KPMG

Cybercrime survey report 2015

November 2015

KPMG.com/in

Table of contents

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Foreword

The last few years have seen an increase in cybercrime across regions and sectors. Given the proliferation of connected technologies, organisations face a significant challenge to be resilient against cyberattacks and incidents. Today, C-level executives and board members are concerned about increasing cyberattacks and newer incidents are being reported.

KPMG in India has been at the forefront in helping clients understand cyberthreats and has been conducting cybercrime surveys, annually.

This year, we are publishing a cybercrime study which puts a finger on the pulse of various business sectors in relation to their concerns on cyberthreat and the mitigation measures that can be implemented.

This survey attempts to analyse the preparedness of organisations to deal with cybercrime and related incidents by unearthing its modus operandi and its extent, besides highlighting preventive measures to deal with this rapidly growing issue.

We hope the survey report provides you with insights that can be leveraged in shaping the cyber risk management posture in your organisation.

Regards,
KPMG in India

Mritunjay Kapur
Partner and Head
Risk Consulting

Mohit Bahl
Partner and Head
Forensic

Akhilesh Tuteja
Partner and Head
EMA IT Advisory - RC

Sandeep Gupta
Partner
Forensic - Cybersecurity

Atul Gupta
Partner
IT Advisory - Cybersecurity

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

An overview of the survey

Current cybercrime scenario in India

Given the growth of cybercrime incidents in India, boards and CXOs are forced to take cognisance of this menace. With confidential strategic data, operational information at stake and reputation on the line, organisations are now beginning to realise the need for building their cyber defences to limit the damage from cyberattacks. As managements work on building a cyber defence strategy, it is vital for organisations to have an understanding of the looming cyberthreat and knowledge of how the business community as a whole is responding. Our survey report provides corporate India's persepctive on cybercrime which is summarised as under:

A snapshot of cybercrime

Perception of cybercrime

94% One of the major threats to businesses

41% Part of the boardroom agenda

Targets of cybercrime

74% BFSI sector is a top target for cybercrime

64% Directors/ management are most vulnerable to cybercrime

Cyber risk management

74% No detailed cyber risk assessment

78% Have no cyber incident response plan

61% Lack data leakage prevention tools

62% No logging and monitoring of critical systems

Frequency of cyberattacks

72% Companies have faced some sort of a cyberattack over the past year

Profile of a cybercriminal

83% Respondents stated that there is external involvement in cyberattacks

Impact of cybercrimes

63% Amounted to financial loss

Cyber governance

58% State that cyber defence expenditure forms less than 5 per cent of total IT spend

Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

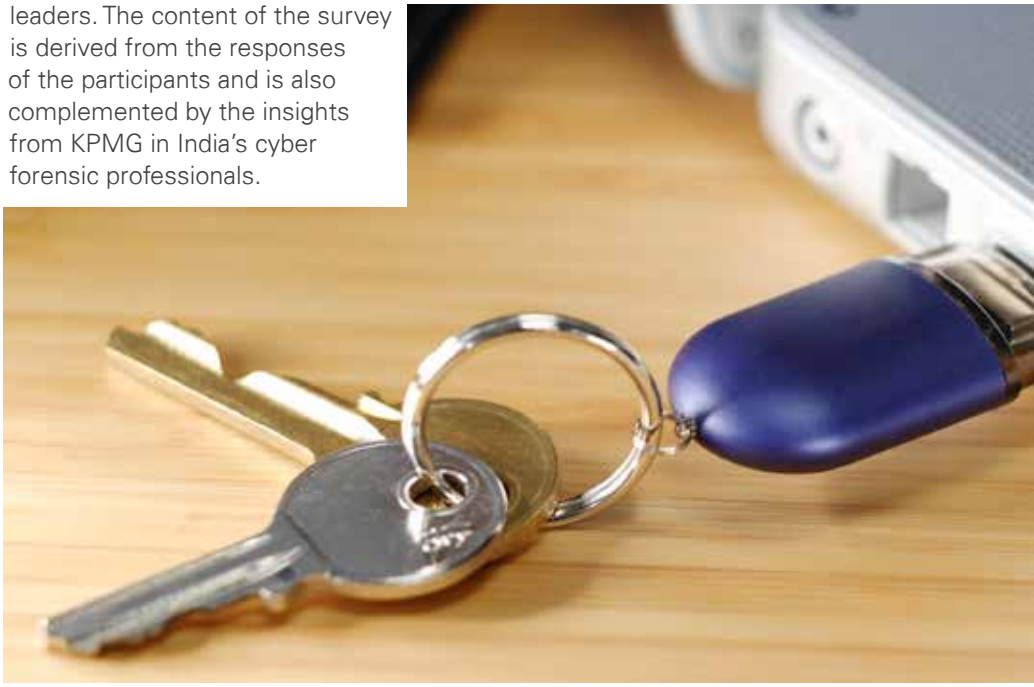
© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

About the survey

The survey aims to provide the industry with a reference point that sheds light on key aspects of cybercrime in terms of industry perception, affected areas of the organisation, and impact and responsive measures that companies have taken. We have also tried to capture the pulse of the industry by publishing cybercrime insights from industry leaders.

KPMG in India has carried out this cybercrime survey across a wide range of Indian companies. An overview of the level of participation is as given below.

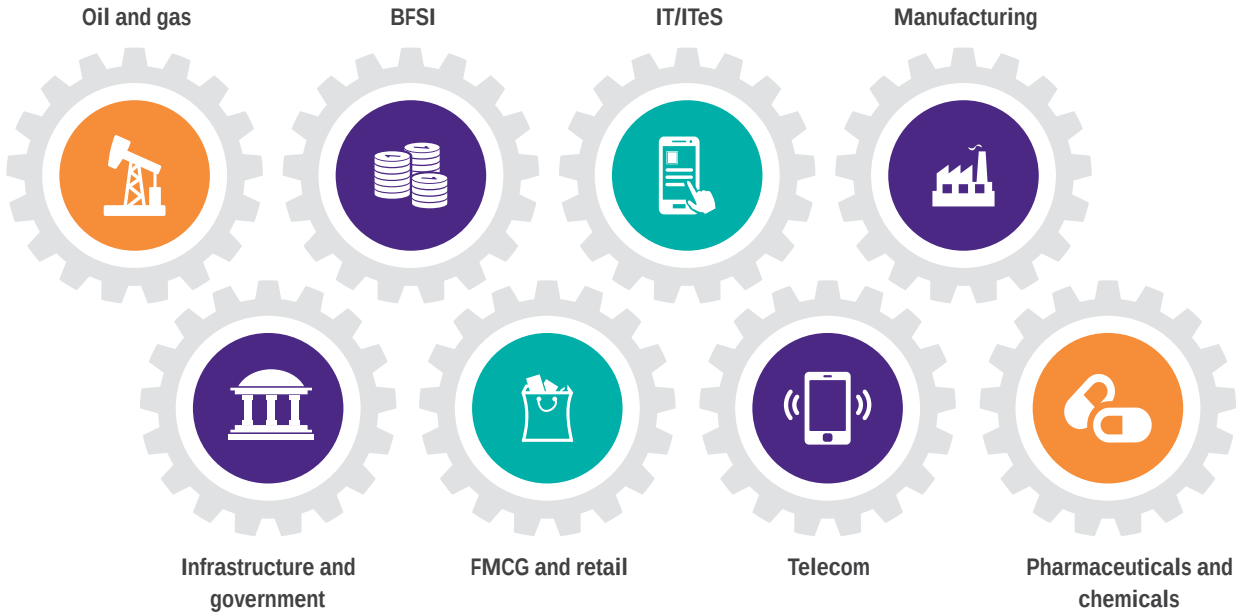
The survey was conducted by using web-based forms and personal interviews with industry leaders. The content of the survey is derived from the responses of the participants and is also complemented by the insights from KPMG in India's cyber forensic professionals.



Profile of the participants

The survey saw over 250 participants from the likes of CIOs, CISOs, CAEs, CROs, COOs* and related professionals from across India.

Mix of participants



* CIO – Chief Information Officer, CISO – Chief Information Security Officer, CAE – Chief Audit Executive , CRO – Chief Risk Officer, COO – Chief Operating Officer.

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Perception of cybercrime in India

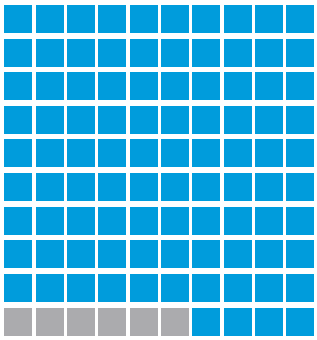
Cybercrime was only perceived as a malaise, impacting large companies and multinational corporates who have their presence in the western hemisphere. However, Indian companies are increasingly being targeted. This spurt has been on account of the following factors:

- Increase in the number of people accessing the internet
- Increase in number of smartphone users
- Dawn of path-breaking transacting platforms such as m-commerce, mobile banking and mobile wallets.

> There is a significant spurt in cybercrimes across enterprises and it is of paramount importance for management to realise that these are no longer a one-time phenomenon. The nature of cybercrime is constantly evolving, specifically with attackers having a solid arsenal of the ever evolving stealth attack.
>
> **Mritunjay Kapur**
> Partner and Head,
> Risk Consulting,
> KPMG in India

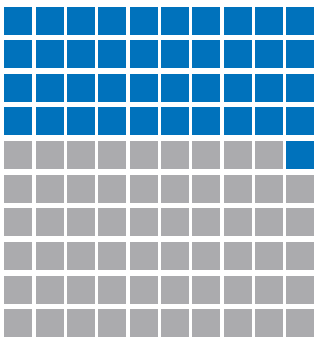
While **94 per cent** indicated that cybercrime is a major threat faced by organisations, only **41 per cent** indicated that it forms part of the board agenda.

Increased awareness at the C-level and board of directors has resulted in cyber risk being recognised as one of the top five risks.



94%

Believe cybercrime is one of the major threats being faced by organisations



41%

State cybercrime is part of the board agenda

Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

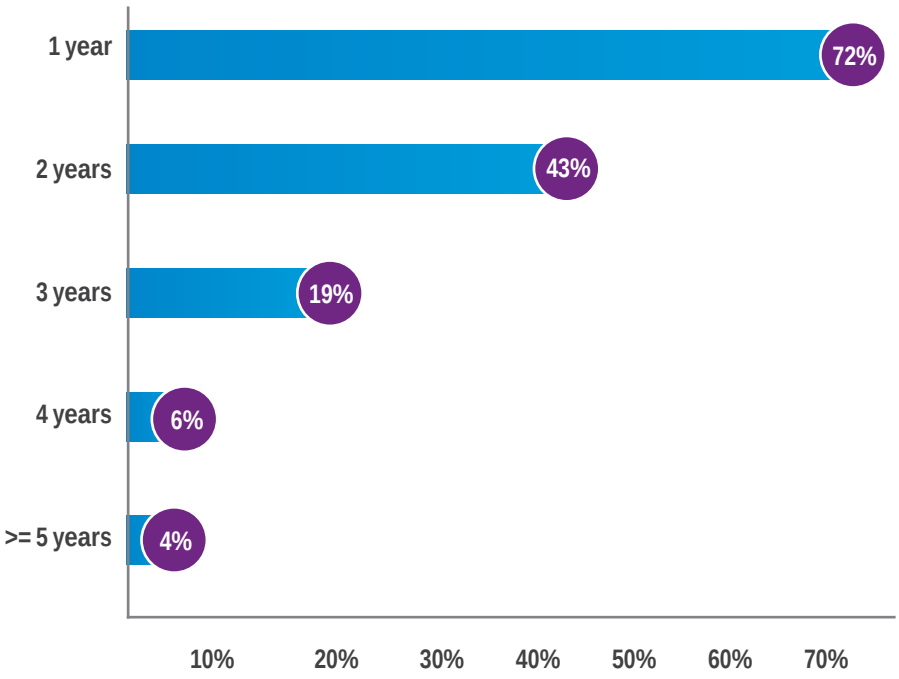
Cybercrime trends in India

The early days of cybercrime attacks saw several of them being carried out for fun, to demonstrate skills, or to achieve one-off financial gains. These days they are motivated by activism and digital espionage. Anyone with access to a computer, an internet connection, a motive, and sufficient knowledge can become a cybercriminal.

Cybercrime in India has dramatically evolved in its nature and scope in the last few years. Cybercrime syndicates are using tools of online deception such as spoofed emails for spear phishing attacks, and spam emails with malware to attack enterprises.

> As organisations march ahead on the digital bandwagon, leverage social media and innovative payment channels, cybercrime is becoming more sophisticated, innovative and is being carried out by organised syndicates. Social engineering, advanced malware, such as ransomware, application layer attacks and cyber extortion, are some of the varied vectors used by cybercriminals. Organisations need to have a comprehensive prevention, detection and cyber resilience framework (PDC model) in place, apart from conducting continuous customer awareness campaigns to manage these threats effectively.
>
> **Sameer Ratolikar**
> CISO, HDFC Bank

Frequency of cyberattacks faced by companies



An alarming
72 per cent
indicated that they have faced some sort of a cyberattack over the past year, indicating an increase in the volume of attacks.

Cyber incidents have not only risen sharply in 2015, the trend is more towards cybercrime with financial motives.

Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Impact of cybercrime in India

Given the growth witnessed by Indian companies and internet penetration, India is now becoming a more integrated part of the global cyber village. Due to this, the number of companies and individuals having online presence has grown phenomenally as technology platforms provide the ease of leveraging the internet for conducting business and financial transactions.

As businesses open themselves up to technology, they are exposed to the risk of cybercrime, which can have far-reaching damages including:

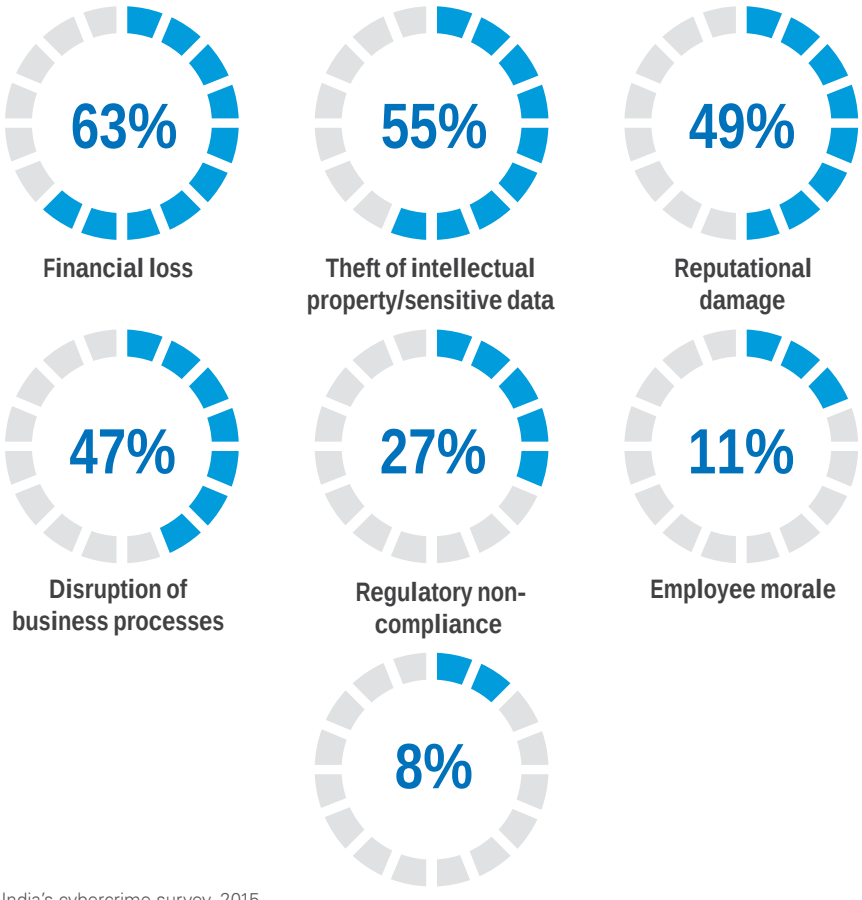
- financial loss,
- loss of reputation,
- operational loss, i.e. impact on physical safety of employees and assets, closure of factory/plant operations.

While cybercrime may have the aforementioned direct impacts, it can also have an indirect impact such as large regulatory fines, contractual penalties and litigation.

> An organisation's preparedness against cybercrime is reflected by its ability to detect an anomaly by leveraging on its repository of cybercrime intelligence and its ability to rapidly respond to cyber incidents. Collaborative intelligence from various sources enhances the organisation's readiness to respond to various types of cybercrimes. However, organisations are unable to limit the impact of cybercrime as they are still faced with challenges of increasing reaction agility, reducing incident response time and absence of a strong legislation to help in effective legal recourse.
>
> **Amit Pradhan**
> CISO, Vodafone India

63 per cent
respondents indicated that cybercrime amounted to financial loss, while 55 per cent also mentioned theft of sensitive information.

Impact of cybercrime on companies



Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

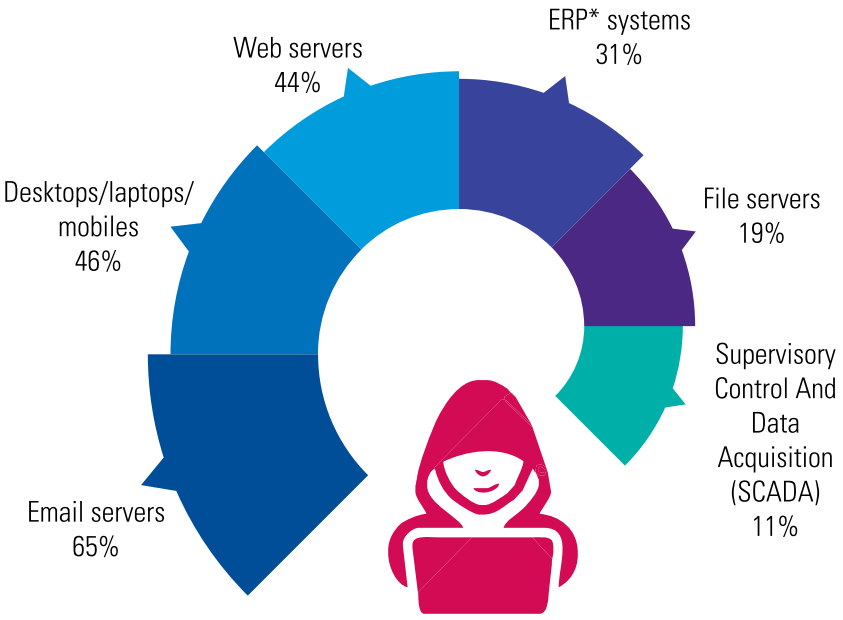
Target and complexity of cybercrime

Cyberattacks by nature are multi-dimensional and complex. As cybercrime progressively evolves into an organised activity, the motives of intruders are no longer limited to only stealing information, but potentially to disrupt business or conduct espionage on behalf of competing organisations. Although organisations understand the need to safeguard their IT infrastructure, intruders have often been a step ahead at exploiting new vulnerabilities in the IT systems and processes of their targets. Needless to say, target organisations have been found inadequately equipped when it comes to countering these cyberattacks. Cybercriminals are now targeting diverse systems to achieve their objective and are scouting for organisations whose systems are most vulnerable. Attacks are increasingly being targeted at a diverse range of systems such as:

- Email and communication systems
- Social media
- Mobile phones
- Programmable logic controllers on factory production/assembly lines
- Automatic teller machines in banks
- Point of sale systems at shops.

> The rising wave of digitisation with diverse applications and services available through multiple channels has compounded the all-pervading cyberthreat. While providing a wider vulnerability base to exploit, it also offers a greater potential return for cybercriminals as they 'follow the money'.
>
> **Venkatesh Subramaniam**
> CISO,
> Idea Cellular Limited

Systems that are targets for cybercrime



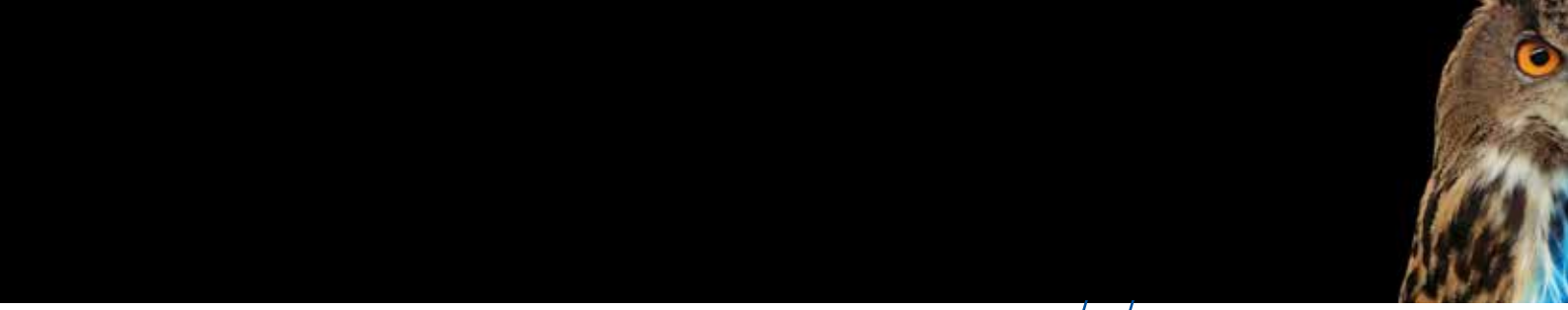
* ERP - Enterprise Resource Planning

Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

65 per cent
respondents indicated that email servers are likely targets for cybercrime, while 46 per cent identified end user systems as targets.

The year 2015 has witnessed an increase in spear phishing attacks targeted at email systems to defraud companies by redirecting foreign remittances/ payments to money mule accounts of hackers.

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



Type of personnel prone to cyberattacks

With the growing ease of transacting technology, people extensively use their computers and mobile phones to carry out banking transactions, to avoid the hassle of long queues and travel. While people leverage on technology to a large extent, the same cannot be said about them using technology in a secure manner. From sharing passwords, to working on malware infected devices, to banking transactions; people make silly yet serious follies that make them vulnerable to cybercriminals.

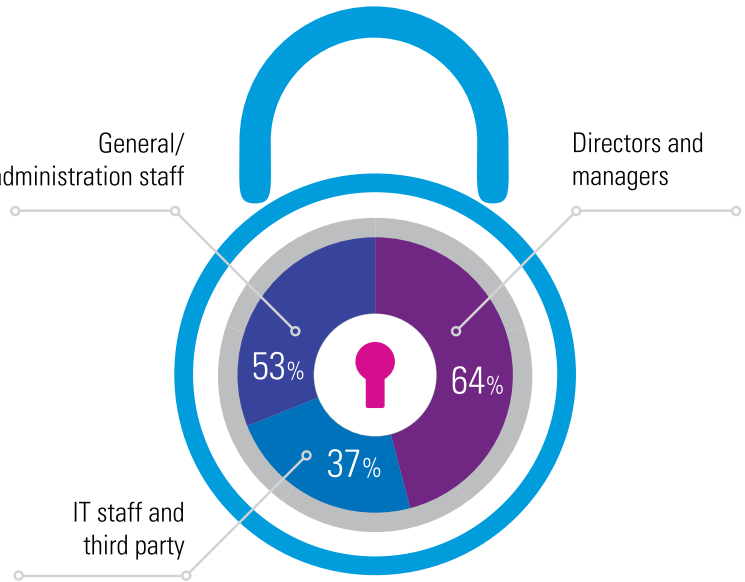
Cybercriminals thrive on three key elements people in general ignore. Firstly, not securing their digital devices; secondly, sharing/insecurely storing access credentials; and lastly, willingness to share personal data with unknown people. Due to these aspects, cybercriminals are able to successfully pull off socially engineered attacks, website spoofing and phishing attacks.

People and vendors are one of the most critical yet one of the weakest links in the cyber defence chain. Cyber investigations of large cybercrimes reveal that social engineering has been the preferred method to extract critical information used for attacks. In this context, it is vital for CXOs to ensure that cyber risk awareness trainings are periodically imparted to employees and vendors.

Akhilesh Tuteja
Partner and Head,
EMA IT Advisory - RC,
KPMG in India

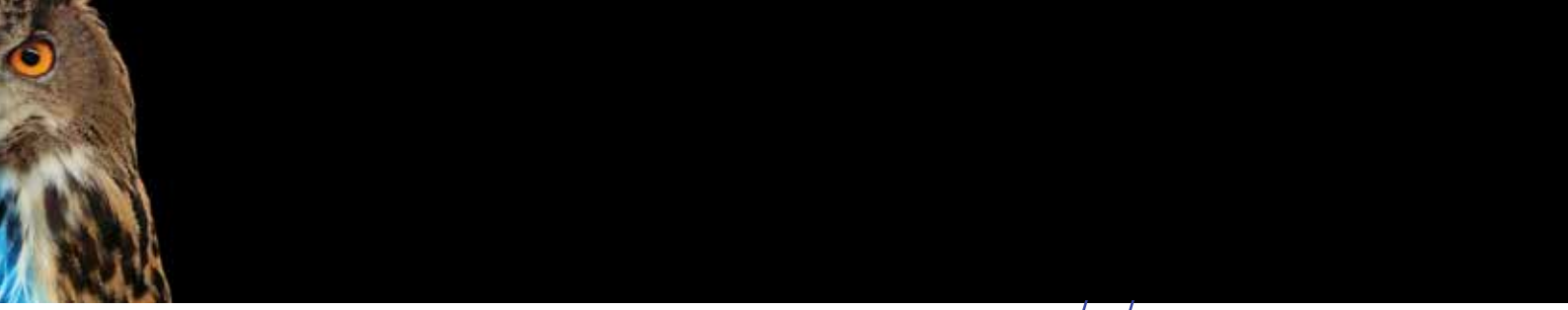
64 per cent
directors/managers, along with general staff, are largely prone to cybercrime.

Personnel that are targeted/most vulnerable to cybercrime



Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



Industries that are targets for cybercrime

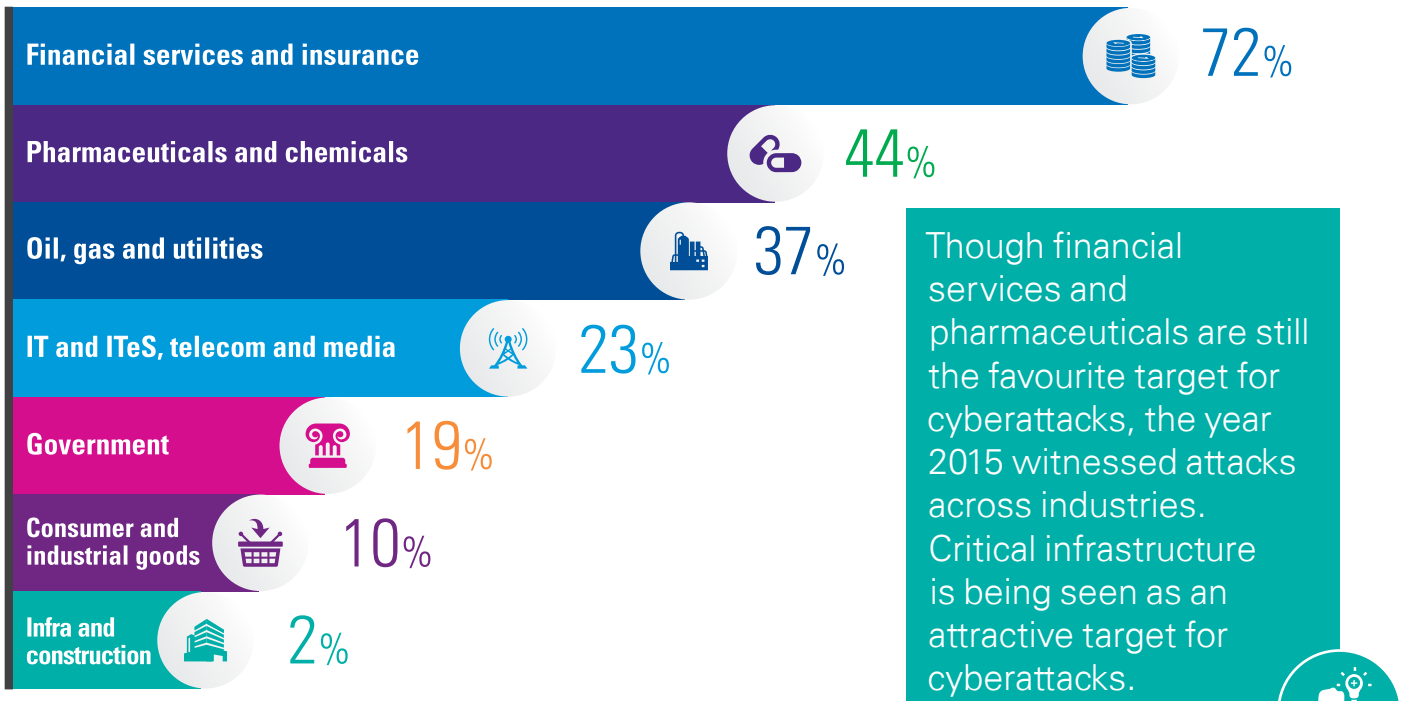
The type of industries that are most prone to cyberattacks depend on multiple factors, such as:

- Profile of the attacker
- Motivation of the attacker
- Cyber security culture at an industry level
- Strength of cyberlaws
- Efficiency of law enforcement agencies to track cybercriminals
- Efficiency of the judiciary to evaluate the nature of the crime and deliver judgements/ conviction.

Apart from the aforesaid external factors, a key aspect that also determines the susceptibility to cybercrime of a particular industry is the nature of data it holds, as well as the value of the data that can be fetched by the cybercriminal, if they were to sell it on the darknet.

> Cybercrime is a threat that pervades across industries. With a wide range of threat sources from political cyber armies and cyber thieves, certain cybercrime syndicates attack in waves where a wide range of businesses are hit with crippling impact. This may range from the largest corporate houses to the smallest family-run businesses.
>
> **Atul Gupta**
> Partner, IT Advisory - Cybersecurity,
> KPMG in India

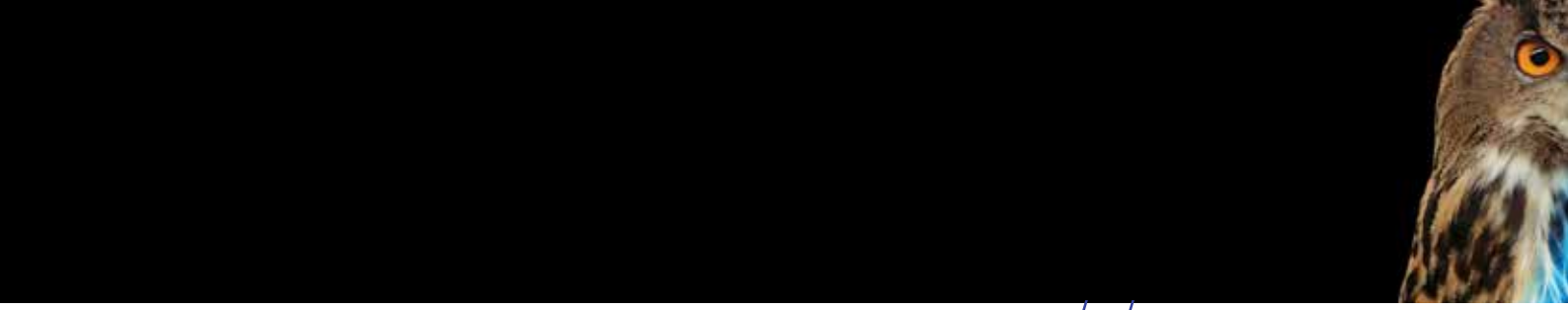
Industries/sectors that are targets for cybercrime



Though financial services and pharmaceuticals are still the favourite target for cyberattacks, the year 2015 witnessed attacks across industries. Critical infrastructure is being seen as an attractive target for cyberattacks.

Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



Nature/method of cyberattacks

Cybercrime attacks can occur in various forms. An illustrative listing of types of the attacks are as under:

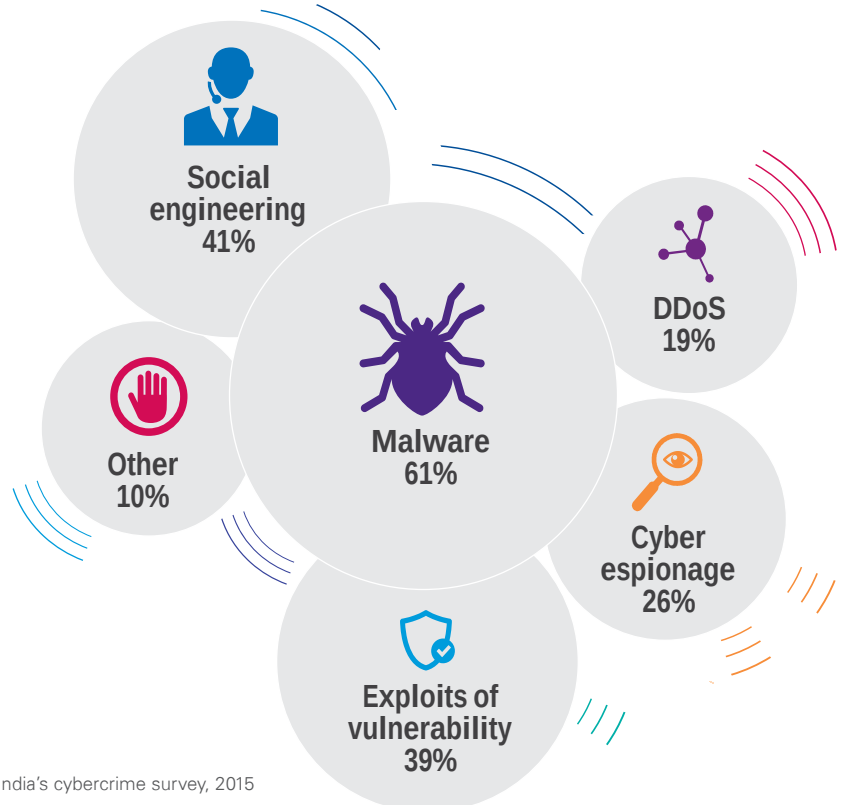
- Email spamming and phishing
- Malware which also includes trojans, virus, spyware, botnets and ransomware infections of target systems/servers
- Social engineering attacks
- Exploitation of technical vulnerability
- Website spoofing and defacement
- Distributed Denial of Service (DDoS) attack, where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack
- Cyber defamation.

Over the years, malware attacks seem to be the most preferred by cybercriminals, since they involve software that gets automatically installed in a user's system or server, without the system owner's knowledge. It takes a different shape based on the nature of attack it is intended to mount and the data it requires. One of the most potent form of malwares used for cybercrime are information stealing malwares and logic bombs. Information stealing malware are designed to steal information such as credit card numbers, banking passwords, email information from computers, mobile phones, etc.

> Boards of large global organisations have started to pay more attention to cyber risk, but there is much more they can do. They need to make sure that they have the right skills and knowledge and treat it as a broader business risk that impacts the organisation beyond IT in areas such as new product and service development, and M&A.
>
> **Malcom Marshal**
> Partner and Global Head, Cybersecurity,
> KPMG LLP (U.K.)

61 per cent respondents indicated that malware, and 41 per cent stated that social engineering, are the nature of cyberattacks faced by companies.

Nature of cyberattacks faced by companies



Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

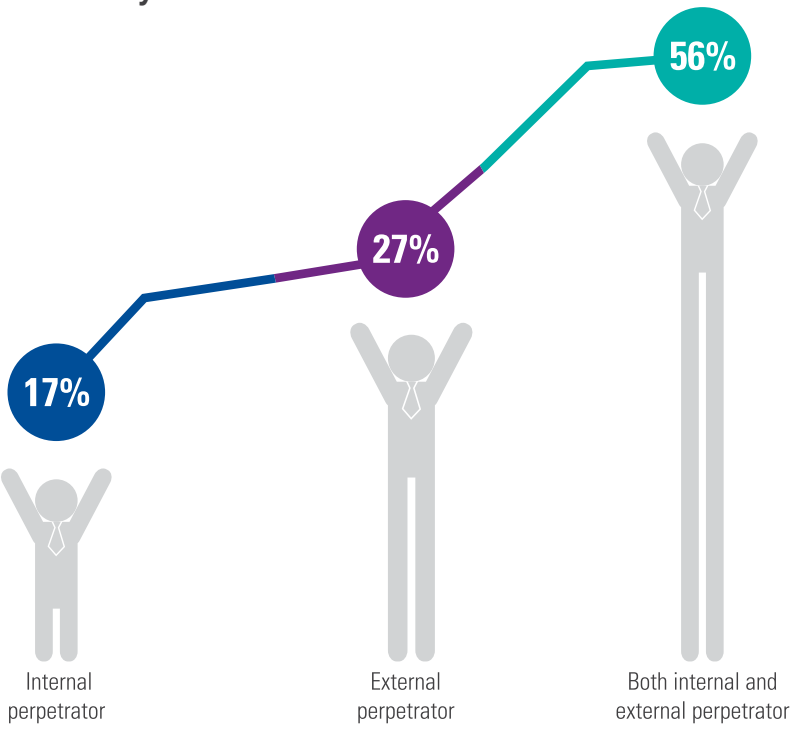
© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Profile of a cybercriminal

Cyberattacks can occur in various forms. The nature of the attacks that an organisation faces depends on the profile of the attacker(s) and the the value that they seek. An analysis of the types of attackers that form part of the threat landscape of an organisation is summarised as under:

- **External perpetrators**
  - **Script kiddies:** These are amateur hackers who have moderate level of technical skills. They typically try to carry out attacks on easy and highly vulnerable networks.
  - **Professional hackers/hackers for hire:** These are professional hackers who carry out attacks on an independent basis on fairly complex systems and/or provide services on hire for remuneration in cash/digital currency.
  - **Hacktivist:** This group of hackers carry out cyberattacks for non-commercial/social purposes (e.g. environmental activists).
  - **Cyber terrorist:** They are criminals who carry out attacks with a political motive to harm the strategic interests/assets of any nation.
  - **Spammers, phishers and online scamsters:** This group of hackers target companies and individuals with a view of obtaining financial information and access credentials for financial fraud. This group heavily leverages social engineering as an attack technique.
  - **Malware engineers:** This group is a highly technically competent bunch of people who develop automated tools and programmes that are used to subvert IT defences of the company and cause damage ranging from information theft, outage and spying. These hackers typically use malware either for their personal purposes or sell them to buyers who are willing to pay their price.
- **Perpetrators internal to the organisation:** Cyberattacks are not always carried out by external parties. Many a times attackers are from within the organisation in the form of disgruntled employees, employees with criminal intent, or even contractor personnel with malafide intent.

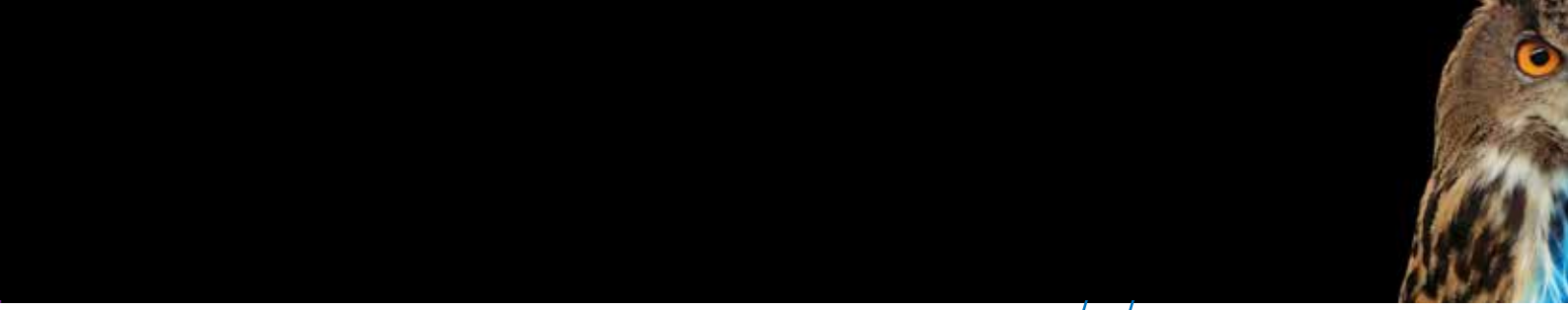
Profile of a cybercriminal



83 per cent
respondents stated that there is external involvement in cyberattacks.

Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



Probable intentions behind cyberattacks

As mentioned earlier, cybercriminals operate with different motives in their mind. In order to effectively manage cyberthreats, it is vital for organisations to understand the motives behind cyberattacks due to the following reasons:

- Motives of the attack have a critical bearing on the technique used in the attack, which can at times give clues on the potential perpetrators.
- Motives of the attack also help affected companies design their cyber defences.

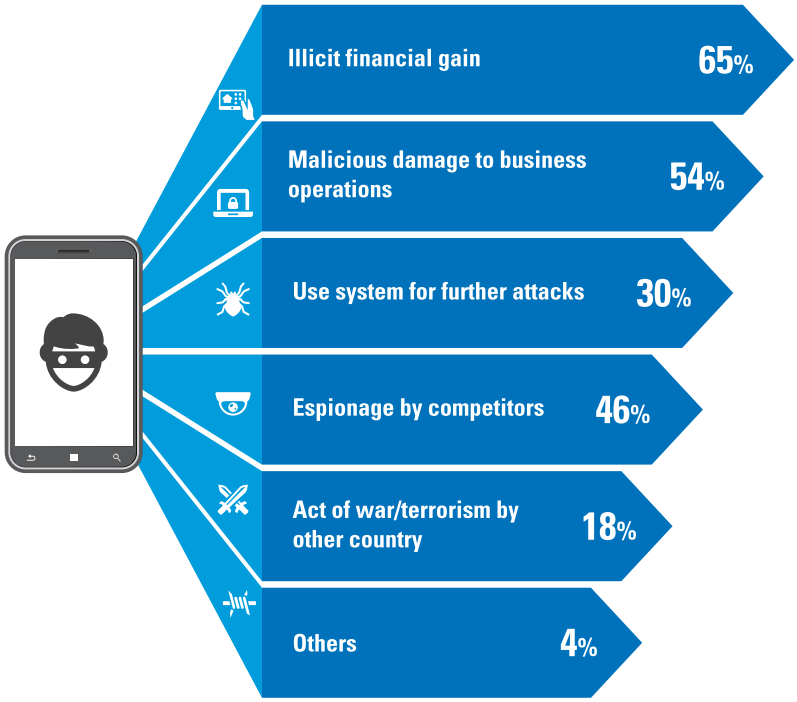
Some of the typical motives cybercriminals have for carrying out the attacks are as under:

- Financial fraud and embezzlement
- Theft of intellectual property/ sensitive information
- Skill testing for new hackers
- Business disruption (outage of production lines, e-commerce sites, trading exchanges, etc.)
- Cyber terrorism to cause grievous damage to a country's strategic assets/general public safety
- Social causes
- Political causes
- Corporate rivalry and espionage.

> Cybercriminals have understood the potential for illicit financial gain and have begun executing highly sophisticated technology driven frauds. These cyber frauds, by nature, are complex and difficult to detect. Cyber forensics, therefore, is becoming a critical component of fraud investigations.
>
> **Mohit Bahl**
> Partner and Head, Forensic, KPMG in India

65 per cent
respondents stated that cybercriminals carry out attacks for financial gains, while another 46 per cent believe corporate espionage to be the motive.

Potential intentions/motives behind cyberattacks



Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Cybercrime risk management

Cyber risk management and governance

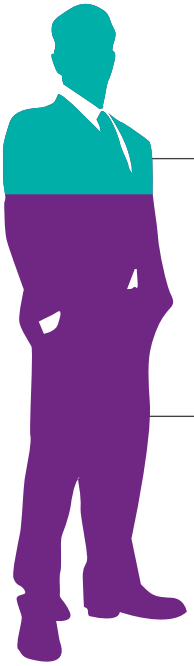
The key to successfully combating cybercrime is to have in place a strong cyber risk management strategy and effective cyber governance. A cyber risk management process can be rated to be reasonably robust if it has the following aspects:

- Resource and time commitment from the board of directors and senior management
- In-depth and detailed enterprise-wide cyber risk assessment that is conducted on a periodic basis
- A cyber defence and resilience strategy that is current and aligned to the results of the periodic cyber risk assessment.

> The key challenge to defend against cybercrime is to determine what is at stake. Organisations are increasingly beginning to change the way risk assessments are conducted by carrying out a deeper level of risk assessment to understand the value of the information they hold and the potential impact it could have if compromised.
>
> **Sunder Krishnan**
> CRO, Reliance Life Insurance

Impact of cybercrime on companies

Is cyber risk management one of the board of directors' top 10 organisational priorities?



23%
Yes

77%
No

What is the spend on information security and cyber defences (infrastructure, tools, personnel and services)?

58%
<5% of IT spend

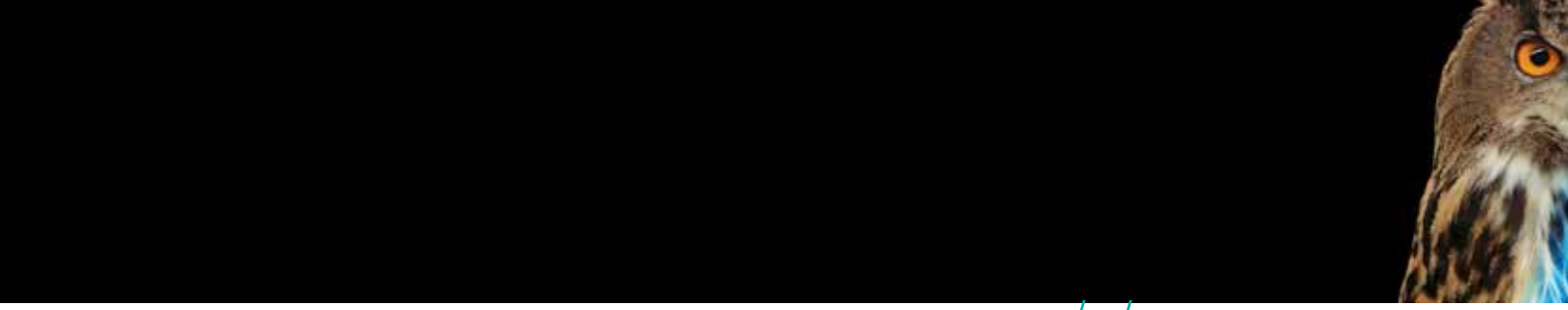
31%
5-10% of IT spend

9%
11-20% of IT spend

2%
> 20% of IT spend

Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



Cyber risk assessment

An in-depth cyber risk assessment can reveal chinks in the armour that can serve as critical inputs for shaping the cyber defence strategy and design of cyber controls within the IT processes. At minimum, the cyber risk assessment should be carried out annually, and additionally, when the following occur:

- Significant change in the IT landscape of the organisation.
- Subsequent to a major cyber incident or knowledge of a cyber threat.
- Frequent news of cyberattacks on industry peers.

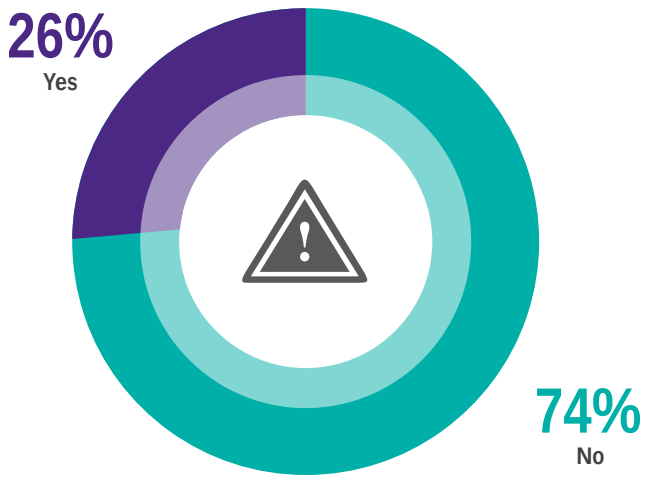
> Today's IT architecture of companies constitutes of a variety of platforms that are distinct from each other while they operate in an integrated manner. Cyberattacks have evolved from being generic to platform specific. As a result, the threat landscape for organisations has increased multifold, thereby putting an organisation's sensitive information at greater risk.
>
> **Sandeep Gupta**
> Partner, Forensic - Cybersecurity, KPMG in India

74 per cent
respondents stated that a detailed annual IT and cyber risk assessment is not carried out.

Cyber risk assessment is not a focussed area for most of the enterpises across functions and people. The focus is only on technology.

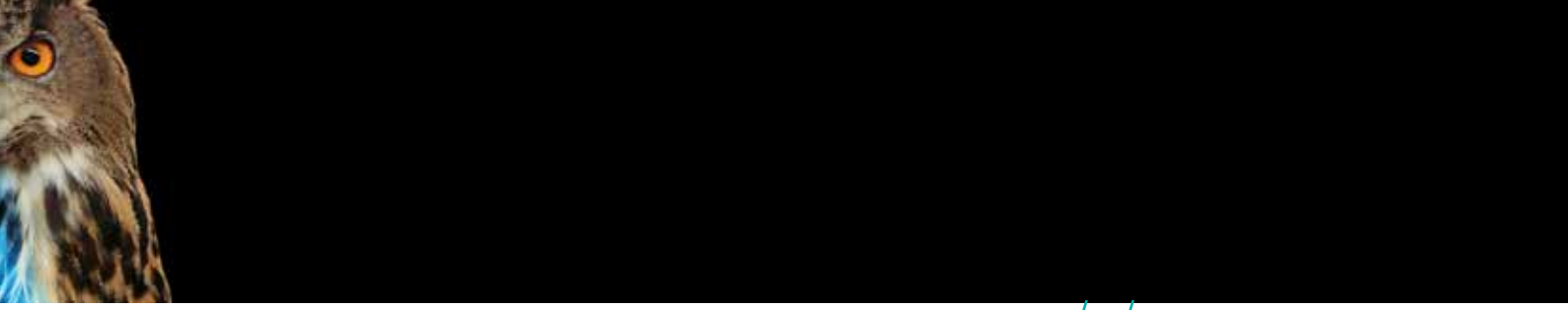
Impact of cybercrime on companies

As part of the annual risk assessment process, do you perform a detailed cybercrime and IT security-centric risk assessment?



Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



Cyber defence strategy: Building cyber resilience

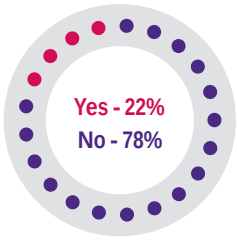
The cyber defence strategy largely depends on the outcome of cyber risk assessments and cybercrime incidents. The focus here is to build cyber resilience using the following measures:

- Building attack detection tools and capabilities
- Designing a cyber intelligence programme
- Bettering the existing IT infrastructure
- Building a continuous training and cyber risk awareness across levels in the organisation.

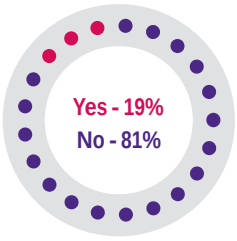
One of the key fallacies about a cyber defence strategy is that it is purely technology-based. A robust strategy is a potent mix of risk inputs, cyber intelligence, people capability, business support and technology. Giving cyber resilience the optimal shape is something that Indian CIOs and CISOs are now beginning to work on.

> Cyber resilience capabilities, generally, remain an enigma for many institutions, for lack of partners and talent to mature the process and intelligence around the products.
>
> **Ashutosh Jain**
> CISO,
> Axis Bank

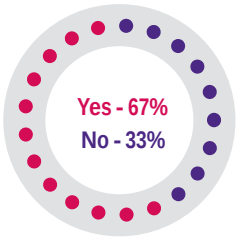
Layers of cyber defence implemented by companies



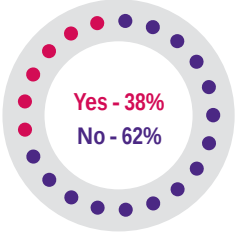
Do you have a cybercrime incident response plan?



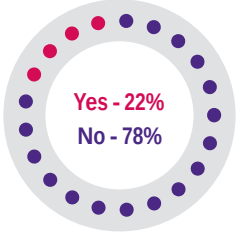
Do you have a cybercrime incident response team?



Do you have technology-based cyber defences?



Do you have the governance process and technology for logging of critical events?

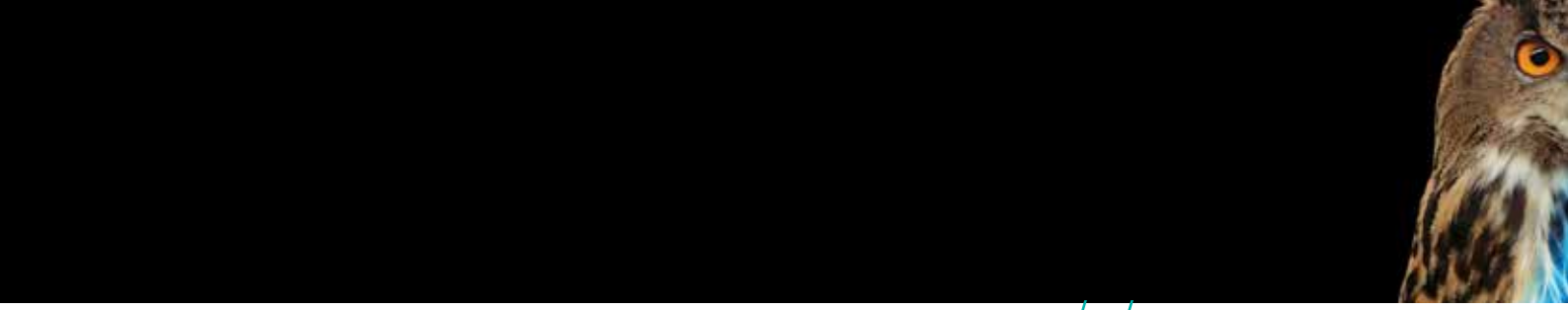


Do you formalise enterprise-wide cyber awareness and education campaign?

78 per cent respondents stated that they do not have a cybercrime incident response plan, while 62 per cent do not have a governance process to log and monitor IT events on their critical systems.

Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



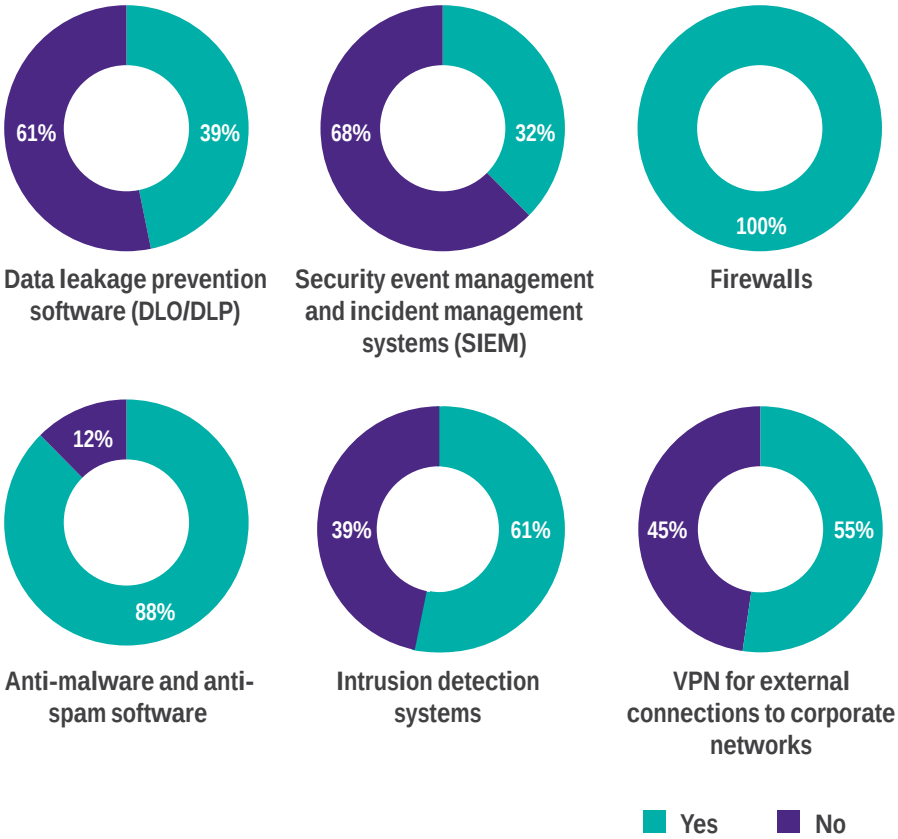
Cyber defence strategy: The technology factor

Technology is one of the crucial factors of an effective cyber defence strategy. Cyber defence technology comes in different ranges; some that protect the perimeter from attacks, some that serve as an intruder alarm, and others that protect end points from being attacked. The mix of tools to be deployed depends on the criticality of the data to be protected, the design of the landscape, the threat perception and the availability of budget. Organisations these days have a choice between open source tools and commercial tools to support cyber defence.

> The mercurial nature of the cyberthreat landscape is the primary reason for keeping CIOs/CTOs on their toes. The key to a successful cyber defence strategy is to put in play pre-emptive actions against cyberthreats in order to strengthen the cybersecurity posture of the enterprise.
>
> **Jayantha Prabhu**
> Chief Technology Officer, Essar Group

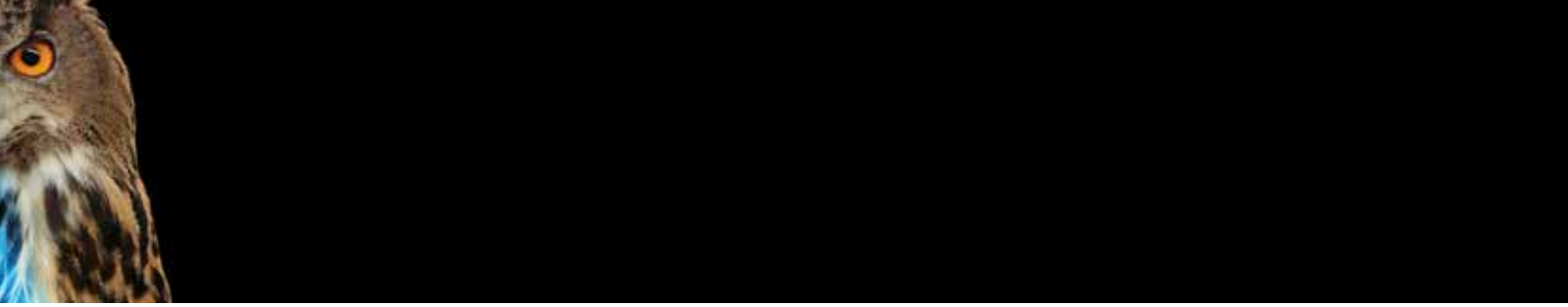
68 per cent respondents stated that they do not have an SIEM to support cybercrime incident detection, analysis, and 61 per cent do not have data leakage with reference to prevention tools installed on servers and end user systems.

Types of cyber defence tools implemented by companies



Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



Cybercrime governance

While organisations play a key role in shoring up their defences, the way law and order is structured also plays a crucial part in tackling cybercrime. An adequate cybercrime enforcement and justice system serves as an effective deterrent to the spread of cybercrime in the following ways:

- Effective response mechanisms by law enforcement authorities enables the facts and digital evidences related to cybercrimes to be captured in a timely manner without being lost.
- Due to the technical and legal skills of the cyber law enforcement agency, a higher rate of prosecutions and convictions are achieved, thereby convicting and keeping habitual offenders behind bars.

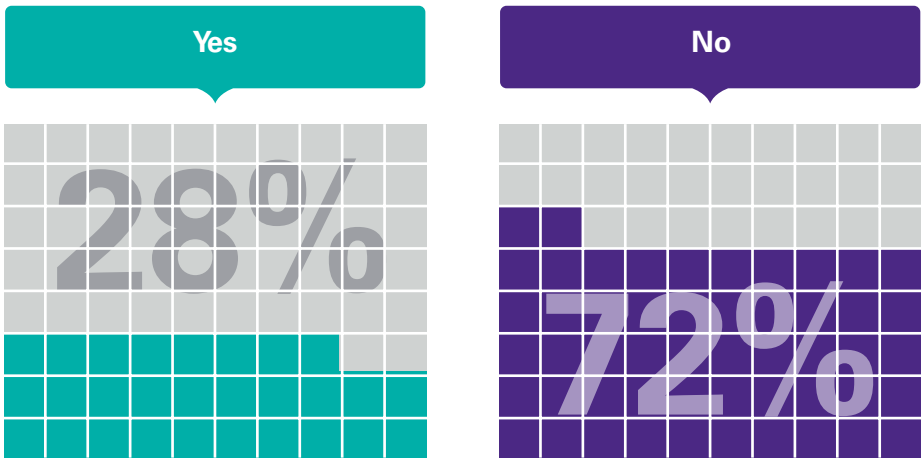
Increasingly, several state governments in India have embarked on a journey of enhancing cybercrime fighting units through a variety of means by:

- Creating specialised cybercrime detection teams to increase detection rates
- Procuring cybercrime detection tools to determine effective evidence capturing and preservation
- Creating mass police force training programmes to impart thorough understanding to key officers on what clues to look for in cybercrime cases and what provisions of the IT Act are to be applied to increase conviction rates.

72 per cent
respondents indicate that the number of cyber response organisations are inadequately equipped, given the level of cybercrimes.

Adequacy of cybercrime response organisations

Do you think there are enough cybercrime response organisations in the country to tackle cyber-related issues?



Source: Analysis carried out on the basis of the KPMG in India's cybercrime survey, 2015

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Conclusion

While organisations work their way into designing the most suitable cyber defence plan, one of the biggest challenges faced by most CIO's in defining a strategy is the blurring lines of the IT perimeter of their organisations due to services moving to the cloud, and employee-centric Bring Your Own Device (BYOD) policies. CIOs are increasingly realising that a successful cybercrime defence strategy requires a synchronised risk view and strong collaboration amongst the business, IT and third party service providers.

Given the above, it is also vital for organisations and CIOs to make a paradigm shift in the way the strategies are designed. This could mean defining strategies based on identifying what information is at stake, rather than basing strategies on what security tools the organisation is missing. While putting cyber defence strategies into play, it is vital for organisations to take cognisance of the following key insights:

Deeper cybercrmie risk assessment: With the constant increase in cybercrime and its impact, it is important for organisations to identify the crown jewels that need to be protected. Enterprises need to carry out cyber risk assessment in depth to ensure that the right assets are adequately protected to limit impact of attacks.

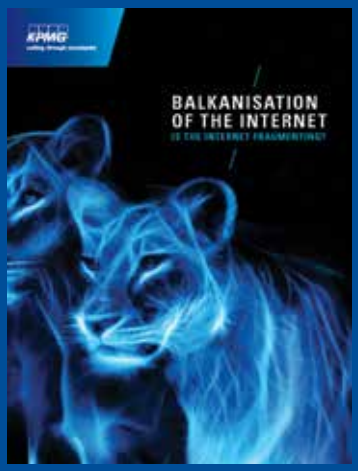
Focus on people: The human element can either make or break the cyber defence strategy of any organisation. No matter how much technology is put in to play for protecting the organisation, weakness on the people security front could negate all investments in cyber defences. It is imperative that organisations build a robust cyber awareness programme that effectively educates its personnel and vendors alike.

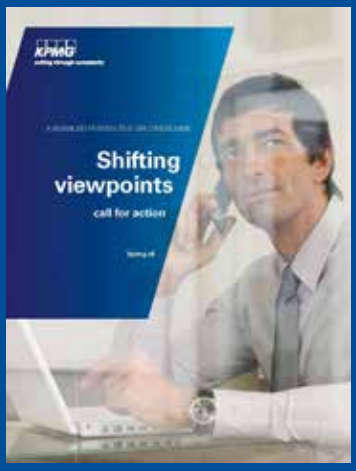
Build cybercrime intelligence: The world of cybercriminals is ever evolving with newer attack techniques being churned out. In this scenario, organisations need to build in a robust cyber intelligence system that can provide CIOs and CISOs contextual information and actionable intelligence to predict an attack.

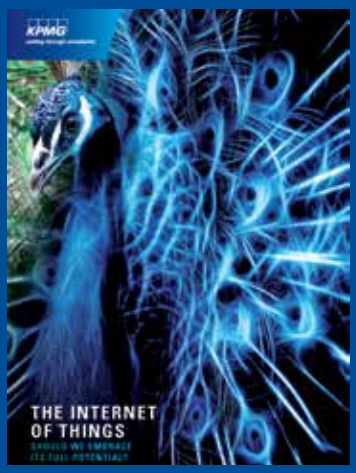
Move towards cyber analytics: Companies have complex IT architectures and diverse platforms to help enable their business operations. With a large threat landscape and a wide variety of threat attacks, organisations need to monitor their systems. It is important for businesses to put in to play a coordinated and robust cyber analytics platform that can serve as an effective predictive, detective and corrective cyber control system.

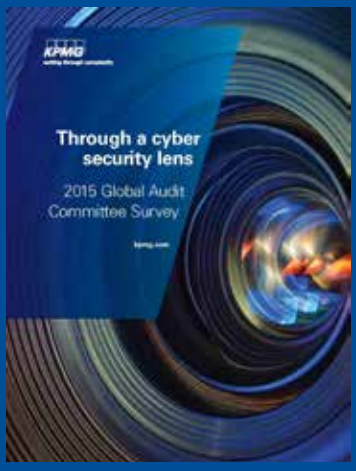
© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

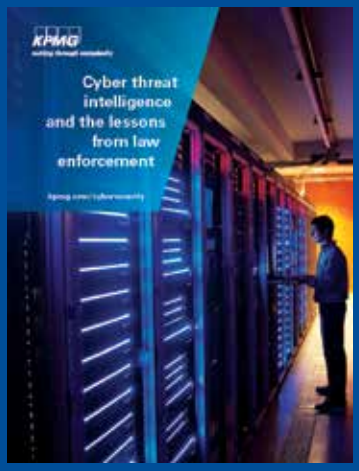
Thought leadership publications

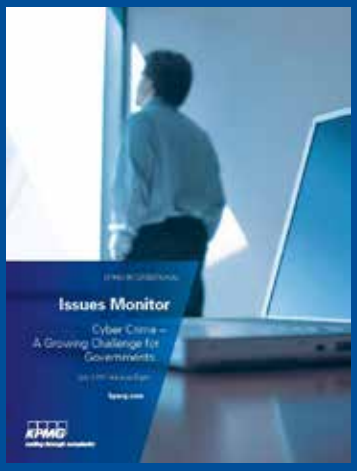












© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

KPMG in India contacts:

Nitin Atroley
Partner and Head
Sales and Markets
T: +91 124 307 4887
E: nitinatroley@kpmg.com

Mritunjay Kapur
Partner and Head
Risk Consulting
T: +91 124 307 4797
E: mritunjay@kpmg.com

Mohit Bahl
Partner and Head
Forensic
T: +91 124 307 4703
E: mbahl@kpmg.com

Akhilesh Tuteja
Partner and Head
EMA IT Advisory - RC
T: +91 124 307 4800
E: atuteja@kpmg.com

Sandeep Gupta
Partner
Forensic - Cybersecurity
T: +91 22 6134 9453
E: sandeepgupta@kpmg.com

Atul Gupta
Partner
IT Advisory - Cybersecurity
T: +91 124 307 4134
E: atulgupta@kpmg.com

Follow us on:
kpmg.com/in/socialmedia

Download KPMG India apps:

#KPMGIndiaCyber

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of the survey respondents, they do not necessarily represent the views of KPMG in India.

© 2015 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

This document is meant for e-communications only. (004_SUR1115)