intelligence and active defense to predict what threats or attacks are heading in their direction and detect them when they do, before the attack is successful. They need to know what will happen, and need sophisticated analytics to detect early-warning signals.

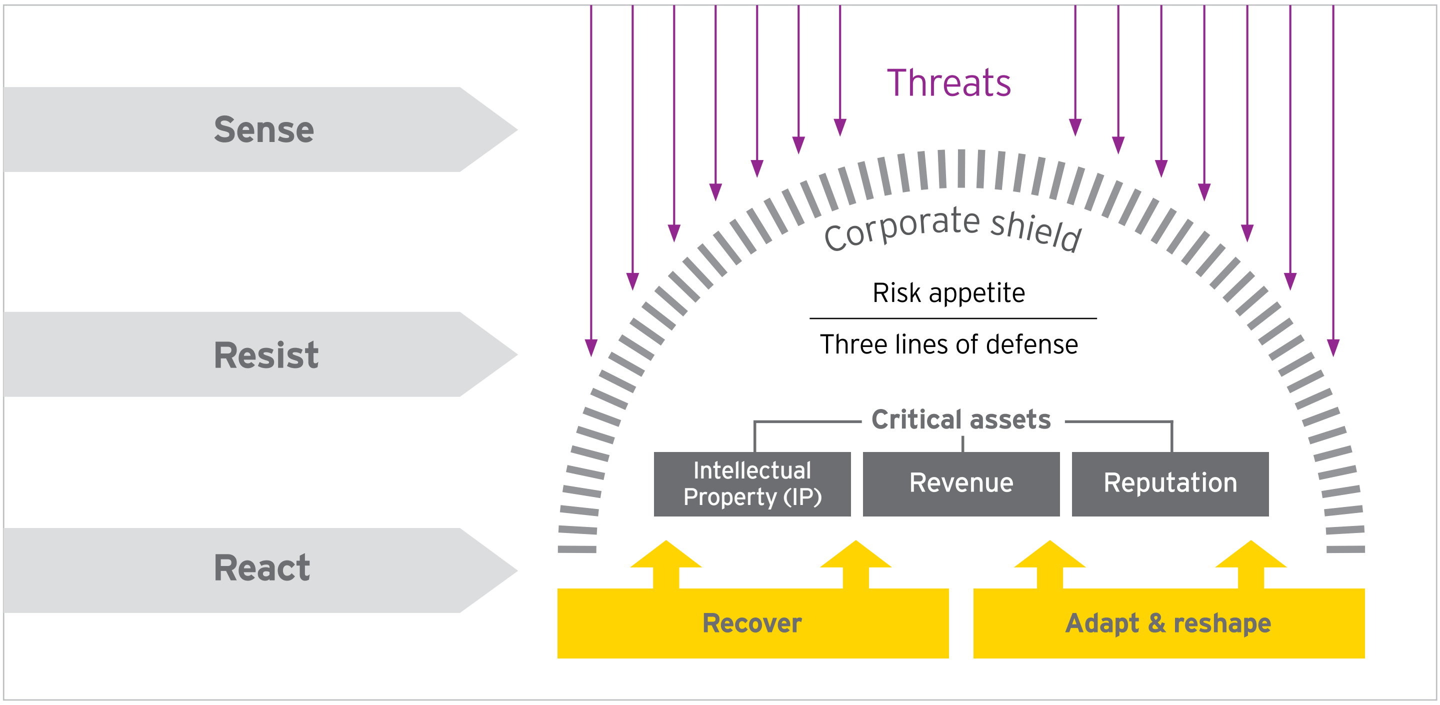
Resist

Resist mechanisms are basically the corporate shield to cyber-attacks. It begins with assessing an organization's risk appetite, followed by establishing the following three lines of defense:

1. First line of defense: Executing control measures in its day-to-day operations
2. Second line of defense: Deploying monitoring functions such as internal controls, establishing legal, risk management and cybersecurity processes.
3. Third line of defense: Establishing a strong internal audit department

React

If Sense fails (the organization did not see the threat coming) and there is a breakdown in Resist (control measures were not strong enough), organizations need to be ready to deal with the disruption, ready with incident response capabilities and mechanisms to manage the crisis. They also need to be ready to preserve evidence in a forensically sound way and then investigate the breach in order to satisfy critical stakeholders – customers, regulators, investors, law enforcement agencies and the public, any of whom might bring claims for loss or non-compliance. They also need to be prepared to bring the organization back to business as usual as quickly as possible, learn from what happened, and adapt and reshape the organization to improve cyber resilience going forward.



The overall picture

Before we explore cyber resilience in more detail, let us first paint a picture of its current status. Overall, the message is positive: organizations are moving in the right direction on the path to cyber resilience.

In recent years, mainly on account of incidents of large cyber heists and attacks, organizations have started investing in their corporate shield. Significant progress has been made in taking measures to strengthen this shield and in the last two to three years, we have also seen organizations focus more on their Sense capabilities.

Most organizations, however, are lagging behind in preparing their reaction to a breach, still ignoring the all-too-familiar statement, "it's not a matter of 'if' you are going to suffer a cyberattack, it's a matter of 'when' (and most likely you already have)." We have summarized the overall picture, and in the following sections of this report, we will explore the components of cyber resilience in more detail.

	Sense (See the threats coming)	Resist (The corporate shield)	React (Recover from disruption)
Where do organizations place their priorities?	Medium	High	Low
Where do organizations make their investments?	Medium	High	Low
Board and C-level engagement	Low	High	Low
Quality of executive or boardroom reporting	Low	Medium	Low

Cyber agility or cyber resilience?

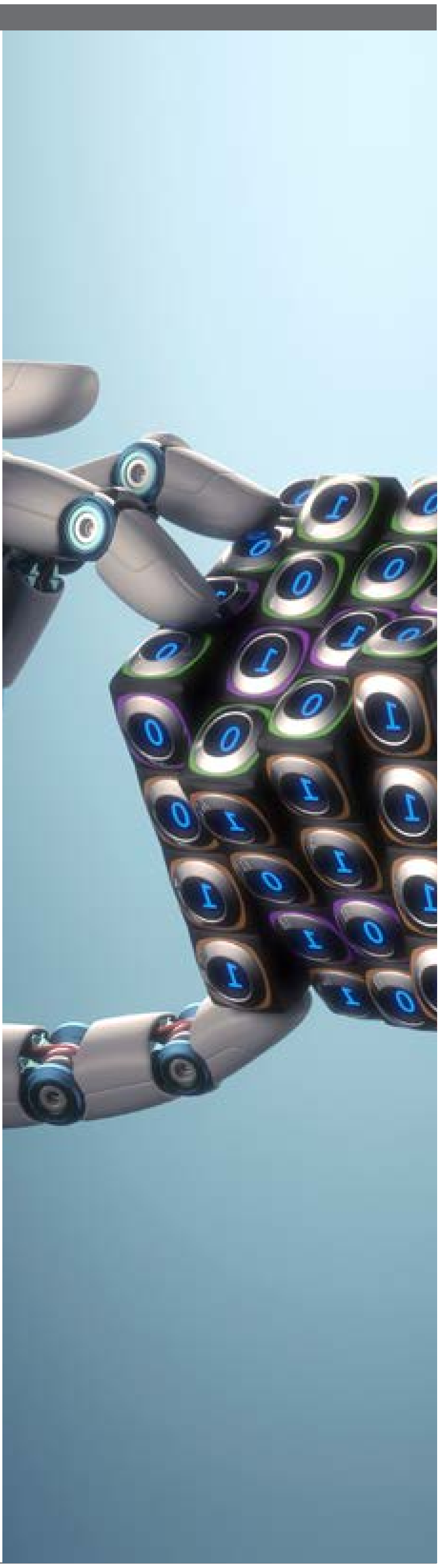
In the cybersecurity space, organizations would like to respond to changes as quickly as possible. Questions like "How can I increase the agility of my cybersecurity systems and processes?" and "How can I quickly respond to what's happening in the cyber space?" are often heard.

Organizations want to know how to predict the next threat, and what are the "hottest" technologies to prevent it. Cyber threat intelligence, cyber threat management and related software and consulting have become priorities in most organizations - all with the intent of increasing cyber agility, i.e., the ability to react to a change in the threat landscape.

Aiming for greater cyber agility is great, and investments on cybersecurity systems are welcome. However, the critical question organizations should ask is: "Are we cyber resilient?" In other words, are your cybersecurity systems and processes strong enough to mitigate all the cyber risks the organization is facing? Cyber resilience is not just about responding to new threats; it is more about creating the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.

Over the past many years, the EY Global Information Security Survey has been shining a spotlight on the cybersecurity issues. Over the last two years, 75% of board members and C-level executives in India, have said that they lack confidence in their companies' cybersecurity processes. Globally, we saw over 86% of board members and C-level executives echo the same lack of confidence in their organization's level of cybersecurity preparedness.

Essentially, what this means is that while cyber agility is critical, it is but a first step towards cyber resilience.



75%

of board members and C-level executives have said they lack confidence in their organization's level of cybersecurity

Sense

While cybersecurity has been an important issue for large corporations for many years, some of the recent high-profile corporate hacking incidents, including those perpetrated by state actors and other sophisticated hacking groups, have made it a truly strategic, board-level issue. There is now an unprecedented expectation from cybersecurity professionals to provide an assurance to the organization's board and senior management that they have the right cybersecurity strategy and remediation processes to address cyber risks and breaches. I am of the view that this change coupled with the dynamically changing cyber threat landscape will drive a new order in terms of how cybersecurity will be managed going forward.

Vishal Salvi
Chief Information Security Officer &
Senior Vice President,
Infosys

A high level of confidence?

Organizations have improved their ‘Sense’ capabilities significantly in recent years. Many organizations are using cyber threat intelligence to predict cyber-attacks, installing continuous monitoring mechanisms, such as a Security Operations Center (SOC), identifying and managing vulnerabilities, and installing active defense. They have become more confident in their ability to predict and detect a sophisticated cyberattack - in a survey carried out in late-2016, 52% of organizations expressed confidence in their ability to do so.

While this is a positive development, our survey indicates that many organizations lack even basic cyber security systems and processes. As a result, these organizations are putting their customers, employees, suppliers, and ultimately their own future at considerable risk. The fact that organizations still have a lot of work to do to enhance their basic Sense capabilities, is witnessed by the following findings in this year’s survey:

- 33% of organizations in India do not have a SOC, compared to 44% globally
- 55% do not have, or have only an informal, threat intelligence program
- 44% do not have, or have only an informal, vulnerability identification capability

In addition to these basics capabilities, there are four specific areas/scenarios that need special attention, which could force an organization to rethink what it is doing.

33%

do not have an SOC

55%

do not have, or have only an informal, threat intelligence program

A breach has occurred, but there appears to be no harm

Of the organizations polled in our survey, 52% would not increase their cybersecurity spending after experiencing a breach which did not appear to do any harm. In most cases, there was harm being done, but there was no immediate evidence found to support that. Cyber criminals often conduct “test attacks,” lie dormant after a breach, or use a breach as a diversionary tactic to throw organizations off the trail of what they are really up to. Organizations should assume that harm has been done every time there is an attack, and if it appears that no harm has been done, they should be even more concerned, as that could be an indication that they have not been able to find it.

52%

would not increase their cybersecurity spending after experiencing a breach which did not appear to do any harm

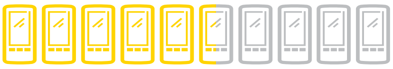
Securing your ecosystem

In our digital and connected world, cyberattack events in organizations’ network of suppliers, customers, regulatory authorities. i.e., the ecosystem can impact the organization itself. This is a major area of risk that is often overlooked, as evidenced by the following findings:

- 68% will not increase their cybersecurity spending in the event that a supplier is attacked – even though a supplier is a direct route for an attacker into the organization
- 58% will not increase their cybersecurity spending in the event that a major competitor was attacked – although cyber criminals often attack other, similar organizations following a successful cyberattack.

An organization’s sensory system is much stronger when events in the surrounding ecosystem are taken into account.

55%



are concerned about poor user awareness and behavior around mobile devices

50%

are concerned about finding hidden or zero-day vulnerabilities

Impact of the IoT

The emergence of Internet of Things (IoT) – physical devices embedded with electronics, software and sensors, and connected to the network infrastructure is beginning to exponentially increase the pressure on organizations' Sense capabilities. The following are just some of the challenges this creates for organizations:

- **Challenges related to the number of devices**

  Organizations are struggling with the huge number of IoT devices that will become part of their networks in a very short period of time. Our findings show that 55% of the organizations surveyed for this study are concerned about poor user-awareness and behavior around mobile devices. A number of organizations are also concerned about their ability to know all their assets (40%), how they are going to keep these devices bug-free (37%), how they will be able to patch vulnerabilities fast enough (40%) and about their ability to manage the growth in the number of access points to their organization (29%).

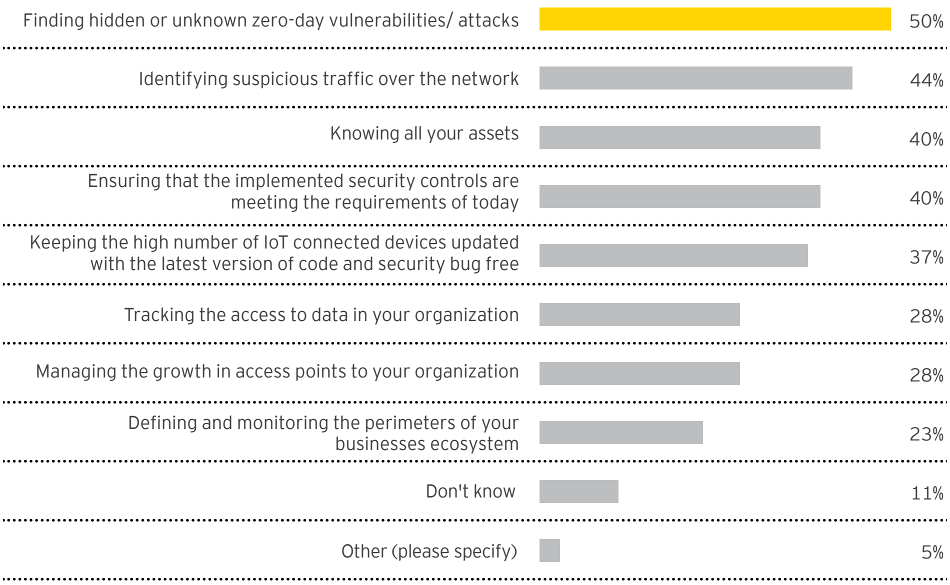
- **Challenges related to the increase in data traffic**

  Organizations doubt that they are going to be able to continue to identify suspicious traffic over their networks (44%), track who has access to their data (28%) or be able to find hidden and unknown "zero-day attacks" (50%).

- **Challenges related to the ecosystem**

  An organization's ecosystem is bound to grow significantly as connectivity to business partners expand and the volume of data exchanges increases. It will become more difficult to identify which part of the ecosystem is most vulnerable to cyber-attacks, thereby impacting the organization itself. It will be even more difficult if the organization's own cybersecurity is fragmented. As a result, many organizations expect difficulties with regard to monitoring the perimeter of their ecosystems (23%).

What do you consider to be the information security challenges of the IoT for your organization?



Information sharing and collaboration are on the rise

Governments and other regulatory bodies/entities are increasingly concerned about cybersecurity. Industry-specific regulations relating to cyber risks are gathering momentum, and legislative interventions are increasing. Therefore, new regulations and laws should be expected. In many parts of the world, standards are being developed for critical infrastructure organizations, and there are calls for greater information sharing and collaboration, as well as mandatory reporting of cyber-attacks, so that cybercrime can be fought together. The National Critical Information Infrastructure Protection Centre (NCIIPC) was created for protection of critical infrastructure against cyber threats. There is a high probability that reporting incidents will become compulsory, and even if it does not happen in the short term, the current cyber threat environment will lead to regulators, stakeholders, business partners and even customers willing to proactively share and collaborate. Be prepared to report and look for opportunities to share and collaborate.

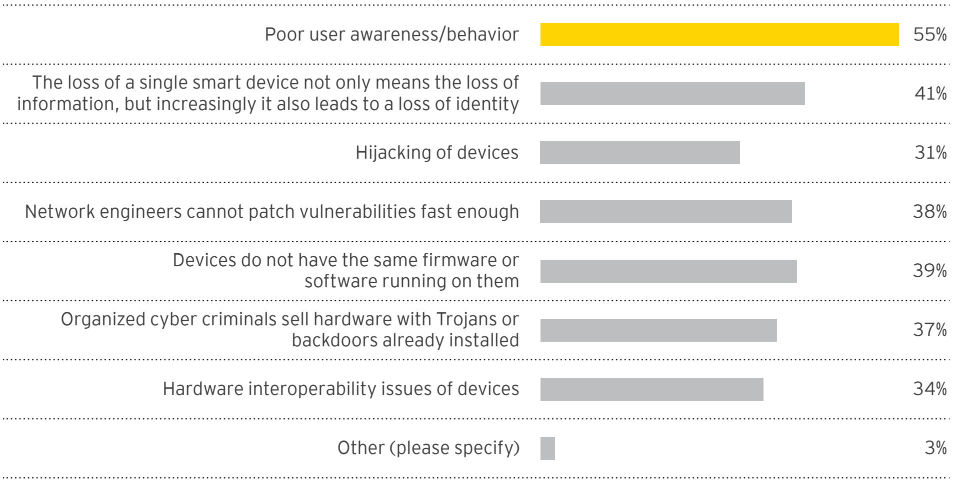
Our survey revealed the following:

- 26% of our responders' SOCs collaborate and share data with others in the same industry
- 44% of our responders' SOCs collaborate and share data with other public SOCs. While this is a positive development, in absolute terms, this is relatively low number due to the low SOC implementation in India

26%

of our respondents' SOCs collaborate and share data with others in the same industry

What are the main risks associated with the growing use of mobile devices (e.g., laptops, tablets, smart phones) for your organization?

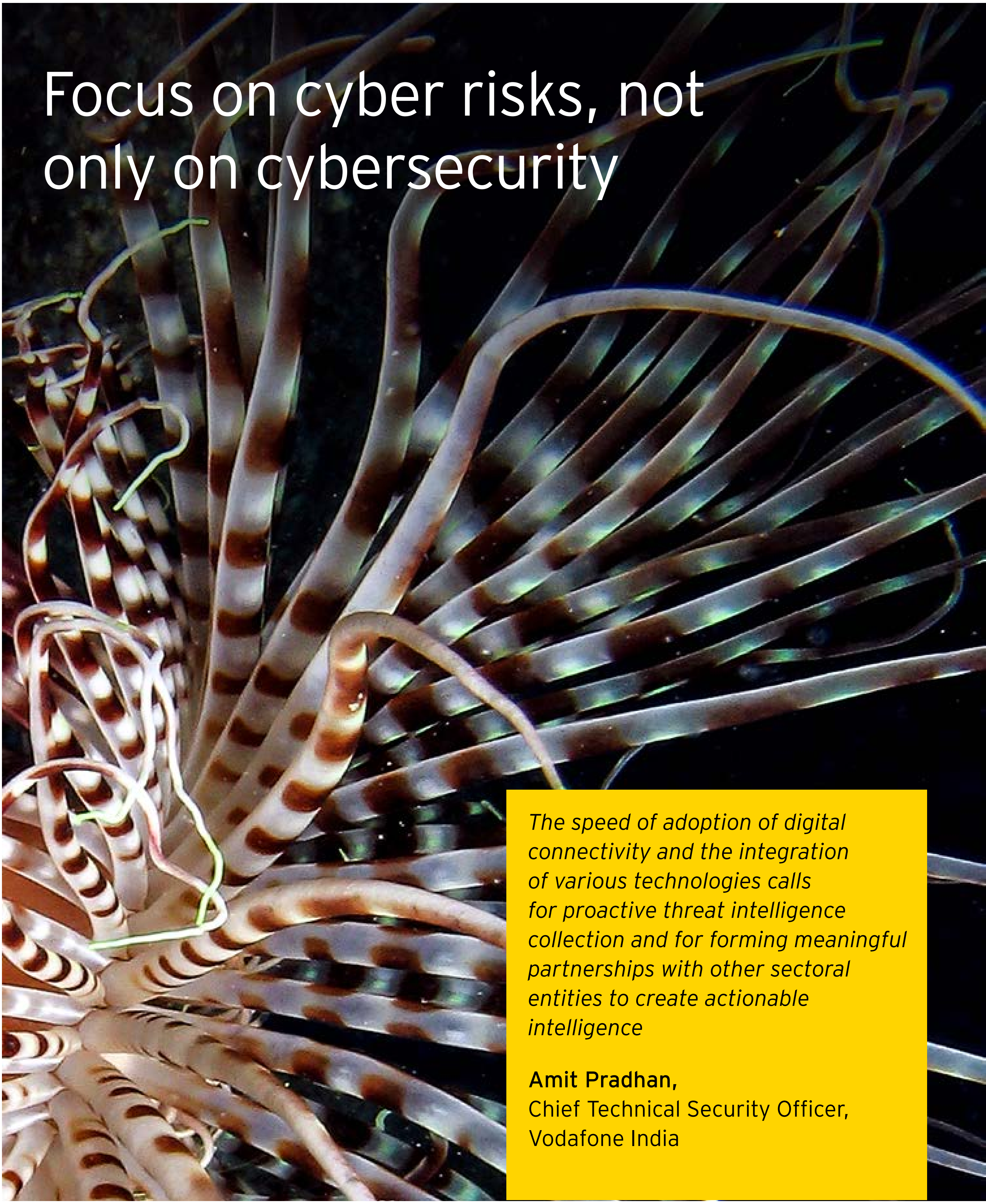


After demonetization, there are a number of reports pointing to a surge in cyber crimes related to One Time Password (OTP) fraud, as well as sprouting of malicious mobile applications

Today's cyber criminals are callous and their behavior and methods are almost impossible to predict

Cyber criminals – like other organized criminals – are highly unpredictable in their behaviour. Their actions convey a different set of values, ethics and morality, and they are often driven by motivations that are hard to fathom. Apart from the more usual and expected fraud and theft, consumers increasingly have fears about crimes related to electronic and cashless transactions, and some critical infrastructure organizations are seeing cyber ransom become a reality. Such is the creativity of the criminal networks that they will always find new ways to launch attacks for personal profit, or to achieve headlines for a cause. Sense, Resist and React have a fundamentally important part to play in protecting the cyber ecosystem, especially with the growth of a cashless economy and the emergence of smart cities, which will rely heavily on IoT.
Without effective cybersecurity, many organizations and governments are not just risking their data and IP, they may be putting individuals at risk, and in the future, we should expect to see even more collateral damage.

Resist



Focus on cyber risks, not only on cybersecurity

The speed of adoption of digital connectivity and the integration of various technologies calls for proactive threat intelligence collection and for forming meaningful partnerships with other sectoral entities to create actionable intelligence

Amit Pradhan,
Chief Technical Security Officer,
Vodafone India

Organizations are striving to improve their abilities to resist attacks, and many organizations can say they are successfully defending against thousands of attacks every day. Attacks take many different and increasingly complex forms. While executing standard cyber control measures in an organization's corporate shield may work against simple Distributed Denial of Service (DDOS) attacks or viruses, it may not work as well against the sophisticated, persistent attacks that organized cyber criminals launch against their targets every day.

- 75% of responders to our survey said that their cybersecurity function did not fully meet their organization's needs

75%

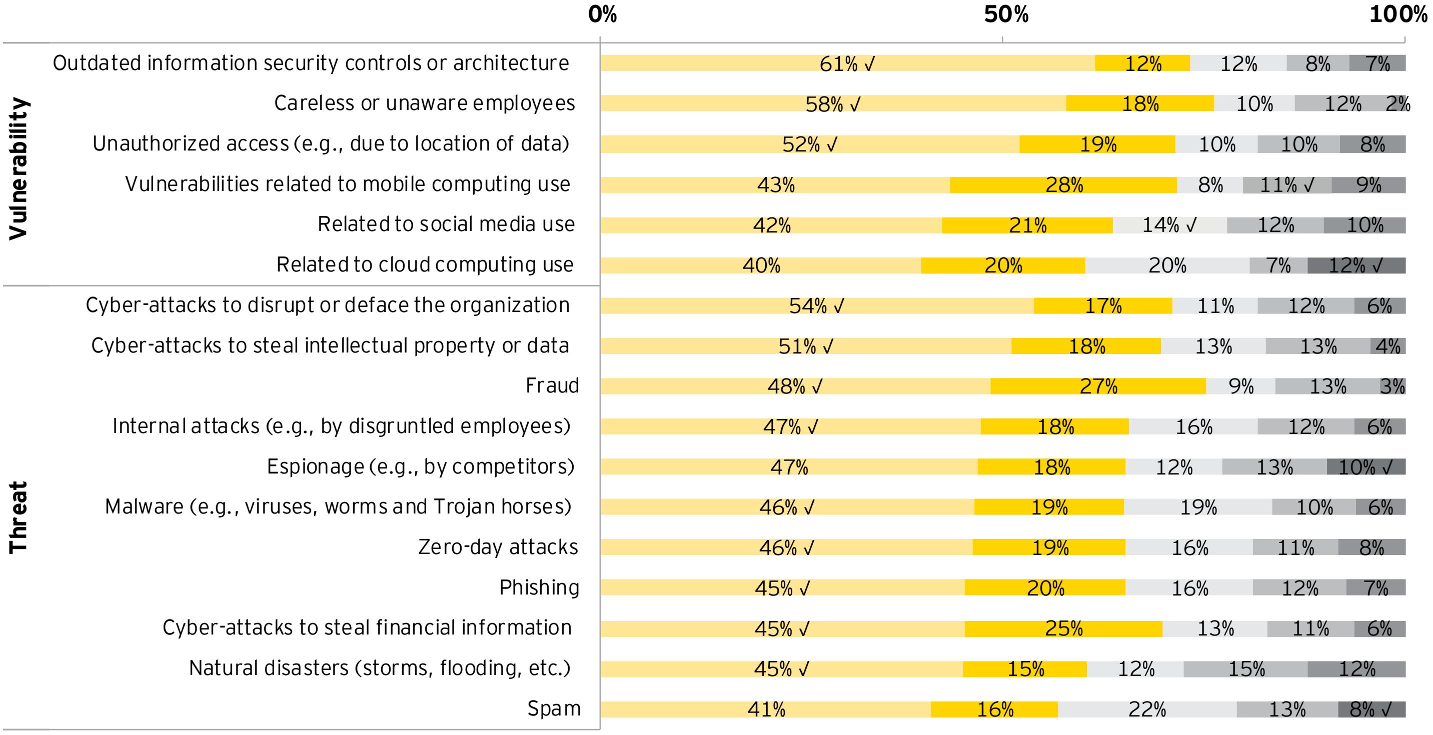
of the responders stated that their cybersecurity function does not fully meet their organizational needs

Focus on cyber risks, not only on cybersecurity

In our recent survey, more than half (61%) the responders said that their outdated information security controls or architecture were one of the biggest areas of vulnerability. Overall, in 2016, organizations saw many vulnerabilities and threats as less of a challenge. However, that confidence in being able to resist attacks has been short-lived in the face of the growth in employee-related risks and threats as well as the increased sophistication with which criminal syndicates are specifically targeting this human weakness. This year there is a significant upswing in how organizations rate their risk exposure. 54% believe that cyber-attacks are primarily targeted at disrupting or defacing the organization's websites or other digital assets, while they also believe that theft of IP or data continues to be an important risk.

Surprisingly, only 58% of the survey respondents from India fear that the next attack will be due to their employees' carelessness or complicity, compared with 78% of global responders who consider this to be a likely source of attack.

Which threats and vulnerabilities have most increased your risk exposure over the last 12 months?



35%

of responders have had a recent significant cybersecurity incident

Where should organizations focus to better resist today's attacks?

Activate your defenses

While the nature of the attacks has changed, resisting, defending, mitigating and neutralizing attacks have long been the necessary core of an organization's cybersecurity strategy. The services and tools an organization can use to resist cyber-attacks have mostly kept pace with the changing cyber threat environment, and many effective solutions are available today. Nevertheless, our survey reveals that 35% of responders have had a recent significant cybersecurity incident, which shows that there is still more work to be done to strengthen the corporate shield. Maturity levels are still low in many critical areas, and improving them would be a significant step forward for any organization.

Percentage of survey respondents who would rate thefollowing information security management processes within their organizations as mature:

- Software security: 22%
- Security monitoring: 8%
- Incident management: 8%
- Identity and access management: 9%
- Network security: 11%

Take an unorthodox approach

The ability to resist cyber-attacks requires a multifaceted approach. Defenses are usually seen as hard barriers - like encryption or firewalls - that stop and neutralize an attack, but there are other ways organizations can minimize the impact of an attack and help the organization with their Resist strategy:

- **Switching from a fail-safe to safe-to-fail**

  Organizations have been right to focus so far on building robust, sturdy, resilient fail-safe operations that can withstand sudden cyber-attacks.

  But in the face of today's unpredictable and unprecedented cyber threats, a fail-safe approach can no longer be the only option. The new aim should be to design a system that is safe-to-fail. Future cybersecurity needs to be smarter as well as stronger, with a soft-resilience approach.

  This means that on sensing a threat, there are mechanisms that have been designed to absorb the attack, reduce the velocity and impact of it, and accept the possibility of partial system failure as a way to limit damage to the whole.

- **From protection to sacrifice**

  Technologies today make it possible to sacrifice portions of information or operations in the interests of protecting the larger network. If configured correctly to the organization's risk appetite this can be performed as an automated response. When the SOC recognizes a high level threat to the system, the system owner receives an alert and the system is shut down to prevent the spread of the threat.

Budgets increase every year, but is it enough?

Cybersecurity budgets have seen year on year increases, with 69% of responders saying that their budgets increased over the last 12 months and 73% saying that their budgets will increase over the coming 12 months. 48% of the responders spent less than INR7 crore per annum in total (which includes people, process and technology) while only 28% claim to be spending between INR7 crore and INR14 crore per annum on cybersecurity.

However, organizations say that more funding is needed, with 40% citing budget constraints as a challenge and 37% of responders saying they need up to 50% increase in budget.

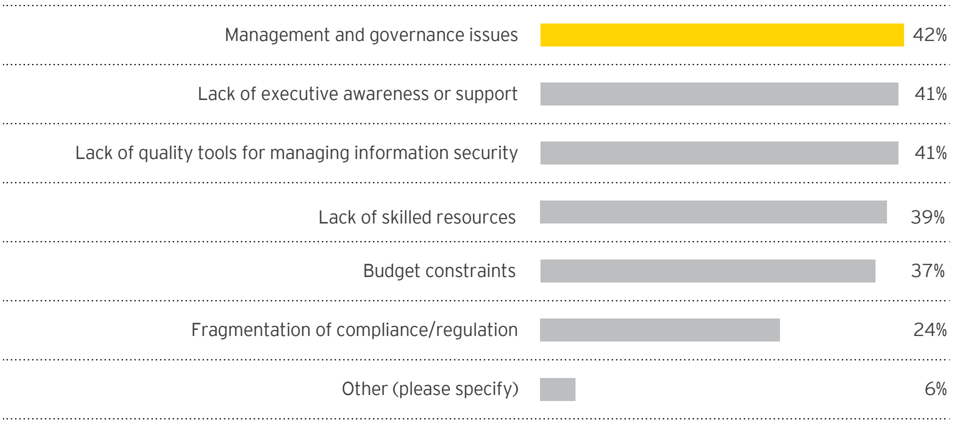
It is not just an increased budget that is needed. While additional investments may help alleviate the skills shortage, it cannot buy the executive support that is also needed. 42% of responders also believe that there is a lack of quality tools for managing information security.

Globally, lack of budgets (61%) and lack of skilled resources (56%) were listed as the main obstacles to information security operations.

69%

of responders say their budgets increased ***over the last 12 months***

What are the main obstacles or reasons that challenge your Information Security operation's contribution and value to the organization?



37%

of responders say they need upto 50% more budget

The role of leadership

Executive leadership and support is critical for effective cyber resilience. Unlike the Sense and traditional Resist activities, which can be seen as the domain of the CISO or CIO, cyber resilience requires senior executives to actively take part and lead the React phase. Our survey has reported that 41% of responders say that there is a lack of executive awareness and support which is challenging the effectiveness of an organization's cybersecurity mechanisms. This suggests that not enough is being done to address this issue or attempts have reached a deadlock and the message is not getting through.

The importance of reporting

Amongst our survey respondents, 49% say that those responsible for information security do not have a seat on the board. In this scenario, the board has to rely on reporting instead. Our survey revealed the following:

- Only 8% have a mature metrics and reporting management process
- Only 30% of reporting processes show where improvements were needed in the organization's information security
- 76% of organizations do not evaluate the financial impact of every significant breach and of those that have had a cyber incident in the past one year, more than half (57%) have no idea what the financial damage has been or could be

Despite of the quality of reporting being so low, it is surprising that only 38% of respondents think their boards are not fully knowledgeable about the risks the organization is taking and the measures that are in place. Based on this response, it may seem like boards are not fully informed of one of the greatest threats to their organizations today.

76%

of organizations do not evaluate the financial impact of every significant breach

57%

have no idea what the financial damage of a cyberattack is or could be

React

With the steep rise that India has seen in the number of attacks coupled with complexity and focussed cyber-attacks on business applications that directly results in monetary loss, it's critical that banks focus on increasing their incident response capabilities to minimize or thwart the extent of damage. The only safe thing to assume today is how better equipped are we to withstand a cyberattack

Sameer Ratolikar
Chief information Security Officer,
HDFC Bank

Today's emergency services: the cyber breach response program

Given the likelihood that all businesses will eventually face a cyber breach, it is critical that companies develop a strong, centralized response framework as part of their overall enterprise risk management strategy.

A centralized, enterprise-wide Cyber Breach Response Program (CBRP) is the focal point that brings together the wide variety of stakeholders that must collaborate to resolve a breach. The CBRP should be led by someone who is experienced with technology, and is able to manage the day-to-day operational and tactical response.

That individual must also have in-depth legal and compliance experience, as these events can trigger complex legal and regulatory issues and significant financial impact.

The CBRP goes beyond the capacity of a traditional program management office. In its coordination and oversight role, the CBRP can help ensure that an organization's business continuity plan is appropriately implemented, that a communication and briefing plan among all internal stakeholders is developed and enforced, and that all breach-related inquiries received from external and internal groups are centrally managed. In short, the CBRP provides guidance to all lines of business involved in the response. The program sets a level of understanding about what information is critical for senior leaders to know — as well as when and how to express it, and allows continuous reaction with precision and speed as a breach continues to unfold over days, weeks or even months.

An effective CBRP must include all key constituencies in a high impact breach. Even as investigators need to work closely with information security and IT personnel to determine the attack vector, exploited networks and systems, and the scope of assets stolen or impacted, the CBRP is the linchpin of an organization's response.

The CBRP not only oversees the process of evidence identification, collection and preservation, forensic data analysis, and impact assessment, but also can direct and modify the investigation based on fact-pattern analysis.
The CBRP helps ensure the smooth and timely flow of information among the internal stakeholders and helps the organization navigate the complexities of working with outside legal counsel, regulators and law enforcement agencies.
A robust CBRP, therefore, enables a cost-effective response that mitigates breach impacts by integrating the stakeholders and their knowledge.

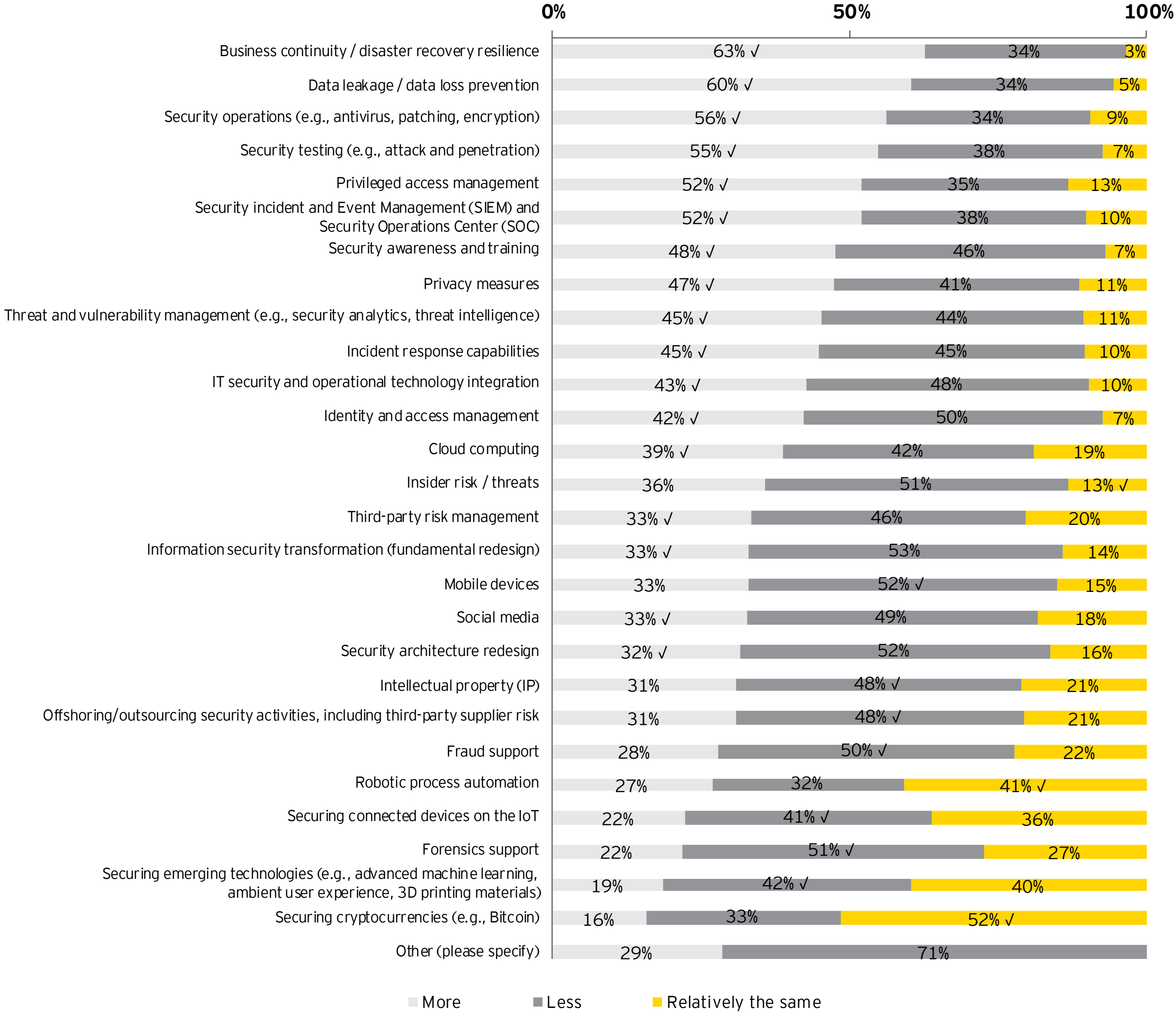
What are the React priorities?

Business Continuity Management (BCM) has been at the heart of an organization's ability to react to a threat, attack or other disruption for many years. As a key area of cybersecurity, it has been a high priority in our survey since 2013, highlighting the importance of having robust React capabilities. Again, this year, 63% of organizations rated it their joint top priority, alongside data leakage/data loss prevention. Security testing (e.g., attack and penetration) and privileged access management were ranked third and fourth, respectively. Security Information and Event Management (SIEM), together with SOCs, were ranked 5th, with 52% of the responders saying that they will spend more in these two areas over the coming 12 months, followed by security awareness and training.

63%

of organizations rated BCM as their joint top priority, alongside data leakage/data loss prevention

Which of the following information security areas would you define as "high, medium or low priorities" for your organization over the coming 12 months?



Where is the money spent?

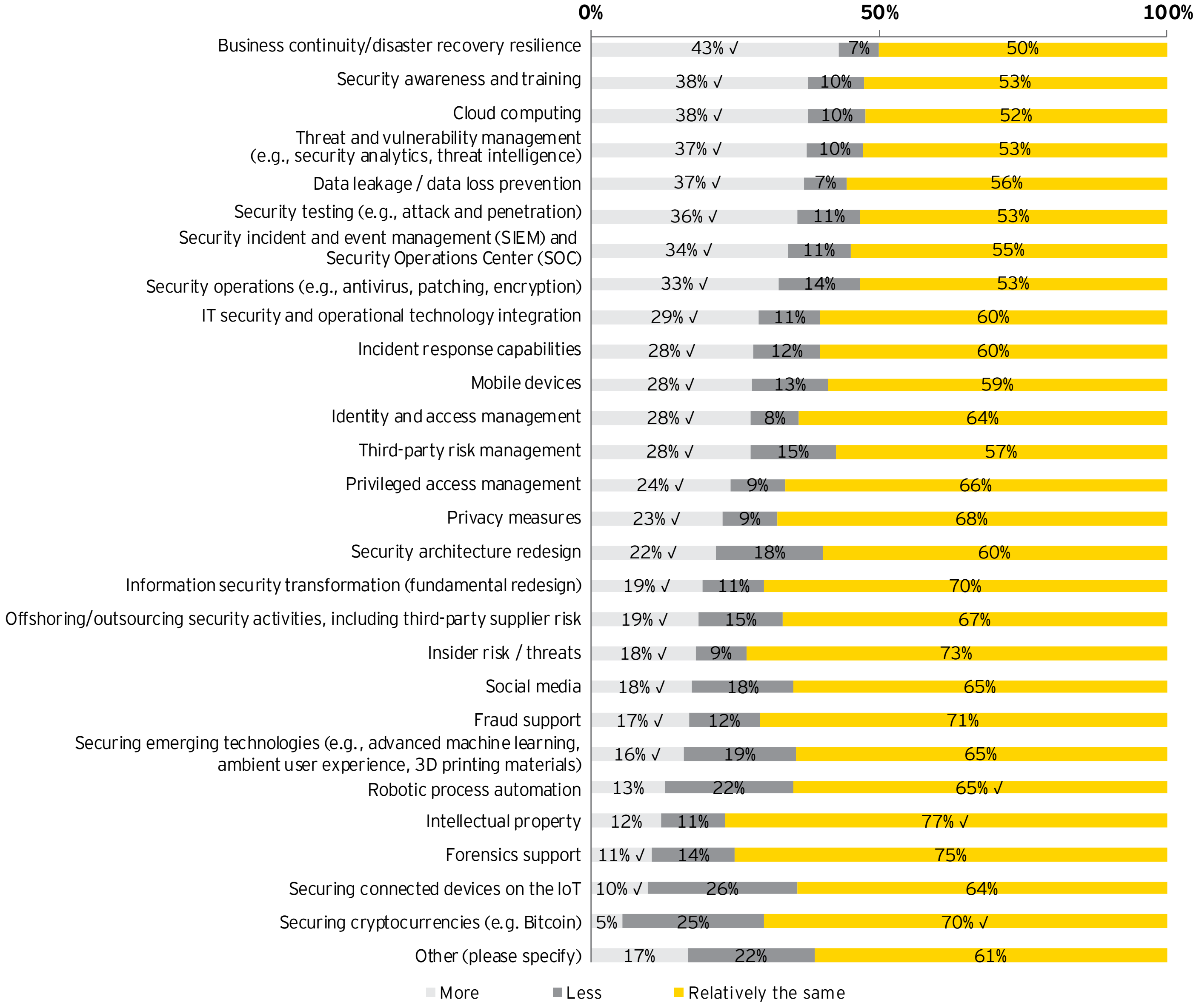
BCM ranks first. However, almost half the organizations feel that it has been well funded in the past and therefore they are now investing in other React capabilities

There is lack of appetite for investing in other adapt and reshape capabilities:

- Adapt: By looking at the threat horizon and threat actors, the resilient organization needs to be flexible and agile to adapt its business processes and protection mechanisms
- Reshape: This is the re-engineering required to improve both the resilient and operational mechanisms for an increasingly secure and sustainable organization

Despite outdated information security controls or architecture being the second biggest vulnerability, 81% of the respondents say that an information security transformation (fundamental redesign) is a medium or low priority, and 78% say a security architecture redesign is a medium or low priority.

Compared to the previous year, does your organization plan to spend more, less or relatively the same amount over the coming year for the following activities?



When reacting to an attack, the board must show leadership

When it comes to immediately dealing with a cyberattack that has damaged the organization or if any weaknesses or failures in the recovery plans become known - the longer these problems continue, the worse the situation will get. Some organizations may physically recover from an attack, but their reputation and trust can be destroyed.

The key is to communicate and lead the communications before traditional news media and social media take over. Too many organizations are still unprepared in this respect.

- 32% do not have an agreed upon communications strategy or plan in place in the event of a significant attack
- In the first seven days after an attack:
  - 32% say they would make a statement to the media
  - 39% would notify regulators and compliance organizations
  - 46% would not notify customers, even when it is customer data that has been compromised
  - 56% would not notify suppliers, even when it is supplier data that has been compromised

32%

of responders do not have an agreed upon communications strategy or plan in place in the event of a significant attack

32%

say they would make a statement to the media

What, how and when to communicate: perspectives from India

- Section 43A of the IT Act has requirements to implement "Reasonable Security Practices and Procedures" (RSPP); however, in the absence of rules or codes framed by the government, parties are free to agree on their own rules relating to RSPPs, including any security standards or privacy policies.
- Under the IT Act and the rules thereunder, there is no obligation to notify the regulator of a breach. However, under the relevant banking regulations, India's central bank, the Reserve Bank of India, has prescribed that banks must notify it, the Computer Emergency Response Team or the Institute for Development and Research in Banking Technology of all security breaches.

3%

of responders have made a significant change to their organization's strategy and plans after a cyber risk assessment

Leading the recovery of the organization

For the CIO or CISO to be able to support the business during the adapting and reshaping phase, they need to fully understand the organization's strategic direction, risk appetite and operations. A robust cybersecurity solution and the organization's overall strategy can be aligned by bringing together the corporate strategy and security teams. However, our survey shows that currently there isn't interaction and coordination between an organization's cybersecurity function and its strategy and planning function.

- Only 3% of responders have made a significant change to their organization's strategy and plans after a cyber risk assessment
- Only 22% say that they have fully considered the information security implications of their organization's current strategy and plans

82%

Conduct self-phishing assessments

Asking tougher questions and closing the gaps

Our survey revealed how much organizations like to rely upon themselves to test or manage their own cybersecurity. In the recovery phase, it may be worthwhile to consider whether this should continue. Currently, the following is true:

- 82% conduct self-phishing assessments
- 42% do their own vulnerability assessment
- 71% conduct their own incident investigation
- 72% do their own threat intelligence analysis

Our survey also found gaps that need to be addressed. Despite careless employees, phishing and malware being such major and known threats, only 26% have an incident response plan that would help them recover from malware and employee misbehavior.

81%

Conduct their own incident investigation

Overall, considerable improvement is still needed from a React perspective

Our survey also found gaps that need to be addressed. Despite careless employees, phishing and malware being such major and known threats, only 26% have an incident response plan that would help them recover from malware and employee misbehavior.

Overall, considerable improvement is still needed from a React perspective

Although React capabilities perform well in the priority ratings, the absolute amounts of money spent in this area are still relatively low. It became clear – from the overall state of cyber resilience (Section 1) – that React is the area where most of the work is still to be done. The more it becomes clear that the corporate shield cannot resist all threats, the more attention the React capabilities will get.

Sense

As the world of consumers and producers becomes ever more connected through digital technologies, it is imperative for companies to protect data and information arising from those processes. Knowledge gleaned from producer-facing and consumer-facing processes increasingly drives competitiveness and is likely to continue to be a game-changer. Given this context, organizations with robust threat intelligence & the ability to detect and respond to early warning signals are more likely to prevent cybercrime, thus safeguarding their ability to compete in future.

Anil Verma,
Executive Director and President,
Godrej & Boyce

Key characteristics of a cyber resilient enterprise

Understands the business

Cyber resilience demands a "whole of organization" response. It begins with an in-depth understanding of the business and operational landscape, to know which business workflows must be preserved so the organization can continue to operate and safeguard people, assets and overall brand equity, despite the cyber-attack.

Understands the cyber ecosystem

Map and assess the relationships the organization has across the cyber ecosystem and identify what risks exist. Perform a risk assessment of the organization's cyber presence in the ecosystem, determining those factors that affect the extent of the organization's control over its ecosystem.

Determines the critical assets — the crown jewels

Most organizations over-protect some assets and under-protect others. In the survey:

- 40% ranked their customers' personally-identifiable information as the number 1 or number 2 information asset most valuable to cybercriminals
- Only 8% rated patented as the IP the number 1 or number 2 most valuable information asset
- Senior executive/board members' personal information was considered valuable after R&D information and corporate and financial information

Determines the risk factors

Cybersecurity functions can only achieve limited success with a limited view of the risk and threat landscape. More important than all of the technologies and tools, that can provide better awareness, intelligence and identification of threats, is the concept of collaboration. Sharing information about the risk and threat landscape of all the business functions allows the organization to understand their broader risk landscape and expose any security gaps. This sharing and collaboration can then extend to other entities (partners, suppliers) within the ecosystem.

Organizations then need to ask the following:

- What more can we do to manage any residual risk?
- Are we prepared to accept a certain level of risk?
- What can we attempt to control and what do we need to accept is out of our control?

Manages the human element with exceptional leadership

After a cyberattack, as in any chaotic situation, individuals need to be prepared and trained on how to respond and behave. With technology supporting the entire organization, every employee will be impacted. Clear communication, direction and example-setting from leadership will be essential, as well as clearly defined roles or tasks that they are able to perform to help the organization become operational again.

Creates a culture of change readiness

The capability to react rapidly to a cyberattack will minimize the possibility of long-term material impact. Organizations that develop superior, integrated and automated response capabilities can activate non-routine leadership, crisis management and coordination of enterprise-wide resources. As a simulation exercise, organizations can challenge the existing crisis management, current practices and risk profile to make sure they are fully aligned with the organization's business strategy and risk appetite.

Organizations should also develop and implement tailor-made war games that would include a review of any command and control center, cyber resilience manuals and plans.

Conducts formal investigations and prepares for prosecution

To protect the interests of the organization in the event of a major cyber-breach, the CIO and CISO should be prepared to liaise with the most senior executives from security, general counsel, external counsel, investigations and compliance. Together they will:

- Collect evidence in a forensically sound way, in order to support a wider investigation
- Establish whether the attackers still have footholds in the organization's networks and systems, and whether harmful malware or ransomware could sabotage the organization again in future
- Perform deeper investigations to understand who carried out the attack, how they performed it, for whom and why
- Be able to bring a claim against either the attacker, and/or criminal prosecution, as well as those who aided and abetted the attacker, or otherwise enabled the attack. Claims can also be brought against product and service providers who failed to meet contractual obligations to build, operate, test or maintain cybersecurity

Resist

As Enterprises and Governments in India, accelerate their Digital Transformation Journeys, Cyber Security will pose the biggest risk to achieve the full potential of Digitisation. As we interact with CxOs of enterprises across verticals, we realize Cyber Security is beginning to be recognized as one of the biggest Business and Reputation Risk they face. A robust Cyber Security Strategy and implementation roadmap for the short and long term, coupled with Board level attention and ownership is a key imperative to mitigate risk. Stakeholder Collaboration, Technology Innovation, Skills development and awareness building are key priorities for India, to address Cyber Security Challenges

Rama Vedashree,
CEO,
Data Security Council of India (DSCI)

Survey methodology

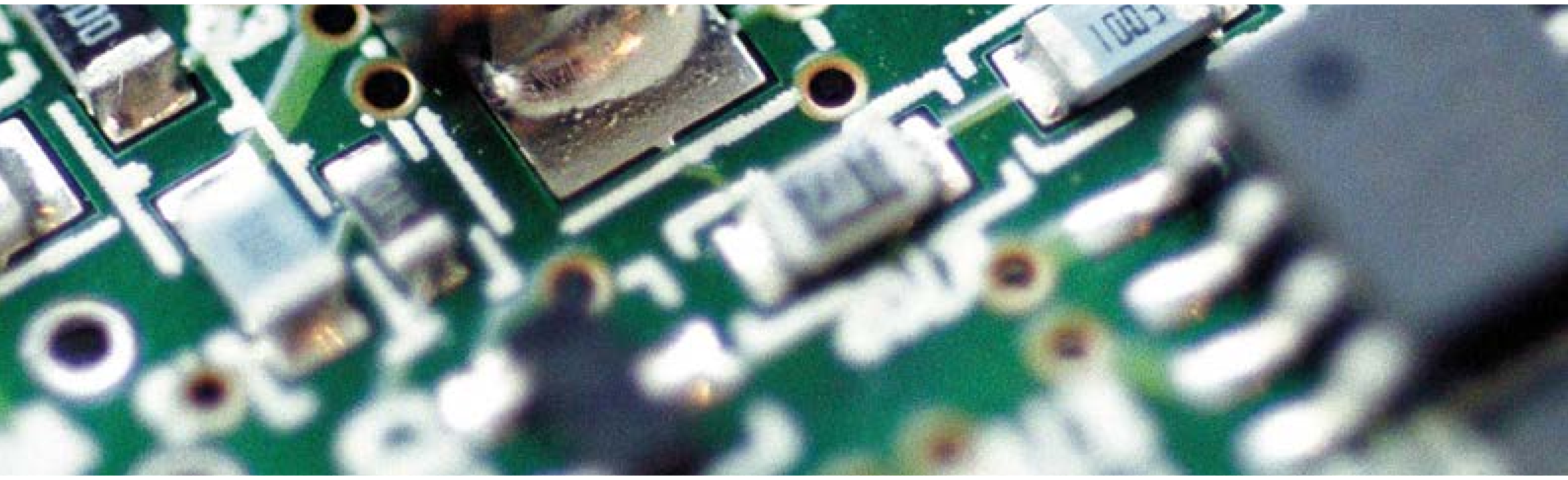
EY's Global Information Security Survey 2016-17 - India Report, captures the responses of 124 C-Suite leaders and Information Security and IT executives/managers, representing diverse industrial segments. These include many of the large globally recognized organizations as well as key government entities. The research was conducted between June-August 2016.

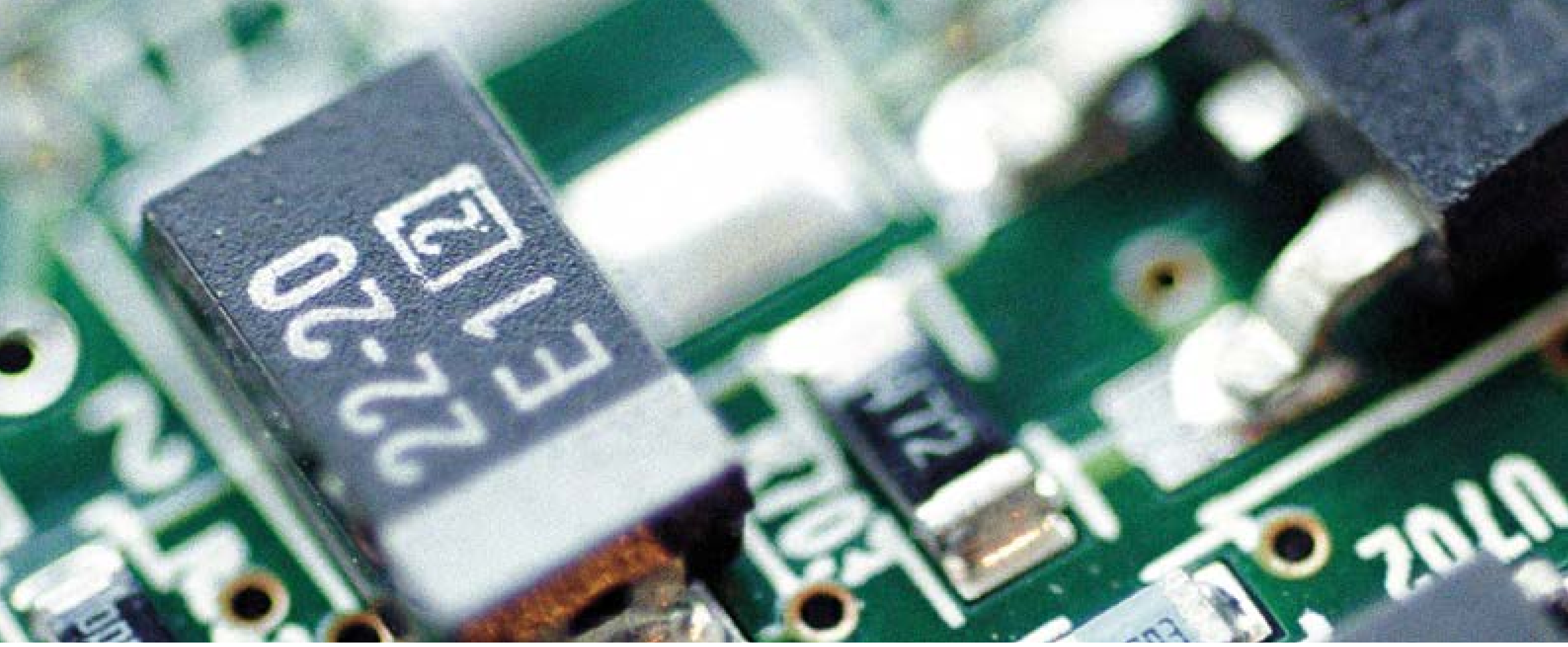
Respondents by position

Chief Information Security Officer	33	26.61%
Information Security Executive	7	5.65%
Chief Information Officer	17	13.71%
Information Technology Executive	5	4.03%
Internal Audit Director/manager	1	0.81%
Chief Technology Officer	7	5.65%
Network/System Administrator	1	0.81%
Business Unit Executive/ Vice President	4	3.23%
Chief Compliance Officer	1	0.81%
Chief Risk Officer	3	2.42%
Others	33	26.61%
Blanks	12	9.68%

Respondents by number of employees

Less than 1,000	22	17.74%
1,000 to 1,999	12	9.68%
2,000 to 2,999	7	5.65%
3,000 to 3,999	1	.81%
4,000 to 4,999	2	1.61%
5,000 to 7,499	3	2.42%
7,500 to 9,999	4	3.23%
10,000 to 14,999	5	4.03%
15,000 to 19,999	1	.81%
20,000 to 29,999	1	.81%
100,000 and above	2	1.61%
Blanks	64	51.61%





Respondents by total annual company revenue

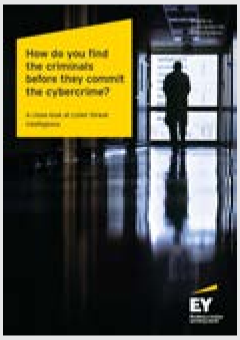
Less than US$10m	2	1.68%
US$10m to less than US$25m	6	5.04%
US$25m to less than US$50m	1	0.84%
US$50m to less than US$100m	2	1.68%
US$100m to less than US$250m	4	3.36%
US$250m to less than US$500m	3	2.52%
US$500m to less than US$1b	4	3.36%
US$1b to less than US$2b	5	4.20%
US$2b to less than US$3b	1	0.84%
US$5b to less than US$7.5b	1	0.84%
US$10b to less than US$15b	1	0.84%
US$15b to less than US$20b	1	0.84%
US$50b or more	2	1.68%
Government, non-profit	7	5.88%
Not applicable	7	5.88%
Blanks	72	60.50%

Respondents by industry sector

Banking & Capital Markets	42	33.87%
Insurance	3	2.42%
Technology	13	10.48%
Consumer Products	4	3.23%
Government & Public Sector	9	7.26%
Diversified Industrial Products	1	0.81%
Power & Utilities	1	0.81%
Retail & Wholesale	4	3.23%
Telecommunications	10	8.06%
Health care	3	2.42%
Media & Entertainment	11	8.87%
Professional Firms & Services	6	4.84%
Real Estate (including Construction, Hospitality & Leisure)	1	0.81%
Oil & Gas	2	1.61%
Automotive	6	4.84%
Mining & Metals	1	0.81%
Life Sciences	2	1.61%
Aerospace & Defense	1	0.81%
Other	4	3.23%

Want to learn more?

Our cybersecurity publications and thought leadership reports are designed to help you understand the issues and provide you with valuable insights about our perspectives. Please visit our Insights on governance, risk and compliance series at ey.com/GRC insights and our website ey.com/cybersecurity.

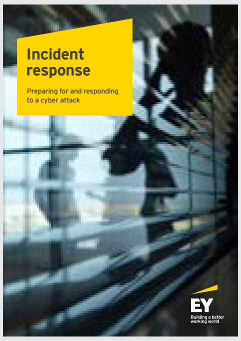

How do you find the criminals before they commit the cybercrime?
EY

How do you find the criminals before they commit the cybercrime?: a closer look at cyber threat intelligence

ey.com/cti

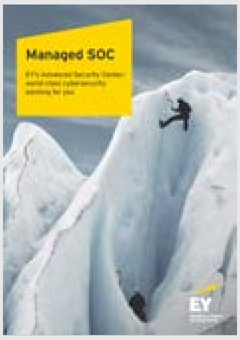
Managed software security services: building a software security center of excellence

ey.com/GRCinsights



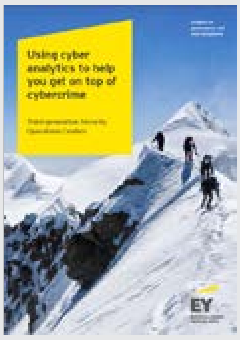
Incident response

ey.com/GRCinsights



Managed SOC: EY's Advanced Security Center

ey.com/soc

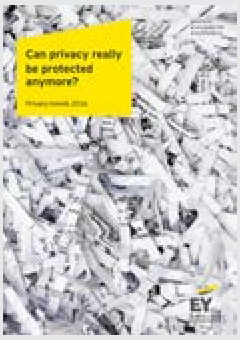


Using cyber analytics to help you get on top of cybercrime: third-generation Security Operations Centers

ey.com/soc

When is privacy not something to keep quiet about?: the EU General Data Protection Regulation

ey.com/GRCinsights



Privacy trends 2016: can privacy really be protected anymore?

ey.com/privacytrends

Active Defense

ey.com/activedefense

Creating trust in the digital world: EY's Global Information Security Survey 2015

ey.com/giss2015

If you were under cyber attack, would you ever know?

For EY Advisory, a better working world means solving big, complex industry issues and capitalizing on opportunities to help provide outcomes that grow, optimize and protect our clients' businesses. We've shaped a global ecosystem of consultants, industry professionals and business alliances with one focus in mind – you.

We believe anticipating, and now actively defending against, cyber-attacks is the only way to be ahead of cyber criminals. With our focus on you, we ask better questions about your operations, priorities and vulnerabilities. We then work with you to create more innovative answers that help provide the approaches you need. Together, we help you achieve better outcomes and long-lasting results, from strategy to execution.

We believe that when organizations manage cybersecurity better, the world works better.

So, if you were under cyber-attack, would you ever know? Ask EY.

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

Notes

Notes

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.

EYG no. 04260-163GBL

BMC Agency

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com/giss

About EY's Advisory Services

In a world of unprecedented change, EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

From C-suite and functional leaders of Fortune 100 multinationals to disruptive innovators and emerging market small- and medium-sized enterprises, EY Advisory works with clients – from strategy through execution – to help them design better outcomes and realize long-lasting results.

A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions. They work with their clients, as well as an ecosystem of internal and external experts, to create innovative answers. Together, EY helps clients' businesses work better.

For questions about cybersecurity, please contact our India Cybersecurity leaders:

Nitin Bhatt	+91 806 727 5127	nitin.bhatt@in.ey.com
Burgess Cooper	+91 22 61921030	burgess.cooper@in.ey.com
Rahul Rishi	+91 116 623 3183	rahul.rishi@in.ey.com
Jaspreet Singh	+91 124 6714310	jaspreet.singh@in.ey.com
Kartik Shinde	+91 22 61920958	kartik.shinde@in.ey.com
Damanjit Uberoi	+91 124 671 4480	Damanjit.Uberoi@in.ey.com
Venkatesh Kulkarni	+911246714808	Venkatesh.Kulkarni@in.ey.com