KPMG

cutting through complexity

FORENSIC TECHNOLOGY SERVICES

Cybercrime survey report 2014

kpmg.com/in

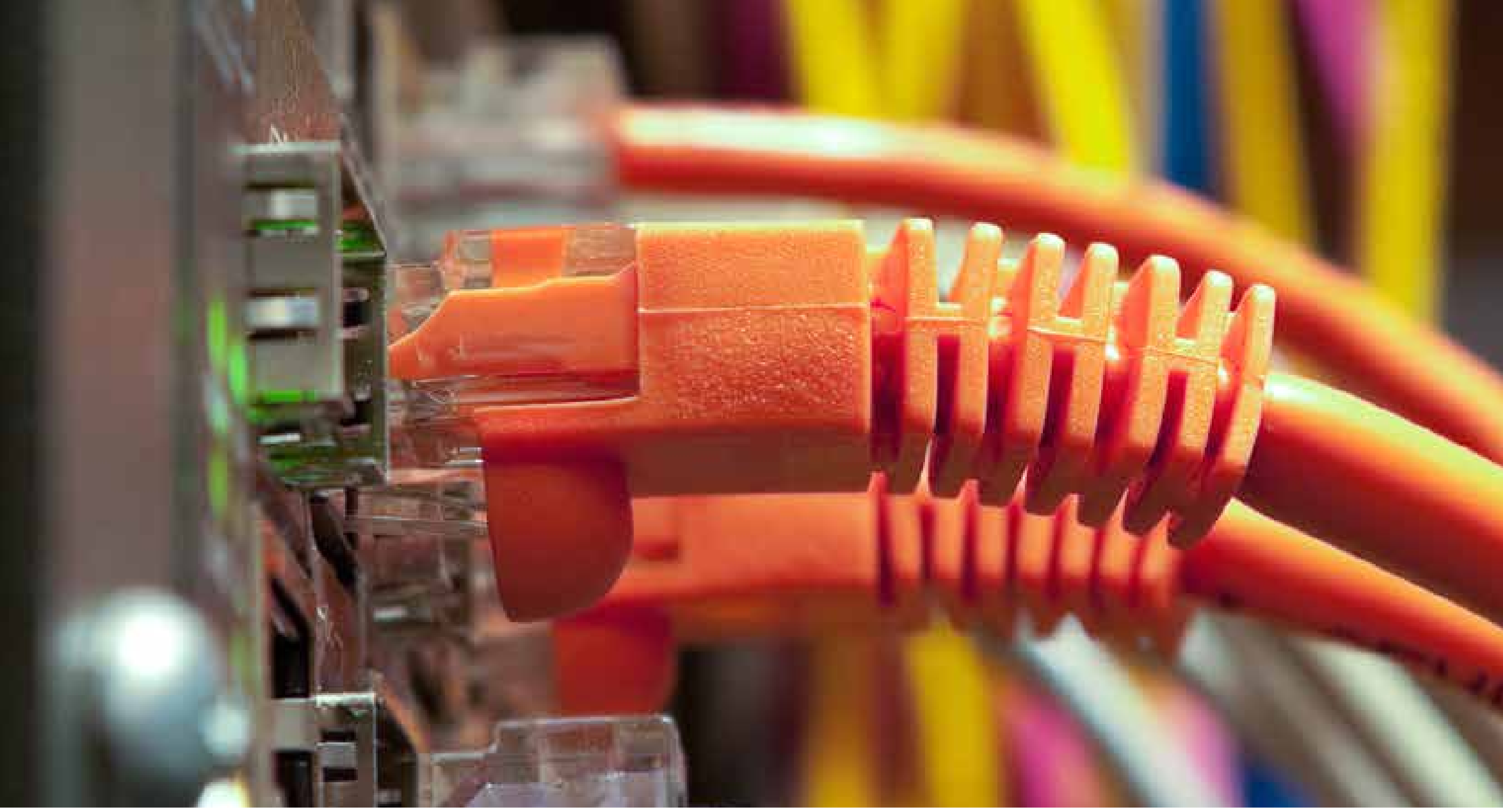


Table of contents

01 Foreword

The use of technology has become an integral part of our lives. Our increasing dependence on technology consolidates itself as a powerful platform that has revolutionised the way we do business and communicate with people, leaving us in the open to threats of cybercrime. We have become complacent to the existence of cybercrime, perhaps putting too much faith in technology. Organisations must recognise this environment and must identify methods to address these risks proactively.

As businesses and individuals increase their reliance on technology, they tend to become exposed to the growing cybercrime threats and the fact remains that we cannot ignore technology. Many businesses may not have taken time to consider whether they have sound cyber-security mechanisms in place, but ignoring this risk could endanger their operations. Through this survey we have analysed the preparedness of an individual or organisation from potential cybercrimes threats, other than highlighting preventive mechanisms to deal with this rapidly growing issue. While large organisations are beginning to take preventive measures to protect themselves, small organisations normally pay insignificant attention to risk assessment or have no funding to put the risk in place.

In view of this alarming increase in cybercrime threats and the need to combat cybercrime, we are pleased to present the KPMG in India cybercrime survey 2014. The survey provides a summary on the complexity of cybercrime and the measures that organisations should take to mitigate such crime, while creating awareness on what one should do to prevent such attacks.

We would like to thank all our participants who have contributed to this survey. Without their support the survey would not have been possible. We believe this survey will serve as an essential reading for the regulatory bodies and corporate leaders.

We hope that you find the survey useful.

Mritunjay Kapur
Partner & Head
Risk Consulting

Sandeep Dhupia
Partner & Head
Forensic services

Sandeep Gupta
Partner
Forensic services

02 About the survey

Genesis of the Survey

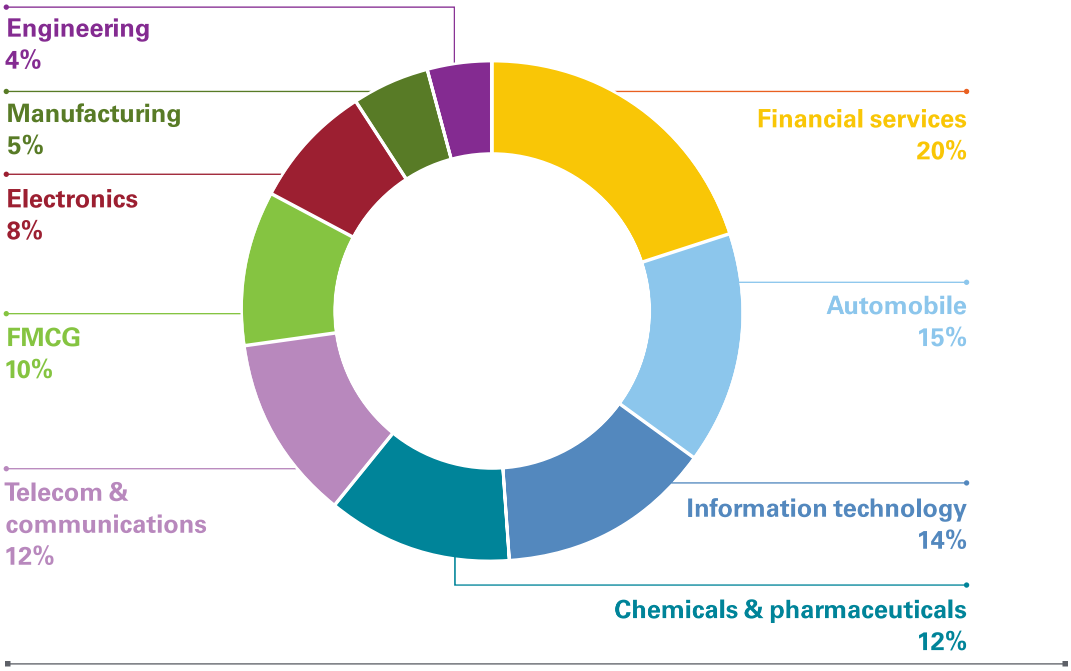
In a digital age, where online communication has become the norm, internet users and governments face increased risks of becoming the targets of cyber attacks. As cyber criminals continue to develop and advance their techniques, they are also shifting their targets focussing less on theft of financial information and more on business espionage and accessing government information. To fight fast-spreading cybercrime, businesses and governments must collaborate globally to develop an effective model that can control the threat.

Cybercrime continues to remain a tough challenge for organisations. Over the years there has been a significant increase in the number of cybercrime attacks prompting organisations to stay alert, seek means to fight cybercrime threats. We, at KPMG, have been on the forefront to help ensure strong security defense mechanisms. In this endeavour, KPMG in India has conducted the 'Cybercrime Survey 2014'. The survey was conducted through an online questionnaire.

Profile of the participants

Over 170 participants from the likes of CIOs, CISOs and related professionals from across India responded to the survey. 75 per cent of the participating organisations have more than 1,000 employees.

Survey participants represent the following industries



Source: Cybercrime survey report 2014, KPMG in India

03 Cybercrime: What does it mean?

What is cybercrime?

Cybercrime is a range of illegal digital activities targeted at organisations in order to cause harm. The term applies to a wide range of targets and attack methods. It can range from mere web site defacements to grave activities such as service disruptions that impact business revenues to e-banking frauds.

When was the first ever cybercrime recorded?

The first cybercrime was noted in 1820 by Joseph-Marie Jacquard, a textile manufacturer in France which produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology[1].

Who is carrying it out?

Cyber attacks can be carried out by a host of people ranging between disgruntled employees, individual hacker, organised cybercrime syndicates to enemy government or an activist.

What is the biggest myth related to cybercrime?

100 per cent Security! 100 per cent security can be difficult to attain and should not ideally be the goal. Instead, one must establish a capability that deals with incidents to help minimise threat and loss.

Are you facing cyber threat and not even realising it?

The information security landscape is constantly evolving. Private and public sector organisations find it difficult to believe they could be a target for cyber attacks. As adversary sophistication increases, many organisations react only after the event or the attack is underway.

Few organisations have the capability to anticipate cyber threats and implement preventative strategies, despite prevention being more cost effective and customer focussed.

Recently security researchers announced a security flaw in OpenSSL, a popular data encryption standard, that gives hackers who know about it the ability to extract massive amounts of data from the services that we use every day and assume are mostly secure. It was called the Heartbleed Bug![2]. Hence, while most boards and CIO's would think that they are not relatively impacted by cyber security threats, the penetration of technology into the daily operations and threat posed by such bugs could alter the risk perception of boards and CIO's.

[1] Introduction to cybercrime - wsilfi.staff.gunadarma.ac.id/Downloads/files/.../W03Cyber+crime.pdf accessed on 5 May 2014

[2] www.businessinsider.com/heartbleed-bug-explainer-2014-4 accessed on 9 April 2014

04 Survey results and analysis

Threat perception of cybercrime in India

Cybercrime can affect any organisation, large or small. Many of the incidents are not publicly known and have not been reported by the media. However, companies in U.S., are legally granted the responsibility to report incidents to the authorities, and the Europe Union is expected to follow suit in the near future[3].

Perception of cybercrime in India

89%

Cybercrime is a major threat

In this increasingly hyper-connected world, cybercrime has emerged as a major threat as acknowledged by an overwhelming 89 per cent of our survey respondents.

51%

Easy target for cyber attacks

Survey result analysis

Distinctly, about 51 per cent perceive themselves to be an easy target for cyber attacks due to the nature of their business. Out of these 51 per cent, about 68 per cent respondents claim that they monitor their cybercrime threats on a daily basis.

Inadequate detection processes may conceal the real number of cybercrime attacks. Although many organisations today are equipped with state of the art security systems, they may still be unable to manage or handle cybercrime incidents.

The first line of defence against any cyber threat is increasing perception and awareness of cybercrimes.

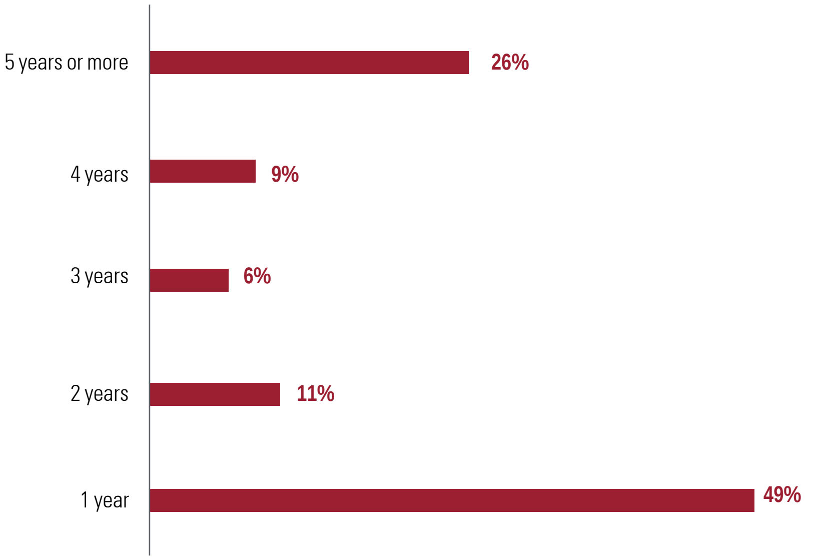
[3] A Nuanced Perspective on Cybercrime, KPMG International, 2012

04 Survey results and analysis

Trends of cybercrime in India

In the past, India used to be a target of cyber attacks for political motivation only. Over the past few years, the global cybercrime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security. Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent. These attacks, which were rarely malicious, have gradually evolved into cybercrime syndicates siphoning off money through illegal cyber channels.

Survey result - Frequency of cyber attacks



Source: Cybercrime survey report 2014, KPMG in India

Survey result analysis

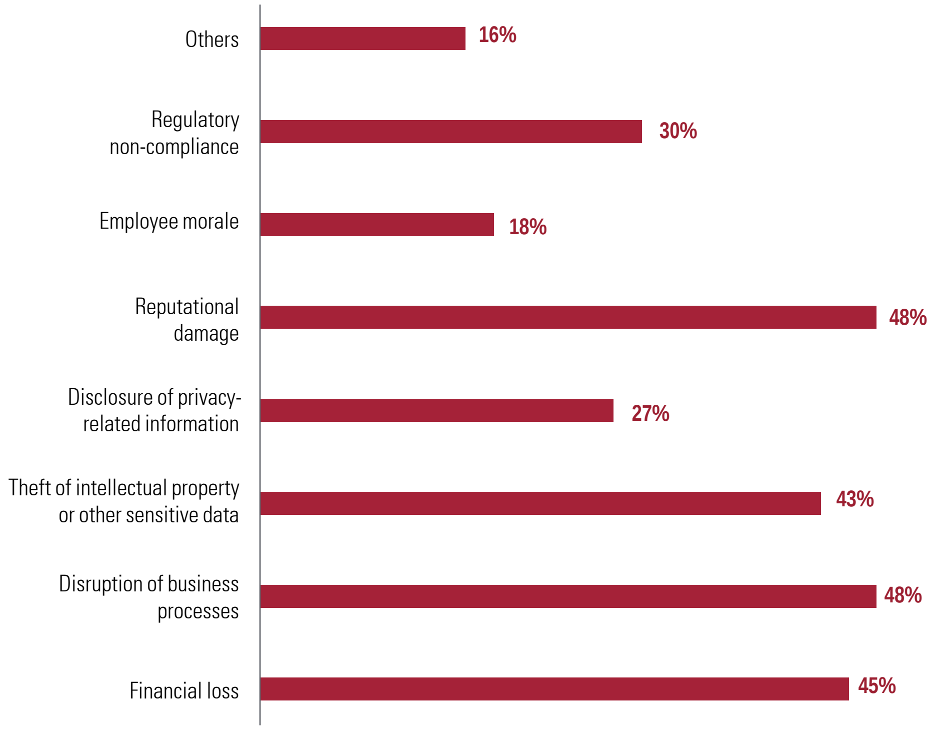
49% of the respondents have experienced cybercrime in the last. It is evident that only half of the respondents have been a victim of cyber attacks in the last year which indicated that the number of cybercrime incidents in India has been on rise.

Cybercrime has seen an increase in frequency in India.

04 Survey results and analysis
Impact of cybercrime in India

Cybercrime can be developed using various methods; worms are one of the most potent form of cyber attacks that can cause serious disruption in business operations. The Stuxnet computer worm is the first known worm to target and tamper with industrial controls. In September 2010, it infected an unknown number of industrial controls worldwide and could stealthily give false instructions to machinery and false readings to operators. Potentially, it could destroy gas pipelines, cause a nuclear plant to malfunction or cause factory boilers to explode. The worm was known to be most active in Iran, but Indonesia, India and Pakistan also reported infections.[4]

Survey result - Impact of cybercrime in India



Source: Cybercrime survey report 2014, KPMG in India

Survey result analysis

48 per cent of the respondents indicated that they suffer disruption of their business processes and reputation damage as a result of a cyber attack. Cyber attacks have often led to financial losses (either direct or indirect) as indicated by 45 per cent of our survey respondents. A majority of the respondents (68 per cent) indicated that they suffered 'less than INR100,000' in terms of financial loss due to cybercrime attacks.

Cybercrime is increasingly seen to cause not only disruption of IT but also financial losses.

[4] www.ft.com/cms/s/0/cbf707d2-c737-11df-aeb1-00144feab49a.html accessed in May 2014

Case study

Multinational company email accounts spoofed

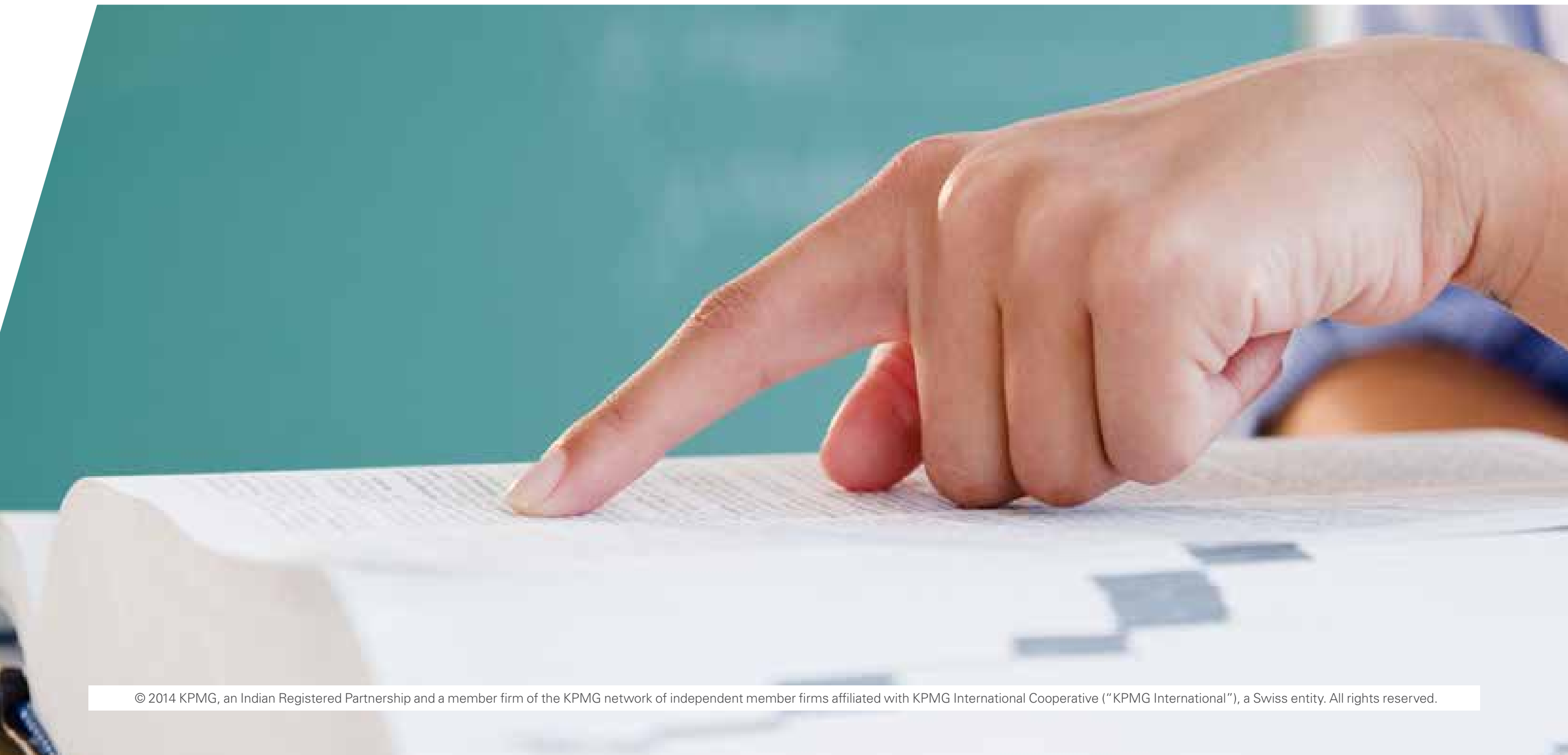
A Multinational company operating in the manufacturing segment received spoofed emails from its customers which were not sent by its employees. The spoofed emails appeared to be genuine as the contents were relevant to the business. The emails were sent to customers requesting them to transfer the pending amount to bank accounts in different location across Asia and Europe. Moreover, targeted customers were mostly from the Asian market with low to medium volume of business.

The company had concerns on its e-mail system being compromised since the emails sent to the customers had genuine business communication in the trail mail.

The company requested Forensic technology team of KPMG in India to investigate the incident and provide its recommendation on security gaps, if any. KPMG analysed the incident in two broad segments - network and e-mails. The KPMG Forensic Technology experts captured forensically sound images of the e-mail server and employees whose e-mail IDs were spoofed to make sure no traces or evidence were lost.

To get an overview of systems that could have been compromised by the perpetrator, KPMG analysed traffic to and from the e-mail server. Furthermore, logs from firewalls were secured and analysed to investigate whether the perpetrator or some other individual had access to the system within the network. By using specialised forensic software, the images were analysed for traces of compromise in user files and artifacts.

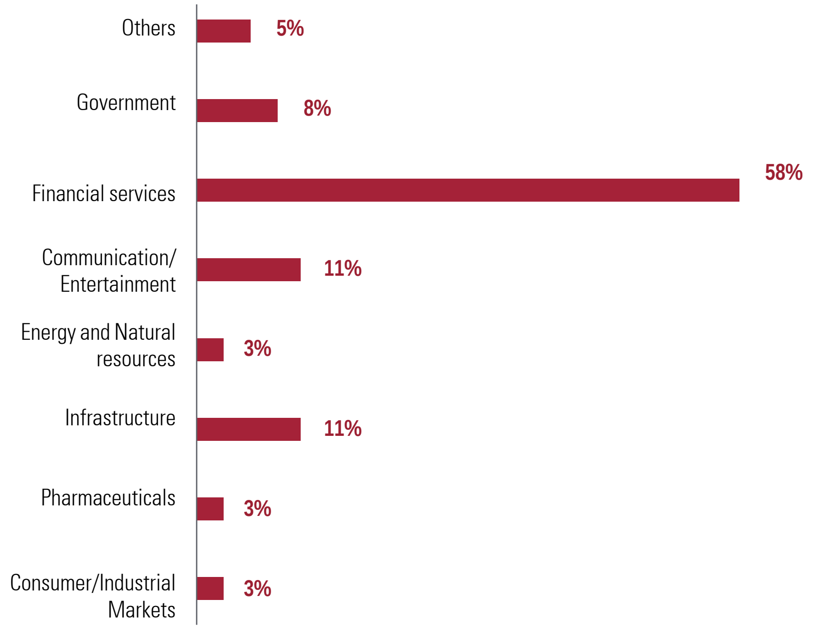
The Forensic investigation of the network and e-mails revealed a list of IP addresses which were linked to the perpetrator. Analysis showed that the perpetrator succeeded in creating and uploading several files to the e-mail server through a malicious code, allowing the perpetrator to send commands to the server from a remote location and gather sensitive business information. Reconstruction of the malicious code installation revealed it was executed by an internal employee who in hand with the perpetrator managed to extract sensitive information.



04 Survey results and analysis
Sectors prone to cyber attacks

In this day and age organisations are extensively using information technology and applications for automation of business processes, also, due to the IT revolution, Internet is now the key medium for business transaction, thereby leaving many sectors vulnerable to cyber attacks. The level of vulnerability of sectors depends on the extent of IT pervasiveness in each of these sectors below, as a result some sectors are more prone to attacks than other sectors.

Survey result - Sectors prone to cyber attacks



Source: Cybercrime survey report 2014, KPMG in India

Financial services sector is most prone to cybercrime.

Survey result analysis

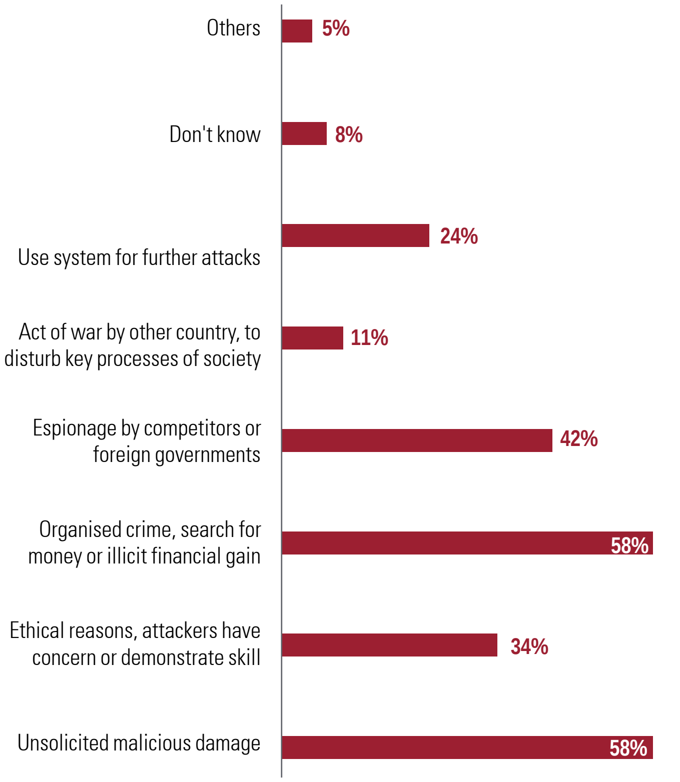
58%

of our survey respondents perceive financial services sector as more likely to be prone to cybercrime. In this sector the value to the attacker would be internet banking and brokerage. Phishing attacks of online banking accounts or cloning of ATM / Debit cards are common occurrences. Often, intruders also send e-mails that contain urgent requests to validate or share internet banking usernames and passwords. The increasing use of mobile / smartphones / tablets for online banking / financial transactions has also increased the vulnerabilities to a great extent.

04 Survey results and analysis
Motivation for cyber attacks

In the early days, cybercrime attacks were mostly carried out for fun, to demonstrate skills or to achieve one-off financial gains. Nowadays, organised criminals operate with carefully planned and executed attacks not necessarily for the financial rewards, but motivated by activism or digital espionage. These new forms of cybercrime have attention from governments all over the world, since they involve serious risks in the field of disruption of vital functions in society.

Survey result - Motivation for cyber attacks



Source: Cybercrime survey report 2014, KPMG in India

Nowadays other types of losses are also gaining importance:

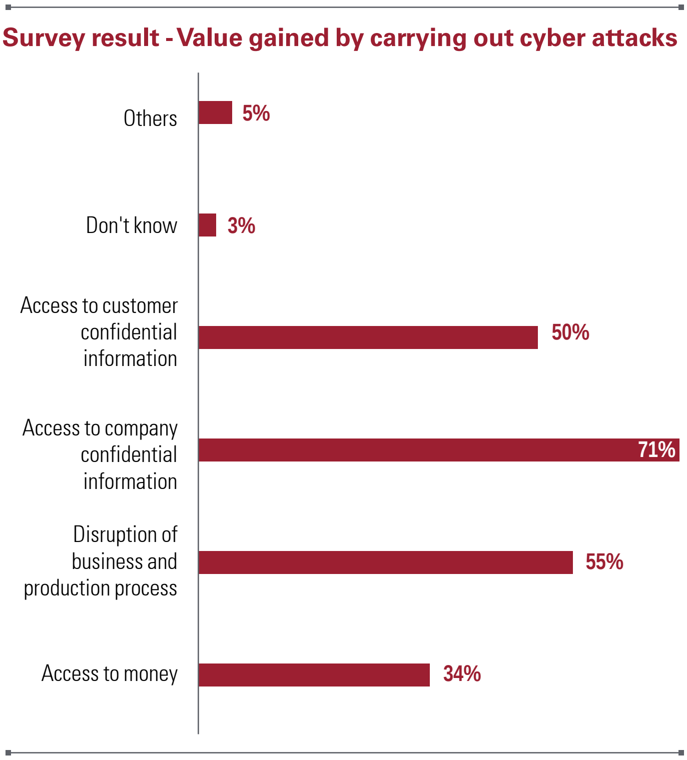
Access to money- The impact on financial losses can range anywhere from a monitor replacement to millions of rupees depending on the extent of damage.

Access to customer confidential information- Losing personal information of customers can result in brand reputation damage, data privacy violations, and other personal liability issues.

Disruption of production and business processes- Execution of data as a programme on the system connected to the reader allowing access to and corruption of sensitive networks and information can intervene in business and production processes causing loss of revenues and shutting down of office.

Source: Cybercrime survey report 2014, KPMG in India

Survey result - Value gained by carrying out cyber attacks



Source: Cybercrime survey report 2014, KPMG in India

Root cause of most cyber attacks is monetary/ financial gain

Survey result analysis

58%

indicated that cybercrime attacks are now taking the shape of an organised crime for illicit financial gains / money or to cause unsolicited malicious damage. Espionage, ethical reasons and using systems for further attacks so far are only recognised as a cause of attack to a limited extent.

71%

of the respondents recognise that access to a company’s confidential information is the foremost value gained by the perpetrator from the attack; however, the impact of cybercrime may not be underestimated.

04 Survey results and analysis
Profile of cyber attackers

Cyber-attackers can be classified based on various aspects such as their qualifications, skill levels, age group and motivations. Based on the aforesaid, sources of cyber attackers can be broadly classified as under:

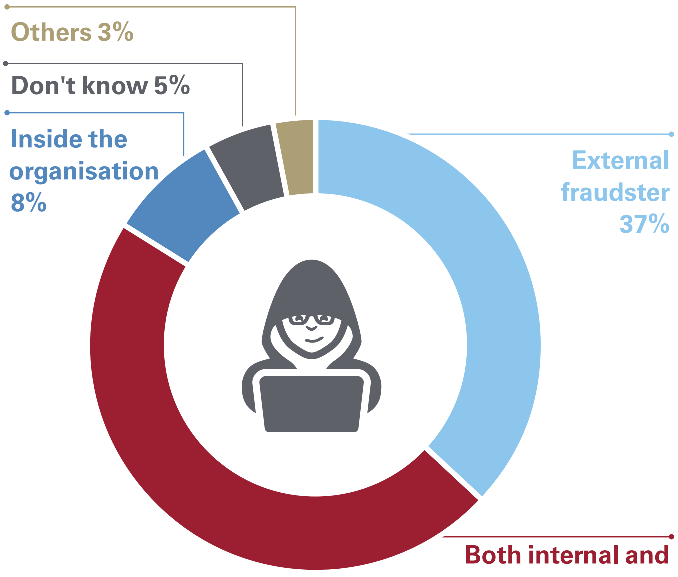
Internal sources

- Disgruntled employees
- Managed services personnel
- Malicious personnel (focussed on industrial/commercial espionage)

External sources

- Cyber terrorists (focussed on defacement)
- Professional hackers/hacking crime syndicates
- Novice hackers

Survey result - Profile of cyber attackers



Source: Cybercrime survey report 2014, KPMG in India

Survey result analysis

37%

Although 37 per cent of the respondents feel risk of cyber attacks comes from an external source, it is imperative that organisations keep a track of insiders with malicious intent or professional intruders constantly seeking access to sensitive information.

47%

of the respondents indicated that the risk of cyber attack is perpetrated by both internal as well as external intruders.

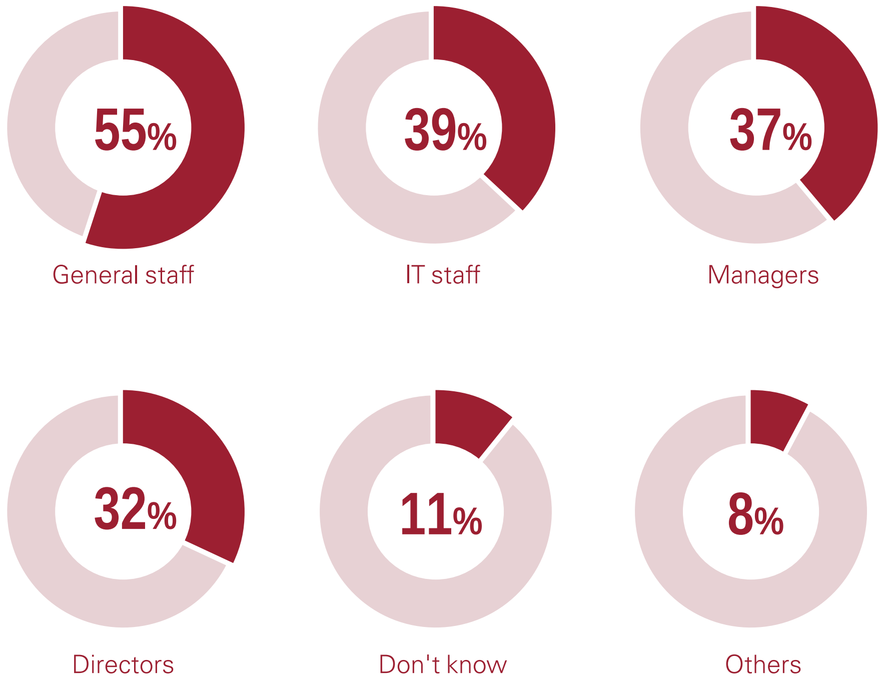
Cyber attacks can be from both internal and external sources

04 Survey results and analysis

Targets of cyber attacks

The battle against cybercrime is a typical example of a rat race that can be a challenge difficult to win. The least one can do, is to be as informed as possible. To do so, organisations need to evaluate their cybercrime or security risk through the eyes of the attacker, and decide which parts of the organisation represent the highest value to the attacker. Accordingly, security measures should be placed along the domains of preventive, detective and response measures and in the areas of people, processes and technology.

Survey result - Targets of cyber attacks



Source: Cybercrime survey report 2014, KPMG in India

Survey result analysis

Needless to say, 55 per cent perceive that the 'general staff' is most prone to cyber attack and require tighter security, followed by IT staff (39 per cent) and then managers (37 per cent).

Staff at lower designations are the most likely targets for cyber attackers

04 Survey results and analysis
Response mechanisms to cyber attacks

Cyber attacks by their very nature are multi-dimensional and complex. As cybercrime progressively evolves into an organised activity, the motives of intruders are no longer limited to stealing information only, but potentially to disrupt business or conduct espionage on behalf of competing organisations. Although organisations understand the need to safeguard their IT infrastructure, intruders have often been a step ahead at exploiting new vulnerabilities in IT systems and processes of their target. Needless to say, target organisations have been found wanting when it comes to countering these cyber attacks.

Survey results

Security policies	Security measures
Standard operating procedures (33%)	Anti-virus software (83%)
User access management (25%)	Anti-spam filters (69%)
External network access control (14%)	Firewalls (81%)
System auditing (8%)	Intrusion detection systems (44%)
Forensic plan (3%)	Encrypted files (47%)
Don't know (8%)	Encrypted login/sessions (39%)
Others (8%)	Biometrics, smart cards/tokens (25%)
	Others (3%)

Survey result analysis

In our survey, a few of our respondents indicated that their organisations are doing their bit, while others are still lagging behind when it comes to enhancing their internal cyber security infrastructure. Further, a small group of our respondents indicated that they have put in place security policies; standard operating procedures 33 per cent and User Access Management (25 per cent).

Cyber attacks can be from both internal and external sources

Survey result analysis

The situation is similar when it comes to adopting specific measures pertaining to prevention and detection of cybercrime. Organisations are imparting trainings to create awareness about cybercrime and cyber-security amongst their employees as suggested by 72 per cent of our survey respondents.

E-mail announcements/posters/banners 39 per cent and face-to-face training events 39 per cent are considered to be the most effective mechanisms for creating cybercrime awareness.

However, less than half of the respondents seem to have implemented preventive measures such as endpoint protection 44 per cent and cybercrime response testing 33 per cent.

Case study

A forensic response

A multinational company offers a closed online environment, which allows it to cooperate and communicate with their clients, partners and other stakeholders. On a daily basis, large amounts of confidential data are being transferred to and from their website, thus making the company an attractive target for attackers. The company was informed by a whistleblower that an attacker gained access to the company's website and/or closed environment.

In response to this news the website was taken offline and KPMG was asked to assist. A collaboration of Forensic Technology and IT Security experts captured forensically sound images of the most critical servers to make sure no traces or evidence were lost. By using specialised forensic software, the images were analysed for traces in system files and properties. Furthermore, logs from firewalls were secured and analysed to investigate whether the perpetrator also had access to the management part of the network which was separated from the web environment by a firewall. To get an overview of systems that also could have been compromised by the perpetrator, KPMG analysed traffic to and from the compromised server(s).

This revealed a list of IP addresses which could have been linked to the perpetrator. The analysis showed that the perpetrator succeeded in creating and uploading several files to the web server that contained a malicious code, allowing the perpetrator to send commands to the server from a remote location. The files were disguised as regular files by having a web server extension and using file names that did not arouse any suspicion. KPMG helped the client by implementing remedial procedures and additional security measures, thus mitigating the risk of further damage and bad publicity.

04 Survey results and analysis

Controls to manage cyber attacks

A vast majority of cyber attacks can be damaging, this can be limited by implementing technology and process controls that are an equitable mix of preventive and detective controls. A quick overview of some basic measures and controls are out lined as under:

Detection measures/controls: Logging of critical events and monitoring central security incidents and events can strengthen the technology detection measures. 24/7 standby crisis organisation and monitoring can be an excellent tool to detect strange patterns in data traffic, identify where attacks converge and observe system performance. This way, information security becomes a continuous process and organisations are enabled to proactively anticipate instead of reactively act on incidents.

Prevention measures/controls: Prevention schemes start with governance and organisation. Relevant responsibilities must be assigned relating to cybercrime. Awareness training programmes in place for key employees in high risk areas is a very helpful tool in preventing attacks. Regular scanning and penetration testing are processes that are used to prevent attacks. Lastly, actions such as end-point workstation protection and computer can help prevent attacks via technology.

Survey Results

1) Controls implemented to manage risk of cyber attacks

Preventive controls	Detective controls
Assign responsibilities with regard to cybercrime (42%)	24/7 standby crisis organisation and thorough monitoring (31%)
Awareness training (72%)	Procedures for follow-up on security events (69%)
Cybercrime response testing (simulating attack) (33%)	Logging of critical events (64%)
Regular scanning and penetration testing (64%)	Central security incident and event monitoring technology to collect and analyse events (44%)
Endpoint (workstation) protection (44%)	Others (3%)
Computer network segmentation (external and internal firewalls) (56%)	
Others (6%)	

2) Typical action/responses to cyber attacks

Actions taken
Performed fact finding (forensic) investigation internally (50%)
Hired external experts for fact finding (forensic) investigation (31%)
Reported the incident to the police (28%)
None (31%)
Others (6%)

Survey result analysis

An analysis of the results reveal that most of the measures have been adopted on a piecemeal basis. About 68 per cent of our respondents indicated that they assigned 'less than 20 per cent' of their IT security budget for preventing cybercrime.

Further in terms of cyber attack response plans, the results revealed about 61 per cent of respondents indicated they have a cyber incident response plan. While 56 per cent indicated that they have a dedicated incident response plan, half of them suggested that they have the capability to promptly cut-off (external) network connections which is more or less a reactive measure.

The nature of actions that organisations take after detection of a cyber attack can potentially set a deterring precedent for intruders. Half of the survey respondents (50 per cent) indicated that they conducted internal fact-finding investigations. However, our experience suggests that internal investigators may lack the technical subject matter expertise to gather appropriate evidence and ability to handle sensitive issues.

Only 37 per cent indicated that they would undertake civil/criminal action. However, about 28 per cent of respondents indicated that they have actually reported the incidents to the police. Potential exposure of sensitive information and the likelihood of reputational damage are the major reasons why organisations resist reporting such incidents to law enforcement/external agencies.

Managements have lower inclination to pursue legal recourse in relation to cybercrime.

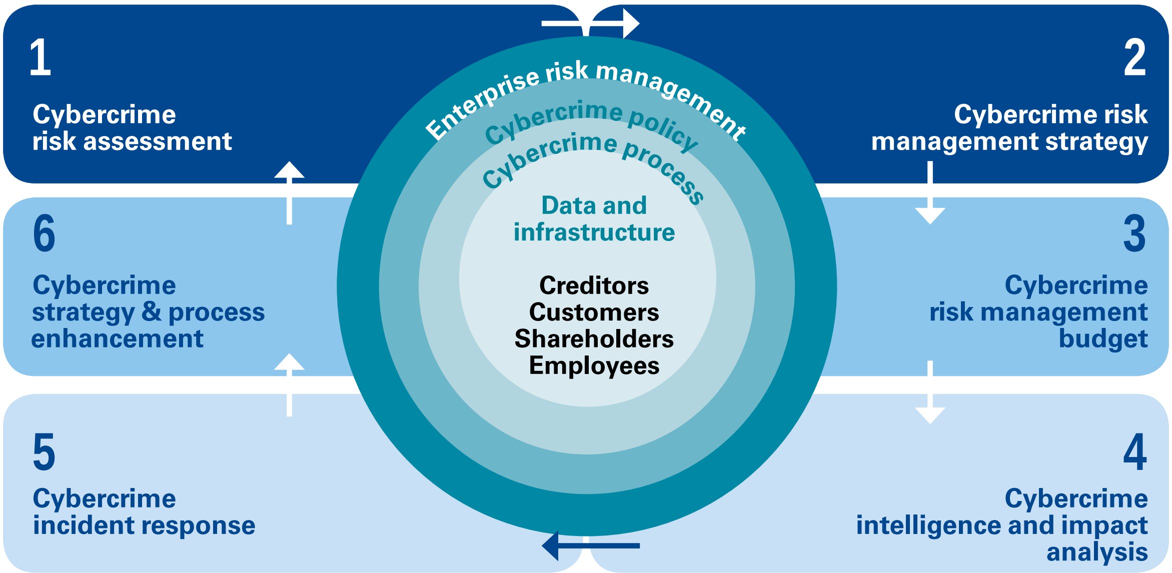
05 Conclusion

A look to the future and roadblocks in the present

With the advent of hand held computing, cyber criminals are now moving beyond computers, and attacking mobile handheld devices, such as smartphones and tablet personal computers (PCs). Cyber attackers have now taken advantage of the increasing popularity of mobile phone applications and games by embedding malware into them. Despite the increasing cyber threat risks, many boards fail to ask these questions or attain satisfactory answers. Often, this happens because the first question can be the most difficult to answer. Cyber threats can be hard to quantify in terms of likelihood and business impact. As a result, many boards do not fully understand the nature of the threat and tend to inaccurately assume that cyber security is a technical issue.

A way forward

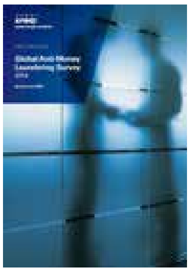
As the old adage goes 'prevention is better than cure' most organisations could gain improved value and security by adopting a preventive approach to tackling cybercrime related risks. Adopting a preventive approach towards cybercrime risk management, however, typically requires a cultural shift that starts with board level executives who can incorporate cybercrime related risks into the enterprise risk strategy. By doing so, leaders can quickly start to identify gaps in the current cybercrime risk management strategy and encourage an organization-wide approach to countering cyber threats. Further, many organizations adopt a piecemeal approach towards cybercrime risk management. A suggested framework for building a sustainable model for cybercrime risk management is outlined as under:


1
Cybercrime risk assessment
2
Cybercrime risk management strategy
3
Cybercrime risk management budget
4
Cybercrime intelligence and impact analysis
5
Cybercrime incident response
6
Cybercrime strategy & process enhancement
Enterprise risk management
Cybercrime policy
Cybercrime process
Data and infrastructure
Creditors
Customers
Shareholders
Employees

Publications from KPMG member firms

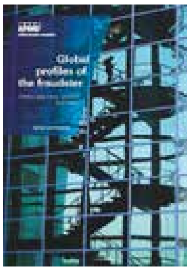
Cyber security: It's not just about technology

This paper provides essential insights for management to get the basics of cyber security right: The world of cyber crime today, Five common cyber security mistakes, The importance of customizing cyber security policies, The critical dimensions of a strong cyber security model, Key questions to help you navigate the 'new normal'



Global anti-money laundering survey 2014

The survey compares firms' AML programs and looks at emerging areas of risk, such as Trade Finance and Tax Evasion, as well as AML trends within the Insurance and Asset Management sectors.



Global profiles of the fraudster

This report contains KPMG's analysis of 596 fraudsters member firms investigated between 2011 and 2013. It is intended to provide the reader with insights into the relationship between the attributes of fraudsters, their motivations and the environment in which they flourish. We have also interviewed KPMG member firms' investigation leaders to gain additional insights.

KPMG in India contacts:

Dinesh Kanabar
Deputy CEO,
Chairman - Sales & Markets
T: +91 22 3090 1661
E: dkanabar@kpmg.com

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

Sandeep Dhupia
Partner & Head
Forensic Services
T: +91 124 3345 008
E: sdhupia@kpmg.com

kpmg.com/in

Latest insights and updates are now available on the KPMG India app. Scan the QR code below to download the app on your smart device.

Google Play | **App Store**

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

Printed in India.