KPMG

Cybercrime survey report

Insights and perspectives

December 2017

KPMG.com/in

Foreword

Ever since the advent of digital age, technology has grown at a rapid speed with IT permeating into every sphere of life. However, this has given rise to an ever evolving class of cyberthreats, affecting individuals and enterprises. The effects of this new adversity have prominently come to light in the last few years, accounting for cumulative losses of billions of dollars across enterprises.

Given the continuous advancement in connected technologies, coping with and being resilient against cyberattacks are among the top priorities of modern organisations. The senior executives of today's enterprises are cognisant of the threats posed by cyberattacks, and are actively looking for ways to safeguard their assets and businesses against these threats. In the current scenario, cyber has truly become a business risk and is not limited to just a technology risk.

Many of today's organisations are driving their cybersecurity programme objectives through their board room agenda. However, these programmes are still catching up with the existing global trends. There is a rise in not only number of cyber incidents, but also reporting of cyber incidents to competent law enforcement authorities and regulators. There is still a long way to go for the Indian diaspora with reference to cyber in terms of red teaming, brand protection and cyber insurance.

KPMG in India has been at the forefront, dispensing information and creating much needed awareness on cybersecurity and cybercrime. The dangers we pulsed have expanded exponentially. This year we saw what is alleged to be state used cyber warfare tools being revealed and leaked in the public domain. In the advent of this, came a series of mutant variations to exploit vulnerabilities across corporate networks and personal computers. Ransomware attack and/or leaking of confidential data to bring down production or stock value is the new normal. How secure and covered are we as individuals and as a responsible corporate?

In order to provide you with a larger picture, we have revised our approach and published this year's cybercrime study. This study is in continuation of our efforts to put forth the perspectives of cybercrime across the industry. In addition, we have also brought forward viewpoints from the Law Enforcing Agency, and end users to provide a holistic view.

The study brings forth cybercrime trends and highlights measures to deal with this rapidly growing issue. We hope the study provides you with valuable insights that can be leveraged in shaping the cyber risk management stance in your organisation.

Mritunjay Kapur
National Head, Markets & Strategy
Head - Technology, Media & Telecom

Akhilesh Tuteja
Partner and Head
Risk Consulting
Co-leader – Global Cybersecurity

Mohit Bahl
Partner and Head
Forensic Services

Atul Gupta
Partner
IT Advisory
Leader - Cybersecurity

Sudesh Anand Shetty
Partner
Risk Consulting

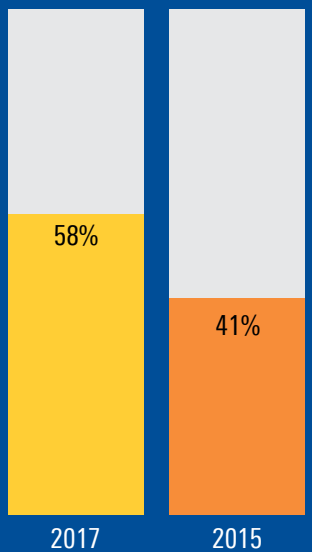
Executive summary

Cybersecurity is among the top challenges being faced by many organisations in the country; coupled with the digital transformation journey, which several companies are either undergoing or plan to undergo. As businesses expose themselves to evolving technology and digital ecosystems, they need to ensure that the risk exposure due to cyber is managed.

Cyberattacks in the current era have become more specialised and concentrated in nature, targeting specific organisations and individuals. With the attack pattern becoming more directed, the impact due to incidents have made alarming damages spanning financial losses, disruption of operational services, erosion of shareholder value and trust. There is a need to understand this threat comprehensively, given the threat is constantly evolving, and create an effective cyber resilient environment to withstand these testing times.

Boardroom agenda and governance

- **79 per cent** of the organisations indicated that cybersecurity was amongst the top five business risks.
- Day by day the board is becoming more serious about cyber risk. This is visible from **58 per cent** organisations including cyber risk as part of the boardroom agenda, which has moved up from **41 per cent** as recorded in the last KPMG study.[1]

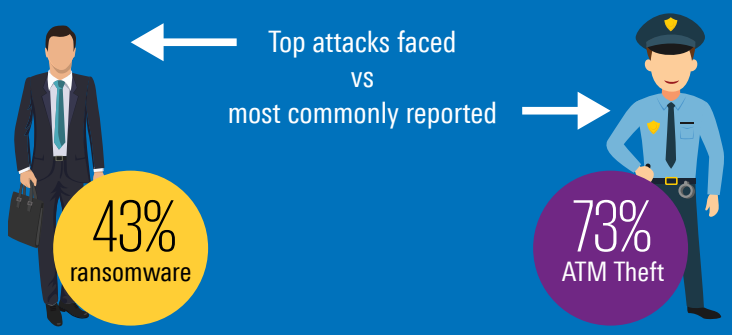


1 KPMG cybercrime report 2015

Targeted cyberattacks

- Malware constitutes the biggest share of cyberattacks faced by organisations, with **73 per cent** of organisations indicating it as a menace, followed by spear phishing (49 per cent).
- **43 per cent** of organisations indicated that they have experienced ransomware attacks in the past year.
- In contrast to organisations views, **73 per cent** of Law Enforcement Authorities (LEAs) indicated that only ATM card theft was the most commonly reported cybercrime to the Cybercrime Investigation Cells, followed by phishing attacks (47 per cent) and data theft (40 per cent).
- **46 per cent** of organisations believe that they are not adequately prepared to handle ransomware attacks as a major threat.

These statistics indicate a paradigm shift in the manifestation of cybercrimes.



Cyber readiness

According to organisations, following are the top five cyber areas where investments are provided pertaining to cybersecurity:

Top three areas that are lagging attention of the organisations are:

Brand protection

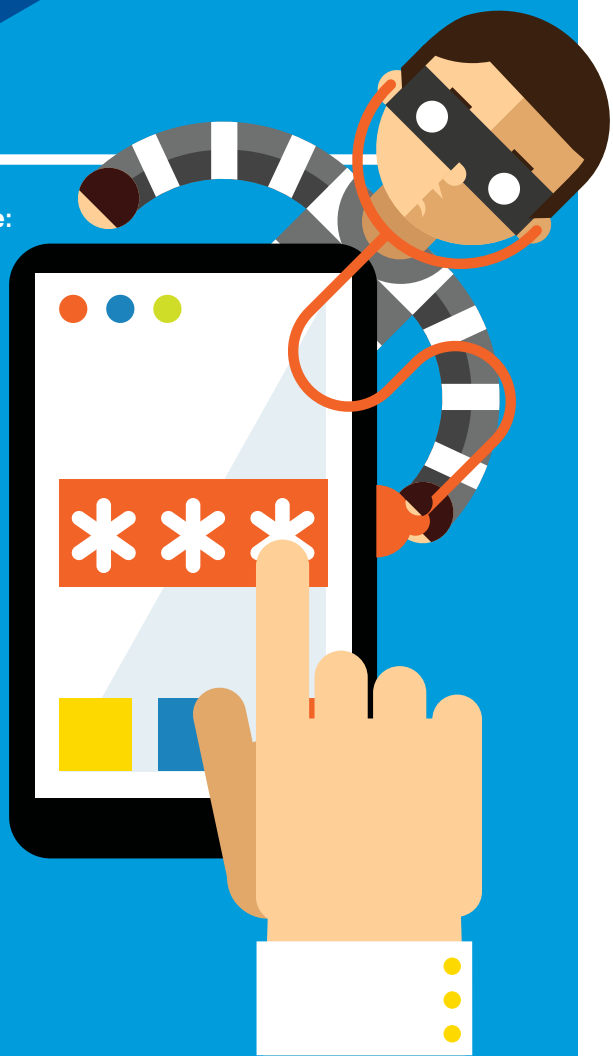
18%

Red team assessment – simulate real cyberattacks

18%

Next-gen technology security

20%



Changing regulatory landscape

According to LEAs, there has been more than **50 per cent** increase in the number of cybercrimes being reported in the last year.

Our study indicates that information availability and/or awareness is key concern. **35 per cent** of the organisations indicated that the information on cybercrime prevention, incident reporting, and related requirements and regulations from the government is not easily known to everyone.

Almost two-thirds of the law agency officials feel that there are not adequate laws, which address concerns related to cybercrime prevention, detection and investigation. They are also in favour of increasing the number of cybercrime cells in the country as well as of creating a central reporting mechanism that will enable an effective response to cybercrime.

Our study further reveals that **40 per cent** of end users feel, cross country jurisdictions being involved is a hindrance in lodging a complaint with cyber cells.

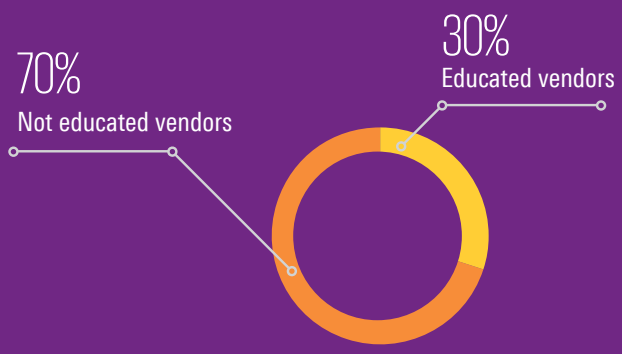
Business ecosystem – third parties

Cyber risk has emerged as one of the key risks in the supply chain

- **48 per cent** of the organisations say that cybersecurity risk assessment is one of the important prerequisites that needs to be addressed before outsourcing.

The current preparedness to address this risk is not adequate, as per the study's outcome.

- Only **30 per cent** of the organisations have clearly defined requirements with reference to cybersecurity expectations, incident response, and data breach prevention and have educated vendors about the same.



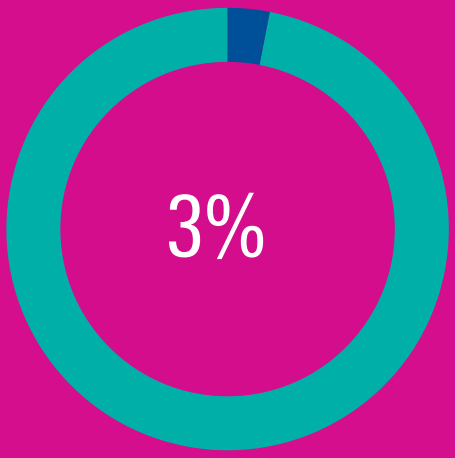
Cyber response and recovery mechanism

- Organisations have realised the importance of having a mechanism to effectively respond to cyber incidents. Our study indicates that **69 per cent** of the organisations are in the process or have formalised cyber response processes and procedures,
- Only **18 per cent** are of the opinion that they are fully prepared to withstand and respond to large scale cyberattacks.

This underscores the growing complexities of new age cybercrimes.

Reporting incidents to law enforcement agencies

- Only **3 per cent** of the organisations have reported a cyber-incident to the local law enforcement agency.



Cyber preparedness - new age technology

- Adoption of emerging technology has increased risks multifold. Our study indicates that **80 per cent** of the organisations use at least one of the top four emerging technologies which are; cloud, mobility, social media, and digital enablement.

However, adoption of new technology has not justified the cyber budget spend in comparison to the emerging risks they bring to the business.

- Only **81 per cent** of the organisations have cybersecurity budgets of less than **10 per cent** of their total planned budgets against risks arising from the adoption of these technologies.

The need to have a holistic view on cybersecurity risk is clearly established from the study. This is further demonstrated by the fact that cyber is becoming a board room discussion.

At this hour, the need is to look at security an as integral element across all business processes and not to be considered as an add-on. Also, to have an effective and balanced strategy, which not only supports in defending against the cyberthreat but also enables organisations to be resilient enough to withstand and respond to cyberattacks.

An overview of the survey

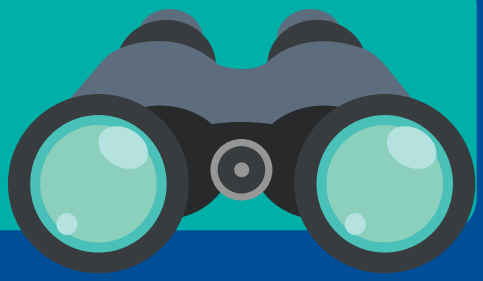
Cyber incidents are multiplying at an alarming pace and they are increasingly becoming more complex causing multiple disruptions in businesses and economies. Today, despite enhanced awareness and significant oversight from CXOs and boards, organisations fall prey to persistent, targeted and sophisticated threats from attackers.

As management of top organisations continue to work on building a cyber-defence strategy, it is vital to have an understanding of the looming cyberthreat and knowledge of how a cyber-response strategy has to be an integral component of the overall cyber framework. With an increased trend of attacks, organisations are now beginning to understand the need for cyber intelligence, cyber resilience and measures to decrease the impact from cyberattacks.

This report provides a holistic perspective on cybersecurity and associated crime with a view on how organisations are gearing up against this threat.

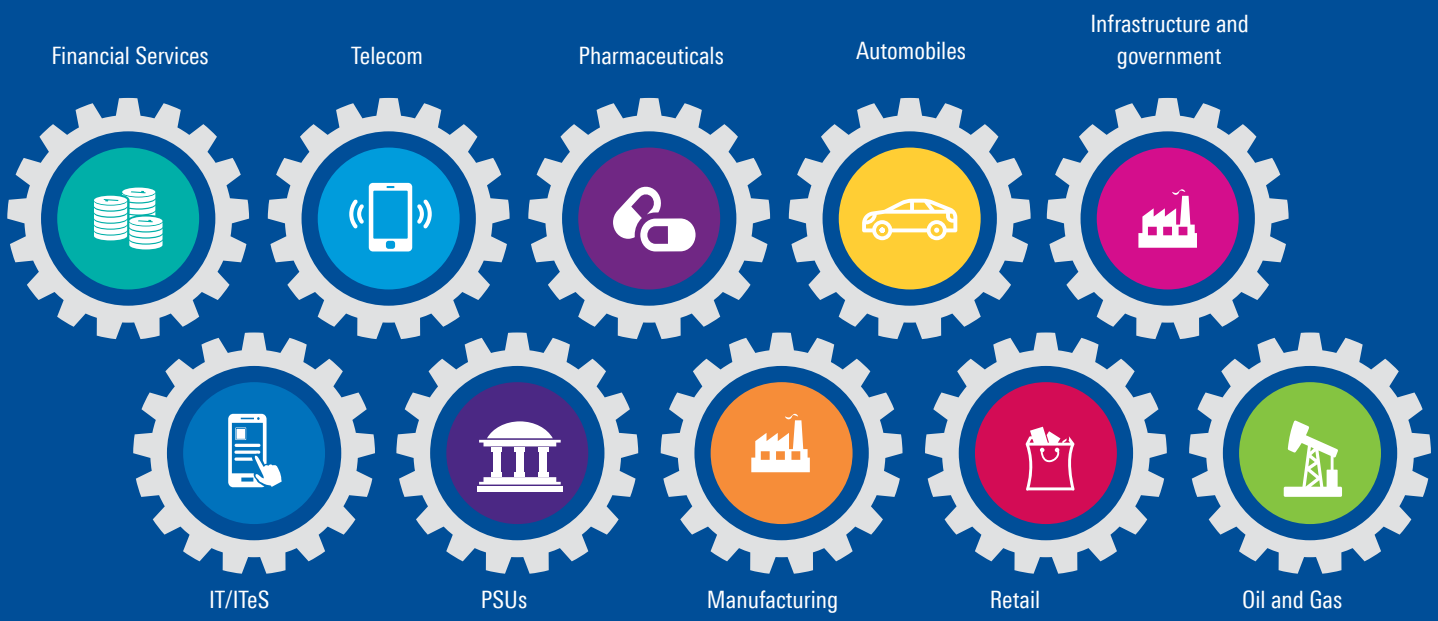
Profile of the participants

Our study witnessed participation from more than **300 individuals from the likes of CIOs, CISOs, CIAs, COOs and security professionals.** The study also saw a wide participation from top law enforcement officers and end users from all over India.



Mix of the participants

The study had a mix of participation from various industry sectors given below:

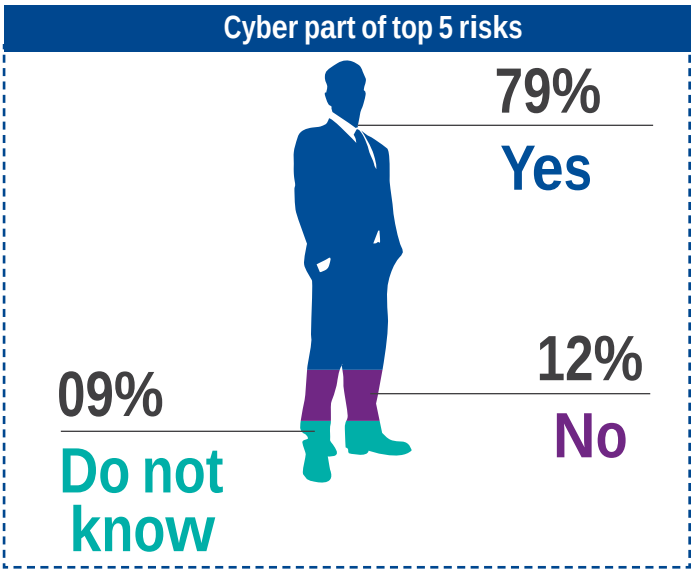


As part of this study, KPMG in India reached out to key law enforcement officers from different states such as Assam, Chhattisgarh, Kerala, Maharashtra, Punjab, Rajasthan, Tamil Nadu, Telangana and West Bengal to get their perspectives on the state of cybercrime and the current framework/ infrastructure needed to tackle such crimes in India.

Table of Contents

Board room agenda and governance

Cyber has clearly emerged as a risk which is impacting organisations across industries. Three out of four corporates have classified cybersecurity as a top five risk concern for organisations.

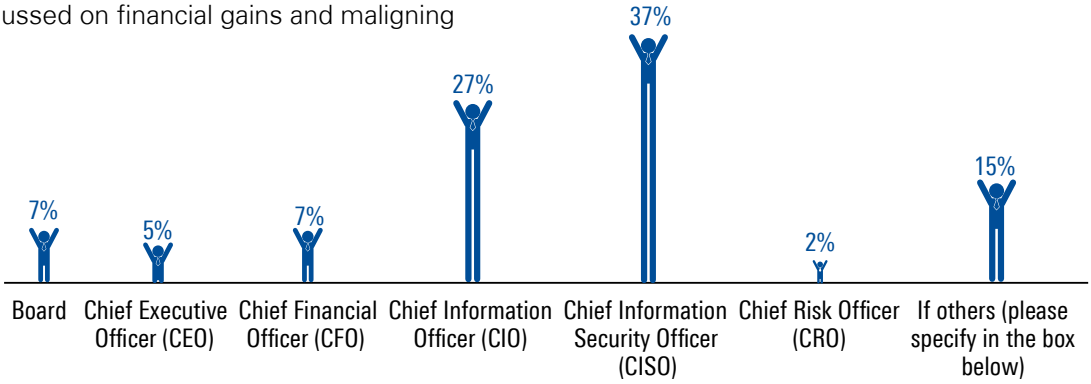


Cybercrime in India is rising rampantly on account of loopholes/snags in new technological platforms, increase in number of smartphone users, growing use of social media and increased thrust on digitisation in every stream of economy and governance. Due to the rise in targeted cybercrimes like DDoS (Distributed Denial of Service), spear phishing and ransomware which are focussed on financial gains and maligning brand reputation, it is important for the management to gear up their defences. As cybercrimes increase, a thorough cyber incident response, risk assessment, root cause analysis and corrective and preventive action are increasingly becoming board level priorities.

Multiple state level players are believed to be constantly engaged in building a war chest of exploits across different products such as applications, operating systems, network and at assembled hardware. These exploits have leaked and are constantly being shared among criminals over the dark web. This potentially exposes every organisation to known however not published vulnerabilities.

Cybersecurity – a major threat

Cybersecurity is a major threat to organisations, with a rise in the number of cyber incidents. Digital technologies have driven the growth of Indian businesses with a huge spurt in online transactions but have also opened the gates for cyberattackers waiting to steal confidential information and sensitive financial data. Organisations are increasingly being afftected, key victims being, stakeholders, employees and third party vendors.



Only **12 per cent** of the organisations feel that the board or the CEO is responsible for managing cyber risks.

27 per cent believe that it is the responsibility of the CIO.

37 per cent believe the CISO is chiefly responsible for managing cyber risks.

While cyber has emerged as a key risk, only **58 per cent** have made this a board room agenda. This is significant improvement from KPMG in India's Cybercrime study 2015 where **41 per cent** of corporates had taken this up as board room agenda, the study indicates increased awareness of the corporate leadership on cybersecurity. However, this continues to be an area where there is a need for catch up compared to the global out look.

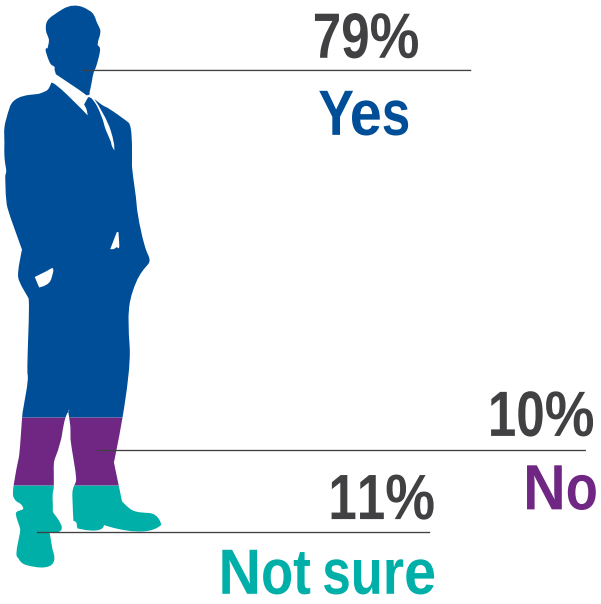
Role of audit committee in cybersecurity

The audit committee plays an important role in ensuring that there is an objective review of the various business risks to which organisations are exposed.

With the increase in cyber incidents across the regions, for instance data hack in a famous financial entity has reinforced that the cyber risk if not managed well, can lead to significant impact. In this case, millions of customers had their personal information compromised and the CEO of the organisation had to resign due to the backlash faced over information leakage.

According to the study, there has been a significant increase (**79 per cent**) in attention provided by audit committees to cybersecurity risks with specific focus on:

- Incident prevention
- Detection
- Response



Cyberattack targets and impact

Cyber incidents are normally associated with financial impact however the study indicates targets that are attacked often:

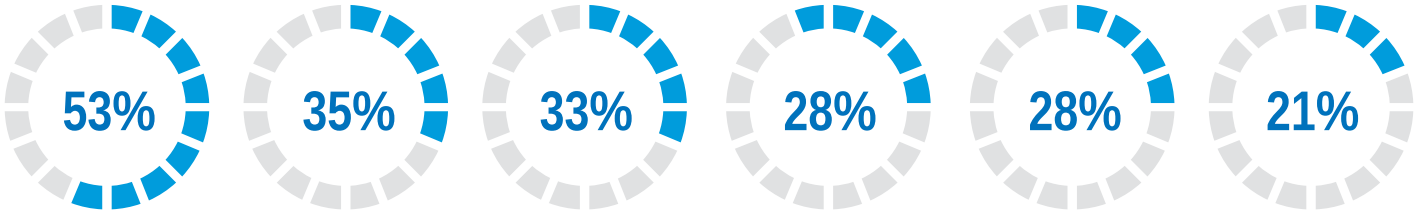
- Disruption of business process
- Theft of sensitive data
- Reputational damage

Financial information continues to be a key attack area. Almost 20 per cent of the organisations have indicated that financial losses, up to USD500,000, have occurred on account of cybercrimes.

The study also highlighted that, there is an impact on the morale of the current workforce in event of cybercrime attack across organisations. The organisations attribute cybersecurity impact on employee morale comparable to financial losses incurred upon.

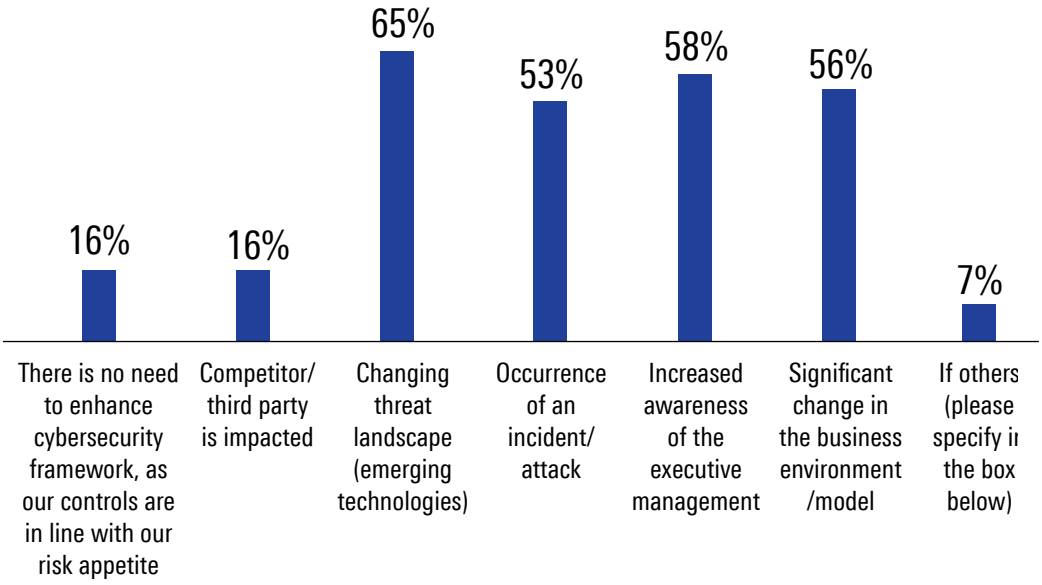
In addition to financial loss, our study indicates that organisations are exposed to espionage.

- **58 per cent** of the organisations believe that they may have been exposed to corporate espionage.
- **32 per cent** of the organisations feel that their CXOs may be vulnerable to cyberattacks.
- **61 per cent** of the organisations feel that they may be bugged and **36 per cent** of the organisations feel that their corporate emails might be read by someone else.



Confidence level on cyber events

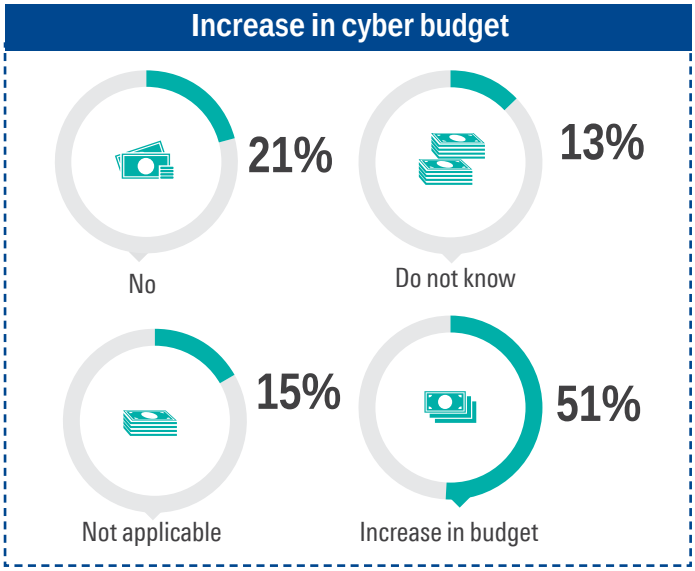
65 per cent of the organisations feel that the changing threat landscape is a key driver for changing risk profile which demands to have an enhanced cybersecurity framework.

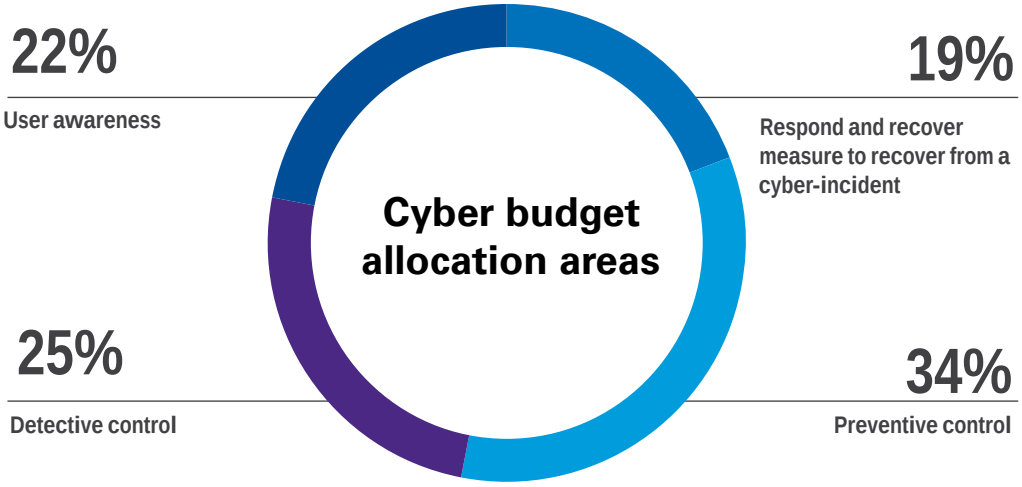


Cyber budgets

Organisations are increasingly becoming aware about cyber risks and their repercussions, according to **51 per cent** of organisations, there has been an increase in cybersecurity/cyber incident response budget as compared to the previous year.

Organisations are spending a majority of their cybebudgets on the preventive controls of cybersecurity. According to entities, preventive controls with a share of **34 per cent** constitute the bulk of cyber budgets in organisations, followed by detective controls, user awareness, and response and recovery measures.



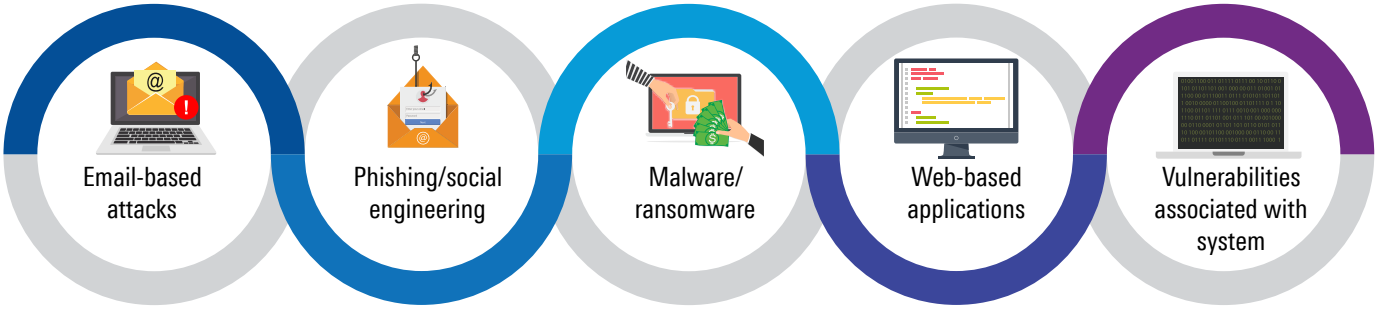


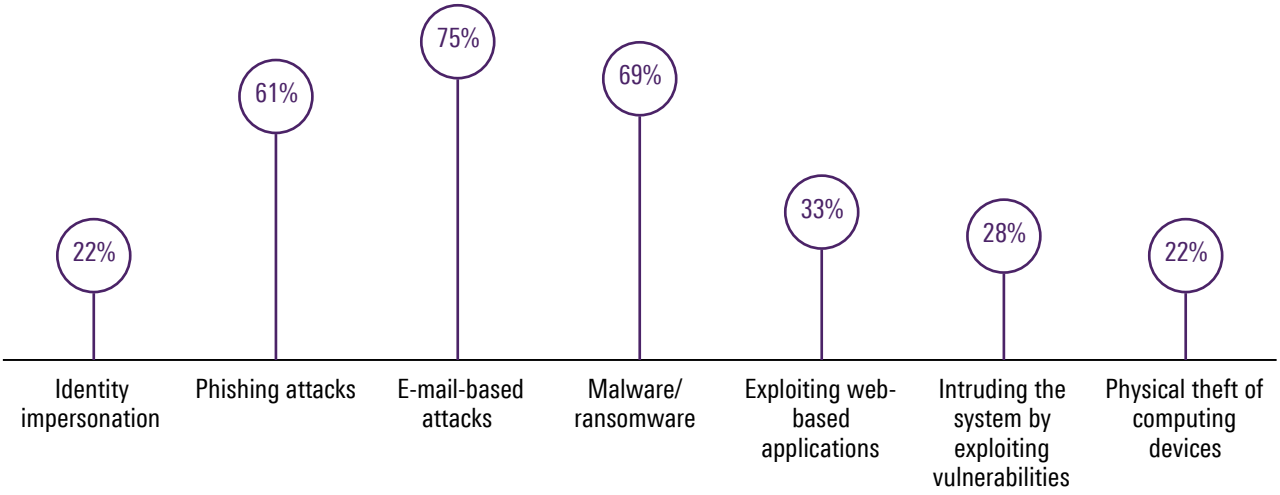
Targeted cyberattacks

Targets for cyberattacks

There are multiple systems and technologies that are being targeted by attackers, using multiple attack measures. There is constant movement towards targeted attacks, which is increasing the likelihood of attacks to take place.

Based on the study, top five attacks faced are:

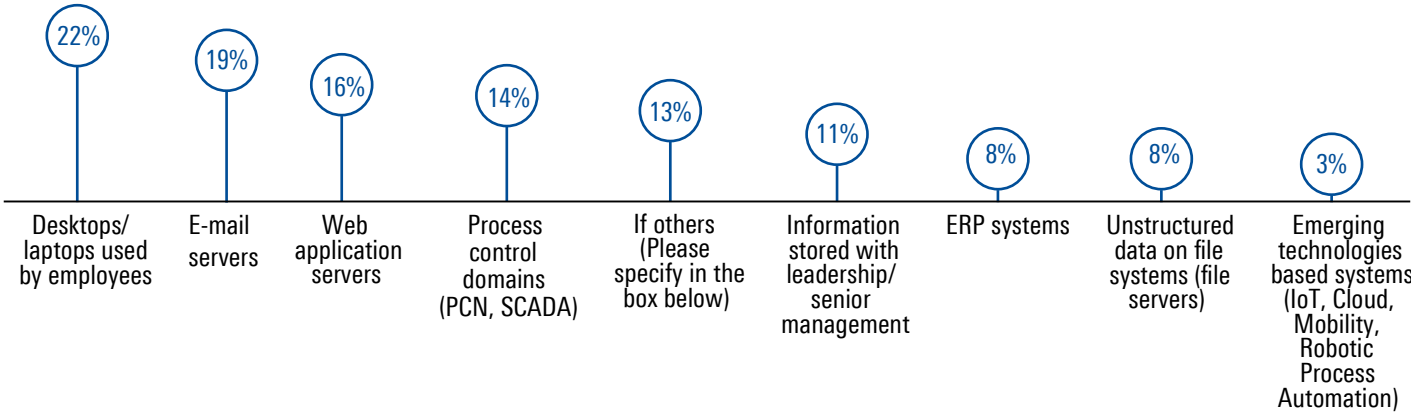




Comparison of top five attacks since the last study published, showcases that email-based attacks have emerged as one of the key access points for cyberattacks, with unsolicited mails becoming a distribution channel for phishing, spywares, malwares and other threats and disrupting business processes. Malware based attacks have also increased significantly from last year.

The study further goes to showcase that organisations main targets of cyberattack are

- Desktops/laptops used by employees
- Email servers
- Web application servers
- Information stored with leadership/senior management
- ERP systems
- Emerging technologies based systems (IoT, cloud, mobility, Robotic Process Automation)



One of the top concerns for IT security teams in organisations is to prevent intruders from gaining access to sensitive data and information on corporate network. From the study, it is observed that insider threats from employees are much more prevalent than outsiders.

Emergence of ransomware attacks

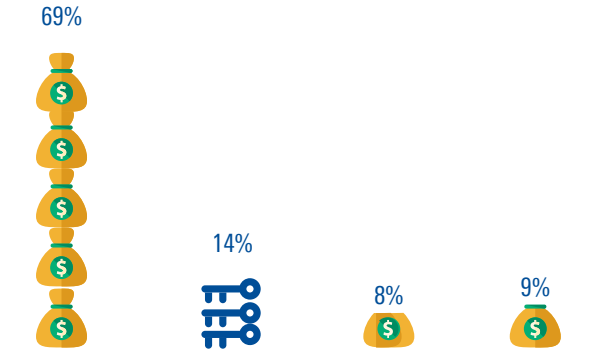
Malwares and ransomware attack methods continue to evolve at a regular basis, which also exposes the effectiveness of security patch deployment. Modern malwares are programmed to attack a specific vulnerability in the systems of target companies which helps attackers spread malware and cause disruption in operation.

Increasingly these attacks are also becoming more focussed.

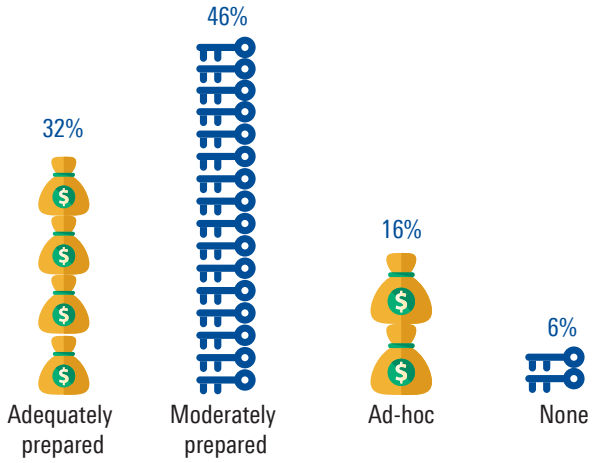
Ransomware is normally associated with mass attacks across industries, however, attackers are now attacking via specifically crafted attacks, which is making this attack lethal.

There is a need for entities to be prepared to withstand ransomware attacks. The study indicates that 46 per cent of organisations believe that they are not adequately prepared to handle ransomware attacks, while 16 per cent feels that they are not aware of what needs to be done in case of a ransomware attack.

Is ransomware a business risk?



Preparedness to handle ransomware attacks



50 per cent of law enforcement agencies are of the opinion that they have the latest tools and technologies available but require an enhanced training programme as well.

69 per cent of organisations are of an opinion that ransomware is a significant business risk and **43 per cent** indicated that they have experienced ransomware attacks in the previous year.

Incidents such as ransomware, data breach and DDoS (Distributed Denial of Service) attacks on organisations are making headlines worldwide. For organisations, dealing with such situations effectively is a key priority. This can be a difficult task due to the changing nature, high complexity and huge volume of cyber incidents.

Cyberattacks – LEA perspective

The cyberthreat environment has evolved dramatically with an array of sophisticated attacks occurring across enterprises.

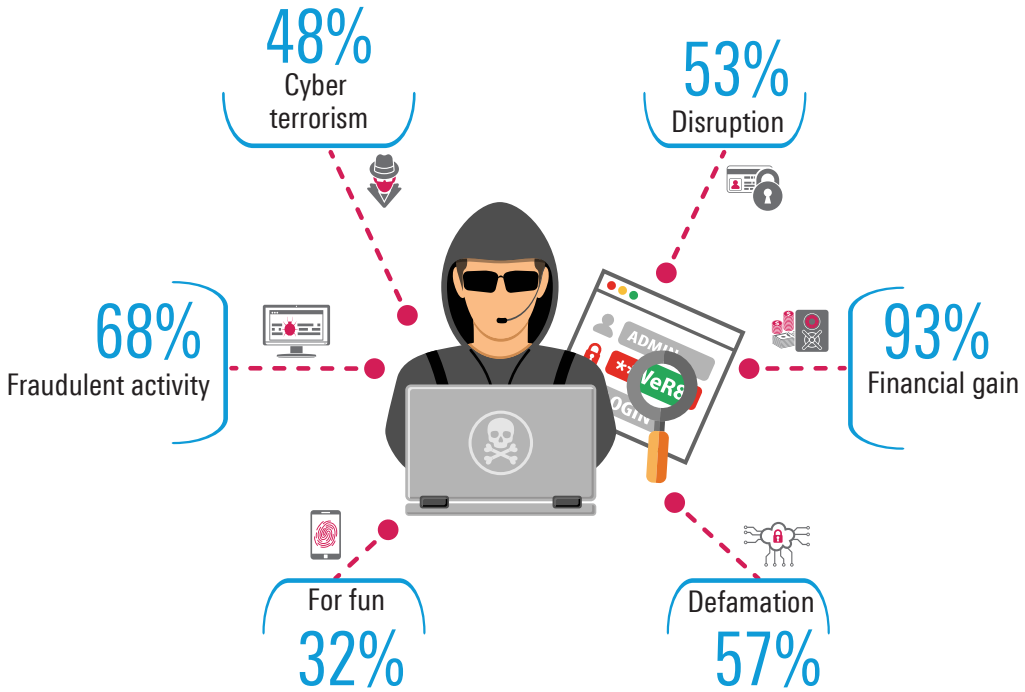
Law Enforcing Agencies (LEA) have been fairly occupied managing cybercrime across individuals and organisations. Attackers tend to have several motives to launch an attack.

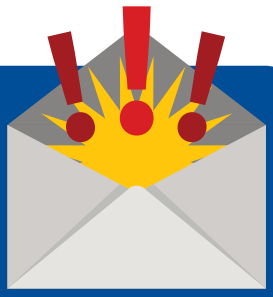
Based on the study performed with the law enforcement agencies, it was noted that following are key motives of cyberattackers:

- Financial gain
- Fraudulent activity
- Defamation
- Disruption
- Cyber terrorism

> LEAs have a reasonably good grasp over the potential threats of cybercrimes, and all police units are investing heavily in building forensic centres,'Cyber Suraksha Kavach, SOCs, capacity building centres like NDCRTC as well as on generating public awareness for building safe and secure cyber space in India. Based on the analysis of cyberattacks that happened over the last year, we have noted that the attacks have become more focussed.
>
> **P. Vimaladitya**
> IPS
> Asst. Director (IT),
> S.V.P. National Police Academy, Hyderabad

Motives of Cyberattacker





India's growth story is highly technology driven and is closely aided by cyber and IT technologies. This has a natural corollary of increasing risks of cybercrimes ranging from phishing attacks to a sophisticated cyber warfare.
The twin graphs of Internet penetration and the consequent cybercrimes are seen rising exponentially in the North Eastern States of India, and particularly in Assam in the previous eight years. To effectively tackle this challenge and to cater to comprehensive needs of Assam Police and upcoming 'NE POL' (North East Police), Assam Police is raising a state of the art AP Cyber dome. This vast project has various components like digital data bank, cyber forensics, cyber intelligence, big data analysis and cybersecurity, amongst others.

Dr. Dhananjay Ghanwat, IPS
SP (Special Branch), Assam
Chevening Scholar

Currently, cybercrime inflicted upon a company has typically significant advanced planning. These include,

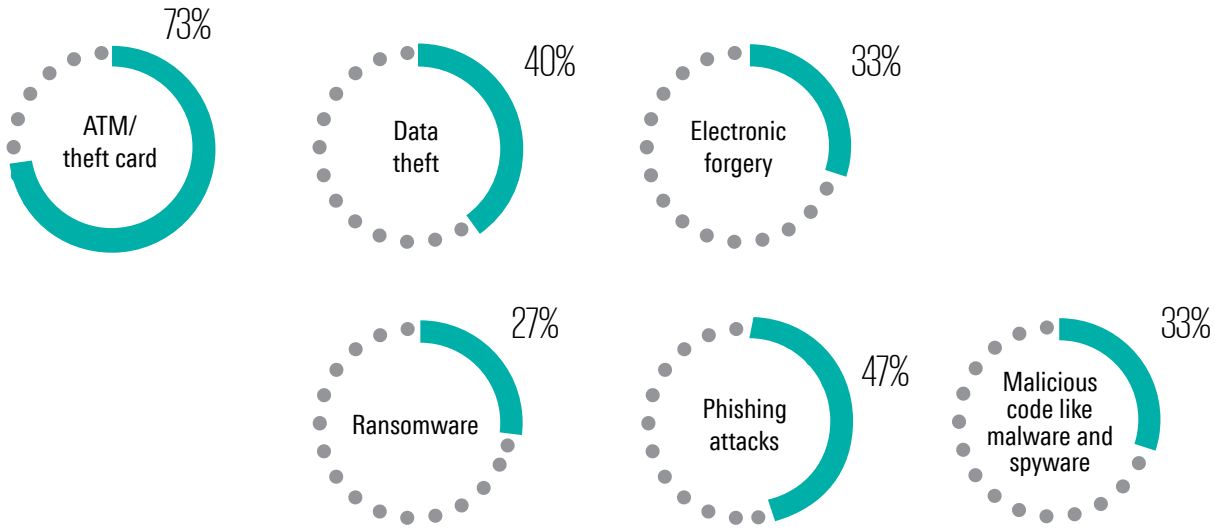
- Reconnaissance
- Dry runs conducted
- Attempts without infectious payload made
- Weak links in the perimeter
- Human element exploited before an actual attack.

Study performed by LEAs further showcase that most reported cybercrimes include:

- ATM card theft
- Phishing
- Data theft

As per the law enforcement agencies, only **30 per cent** of the law enforcement cadets are skilled and experienced to deal with cybercrime.

Top cybercrimes reported to LEA



Cybersecurity readiness

Organisations are increasingly adopting different measures to combat cybersecurity risks which include development of a thorough cybersecurity framework, risk assessment, cybersecurity awareness trainings, etc.

Emerging technology adoption at a fast pace, across organisations, is leading to a dynamic risk profile which mandates to have a comprehensive cybersecurity framework. The framework which consists of standards, guidelines and best practices ensures that the critical infrastructure is protected and helps organisations to manage cybersecurity related risks. Organisations are looking to adopt global frameworks which go beyond ISO 27001.

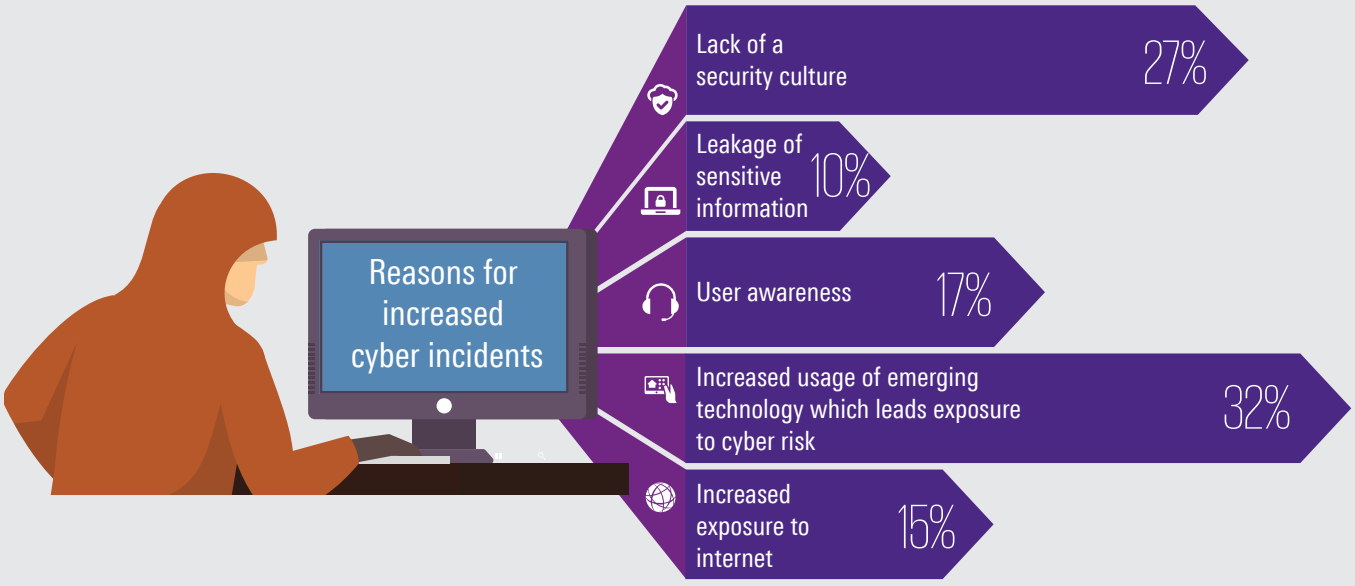
NIST is increasingly being adopted and implemented by a wide range of organisations for proactive risk management as it contains guidelines and best practices on governance, asset management, data security, access control, response planning and risk mitigation. Adoption of any global cyber framework requires customisation and organisations are taking this as a central piece of work during the framework adoption stage. Security by design is an approach which can be taken while developing an effective cybersecurity framework as it takes measures and best practices such as continuous testing, authentication measures, etc. and reduces the impact of security vulnerability.

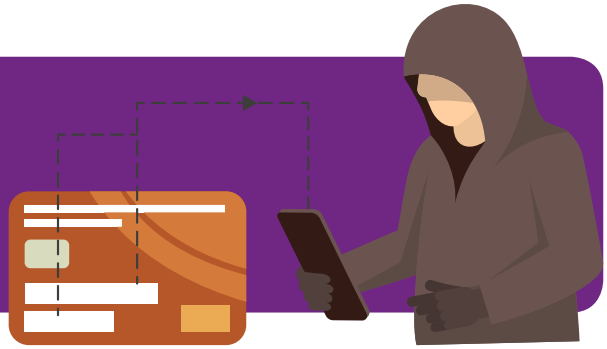
Cyber incident response is a key element of cyber strategy, it helps organisations to respond in an effective manner to cyberattacks. The study indicates, cyber response is an emerging area and 29 per cent of organisations believe the cyber incident response teams and cybersecurity specialists in organisations require major skills and talent enhancement.

Increased cyber incidents in organisations

There is a steady increase in incidents across industries, due to dynamism of threat environment and ease of initiating cyberattacks. The study showcases that:

- **32 per cent** organisations indicate that the adoption of emerging technology like cloud, block chain, mobility and digital enablement is exposing organisations to newer cyber risks
- **27 per cent** organisations attribute the incidents to lack of security culture.





Measures in place to manage cyber risk

Organisations are consciously moving forward to ensure that effective measures are established. The study indicates that:

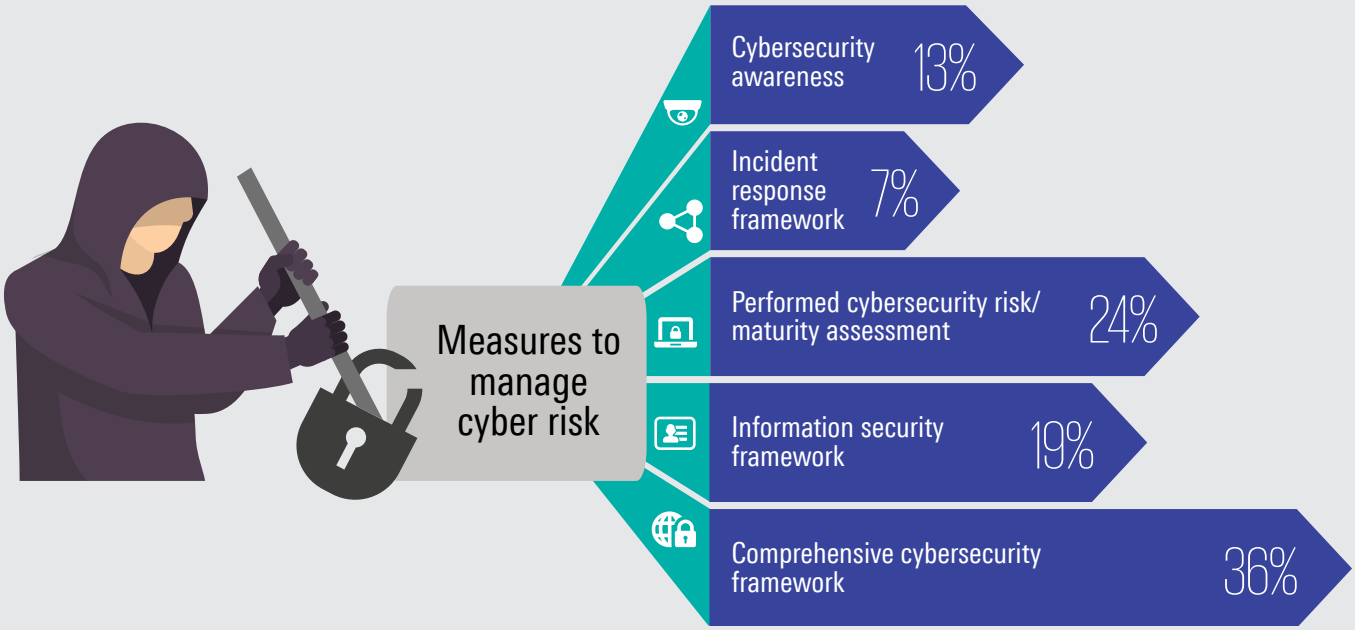
- There is a significant focus on establishing a robust cybersecurity framework which is aligned to address regulatory requirements.
- Cybersecurity risk assessment and maturity assessment has been performed, which shall lead to a detailed road map to implement various initiatives to effectively address cyber risk.
- Importance of having incident response framework is emerging and there is an initial trend of embedding incident response as part of the overall cyber framework.

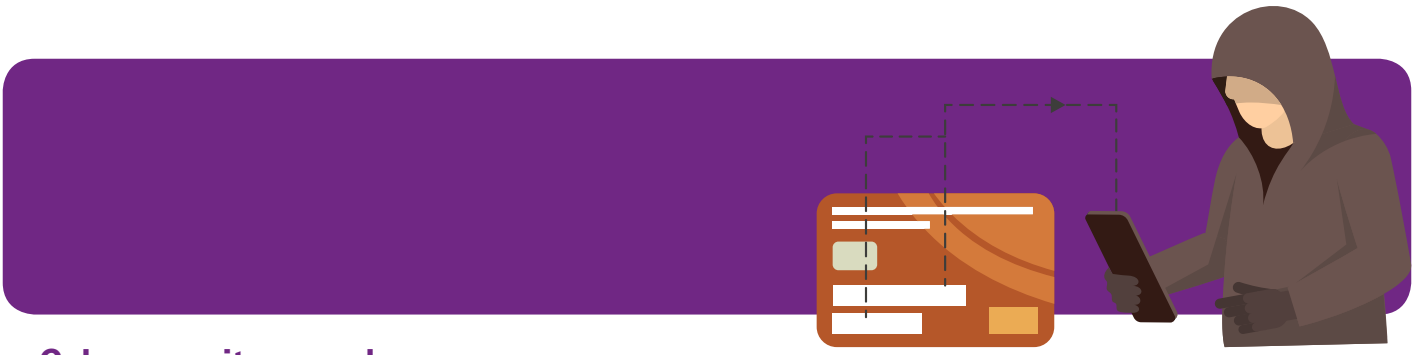
The study indicates that 'cyber insurance' being used as a strategy for addressing the risk is either not well understood or the focus is to establish baselines and then go for insurance. However, it appears that cyber insurance is still at a nascent stage.

Need for cyber insurance

Cyber insurance covers a business' liability to compensate in case of a cybersecurity incident. Cyber insurance cannot defend an organisation against cybercrime; however it can compensate for losses due to cybersecurity incidents.

Organisations need to form a structured approach to cybersecurity with emphasis on security measures for third party transactions, aligning risk mitigation strategies with the changing threat landscape, and cyber insurance.





Cybersecurity spend

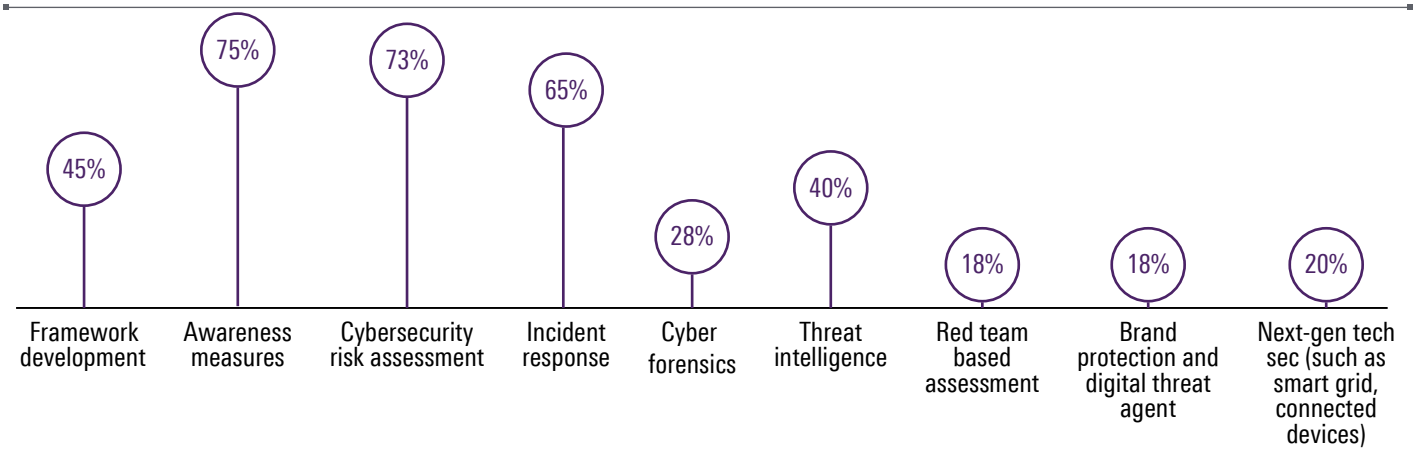
Investments in prevention of cybercrimes are organisations key priorities in recent times. It is good to note that businesses focus is on awareness measures, as insider threats to cybersecurity can be combated by an increased level of awareness. Key investments are crucial in helping companies strengthen their defences against advanced cybercrime risks. Organisations should also have a look at more advanced techniques to combat cybercrime and invest more in diagnostics programmes, cyber threat intelligence and incident response.

Human element can either break or make the cyber defence strategy of any organisation. Employees continue to remain one of the weaknesses despite focus on awareness of cybersecurity. Advancements in social engineering techniques have led to many successful attacks on end users. Organisations are continuing to make investments in cybersecurity to enhance awareness among employees on cyber risk.

- Awareness - Effectiveness of cyber awareness is one of the key criteria of successful cybersecurity programmes. Organisations are adopting newer and innovative approaches towards increasing awareness such as gaming, cyber drills, and situational videos. While our study indicates that awareness is key investment focus, however, a majority of it continues to follow the traditional approach rather than involving external support to drive a multi-channel awareness programme. Cybersecurity risk assessment – There is an increased focus on performing cybersecurity risk assessment to ensure that risk profile is thoroughly developed and adequate risk treatment strategies are formalised.
- Incident response – Organisations have realised that cyber incidents are a reality and there is increased need to prepare an organisation to respond to such incidents.

The areas that are being focussed and invested in indicate that many of the organisations are in the process of establishing a strong foundation. However, with the threat profile changing at such a significant pace, there is a need to adequately invest in emerging areas like:

Top 3 cybersecurity spend area	Least 3 cybersecurity spend area
Awareness	Digital brand protection
Cybersecurity risk assessment	Cyber drills (Red team and blue team)
Incident response	Next-gen technology security such as smart grid and connected devices



Interview

Hari Kishore Kusumakar, IPS
Additional Commissioner of Police (IV), Kolkata

There has been more than 50 per cent increase in cybercrimes being reported in comparison to last year.

67 per cent of LEAs feel that adequate laws are not in place, which address concerns related to cybercrime prevention, detection and investigation.

73 per cent of LEAs feel they are not adequately equipped to handle cyber related issues.

Q 1: How far has the cyberthreat landscape changed in India?

During the initial years after the enactment of IT Act 2000, police officers would typically receive complaints related to identity theft and phishing attacks. However, these days, a sizable number of complaints are about circulation of fake photos/videos on social media with malicious intention as well as of fake call centres trying to cheat people in India and abroad through phishing calls.

Here, we should also be mindful of the fact that FIRs registered with the police may not be a real indicator of the cyberthreat scenario in India, as many of the bigger frauds and scams committed by organised white collar criminals are not being reported to the police for various reasons.

Q 2: What are some of the key reasons for the growing cybercrime incidents in India?

In the absence of integrated databases of individuals, it is easy for cyber criminals to hide their identity. Cyber criminals can manage to open bank accounts and obtain mobile SIM cards under fake identities. Currently, the whole nation is adopting more and more digital platforms without having real understanding of threats and vulnerabilities of these media. Also, many top service providers (Read: Email Service Providers, Social Media Platforms and Cloud Service Providers, etc.) are based outside India, who are not extending their fullest cooperation to the Indian Law Enforcement Agencies.

Q 3: How far have the law and the sub ordinate legislations kept pace with the emerging cybercrime scenario?

The IT Act 2000 was introduced in India primarily to facilitate e-commerce by making e-contract legally valid and enforceable by adjudicating courts. There was a small section on cybercrime, which was expanded a bit in the IT (Amendment) Act 2008. But what we need today is a comprehensive Cyber Crime Penal Code on the lines of developed countries. Along with penal act, we also need a matching procedural law to make prosecution of cyber criminals easy and fast. At present, there is a lot of ambiguity on admissibility of digital evidences produced by police and prosecution.

Q4: What is your take on the preparedness of law enforcement authorities (LEAs) in India to contain and investigate cybercrimes?

I think Indian LEAs have responded well to this latest challenge and by now, almost all the states have set up Cyber Police Stations for handling hi tech crime cases exclusively. Our Investigating Officers also learned tit bits of cybercrime Investigation on their own without any formal training for skill development in this field. Government Examiners of Questioned Documents of various

The views and opinions expressed herein are those of the interviewee and do not necessarily represent the views of KPMG in India.

Central Forensic Science Labs also rose to the occasion by learning Digital Forensics on their own and gave statutory 'Expert Opinion' for successful prosecution of the offenders in various courts.

However, we are facing various challenges as well. For example, in the last decade, Indian LEAs have depended heavily on metadata of mobile telephones to crack criminal cases. However, with the advent of VoIP and with high internet penetration, we need to upgrade ourselves to 'digital forensics' to collect evidence as internet metadata may not be that useful from an investigation point of view. At present this domain is completely vendor driven and tool based. We need to improve our skills so that we can use these hardware and software tools optimally.

Q 5: What are the key steps you foresee to improve the preparedness of the Indian Criminal Justice System to improve detection and conviction in technology induced crime.

So far all the agencies of the Criminal Justice System have unilaterally responded to this newly discovered menace. As a way forward, we need a well conceptualised skill development programme for all Investigation, Prosecution and Adjudication agencies and proper procedural framework among all stakeholders to bring cyber criminals to the book.

Since cybercrime is here to stay, the key stakeholders dealing with cybercrime need to understand this subject properly. To achieve this, we need a massive capacity building exercise during their induction and mid-career training programmes.

Also, there is a need to raise special cadres of Computer Crime Investigators and Digital Forensics Experts with IT background as the whole world is going paperless and entire communication trail is available only in digital forms. Investigation agencies of developed countries have already started recruiting Computer Science graduates in large numbers. Now, it is our turn.

Q6: How according to you, the corporate sector can contribute to improving cybersecurity preparedness in India?

Requirements of Law Enforcement Agencies are quite different from corporates. However, because of their better exposure to advanced technology, the corporate sector can be of great help in filling the skill gap among government officials.

In this regard, it would be helpful if the corporates bring customised solutions suitable for our environment. So far, they are simply importing solutions from outside and offering it to Indian LEAs as it is. These solutions are not only very costly but also do not meet our requirements fully.

73 per cent of cybercrimes reported were with respect to ATM/card thefts.

80 per cent of LEAs have demanded strengthening cyber laws in India.

Only 29 per cent of LEAs feel that adequate measures have been taken to improve cybersecurity awareness.

43 per cent of LEAs find it challenging to identify where to report an incident when it comes to cross border cybercrimes.

64 per cent of LEAs feel that the number of cybercrime cells in the country should be increased.

65 per cent of LEAs are of the opinion that a central reporting mechanism will enable an effective response to cybercrimes.

The views and opinions expressed herein are those of the interviewee and do not necessarily represent the views of KPMG in India.

Changing the regulatory landscape

While organisations are gearing up to strengthen their defences against cyberattacks, cyber laws and regulations also play a very important role in helping organisations tackle cyber risk.

On one side a well-structured law enforcement system can act as a deterrent to cybercrimes and simultaneously having a strong regulatory framework can provide organisations with robust cybersecurity controls.

Are LEA adequately prepared to tackle problems related to cybercrime?

73% No

20% Not sure

7% Yes

"Considering the multi-disciplinary needs to handle cybercrimes, the Law Enforcement Authorities in India are constantly on the roll. Upgradation of our technical infrastructure and requisite cybercrime investigation skillsets are currently high on our agenda."

Balsing Rajput
Superintendent of Police (Cyber), Maharashtra
Chevening Fellow on Cyber security

Changes in the regulatory framework in India in recent times

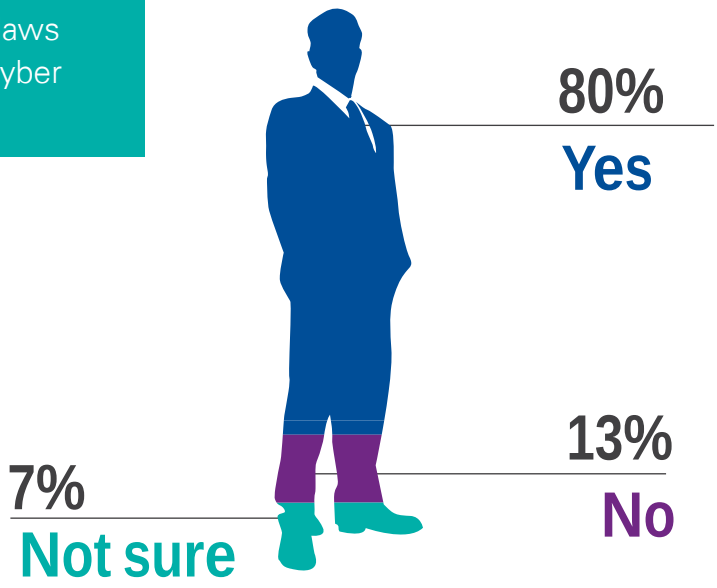
India is embracing technology at a break neck speed with increased usage of digital transactions, technological platforms, e-commerce and social media. Technology and innovation are key drivers to economic growth and development in India with an array of initiatives by the Indian government such as 'Digital India' and 'Make in India' which aim to transform India into a technology driven and digitally empowered nation through the use of investments and skill development programmes.

With a transition to digital economy, India is now also a target for cyber criminals and hackers with large amount of consumer data stored digitally at their disposal. It is a big challenge for organisations and people now to protect their assets against cyberattacks. Many organisations in India are now aware of the challenges of cybersecurity and have taken steps to build resistance against cybersecurity threats like implementing global best practices, creating frameworks, encouraging open standards and promoting cyber resilience. Some of the recent circulars released by RBI, financial institutions like SEBI (Securities and Exchange Board of

India) and IRDAI and other regulators that talk about cybersecurity framework and cyber resilience are:

1. **Banking/Financial Sector** - RBI has come up with a notification on 'Cyber Security Framework for Banks' on June 2016, which recognises the growing cyberattacks in the banking sector and provides guidelines to combat cyberthreats.
2. **NBFC sector** – RBI has released a circular on 'Information Technology Framework for the NBFC Sector' on June 2017, which provides guidelines to implement cybersecurity framework.
3. **Insurance sector** - IRDAI has released a circular on 'Guidelines on Information and Cybersecurity for Insurers' on April 2017, which highlights the importance of a comprehensive framework for information and cybersecurity.
4. **Stock Exchanges, Clearing Corporation and Depositories** – SEBI has released a circular on 'Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories' on July 2015, which provides guidelines to implement cybersecurity and cyber resilience framework.
5. **Issuer and Share Transfer Agents** - SEBI has recently released a circular on 'Cyber Security and Cyber Resilience framework for Registrars to an Issue/Share Transfer Agents' on September 2017, which speaks of the need to strengthen its cybersecurity and cyber resilience framework by identifying critical IT assets and risks associated with such assets and recover from incidents through incident management and business continuity framework.
6. **Department of Telecommunications (DOT)** – Department of Telecommunications has issued general guidelines on May 2017, for securing information and sensitive personal data or information in compliance with the Aadhaar act. These guidelines give information on awareness trainings, authentication mechanism and storage of information.
7. **Power** - Central Electricity Authority (Ministry of Power) have established a four sectorial CERTs under the Ministry of Power for reviewing the needs of cybersecurity in critical infrastructure sector.

Is there a need to strengthen laws to prevent cyber terrorism?



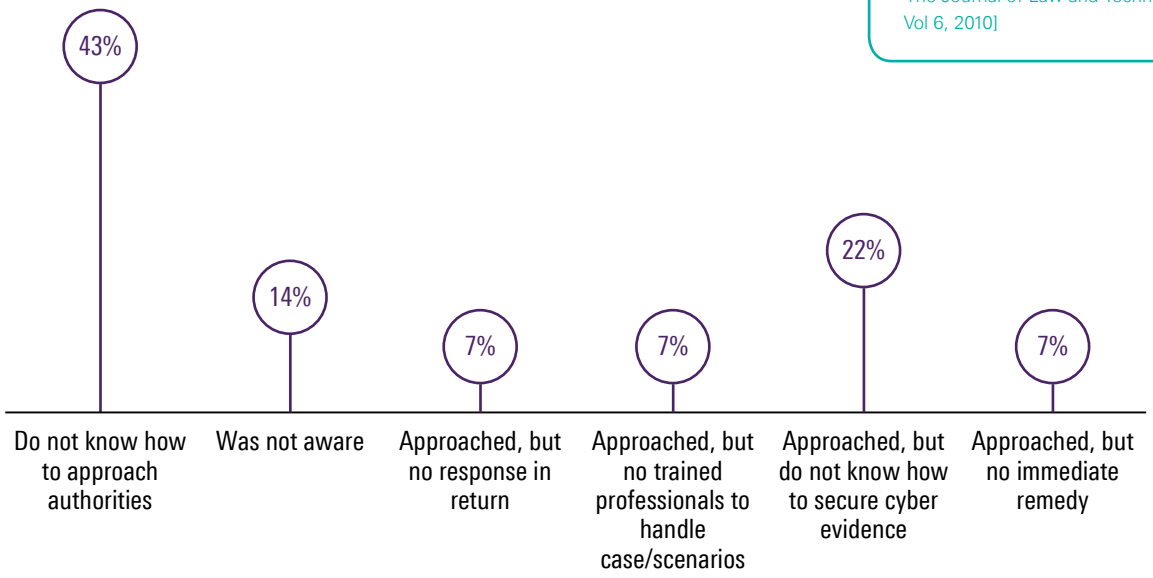
Cybercrime is a threat that has proliferated across industries and regulators in conjunction with law enforcement agencies play an important role.

Many companies do not report cyberattacks as

- **29 per cent** of companies do not feel the incident is serious enough to report to a law enforcement agency.
- **12 per cent** of companies are worried of the negative publicity and would like to protect their brand and reputation.

Cyber by nature is not bound by geographical boundaries and that is causing this crime to be borderless. In case of a trans-border cyberattack, 71 per cent of organisations believe that they find it challenging to identify where to go and report the crime. 57 per cent of law enforcement agencies said that they are facing the same challenge.

> "The traditional approach to jurisdiction invites a court to ask whether it has the territorial, pecuniary, or subject matter jurisdiction to entertain the case before it. With the internet, the question of territorial jurisdiction gets complicated largely on account of the fact that the internet is borderless."
>
> **Hon. Justice S. Muralidhar**
> Judge, High Court of Delhi
>
> ['Jurisdiction Issues in Cyber Space' - The Journal of Law and Technology, Vol 6, 2010]

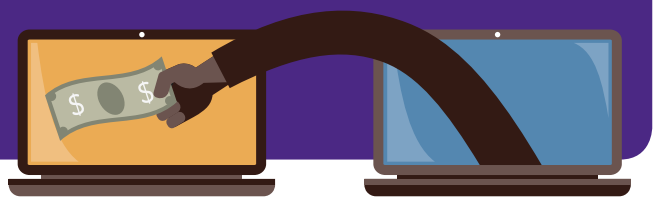


56 per cent of corporates have expressed that the government agencies are inadequately prepared to handle cybercrime.

36 per cent of organisations are unaware of the different rules and services provided by the Government of India for reporting of cyber incidents.

54 per cent of end users believe government agencies are not adequately equipped to handle cybercrime, incident response and cybersecurity related issues.

Business ecosystem – third parties



The outsourcing of business and IT operations come with their share of risks. Key security risk is due to the fact that the organisations do not have a firm control over the controls and policies followed by contractors and third party vendors.

Case study #01

Impact of debit card data compromise across multiple banks.

What: Debit card information of patrons was compromised, it resulted in unauthorised money withdrawal and misuse of customer information.

Why: Payment network managed by third party completely. This network got infected with malware leading to data/system compromise.

Case study #02

A global telecom giant suffered a data breach

What: The personal data of over 150,000 customers including their names, addresses, dates of birth, phone number and email addresses was hacked by an attacker. In this case, the bank account details were also stolen. Most of the customers complained of receiving several spam calls.

Why: Weak configuration of customer database. This database was part of the companies' acquisition of another organisation way back in 2009. The data was accessed through an attack on three vulnerable webpages within the inherited infrastructure. An investigation revealed that employees at one of their third party suppliers used the online company portal to access large amount of customer data.

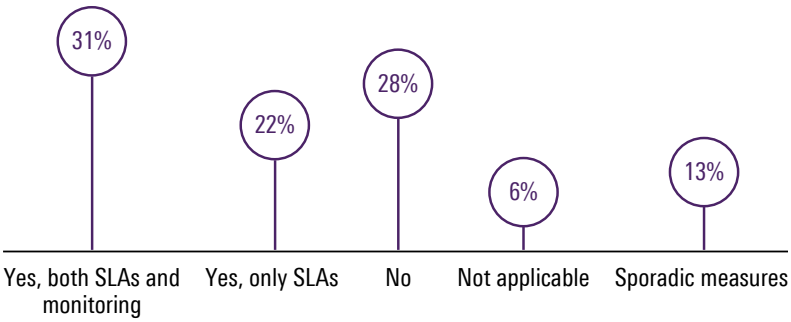
*KPMG in India's analysis, 2017, based on secondary research

48 per cent of the organisations stated that cybersecurity risk assessment needs to be further enhanced to mitigate the risks related to outsourcing.

Only **31 per cent** of the organisations have indicated that there are defined Service Level Agreements (SLAs) and monitoring of vendor systems to detect a data breach.

61 per cent of the organisations rely on third party risk assessment by an internal team, while only **18 per cent** said that they rely on the assessments performed by an external team.

58 per cent of the organisations stated that they cannot claim damages from the third party with respect to security breaches caused by them.

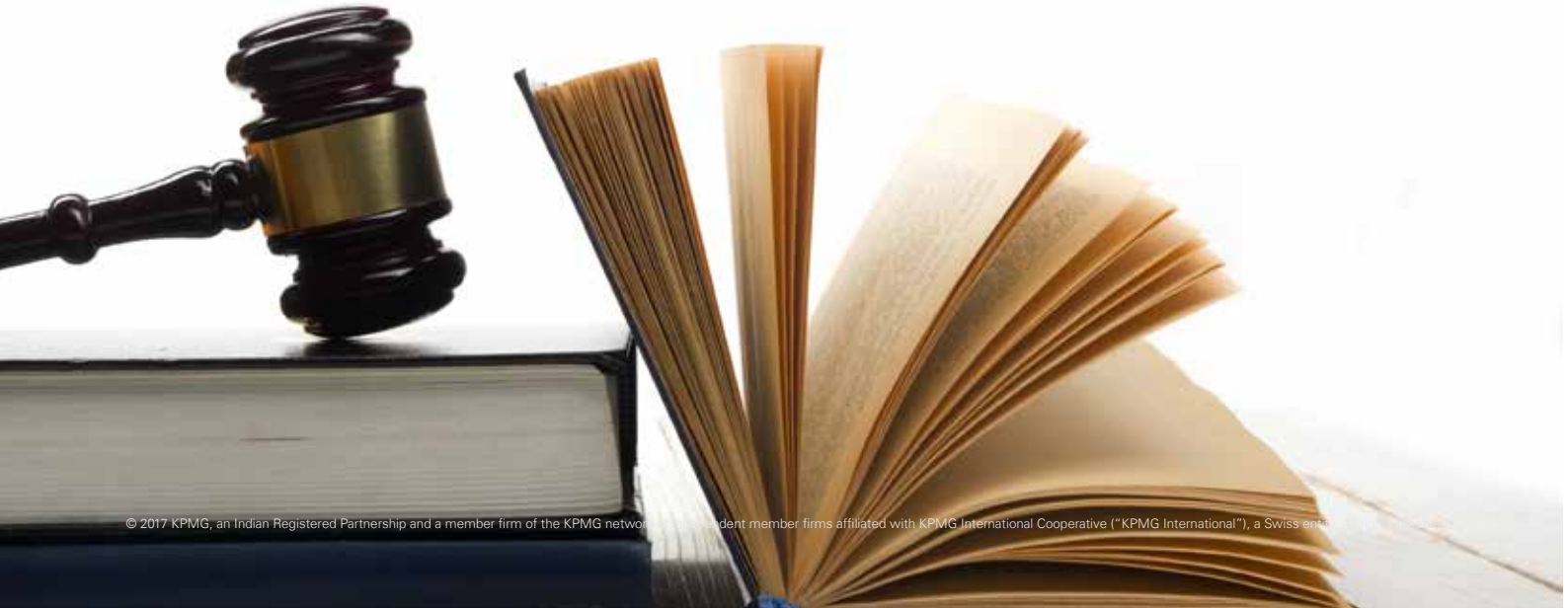


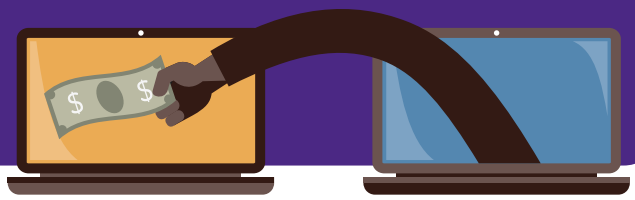
Regulations for managing third party risks

Outsourcing brings several risks such as operational risks, strategic risks, reputation loss, and systemic risks. RBI has come up with a set of guidelines for banks to manage third party and outsourcing related risks. According to RBI, banks must ensure that outsourcing does not result in internal controls being compromised. Some of the guidelines are:

- Banks should not outsource core management functions like management and corporate planning.
- It is important to follow due diligence in relation to third party risks like considering laws, regulations and guidelines regarding approval, registration and licensing.
- The contingency plans based on risk scenarios must be in place and tested regularly.
- Periodic onsite review should take place for the outsourced arrangements to identify risks related to outsourcing.

Other regulatory bodies across the globe have also started specific regulations/guidelines for outsourcing organisations. Following are some key regulations with respect to outsourcing:

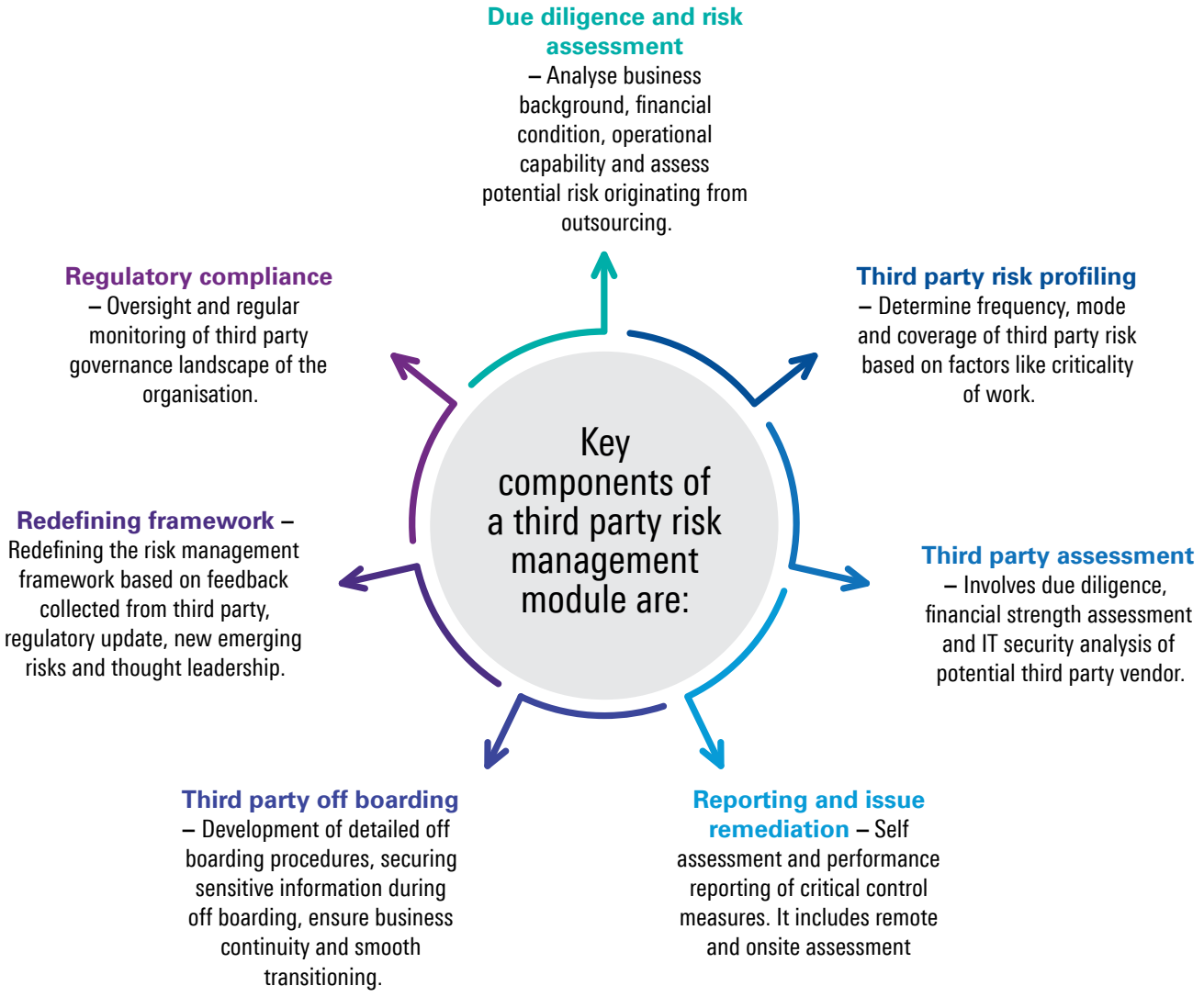




Third party risk management

A proactive third party risk management module helps in identifying, accessing and mitigating risks arising due to third party vendors and outsourcing. Third party risk management includes designing/redefining a third party risk management framework, conducting due diligence and risk assessment of third parties, self-assessment review and onsite assessment and issue remediation.

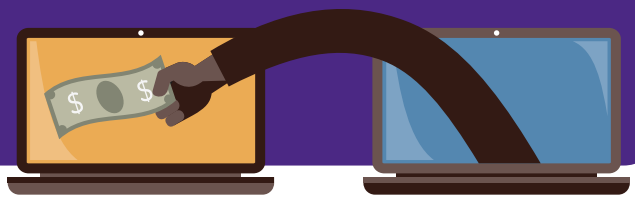
There are several challenges related to third party risk management because of failure to properly understand the risk and cost associated with managing it, lapse in ongoing monitoring and due diligence hence there are various third party assessment tools which help in evaluation of third parties by providing a baseline for assessment of outsourcing provided.



Country-wise third party/outsourcing key regulations/guidelines

Country	Regulator	Name of regulation/guideline
Singapore	MAS[1]	Singapore - MAS Guidelines on Outsourcing
	MAS[1]	Singapore - MAS Technology Risk Management guidelines
Hong Kong	HKMA[2]	Supervisory Policy Manual - TM-G-1 - General Principles for Technology Risk Management
		Supervisory Policy Manual - SA-2 – Outsourcing
	HKMA[2]	HKMA- Circular on Customer Data Protection
	HKMA[2]	HKMA Compliance Assessment Form on Technology-related Outsourcing Project
	HKMA[2]	HKMA Compliance Assessment Form on Technology Outsourcing to Public Cloud
Australia	APRA[3]	Australia - Prudential Standards CPS 231 Outsourcing – 2017
	APRA[3]	Australia - Outsourcing Involving Shared Computing Services
China	CBRC[4]	Guidelines for supervision over Information Technology Outsourcing Risks
	CBRC[4]	Guidelines on the Management of Outsourcing Risks of Banking Financial Institutions
	CBRC[4]	Opinions of Shanghai Branch of China Banking Regulatory Commission on Strengthening the Supervision over the Outsourcing of Foreign-funded Banks in Shanghai Municipality
	CBRC[4]	Notice of the General Office of China Banking Regulatory Commission on Strengthening Banking Financial Institutions' Risk Management of Non-Stationed Concentrative Outsourcing of Information Technology
	PSBC[5]	Notice on Issues Relating to Proper Protection of Personal Financial Information by Financial Institutions in Banking Industry
Japan	FSA[6]	Comprehensive Guidelines for Supervision of Major Banks
	JFSA[6]	JFSA Guidelines for Supervision
Luxembourg	CSSF[7]	CIRCULAR CSSF 12/552 - Central administration, internal governance and risk management
	CSSF[7]	CIRCULAR CSSF 15/611 - Managing the risks related to the outsourcing of systems that allow the compilation, distribution and consultation of management board/strategic documents
	CSSF[7]	CIRCULAR CSSF 06/240 Administrative and accounting organisation; IT outsourcing and details regarding services provided under the status of support PFS
	CSSF[7]	Grand-Ducal Regulation of 13 July 2007 relating to organisational requirements and rules of conduct in the financial sector
	CSSF[7]	Law of 5 April 1993 on the financial sector

1. http://www.mas.gov.sg/
2. http://www.hkma.gov.hk/eng/index.shtml
3. http://www.apra.gov.au/Pages/default.aspx
4. http://www.cbrc.gov.cn/english/index.html
5. http://psbc.com/en/index.html
6. http://www.fsa.go.jp/en/
7. http://www.cssf.lu/en/



Country	Regulator	Name of regulation/guideline
Swiss	FINMA[8]	FINMA Circular on Outsourcing
United Kingdom	FCA[9]	FCA - PRA Outsourcing (SYSC 8)
	FCA[9]	FCA - Guidance for firms outsourcing to the 'cloud' and other third-party IT services
	FCA[9]	FCA Considerations for firms thinking of using third-party technology (off-the-shelf) banking solutions
	FCA[9]	FCA - PRA Outsourcing (SYSC 13.9)
	PRA[10]	Prudential Regulation Authority Rulebook Part 1 Outsourcing
	MiFid[11]	MiFID II legislative text SECTION 2 OUTSOURCING
Germany	BaFin[12]	BaFin - Circular 10/2012: Minimum Requirements for Risk Management (MaRisk BA)
United States of America	FED[13]	Federal Reserve Guidance on Managing Outsourcing Risk
	FDIC[14]	FDIC GUIDANCE FOR MANAGING THIRD-PARTY RISK
	FFIEC[15]	FFIEC Booklet Outsourcing Technology Services
	OCC[16]	OCC Bulletin 2013-29 Third Party Relationships
	FINRA[17]	NASD Notice to Members - JULY 2005
	FFIEC Appendix J[18]	FFIEC BCM Booklet Appendix J: Strengthening the Resilience of Outsourced Technology Services

8. https://www.finma.ch/en
9. https://www.fca.org.uk/
10. http://www.bankofengland.co.uk/pra/Pages/default.aspx
11. https://www.fca.org.uk/markets/mifid-ii
12. https://www.bafin.de/EN/Homepage/homepage_node.html
13. https://www.federalreserve.gov/
14. https://www.fdic.gov/
15. https://www.ffiec.gov/
16. https://www.occ.treas.gov/
17. http://www.finra.org/
18. https://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-j-strengthening-the-resilience-of-outsourced-technology-services.aspx

* Information accessed as on 30 November 2017

Cyber response and recovery mechanism

Cyber incident response has emerged as one of the key areas where organisations need to focus to protect their critical infrastructure. Incident response requires a combination of technical preparedness (tools and technology) along with implementation of right processes, with defined roles and responsibilities. There are four main components of an incident response plan which include:

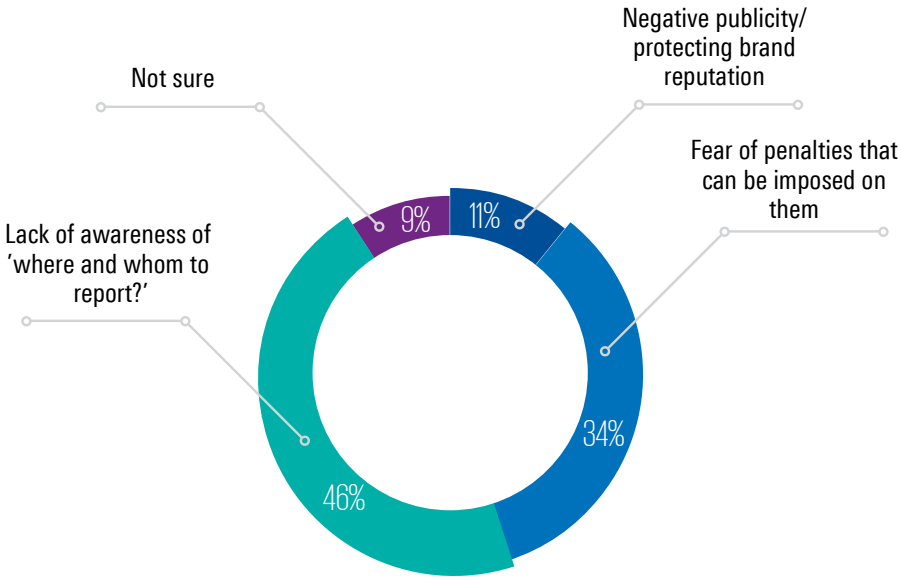
- Policy, definition and scope
- Incident assessment and reporting
- Incident countermeasures
- Identifying and monitoring corrective actions

Cyber incidents in organisations

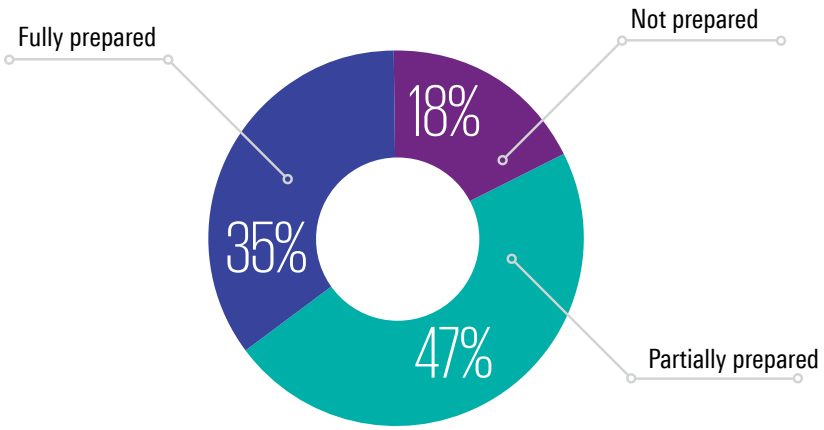
According to the 46 per cent of end users, lack of awareness is the main reason of incidents not being reported by employees, while 34 per cent said that on account of fear of penalties, they refrain from reporting the cyber incidents.

18 per cent of the surveyed organisations say that they are prepared for a large scale cyberattack which is a key concern. With the constant rise in cybercrime and its impact, identifying key assets and protecting them is extremely important. The enterprises need a layered defence and a cyber-intelligence programme to combat bigger scaled cyberattacks. This can ensure quick recovery from the attack and bare minimum loss.

Reasons for not reporting cyber incidents in organisation



Organisation's preparedness to handle large-scale cyberattacks



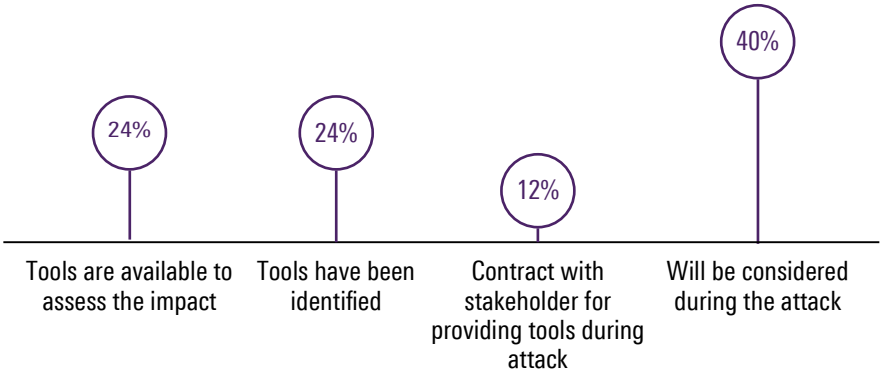
Recovery and response

With the constant increase in cybercrime and its impact, it is important for organisations to identify key assets that need to be protected. **42 per cent** of the organisations have setup an emergency response team, while **36 per cent** of organisations possess cyber forensic and investigation skills internally. Enterprises need to carry out cyber risk assessment in depth to ensure that the right assets are adequately protected to limit the impact of attacks.

24 per cent of organisations have identified tools to assess the impact of a cyberattack. **40 per cent** of organisations say that they will consider the tools required during the attack. This can be too late to curtail the extent of damage.

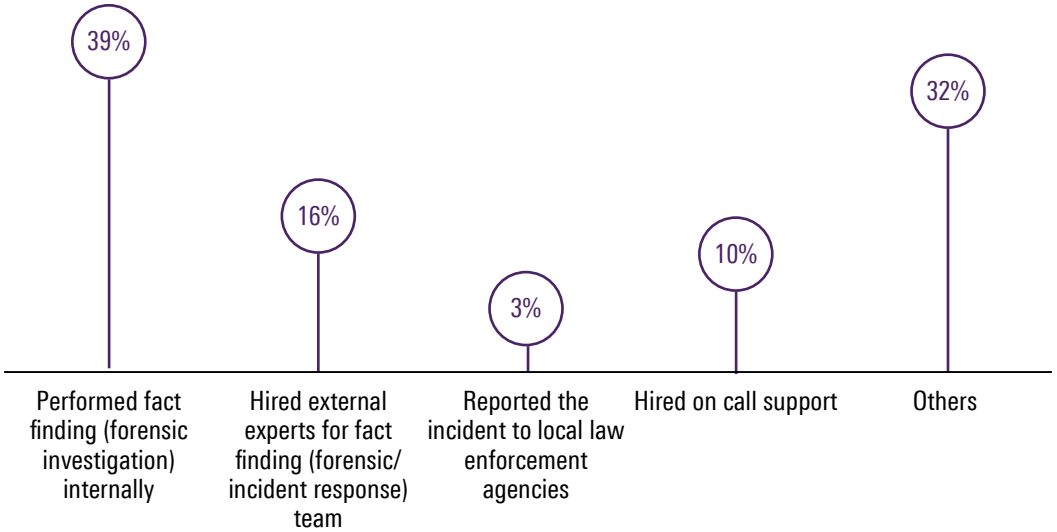
One of the key aspects of cyber crisis management is rehearsing and practicing. Current cybercrime attacks have led to formation of enterprise-wide special teams which require trainings like business continuity, incident management, cybersecurity drills and crisis management exercises. Cybersecurity drills must be conducted to test the effectiveness of a crisis management plan and improve cyber intelligence.

Use of tools for response & recovery



Measures post a cyberattack

66 per cent of the organisations indicated that they are aware of the legal impact due to cybersecurity related incidents. However, 34 per cent said that they do not know the mechanisms put in place to address such legal risks. Further, only 3 per cent said that they have reported a cyber incident to a law enforcement agency after becoming aware about it.



Cyber preparedness - new age technology

Preparedness for cyberattacks extends beyond having the right leadership, budget, staff, framework and governance in place. One critical aspect of an effective cybersecurity strategy is a commitment to enhancing cyber awareness, education and training across the organisation.

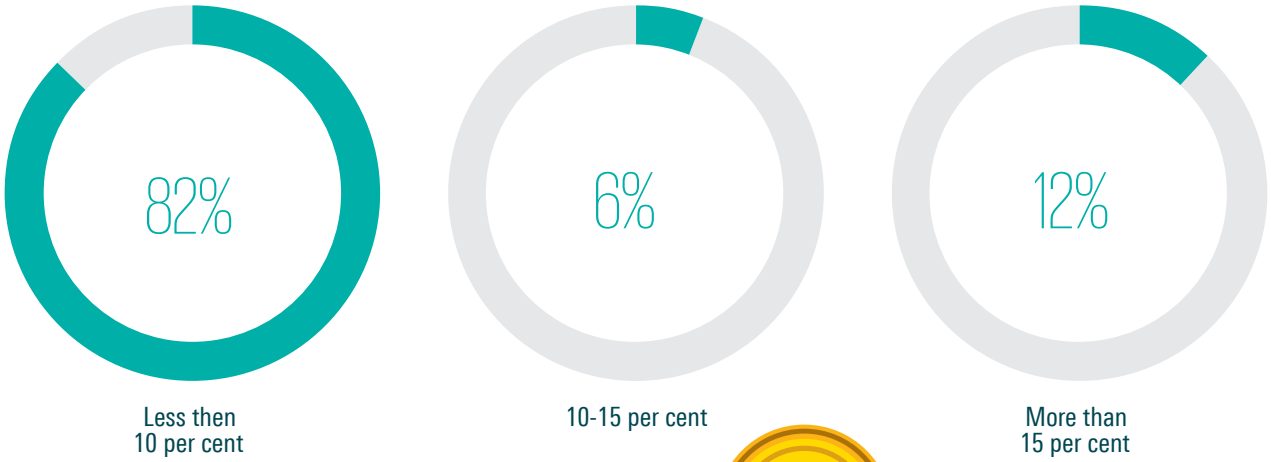
The move to a digital world dominates the enterprise planning cycle, and is key to most major business initiatives. For the organisations to move to a safer and more sustainable place in the digital world, it is necessary to apply a cyber risk lens to everything you do.

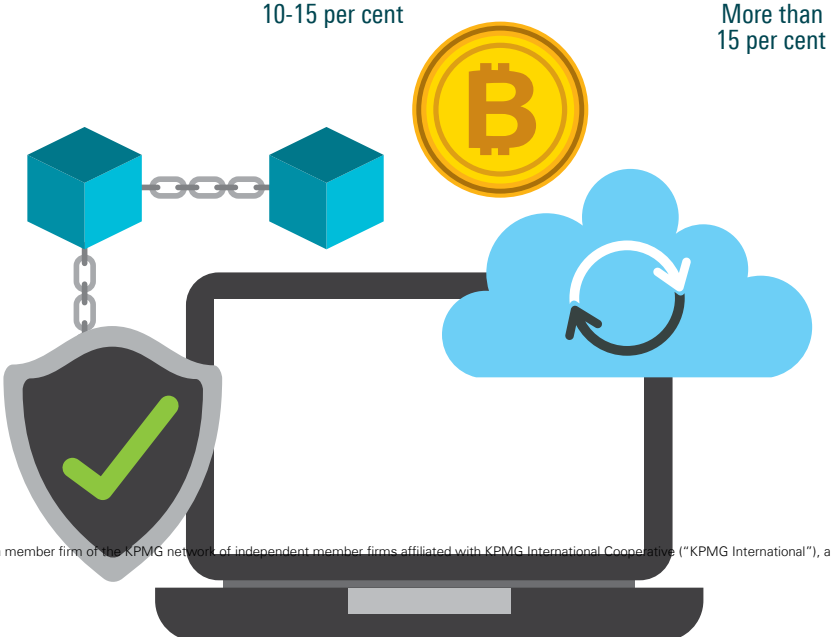
Organisations today need to understand that cyber risks are not just IT or security risks – they are business risks and have the potential to slow down, or shut down the business entirely. The pace of emerging/new technology being adopted/changing is very high. In this scenario, traditional risk assessments of these emerging/new technologies will not suffice. Hence, most of the organisations have adopted 'Security-by-Design' approach. Security by Design approach imbibes cybersecurity as part of normal business operations rather that just as add on.

According to organisations, some of the top emerging technologies used by them include cloud (79 per cent), mobility (91 per cent), social media (90 per cent), big data analytics (39 per cent) and robotics (26 per cent).

67 per cent of the organisations in India believe that user awareness and training is a major risk related to the adoption of emerging technologies. However, at least 65 per cent of them are already using one of the top four emerging technologies. Even though user awareness and training is considered as top priority, 82 per cent of the organisations with a budget of less than 10 per cent for cybersecurity are not willing to invest enough money on emerging technologies.

Investment in emerging technologies vis-a-vis cyber budget





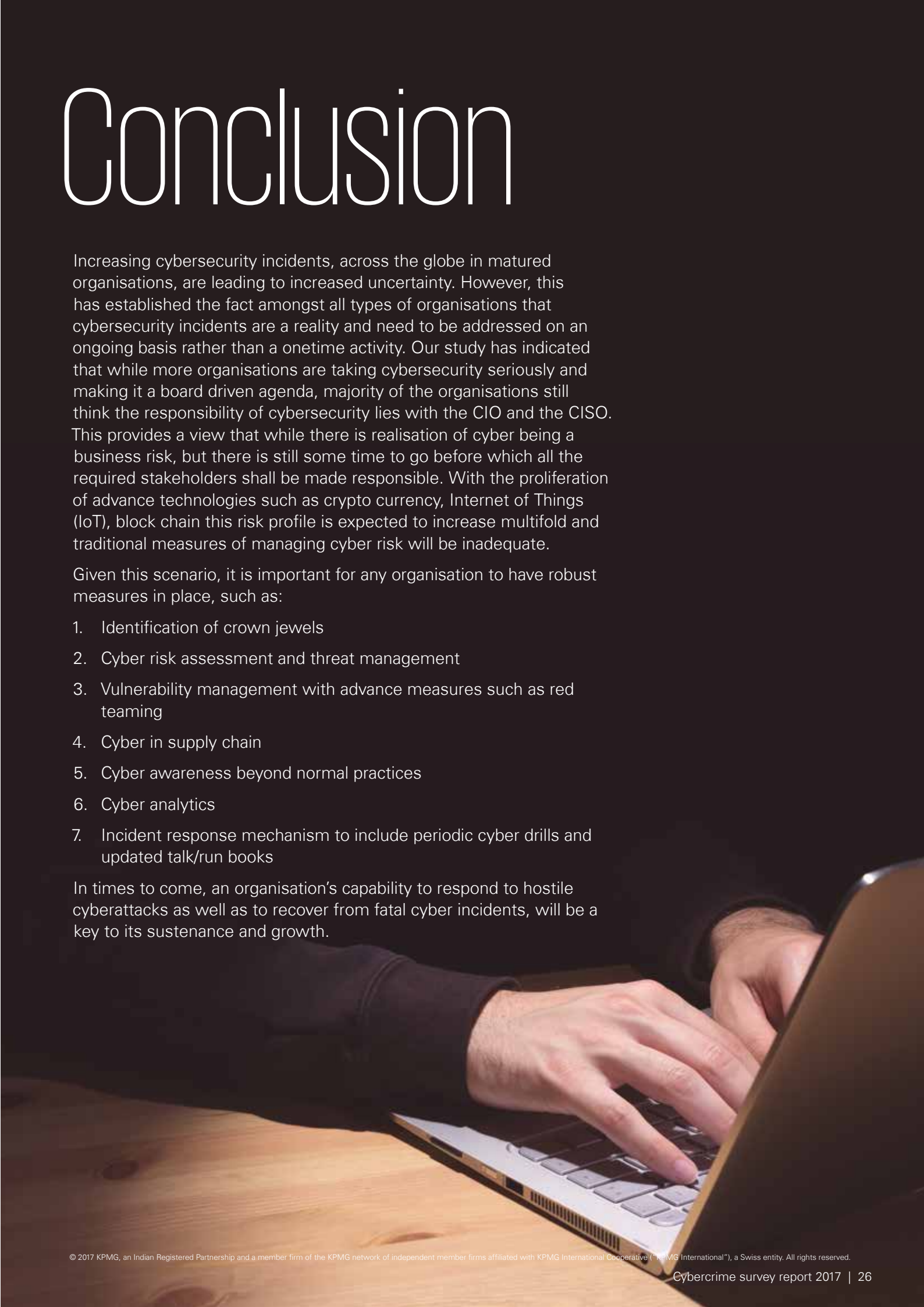
Conclusion

Increasing cybersecurity incidents, across the globe in matured organisations, are leading to increased uncertainty. However, this has established the fact amongst all types of organisations that cybersecurity incidents are a reality and need to be addressed on an ongoing basis rather than a onetime activity. Our study has indicated that while more organisations are taking cybersecurity seriously and making it a board driven agenda, majority of the organisations still think the responsibility of cybersecurity lies with the CIO and the CISO. This provides a view that while there is realisation of cyber being a business risk, but there is still some time to go before which all the required stakeholders shall be made responsible. With the proliferation of advance technologies such as crypto currency, Internet of Things (IoT), block chain this risk profile is expected to increase multifold and traditional measures of managing cyber risk will be inadequate.

Given this scenario, it is important for any organisation to have robust measures in place, such as:

1. Identification of crown jewels
2. Cyber risk assessment and threat management
3. Vulnerability management with advance measures such as red teaming
4. Cyber in supply chain
5. Cyber awareness beyond normal practices
6. Cyber analytics
7. Incident response mechanism to include periodic cyber drills and updated talk/run books

In times to come, an organisation's capability to respond to hostile cyberattacks as well as to recover from fatal cyber incidents, will be a key to its sustenance and growth.



Acknowledgements

We would also like to acknowledge the core team from KPMG in India who worked extensively in preparation of this compendium:

Arzan Elchidana
Ishita Mogra
Iqra Bhat
Jatin Rishi
Jaya Srivastava
Mubin Shaikh
Namrata Mehta
Neha Randive
Pushkar Bakore
Rahil Uppal
Ravindranath Patil
Sasha Arora
Sharon Dsilva
Yaminee Nahar

KPMG in India contacts:

Mritunjay Kapur
National Head, Markets & Strategy
Head - Technology, Media & Telecom
T: +91 124 307 4797
E: mritunjay@kpmg.com

Akhilesh Tuteja
Partner and Head
Risk Consulting
Co-leader – Global Cyber Security
T: +91 124 307 4800
E: atuteja@kpmg.com

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

Atul Gupta
Partner
IT Advisory
Leader – Cyber Security
T: +91 124 307 4134
E: atulgupta@kpmg.com

Sudesh Anand Shetty
Partner
Risk Consulting
T: +91 226 134 9703
E: sashetty@kpmg.com

Follow us on:
kpmg.com/in/socialmedia