Over the last few years, there has been an exponential rise in targeted cyber-attacks which are aimed at financial gain. Many small and large enterprises have reported phishing attacks, where hackers used ‘spoofed’ emails and fraudulent invoices that appear to be sent from known sources such as the email accounts of their Chief Executive Officer, Chief Financial Officer etc. This convinced the employees to transfer funds to the hacker posing as a genuine vendor. The modus operandi by hackers is also growing in sophistication, frequency and extending beyond geographical boundaries, making it complex to track and sometimes even remediate.

Incidents around ransomware, a type of malware were also noticed in India last year. Newspapers reported multiple cases impacting public and private enterprises as well as individuals who lost critical data due to the ransomware infection. The malware encrypted the data and hard drives of infected computers; this practically meant data loss for the companies unless they paid the demanded ‘ransom’ to the hackers which was typically in the form of Bitcoins.

Data breach incidents and DDoS (Distributed Denial of Service) attacks also made headlines worldwide, however, these are mostly large, global companies and Internet Service Providers (ISPs) which saw a significant loss of revenue or customer information. Relatively smaller incidents have often gone unreported and steered clear from the public eye. But they usually keep the security teams of these corporations and their C-suite quite overwhelmed, which is largely due to the volume of attacks. The pile of log data generated by these mass attacks is sizeable, making security teams rely primarily on big data analysis tools to help them. This approach has been exploited by hackers, who hide their ‘main’ attack in the barrage of low level incidents. This ‘main’ attack is tailored for the specific company and tends to go undetected by the typical ‘off the shelf’ security solutions.

The financial loss suffered from cyber incidents mentioned before can be substantial. It can also lead to bigger risks such as disruption in business continuity, loss of reputation and customer trust, which can be detrimental, especially for industries that rely heavily on data and intellectual property. These include sectors such as Information Technology (IT), e-commerce and retail, financial services and pharmaceuticals.

Today, a company’s ability to deal with such situations effectively is a priority but at the same time, it can be difficult due to the nature, complexity and volume of cyber incidents.

The country is rapidly moving towards a digital economy and will become a hotbed for global cyber criminals. Increasing adoption of digital banking, wallets, mobile banking are some areas that might attract targeted attacks from cyber criminals.

What could separate the better prepared company from the rest could be their ability to predict the impact of an incident, after it is discovered. In line with this, our report attempts to answer the question, are businesses operating in India ready to deal with cybercrime incidents?
Cyber-attacks around the world continue to escalate in terms of frequency and intensity, becoming a profound issue for companies today. Most cybercrime incidents that took place last year spiked the emergence of a new set of cybercriminals, whose aim was not only financial gain but also causing disruption to the public and nation at large. Another interesting feature of these incidents was that not only corporates but also the Government were attacked by cybercriminals. Thus, the threat from cybercrime is multi-dimensional, targeting citizens, corporates and the Government at an alarming rate.

To better address this issue and enhance the security of digital transactions, and the overall cybersecurity environment in India, the Government made a substantial announcement in the Union Budget 2017. The establishment of a Computer Emergency Response Team known as CERT-fin for the financial sector was a step in that direction. Recent media reports also suggest that adequate budgets will be allocated for cybersecurity-related initiatives, which, if made, could help in deterring cases of cyber incidents in India to a large extent. On the other hand, the Reserve Bank of India (RBI) has also been taking steps to ascertain a secure digital atmosphere by stressing on data sharing and cyber intelligence for banks, which is one of the most vulnerable sectors to digital fraud today.

Furthermore, numerous other factors such as increased public awareness, the Government’s commitment on delivering the assurance of ‘Digital India’ and a push toward becoming a cashless economy have further prompted companies to safeguard their critical assets by investing in cybersecurity measures. Thus, a joint effort by the Government, banks, corporates and individuals in setting up cybersecurity measures can help in achieving the nation’s cybersecurity objectives. The aim is to set up pre-emptive measures for damage control before it turns out to be a nightmare for one and all.

The aim of this report is to stress on the importance of creating a robust cyber incidence response mechanism to better equip India Inc. in combatting cyber-attacks in a more streamlined manner.

Brijesh Singh, IPS
Inspector General - Cyber, Maharashtra
One fifth of the survey respondents stated that employees are one of the weakest link in the company’s defence mechanisms against data theft, system tampering or DDoS.

However, more focus is still toward mitigating attacks from unknown hackers. Therefore, companies should focus their efforts to manage both insider risks as well as external threats.

The survey revealed that only 29% of the companies mentioned approaching specialists to assist them.

Cyber incidents are growing at an alarming rate in India. However, a little more than one third of the survey respondents have been able to detect these incidents effectively.

Most companies approach the team which is easily accessible to them for help rather than a specialist to deal with cybercrime incidents.

The trend shows that companies approach a team which is available and accessible post a cyber incident. More than 70% approached the existing IT team to investigate the matter if there was a cyber breach. In terms of functioning, these teams are typically mandated to handle the overall IT processes. Surprisingly, none of the companies listed their public relations or legal functions in the list of priority teams they would approach once a breach is detected.

The survey highlights that most companies tend to approach the local cyber cell and police station for filing an FIR and seeking assistance with the investigation.

Currently, disclosing a cyber breach is not mandated by the law in India, hence the legal and regulatory framework may need to be redefined to deal with increasing volumes of cases. This would be critical as reliance on technology grows with initiatives such as ‘Digital India’.

Companies are unable to detect incidents effectively and are being held back due to low understanding of the motive of the attack.

This means that a majority (about two third) of businesses were unable to detect a cyber incident and could result in serious repercussions for their internal and external stakeholders. Companies operating in India would therefore need to better equip themselves to not just detect these incidents but also do so quickly, i.e. within 24 hours of an incident.

34% believe that the laws and regulations are not clear.

Currently, disclosing a cyber breach is not mandated by the law in India, hence the legal and regulatory framework may need to be redefined to deal with increasing volumes of cases. This would be critical as reliance on technology grows with initiatives such as ‘Digital India’.

Significant time spent in approaching local authorities and ISPs.

The survey highlights that most companies tend to approach the local cyber cell and police station for filing an FIR and seeking assistance with the investigation.

55% respondents said that there is a need for stringent laws around cybercrime, which need improvement.

Employees are the second largest source of incidents after unknown hackers.

Executive summary
40% of the respondents believe their techniques around proactive monitoring of cybercrime are effective.

44% of the respondents have robust data protection programs.

However, 72% of respondents believe their IT security teams do not have enough specialists to deal with cybercrime incidents.

As per a McAfee report\(^1\), India is estimated to be losing 0.21% of its GDP to cybercrime and the numbers of incidents are increasing each year.

These incidents take place due to gaps in the existing defence mechanisms. The role of investigators would be crucial in helping companies strengthen their defences against advanced cybercrime risks, which are either undetected or not diagnosed accurately. Companies also would have to look at more advanced techniques to combat cybercrime and invest more in diagnostics programs, cyber threat intelligence and incident response. The quality of investigation feeds back into the company’s cyber defence strategy in terms of loop holes exploited by the hacker during an incident. If the investigation is not concluded properly then such loop holes may never get discovered.

Social media emerges as a big risk area

Most of the respondents (almost 90%) unanimously identified social media as a big risk from a cybercrime perspective. This is fuelled by the fact that social media will be an important part of their company’s technology footprint and they need to be prepared in dealing with the risks associated with this channel.

Employees post extensive details regarding their work profile on social networking websites. These social media platforms act as a gold mine for cybercriminals to identify and target key individuals for a successful breach.

Companies believe that their processes are capable of dealing with cybercrime incidents however the quality of staff needs improvement

Trainings and mobile technologies took the top two slots in terms of investments going forward. Investments around detection and investigation of cybercrime incidents were at the bottom of investment priorities.

with less than 50% of respondents planning to increase spend on these.

Companies need to invest more in investigative capabilities

44% of the respondents have robust data protection programs.

However, 72% of respondents believe their IT security teams do not have enough specialists to deal with cybercrime incidents.

As per a McAfee report\(^1\), India is estimated to be losing 0.21% of its GDP to cybercrime and the numbers of incidents are increasing each year.

These incidents take place due to gaps in the existing defence mechanisms. The role of investigators would be crucial in helping companies strengthen their defences against advanced cybercrime risks, which are either undetected or not diagnosed accurately. Companies also would have to look at more advanced techniques to combat cybercrime and invest more in diagnostics programs, cyber threat intelligence and incident response. The quality of investigation feeds back into the company’s cyber defence strategy in terms of loop holes exploited by the hacker during an incident. If the investigation is not concluded properly then such loop holes may never get discovered.

Social media emerges as a big risk area

员工在社交媒体上发布了其工作资料的详细信息。这些社交媒体平台是网络罪犯的宝库，他们可以利用这些资料来识别和针对关键个人以实现成功入侵。

40% 的受访者认为他们对主动监控网络犯罪的技术是有效的。

44% 的受访者拥有强大的数据保护计划。

然而，72% 的受访者认为他们的 IT 安全团队缺乏足够的专家来应对网络犯罪事件。

根据 McAfee 的报告\(^1\)，印度每年估计会失去 0.21% 的 GDP 给网络犯罪，而且事件的数量每年都在增加。

这些事件的发生是由于现有防御机制的漏洞。调查人员的作用至关重要，可以在帮助公司加强针对高级网络犯罪风险的防御中发挥作用，这些风险要么未被检测到，要么未被准确诊断。公司还必须考虑更先进的技术来对抗网络犯罪，并在诊断程序、网络威胁情报和事件响应中投入更多的资金。调查的质量会反作用于公司的网络防御策略，影响公司被黑客在事件中利用的漏洞。

Most of the respondents (almost 90%) unanimously identified social media as a big risk from a cybercrime perspective. This is fuelled by the fact that social media will be an important part of their company’s technology footprint and they need to be prepared in dealing with the risks associated with this channel.

Employees post extensive details regarding their work profile on social networking websites. These social media platforms act as a gold mine for cybercriminals to identify and target key individuals for a successful breach.

Responding to cybercrime incidents in India | 4

---

1 Net Losses: Estimating the Global Cost of Cybercrime
“Cyber security is critical for safeguarding the integrity and stability of our financial sector. A Computer Emergency Response Team for Financial Sector (CERT-Fin) will be established.”

Arun Jaitley, Finance Minister, Minister of Corporate Affairs in the Cabinet of India said in his Budget Speech in the Lok Sabha.
The technology landscape has been transforming rapidly, with changes in the last couple of years being relatively drastic and unpredictable. Some of the game-changing technologies that emerged in this period include cloud, big data, mobile and social media, which offered new capabilities and benefits for businesses, but also introduced new risks. With widespread adoption, these technologies have the potential to puncture a hole into the protected boundary of enterprises and put sensitive information at risk. As such technologies continue to transform at an accelerated pace, the associated risks could perhaps increase in geometric progression.

Today, cyber criminals are well funded, persistent, sophisticated and globally coordinated. Their level of knowledge and the understanding of new technologies supersedes most others. This, coupled with companies trying to integrate their systems and processes with new technologies and platforms, further broadens the areas vulnerable to attacks.

The advent of cybercrime was characterised by usage of Trojans or worms, scams, keyloggers, phishing and adware. The hackers’ attack vector was very similar to the military strategy involving ‘carpet bombing or saturation bombing’. This was used by various countries during the World War II, where thousands of unguided bombs would be dropped on the enemy soil without any specific target. Hackers used the same strategy and went after the masses for even small gains per hit as for them there is no cost per attack.

With the turn of the decade and with more sophisticated cyber-weaponry at their disposal, the hackers turned their focus on more lucrative targets. Instead of throwing their net around for small fish, they started going after the big whales. Attacks on core banking infrastructure, advanced persistent threats, ransomware attacks using social engineering and DDoS attacks using botnets created out of the internet of things (IoT) devices have now turned out to be the flavour of the season.

The cybersecurity controls deployed have also evolved in the last decade as the awareness amongst the organizations has increased. Instead of focusing on ‘prevention’ after the incident, the focus is now on detecting the attacks in real time and responding to them in an appropriate manner.
Cyber-attacks on the rise

Today, cybercrime is one of the fastest growing fraud risk in India. Our survey highlights that respondents across India witnessed a cybercrime in past two years.

As per our survey, sectors that have witnessed a cyber-attack are

- **26%** Technology, Media & Telecommunication (TMT)
- **24%** Financial Services (FS)
- **8%** Automotive & transportation
- **8%** Government & Public Sector Units (PSU)
- **8%** Real Estate, Construction & Hospitality
- **8%** Retail & Consumer Products
- **5%** Education
- **3%** Health & Life Sciences
- **3%** Manufacturing & Engineering
- **3%** Food & Beverages
- **2%** Energy
- **1%** Automation and Defence projects

TMT and FS are the top two sectors that witnessed most cybercrimes. Further analysis of the survey responses reveal that these incidents were targeted attacks, aimed to extract and exploit specific companies and sectors. These are not mass cyber sweeps or annoyances such as adware, tracking malware, standard keyloggers but focused attempts to breach specific companies with motives that are well planned.

In February 2017, Reserve Bank of India asked banks to report any cyber security incident within two to six hours.³

An oil and gas company was hacked in 2015, where cyber criminals duplicated (with minor changes) the official email address of a senior official. It was reported that this was used as a ploy to get one of their clients to transfer a payment to the hacker’s account, leading to losses to the tune of a few hundred crores. Incidents like these highlight the increasing trend of cyber criminals gaining access to corporate email addresses, and subsequent reporting with the local authorities.

³ The Times of India, ‘Report cyber attacks in 6 hrs: RBI to banks’
A securities and brokerage firm became a victim of a ransomware attack. The hacker demanded a ransom of two Bitcoins for each system which was infected. Upon investigation, it was discovered that several other critical systems were infected with the same ransomware. Emails with malicious attachments appeared to be originating from a foreign location and was identified as the source of infection. The organization decided to take a proactive approach towards security with the focus on real time monitoring to thwart such attacks in the future.
Detecting perpetrators and their modus operandi

According to our survey, companies are likely to witness cyber-attacks because of an employee as compared to external factors. Employees have emerged as the primary entity found to be behind cybercrimes which have been investigated in past two years.

Many organizations have realized the need to have controls around processes and technologies to combat threats and protect sensitive information. Historically, organizations have focused more on protecting their information systems and assets against intruders and hackers from the outside. As a first step, almost all of them have implemented security technologies for protecting their valuable information by implementing firewalls, intrusion detection, anti-virus, anti-spam, anti-spyware and other tools.

There have been many cases of financial crime, data theft and espionage where an insider was found to be involved. Such cases have alerted the organizations. Though with all the systems in place, there is an increasing threat to the corporate security of organizations that comes from within.

This risk could be from current and former employees, contractors and other internal personnel, who pose a major threat due to the available knowledge and their access to sensitive company data and information.

Corporate espionage

In past two years, India has seen a rise in corporate scams and cases of espionage. Keyloggers, Trojans, hiring professional hackers and bribery are some of the means by which espionage can be performed. Bribery also continues to pose significant challenge in India, where a bribed insider could be involved with corporate espionage. This has resulted in an urgent need to improve detection and prevention measures around data theft. Corporate espionage has been identified as the second most critical motive for a cybercrime and would continue to pose serious threat to companies in a highly competitive market such as India.

Government impetus

Indian companies will have to be well equipped to be able to deal with cybercrime going forward. Recognizing the serious threat India faces, the Government announced an investment of INR 400 crore for a cybercrime control hub “Indian Cyber Crime Coordination Centre” (IC4), which will be set up to check cybercrime. One of the priorities of IC4 will be to check attempts by international gangs to penetrate the Indian Government’s official communication network and hack them.

Who is behind cybercrimes witnessed in last two years?

- 32% Unknown hackers
- 19% Employees
- 17% Competitors
- 14% Hacktivists
- 7% Vendors
- 6% Foreign state sponsored
- 5% Customers

According to our survey, companies are likely to witness cyber-attacks because of an employee as compared to external factors. Employees have emerged as the primary entity found to be behind cybercrimes which have been investigated in past two years.

Many organizations have realized the need to have controls around processes and technologies to combat threats and protect sensitive information. Historically, organizations have focused more on protecting their information systems and assets against intruders and hackers from the outside. As a first step, almost all of them have implemented security technologies for protecting their valuable information by implementing firewalls, intrusion detection, anti-virus, anti-spam, anti-spyware and other tools.

There have been many cases of financial crime, data theft and espionage where an insider was found to be involved. Such cases have alerted the organizations. Though with all the systems in place, there is an increasing threat to the corporate security of organizations that comes from within.

This risk could be from current and former employees, contractors and other internal personnel, who pose a major threat due to the available knowledge and their access to sensitive company data and information.

Corporate espionage

In past two years, India has seen a rise in corporate scams and cases of espionage. Keyloggers, Trojans, hiring professional hackers and bribery are some of the means by which espionage can be performed. Bribery also continues to pose significant challenge in India, where a bribed insider could be involved with corporate espionage. This has resulted in an urgent need to improve detection and prevention measures around data theft. Corporate espionage has been identified as the second most critical motive for a cybercrime and would continue to pose serious threat to companies in a highly competitive market such as India.

Government impetus

Indian companies will have to be well equipped to be able to deal with cybercrime going forward. Recognizing the serious threat India faces, the Government announced an investment of INR 400 crore for a cybercrime control hub “Indian Cyber Crime Coordination Centre” (IC4), which will be set up to check cybercrime. One of the priorities of IC4 will be to check attempts by international gangs to penetrate the Indian Government’s official communication network and hack them.
What can organizations do?

Our survey highlighted an alarming 33% responses that suggested that companies were unable to conclusively close a cybercrime incident investigation.

The business landscape today is led by digital disruption and is constantly changing. What companies would typically know and do to tackle risks, proactively as well as reactively, may no longer be sufficient to protect them from the onslaught of new and emerging cyber-attacks. The need of the hour is to build robust cyber defence strategies which can help contain complex cyber breaches, provide remediation approach and root cause analysis.

To combat the risks arising in this complex cyber ecosystem, organizations may undertake a cybersecurity defence model, encompassing following stages.

### Prevent
Proactive identification of current or future risks associated with an organization

### Detect
Identification of potential hacks based on cyber threat intelligence

### Respond
Providing consistent and reliable response to the incidents

### Investigate
Investigating the incident and identifying the root cause

### Adapt
Incorporating assessment or investigation findings to the existing information security procedures

---

Case study 2

A bank identified malicious activity on their local IT system in one of their branches. Forensic analysis of the system revealed that the local IT administrator’s system was infected with a malware and was being used to perform lateral movement into the bank’s network using the escalated privileges.

Upon further investigation of the environment in the bank, it was discovered that hackers were attempting to perform unauthorized transactions into fake accounts. The bank decided to do a full security review of the infrastructure based on the RBI and SWIFT guidelines, to identify and address any other security gaps.
Ransomware

Ransomware is a sophisticated malware that circumvents security layers to render the affected user’s computer files inaccessible, by either locking them up or encrypting them. The user is then asked to pay a “ransom” to regain access to the data. Ransomware attacks have increased in recent time, and are expected to rise further. This is because unlike other malware, ransomware does not even require elevated or administrative credentials, making it even difficult to control.

Globally, there has been a spurt in cases where ransomware has been targeted at the C-suite. Trend shows that while initially it would just encrypt important files on the computer, but now it can encrypt the complete hard drive as well as the bootloader to ensure that the computer does not even start. As the “ransom” typically accepted in Bitcoins or other cryptocurrency, it is nearly impossible to trace it to the beneficiary.

The Internet of Things

Today, devices connected to the internet such as CCTV cameras, smart televisions and home routers have little or no security controls, and are potentially easy to compromise and abuse. With the IoT, hackers can use this to their advantage by creating a virtual inter-connected network (botnet) of these hacked devices and generate huge amount of internet traffic directed towards web facing servers causing massive disruptions.

IoT means that all physical objects will possess an internet protocol (IP) address, and get transformed into mini computers. The last major disruption using these IoT devices had almost reached 1Tbps (1 terabit per second)*, forcing most of the popular websites around the world to go offline for hours. Such devices can also be hacked for sensitive data or disruption. Increasing technology innovations can make this a key area of concern in the future.

Social Media Platforms

The ubiquity of social media for personal as well as business interactions has risen significantly. Consequentially, the risks associated with it have also augmented. When it comes to cybersecurity, employees with low awareness of the potential hazards of extensive social media usage could be the “weak links” in an organizational set up. The introduction of the social media platforms can also lead to gaps in security. It is common for individuals to have their personal information (date of birth, phone number, email address etc.), job profile available and accessible on social media platforms, making the hacker’s job only easier. Phishing emails or spoofing are some emerging techniques through which hackers can compromise the systems of unsuspecting employees.

*SC Magazine ‘OVH suffers 1.1Tbps DDoS attack’
Mobile

With the advent of the mobile era in the 21st century, the dependence on mobile devices to facilitate a large number of functions as well as transactions increased phenomenally. Dubbed as the primary screen, organizations are encouraging employees to use mobile devices (bring your own device or BYOD) for accessing emails and servers, to enable them to connect to the organization’s network from anywhere. However, hackers are trying to exploit the vulnerabilities of mobile applications, using phishing websites and social media tricks to harvest credentials of unaware users. Going forward, organizations should adopt appropriate frameworks for confidentiality and integrity of their data, along with facilitation of mobile access for sustainable growth.

Cryptocurrency

Cryptocurrency or virtual currency is a type of exchange currency where cryptography is used to process payments, safeguard transactions and limit the production of additional units. The Blockchain technology, where a decentralised ledger keeps a logs of all transactions, creates the foundation for these cryptocurrencies. These currencies work independent of central banks and Governments and there are a number of cryptocurrencies available for use online such as Bitcoins, Litecoins or Dogecoins. The value of this virtual currency is unaffected by country-specific economies, as the currency is finite in number and depends on factors such as usage, supply and demand.

The challenges in using virtual currency is that these systems are capable of facilitating tax evasion or illegal activities because of the anonymity factor which is built into the system. As a result, Bitcoin is a preferred mode by hackers for ransomware. That said, the number of transactions done globally are rising - statistics available on blockchain.info suggest that per day transactions for Bitcoins have increased from approximately 100,000 transactions in January 2015 to approximately 350,000 transactions in January 2017, a 250% rise. The rise in usage can lead to a surge in cyber-attacks, raids and fraud.

Digital Payments

The last decade saw the introduction of digital and mobile banking facilities such as mobile wallets, net-banking, NEFT, RTGS and banking applications for convenience. With demonetization, the use of plastic and digital money has increased exponentially, making it a lucrative opportunity for sophisticated attackers to steal money by employing various tactics relating to different modes of payments. With the nudge to move to a cash less society, various digital payments platforms, wallets etc. are being used extensively by individuals for the smallest of transactions. Therefore, cyber attackers will look to finding new ways to exploit the situation by targeting individuals and digital payment service providers. This may be done by exploiting technical and process loopholes as well as lack of user awareness around the do's and don'ts.
This report is prepared by the Forensic & Integrity Services team of EY in India. The objective of this report is to understand the level of readiness of businesses operating in India to detect cybercrime incidents and measures put in place to respond to such incidents.

For drafting this report, we have defined an incident relating to cybercrime or cyber-attack as an event which involves intentional breach of a company’s security. This would also involve a computing device with an intent to cause harm and a human involvement. The outcome of a cybercrime incident might result in financial risks, reputation risks and legal repercussions resulting from loss of confidentiality, integrity and availability of data and or systems.

Based on our experience of conducting cybercrime incident response engagements, we have identified key risk indicators and problem areas. This experience helped us keep our survey focused around cybercrime incident response.

Note: Some of the percentages in the charts total to more than 100%, since the respondents were allowed to make multiple selections. Not all the questions in the survey were answered by all the respondents. Therefore, all the percentage figures are derived from the total number of respondents who answered a particular question and not on the total number of overall respondents.
About EY's Forensic & Integrity Services

Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

Our services

- Investigations & Compliance
- Forensic Diligence
- Claims & Disputes
- Forensic Data Analytics
- Discovery
- Privacy & Cyber Response

Contact us

Arpinder Singh
Partner and Head - India and Emerging Markets
Direct: +91 12 4443 0330
Email: arpinder.singh@in.ey.com

Sandeep Baldava
Partner
Direct: +91 22 6192 0817
Email: sandeep.baldava@in.ey.com

Vivek Aggarwal
Partner
Direct: +91 12 4464 4551
Email: vivek.aggarwal@in.ey.com

Mukul Shrivastava
Partner
Direct: +91 22 6192 2777
Email: mukul.shrivastava@in.ey.com

Anurag Kashyap
Partner
Direct: +91 22 6192 0373
Email: anurag.kashyap@in.ey.com

Rajiv Joshi
Partner
Direct: +91 22 6192 1569
Email: rajiv.joshi@in.ey.com

Yogen Vaidya
Partner
Direct: +91 22 6192 2264
Email: yogen.vaidya@in.ey.com

Dinesh Moudgil
Partner
Direct: +91 22 6192 0584
Email: dinesh.moudgil@in.ey.com

Jagdeep Singh
Partner
Direct: +91 80 6727 5300
Email: jagdeep.singh@in.ey.com

Amit Rahane
Partner
Direct: +91 22 6192 3774
Email: amit.rahane@in.ey.com

Vikram Babbar
Partner
Direct: +91 22 6192 2155
Email: vikram.babbar@in.ey.com

Harshavardhan Godugula
Partner
Direct: +91 40 6736 2234
Email: harshavardhan.g@in.ey.com

Vinay Garodiya
Partner
Direct: +91 22 6192 2164
Email: vinay.garodiya@in.ey.com

Ranjeeth Bellary
Associate Partner
Direct: +91 22 6192 0172
Email: ranjeeth.bellary@in.ey.com

Responding to cybercrime incidents in India | 14
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

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

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

© 2017 Ernst & Young LLP. Published in India.
All Rights Reserved.

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