At a glance:

Executive summary Pg 3/Introduction Pg 4/Hacktivism and mass defacement Pg 6/
Corporate espionage Pg10/Phishing and Skimming Pg12/ Cyber crime: An internal threat Pg17/
BYOD Pg 19/ Cloud computing Pg 21/ Cyber threats: Adopting proactive approach
to tackle it Pg 23/ Conclusion Pg 25

Invading privacy:

Cyber crimes on the rise

pwc

www.pwc.com/india

Preface

Whether an infiltration is criminally or politically motivated, a cyber attack can have a negative impact on a company's value, reputation and ability to generate revenue. Businesses face serious threats from cyber criminals and senior management need to take these risks more seriously.

The PwC report, Invading privacy: Cyber crimes on the rise, assesses key emerging cyber crime trends related to organisations in India. It provides analysis on trends such as hacking and website defacement, corporate espionage, phishing and skimming, emergence of BYOD and the growth of cloud computing.

We hope the report plays an important role in helping enterprises shape their efforts and strategies to manage the emerging risks posed by cyber crimes and gain competitive advantage in today's technology-driven environment. We look forward to your comments and feedback.

Sivarama Krishnan
Executive Director
PricewaterhouseCoopers, India
Email:sivarama.krishnan@in.pwc.com

Executive summary

With increasing dependency on technology — be it cell phones, tablets or laptops, a new breed of tech-savvy fraudsters is coming out with new and more innovative ways of carrying out cyber attacks, thus posing a new set of challenges.

Our analysis reveals the following key emerging trends in cyber crime pertaining to organisations in India:

- A tremendous rise in the number of hacking incidents reported and an increasing risk of website defacement faced by government and private organisations.
- Corporate espionage emerging as a key cyber threat for business.
- Identity theft through phishing and skimming as one of the biggest pain points for the financial services sector.
- Internal stakeholders the gravest challenge to information security.
- Emergence of Bring Your Own Device (BYOD) based access to corporate systems. Malware attacks coupled with employees' access to social media websites on their personal devices pose serious security challenges to Indian organisations.
- Growth of cloud computing resulting in cyber crime exposure

The rising trend of hacktivism in India which involves hacking and website defacement by fraudsters motivated by political causes is becoming an increasing concern for the government as well as private organisations. Using Distributed Denial of Service (DDoS) attacks as one of the methods, hackers are able to access an organisation's sensitive data leading to data loss and reputational damage.

Organisations are using every possible opportunity to gain an edge over their competitors by bringing together strategy, technology and market intelligence. Consequently, the threat landscape resulting from corporate espionage has evolved, gone digital and is certainly more dangerous.

With the emergence of online and mobile banking, the financial services sector has become increasingly vulnerable to cyber crimes, particularly phishing and skimming. Phishing and skimming attacks involve identity thefts by stealing confidential and personal information of customers. This not only leads to reputational damage and customer loss but also involves heavy financial losses that have to be ultimately borne by the bank or the financial institution.

As organisations' IT infrastructure is becoming more sophisticated, internal stakeholders are using advanced tools to commit cyber crimes within the organisation. Cyber attacks occur more from internal sources rather than external.

With more opportunities for cyber criminals to access sensitive data, the lack of a robust legislative framework and inadequate cloud computing strategies of organisations, the risk relating to data privacy and security could potentially increase in India.

Undoubtedly, cyber security has become one of the significant concerns for organisations and protection of information assets has become top priority for business leaders in corporate India.

Introduction

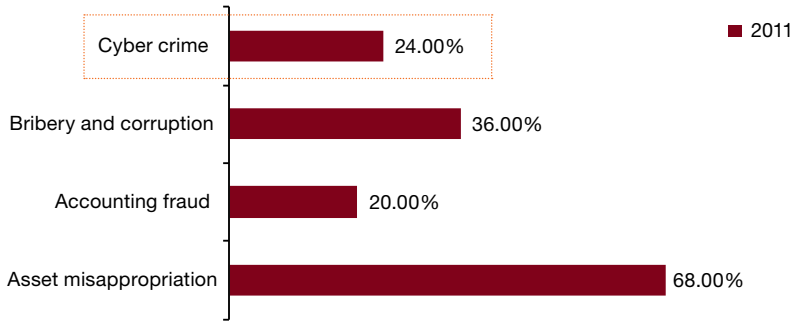
Cyber security risks and the increasing awareness, occurrence and impact of cyber incidents confronting corporations are a rapidly growing concern to investors, senior executives, and policy setters. Driving this concern are unprecedented corporate dependencies on digital technologies which are growing at an exponential rate. PwC published a study on insider threat in collaboration with the Data Security Council of India (DSCI) and the Global Economic Crime Survey in 2011, followed by the State of Information Security Survey India in 2013. This report builds on these surveys. We have used secondary research on PwC proprietary data and publicly available information to highlight some of the major cyber threats emerging in India.

In the past, cyber security was classified as an IT issue, resulting in a communications chasm between business managers and security professionals. It has now taken priority in board meetings.

Cyber crime ranks as one of the top four economic crimes perceived by Indian organisations.

According to the PwC Economic Crime Survey India Report, 2011, cyber crime has been reported as one of the top economic crimes experienced by organisations in India out of the four economic crimes--fraud, cyber crime, bribery and corruption and asset misappropriation.

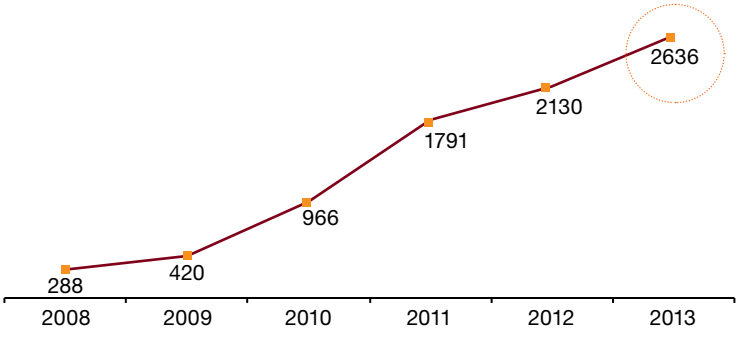
Top economic crimes experienced by organisations in India



Cyber crime has been increasing at an alarming rate in India. The number of cyber crime cases registered under the IT Act in 2011 were 1791, an 85% increase since 2010[1]. As per PwC analysis, this number is expected to increase to 2636 in 2013, a 173% increase since 2010.

With an increase in cyber crime organisations can build their competitive advantage by taking a strategic view of threat management that builds operational resilience and enables sustainable growth. While the threat of crisis is embedded in doing business today, it is worth noting that opportunity does not exist without threat.

Number of cyber crime cases registered under the IT Act

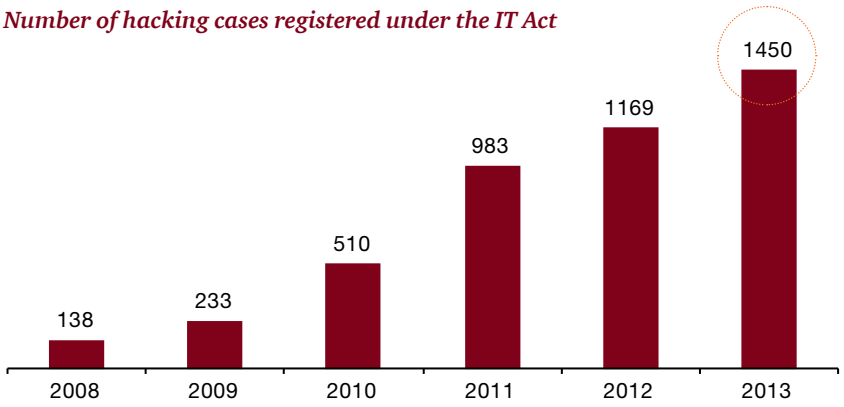


[1] Crime in India' report 2007-2011, (National Crime Record Bureau)

Hacktivism and mass defacement : A nuisance to organisations

Hacking has been one of the most commonly used methods of cyber attack. According to a National Crime Records Bureau (NCRB), there has been a tremendous rise in the number of hacking incidents reported in India. The number of hacking cases registered under the IT Act increased from 510 in 2010 to 983 in 20111. As per PwC analysis, this number is expected to increase to 1450 in 2013, a 184% since 2010.

Number of hacking cases registered under the IT Act



Hacktivism

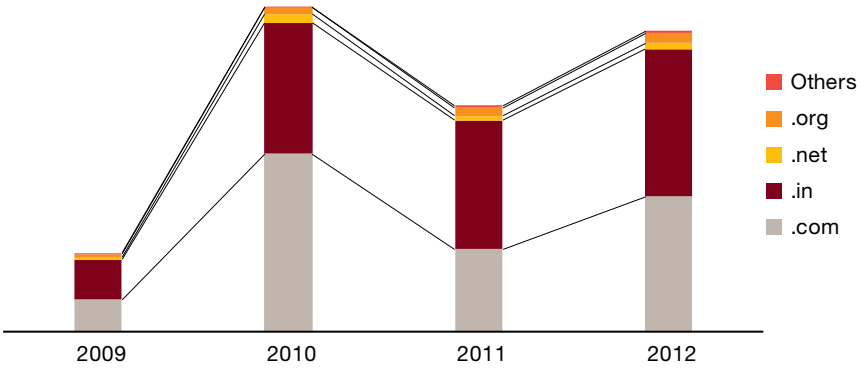
Adding hacking to political activism gives us hacktivism, a phenomenon that has emerged recently in India, marking 2011 as the 'year of the hack'.

In addition to website defacement and distributed denial of service, hackers have been making use of social media for newer sophisticated attacks. Hacking attacks are tailored to target a particular organisation or entity and are often focussed on gathering sensitive data with monetary value. However, recent trends have shown a change in the data security landscape.

Traditionally, companies and organisations have been trying to fight off digital attacks by cyber criminals looking for information that can be sold for money, but the aim of hacktivist groups is to get sensitive information belonging to the organisation for social or political purposes and not for financial gain. Hacktivists typically carry out DDoS attacks to disrupt a website's operations.

Nearly14,000 websites were hacked by cyber criminals till October 2012, an increase of nearly 57% from 2009.

Number of Indian websites defaced



Defaced websites have been a common concern among government departments and private organisations. Website defacement is a form of hacking. It involves substituting the home page of a website by a system cracker that breaks into a web server and alters the hosted website, creating one of his own. The total number of websites defaced in 2012 was 23014, a 282% increase since 2009. Of these, websites with .com and .in domains experienced the highest number of attacks.[2]

[2] Crime in India' report 2007-2011, (National Crime Record Bureau)

The protests continue

2012 was the year of protests across the country. The worldwide group of web hacking activists, known as 'Anonymous' held protests in several cities against what they claimed was the 'growing censorship of the internet by the government' in the country.

A brief overview of Anonymous India's infamous hacks during 2012 is as follows:

Anonymous takes down the website of Indian political party and the Supreme Court of India	A day after the government proposed a new plan to censor the internet, the websites of an Indian political party and the Supreme Court of India went offline for a couple of hours, caused by an attack by Anonymous India.
Anonymous hacks into leading broadband and telecommunications company servers	A leading broadband and telecommunication company's customers were unable to access Facebook, Twitter and other sites for several hours after hacker group Anonymous reportedly hacked into their servers.
Defacing of political party websites	Anonymous downed a political party's website and the parent party's website, with a message and a nice background score. This was in retaliation for the opposition to not having done anything to curb the government's web censorship policies.
Official website of IT minister defaced	Anonymous hacked into the official website of the IT minister and defaced it with unflattering comments about his mental abilities.
State-owned telecom company website down for six hours	An Indian state-owned telecommunications company website was attacked by Anonymous, accusing the company of censoring content on the internet.
Anonymous India brings down an educational institution's website	Websites of one of the major educational institutions was hacked into and brought down for nearly nine hours by this group.

The impact

Hacktivism results in major reputational damage to targeted organisations and government agencies. Hacktivists use social media to publicly announce the details of their attacks. This also has an impact on the brand value of a company that has been a victim of hacking as customers lose faith in the organisation's information security. Moreover, hacktivism leads to high-profile information breaches and data loss.

The organisations targeted by hacktivists are not the only victims. The spilling of personal details, such as login credentials, email addresses and even physical addresses puts many innocent people at a greater risk of phishing, spamming and identity theft. The impact caused by this phenomenon is evident from the incidents highlighted below:

1 *Leading fast food service restaurant's India website hacked, customer details leaked*

In September 2012, the Indian website of a popular fast food retailer was hacked into by a Turkish hacker group. Details of about 37,000 accounts, including names, phone numbers, email addresses, passwords and city details were leaked.

The company's India website was hacked into using the SQL injection method and remote file inclusion, one of the most common methods for stealing private data from web databases. Through this, the hacker typically tricks the site's database into revealing data that should be hidden by 'injecting' certain commands.
(Source: www.business-standard.com)

2 *Leading software corporation's store hacked, usernames and passwords stolen (India)*

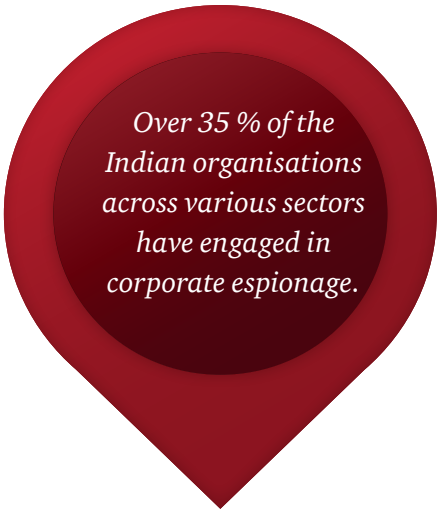
In February 2012, hackers, allegedly belonging to a Chinese group, struck at the company's website, stole login IDs and passwords of people who had used the website for shopping.

Following, the members of the group posted a message on the company's website saying 'unsafe system will be baptised'. The website seemed to have been taken offline by the software corporation.
(Source: The Times of India)

Corporate espionage: India's new booming sector

With increased economic pressure, ever increasing competition and proliferation of new technology platforms, companies are using every possible opportunity to position their brand, launch new products and retain the best people through personal websites and social media. Consequently, the threat landscape resulting from corporate espionage has evolved and has now gone digital, becoming more dangerous. Corporate spying is prevalent in sectors such as electronics and infrastructure, which are considered more vulnerable to fraudulent practices.

Facing the threat are an organisation's intellectual property (IP) (electronic communications and files), research and development (R&D) reports, large databases, sensitive networks and information like research and development processes, innovations, product specifications, new marketing and sales strategies . Corporate espionage cases are being reported from across sectors -IT-BPO, infrastructure, FMCG, banking, insurance, manufacturing and telecom sector.



According to a survey by the Associated Chambers of Commerce and Industry of India (ASSOCHAM) more than 35% of companies operating in various sectors across India have been engaged in corporate spying to gain an edge over their competitors and have even started spying on their employees via social networking websites.

Corporate espionage has become a major concern for organisations as almost 80% CEOs are using services of detectives and surveillance agencies to spy on their ex-employees, employees' lifestyle, know their whereabouts constantly apart from the usual pre and post-employment verification[3].

Some recent cases

Private insurance company data stolen	In 2013, the customer data of a reputed private insurance company was stolen by three people and used for negative publicity of the company, its policies and schemes. These individuals were owners of a rival company and indulged in corporate espionage. They breached the Information and Technology Act and section 379 of the Indian Penal Code for committing theft of customer data. (Source: DNA)
A leading multinational conglomerate company levelled corporate espionage	In 2012, a leading multinational conglomerate company levelled corporate espionage charges against an employee of another conglomerate for stealing a particularly sensitive display technology used in smartphones and other mobile devices. Samsung is seeking recourse in the courts demanding the accused firm to make a public apology pay a fine of roughly about 10,000 USD and guarantee that it will not steal engineers moving forward. The accused is filing a countersuit alleging defamation. Six employees of the accused are expected to be involved in this. The judgement is still awaited. (Source: www.intelNews.org)

[3] Economic Times – 2011 (Corruption trouble: Corporate espionage on rise in India)

Social networking sites such as Facebook, Orkut, YouTube, Twitter, Google+, Linkedin and others are being heavily used to dig out relevant information about rival companies, their schemes, policies, new products, confidential information, financial details, prior announcement of senior management moving out and attrition of employees.

According to the ASOCHAM survey [4], 73% top officials in various companies have been a victim of corporate espionage via social media.

It is possible for anyone, including competitors, to learn about an organisation's core values, hierarchy, communication style, organisational motivation, industry environment, employee morale, business challenges, systems and processes, competitive information and intellectual property through direct revelations, unmonitored tweets and logical deductions gathered from social media. Corporate espionage is not only prevalent at corporate level but is being practiced at an individual level as well.

Organisations are increasingly using social networking sites to keep a track of their rival companies and employees.

The impact

Corporate espionage within the workplace and corporate environment can have a devastating impact on the business entity in which it is occurring. The losses can also have an impact on the confidence of the local, state or national economic conditions based on the size of the business affected by such an activity. It's difficult to quantify the potential losses due to corporate espionage since it's not easy to measure what effect a stolen ad campaign might have had, or how a stolen design might have dominated the market. But it's hitting the Indian market in a big way. IP theft and theft of confidential data are likely to happen via corporate espionage.

As an instance in 2011, a leading manufacturer of engineering solutions agreed to pay Pennsylvania-based company 38 million USD to settle a lawsuit over the alleged theft of proprietary water purification technology [5].

[4] Corporate espionage via social media rampant in India Inc.: Assocham Survey 2012

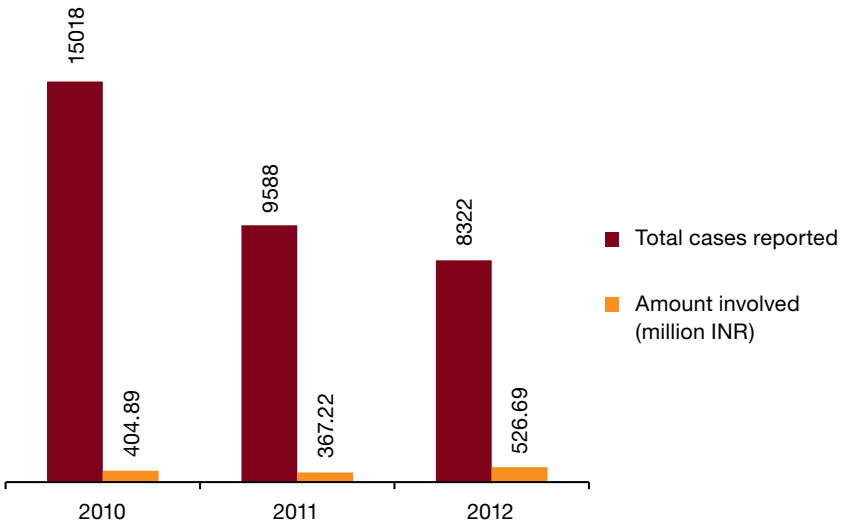
[5] http://www.globalpost.com/dispatch/india/101223/industrial-espionage-corporate-india

Phishing and skimming: An epidemic for financial services

Majority of the banks in India have migrated to online and mobile banking. Most of the transactions are conducted via payment cards, debit and credit cards, and electronic channels such as ATMs. Consequently, both private and public banks, as well as financial institutions in India are becoming increasingly vulnerable to sophisticated cyber attacks.

According to the RBI, 8322 cases of cyber frauds were reported in 2012 amounting to 527 million INR. Although the number of cases reported has decreased from 15018 cases reported in 2010, the amount involved in such cases has increased from 405 to 527 million INR in 2012 implying that the average value per cyber fraud case has increased significantly.

Total cases reported
Amount involved (million INR)



One of the most common forms of cyber attacks relating to banks is phishing, a financial scam in which fraudsters use social engineering techniques and spyware or malware codes to steal confidential financial and personal information of customers such as bank account numbers, credit card numbers, internet banking passwords, etc. These details can also be used for siphoning money off customers' bank accounts, a loss that has to be ultimately borne by the banks themselves. Typical phishing attacks involve sending emails messages to customers containing logos or images impersonating to be financial institutions.

These emails usually contain a web link which is a malicious web page that looks exactly like the financial institution's webpage. Majority of these attacks are done for financial gain.

As per a recent study India ranks among the top five countries targeted by phishing attacks, accounting for 7% of the world's total phishing attacks.

In 2012, there was 187% increase in phishing attacks on various Indian banks.

One in four phishing attacks used the .IN domain and involved targeting the bank balances of customers. Although these attacks originated from all over the world, Hyderabad hosted the second highest number of phishing attacks in the country. Interestingly, emerging cities such as Chandigarh, Bhubaneshwar, Surat, Cochin, Jaipur, Vishakhapatnam and Indore are also experiencing phishing attacks.[6]

Some recent cases

RBI warns against fraud emails	In May 2012, the RBI warned against fraud emails from mail id: alert@rbi.org. The mails were sent by unscrupulous entities offering a new online security platform and asking customers to share information. According to the mail, the new online security platform offered to prevent online identity theft in internet banking. The email further asked the recipient to download attachment and update their information. The RBI cautioned the public not to open such emails or try to download the attachment on their computer. (Source: The Economic Times)
Police bust gang of fraudsters phishing bank accounts	In April 2012, an Indore-based gang of fraudsters involved in phishing the accounts of customers across the country of two leading banks in India were busted. The gang had opened fictitious accounts in their names in at least two dozen different banks in the city. These accounts were utilised to siphon off the money from the account holders of these banks through phishing. The money was later withdrawn from the fictitious account through ATM or cheques. The accused have been booked under section 419, 420 IPC and 66 IT Act. Further investigations are on. (Source: The Times of India)

[6] Symantec Intelligence Report, May 2012

Social media sites such as Facebook, Twitter and LinkedIn might not be the real source of cyber crime, but criminals can use them effectively (phishing attacks). For example, they may use these techniques to collect information on a target (also known as 'spear phishing'), research members of staff, or install malware on the target's computer, very easily.

Credit cards have always been one of the biggest targets for cyber criminals; the most common form of credit card frauds involves skimming. With the rapid increase in the use of plastic money, India is witnessing a tide of skimming frauds.

Skimming is a hi-tech forgery that involves copying of customer and card information stored on the magnetic strip of a credit card, including the CVV number, by using an electronic device known as the 'skimmer'. When the credit card is swiped through such a device, it reads and captures the information stored on the credit card. This information is used by the fraudster to create a cloned card which can then be used to make unauthorised and fraudulent transactions. Skimming frauds are extremely difficult to detect as the credit card is not actually stolen or reported. The customer to whom the card belongs becomes aware of the fraud only when a transaction is made using the cloned cards.

Between Oct-Dec 2012, there were 1590 cases of credit card frauds reported involving an amount of 94.86 million INR.

The number of credit card frauds is increasing despite the various proactive measures taken by Indian banks to set up internal control systems to mitigate frauds relating to skimming or cloning of credit cards. As per the RBI statistics, in the quarter ended December 2012, there were ***1590 cases of credit card reported involving an 94.86 million INR*** as compared to 1327 cases reported in the quarter ended September 2012 involving 49.29 million INR.

The two most common types of skimming attacks occur at the following locations:

- ATMs
- PoS (point of sale), either by employees who use handheld skimming devices or fraudsters who swap PoS devices with devices that have been manipulated to capture unauthorised card information. e.g., swiping credit cards at restaurants or petrol pumps.

Most banks believe that the card information is captured through retail outlets that have been compromised. The cases range from fraudsters using captured information for making international online transactions or for transactions used in local shops. Despite implementing various controls, credit card skimming continues to rise.

Some recent cases

Skimming fraud hits Chandigarh petrol pumps	In January 2013, two residents of Chandigarh received credit card bills for shopping done in Mumbai and Hyderabad. The money was deducted from their accounts before they could even approach the bank. People are losing money by making payments at petrol pumps in Chandigarh city. Nearly 55 cases of skimming have been reported from petrol pumps in Chandigarh over the last six months. In these cases, miscreants cloned the cards and shopped at faraway places such as Mumbai and Hyderabad. The scam is worth lakhs. (Source: The Times of India)
Credit card data hacked, crores stolen	In April, 2012, a gang of fraudsters were arrested in Hyderabad for skimming and cloning credit and debit cards using a complex modus operandi of hacking international IP addresses, internet *hawala*, and spying and electronic data theft. The racket came to light in May 2011 when people who visited two malls complained that huge amounts were withdrawn from their accounts. The gang succeeded in skimming off 4 to 5 crore INR from unsuspecting credit and debit card holders across the country — from Hyderabad to Delhi, Kolkata to Bangalore. They used 15 point of sale (electronic draft capture) skimming machines, one ATM data skimming machine, ATM dome cameras, electronic magnetic writers, card printers and ATM pin pad skimmer machines and even placed spy cameras at ATMs which picked up the PINs of users. (Source: The Indian Express)

The impact

Banks are the worst hit when it comes to cyber frauds, particularly phishing scams. As per the RBI statistics, cyber crime in Indian banks accounted to around 527 million INR in 2012 as compared to 405 million INR in 2010. In most of the cases relating to phishing attacks affecting banks, it was observed that phishing attacks not only cause reputational damage and customer loss, but the banks have to bear the loss caused to customers on account of money siphoned off their bank accounts.

Top card issuing banks have seen unauthorised transactions totalling around 300 million INR so far by an international syndicate.

Financial losses due to cyber crime in Indian banks accounted for close to 527 million INR in 2012, a 30% rise from 2010.

Moreover, between October to December 2012, the Indian credit card industry was targeted by a series of credit card frauds involving skimming and cloning of card information leading to unauthorised transactions totalling around 300 million INR.[7]

Top card issuing banks have seen unauthorised transactions totalling around 300 million INR so far by an international syndicate.

Most banks believe that the card information is captured through retail outlets that have been compromised. The cases range from fraudsters using captured information for making international online transactions or for transactions used in local shops. Despite implementing various controls, credit card skimming continues to rise.

Both the cardholder and the bank have to bear the brunt of the skimming fraud. When the fraudster makes unauthorised purchases with the cloned credit card, the credit card bill goes to the cardholder. When the credit card is swiped on the tampered skimmer device, the bank has to immediately make payment to the retail outlet where the purchase was made. However, if the cardholder can prove that he or she is not at fault, it is the bank that has to bear the loss. In India, there is no reversal of charges which means that even the money is restored to the cardholder; he or she may still have to bear a certain amount of loss. Besides this, the bank may have to incur further costs in terms of reissuing credit cards to these cardholders or even replacement of PoS machines. For instance, in the wake of recent skimming frauds, a leading bank has started replacing some PoS machines at merchant establishments.

[7] Times of India, February 2013

Cyber crime: An internal threat

Most of the cyber threats originate from within the organisation and it is a growing concern across all sectors. Actions of a single insider can cause considerable damage to an organisation including lost staff hours, negative publicity and financial damage. The source of these threats could be employees, vendors, suppliers and partners but in most instances, cyber crimes are done by existing employees of the organisation.

The fact that cyber crime is an internal threat more than an external one is not surprising since internal employees (fraudsters) have a deep insight into the organisation's functionalities, security measures and weaknesses of the internal controls that prevent fraud.

PwC analysis has shown that though the likelihood of the attack from insiders may be very low as compared to external threats, the magnitude of the impact is at least 10 times more than that of the total impact an external attacker can cause. This is because an insider attack is committed by people who know the organisation's most sensitive secrets and vulnerabilities and have access to its systems.

According to the PwC Economic Crime Survey 2011 India, 60% organisations believed that the perpetrators were among their own staff and only 36% pointed to outsiders.

Sixty per cent Indian organisations believe that internal employees are responsible for cyber attacks and economic crime.

Nearly 58% key decision makers see employees in IT department as the biggest source of cyber threat.

It was also observed that two-thirds of key decision makers in Indian organisations see insider threat as the most serious security threat facing them. The IT department is the major source of cyber threat since it has well-trained; educated and skilled staff who have access to the operating systems, databases, or business applications.

In most cases, breaches by insiders are committed by individuals who are motivated by greed, selfishness, or antagonism towards the management leaking confidential information outside the organisation.[8]

Moreover, social media sites such as Facebook, Twitter, and Linkedin, etc. are being used by insiders to commit security breaches by knowingly or unknowingly posting or sharing sensitive information of the organisation.

The impact

Insider threat not only weakens the organisation from within by exposing its sensitive information but also poses a greater risk where a malicious outsider can take advantage of an inadvertent insider leading to larger impact on an organisation. This enables fraudsters to conduct activities that cannot be easily detected. Thus, the confidentiality and integrity being compromised by employees accessing the organisation's systems and data is a primary concern.

The internal threat cannot be completely avoided as insiders will always pose threats to organisations through both malicious behaviour and unintentional mistakes. These threats cannot be mitigated by technological solutions alone. A combination of technical and administrative solutions is required to adequately address the rising tide of cyber crime from within the organisation.

[8] The threat within A study on insider threat by DSCI in collaboration with PwC

BYOD: Benefits v/s security risks

BYOD is the latest buzz word in the IT industry. Company desktops are becoming a thing of the past, as organisations are increasingly allowing, and even encouraging employees to bring their domestic, consumer devices into the workplace and access corporate applications.

This not only allows application availability at anytime, from anywhere, but can also help business slash procurement costs. The smartphone or tablet phenomenon is expected to fuel this trend, and will drive uptake of the virtual desktop infrastructure (VDI), wireless networking and end-point security solutions in the corporate arena in the coming years but this is still a distant dream for India.

The BYOD trend in India is on a rise. Today, IT leaders are abandoning their rigid outlook, lockstep approach to security and are adopting a new 'any device' policy that supports popular mobile operating systems and enables user-owned devices to connect to corporate resources.

Nearly 54% Indian organisation have accepted the BYOD model.

According to a recent survey, India stood first among its global counterparts in accepting BYOD with 54% of Indian organisations allowing employees to bring their own devices.[9]

Companies have now started to go beyond the risk-averse approach, have accepted the increasing BYOD trend and have moved beyond the basic 'BYOD' connectivity to create a better workplace experience.

A recent study report shows that BYOD is making progress within the corporate environment, with 60% of employees using personal devices for work. Interestingly, India is one of the countries with some of the highest usage–80%, second only to China with 92 %. The report also shows that 82 % of companies say they already allow BYOD or will do so within the next 24 months. It is a relatively recent trend where employees are allowed and even encouraged to bring personally-owned devices to workplace and use them to access company resources such as email, file servers, and databases.[10]

[9] ISACA (Information Systems Audit and Control Association), 2012 IT Risk/Reward Barometer

[10] CISCO Study, 2012

Most organisations, globally, are now enabling BYOD in the enterprise, with a staggering 95% of respondents saying their organisations permit employee-owned devices in some way, shape or form in the workplace. This study also concluded that the average number of connected devices per knowledge worker is expected to reach 3.3 by 2014, up from an average of 2.8 in 2012. BYOD is perceived by most respondents to be a gateway to greater business benefits. Over three-fourths (76%) of IT leaders surveyed categorised BYOD as somewhat or extremely positive for their companies, even while seeing significant challenges for IT.[11]

The above reports show that the BYOD trend has arrived in India and is expected to rise in the near future. However, with the increasing use of mobile devices at work provide unexpected and unlimited opportunities for cyber criminals to attack mobile devices and wireless networks. Phones and mobile devices can be targeted in denial of service attacks, and cyber criminals may also exploit mobile banking applications to carry out fraudulent activities.

According to a study conducted by PwC in 2013 on BYOD, the weakest link in mobile device security is often the user and liability often originates at the top. C-level executives have exceptions to use personal devices, but these leaders pose the greatest risk because they have access to the company's most important information. There are numerous benefits of BYOD that are undeniably compelling but at the same time it opens the door to potential data breaches and leakage through mechanisms such as malware.[12]

[11] Study report published by British Telecommunications plc (BT), 2012

[12] PwC study - Bring your own device: Agility through consistent delivery 201

Cloud computing: A new source of cyber threats

The growing popularity as well as dependency on cloud computing and virtualisation among companies could lead them to being possible targets of cyber criminals. Cloud computing, on one hand, offers significant benefits and cost savings but on the other hand, moves servers outside the traditional security perimeter bringing it within easy reach of cyber criminals. As more data gets distributed around the internet via 'cloud', opportunities for data infection or theft are increasing. This has posing new complications to the security landscape of various Indian organisations[13].

The rise of cloud computing has complicated the security landscape for organisations.

Only 31% organisations have strategies for cloud computing indicating a lag in adoption rates.

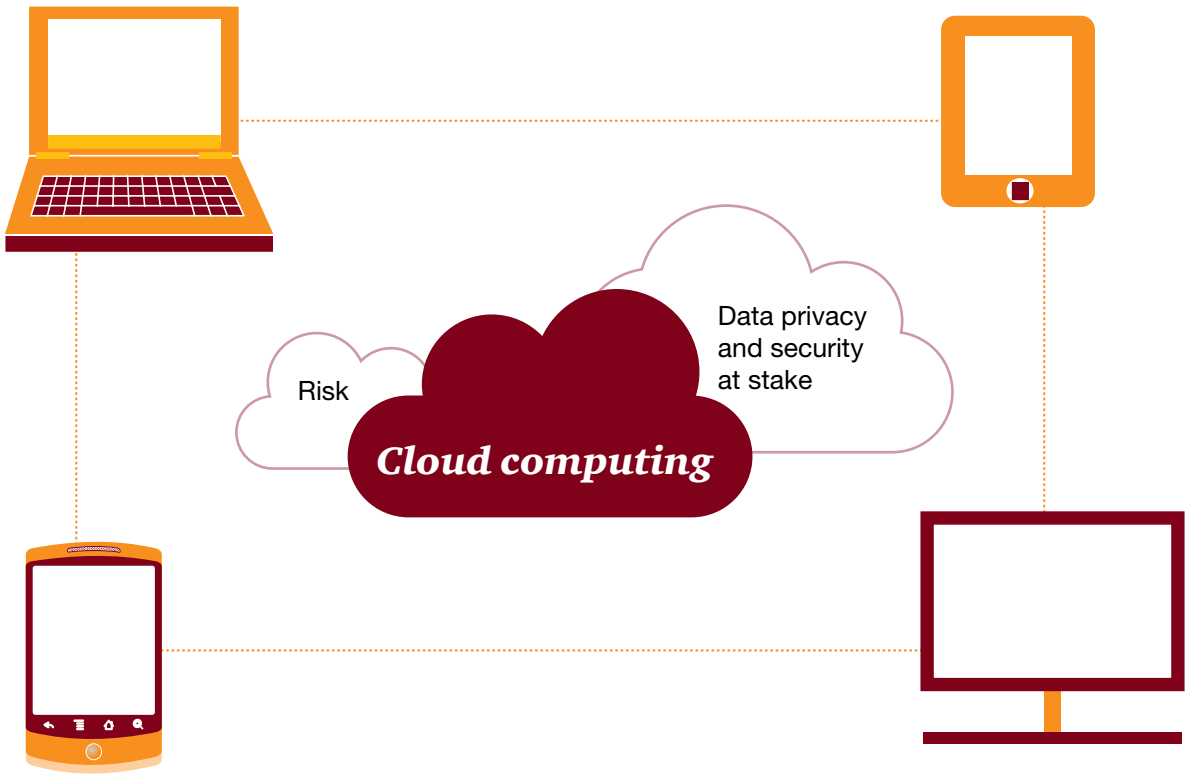
[13] Annual information security survey (2011), conducted by PwC in conjunction with CIO and CSO magazines

One of the top concerns with cloud computing is the issue of data privacy and security. Cloud computing represents a risk, as it moves data and information into the hands of a third-party provider for storage, processing, or support. Cloud computing builds a new layer of risk especially where sensitive data resides such as wide distribution of information across different jurisdictions, with different legal frameworks regarding data security and privacy and making it even more difficult to govern and regulate the information.

Other challenges that cloud computing poses are around governance, tie-in to the vendor, extension of the security model to the provider, connectivity and reliance on third party SLA's. Cloud computing security issues are largely unresolved in India, since it has no formal cyber security law in place covering this new technology. The lack of clear legislative safeguards has resulted in increased risks for companies adopting cloud computing.

India is not yet ready for cloud computing as most of it is dependent on service providers and many organisations do not have mature IT infrastructure to mitigate the risks posed by cloud computing. In India, technology adoption is moving faster than security implementation for new technologies. Only 31% of the organisations in India have strategies for cloud computing.[14]

Thus, before going for cloud computing services organisations should be aware of vulnerabilities resulting from the use of cloud services and mindful of the availability of cloud services to employees within or outside the organisation.



[14] PwC's Global State of Information Security Survey, 2013

Cyber threats: Adopting proactive approach to tackle it

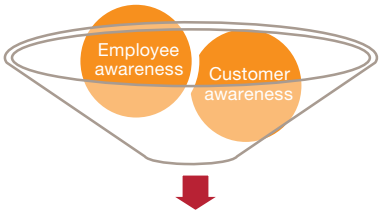
Corporations in India will need to adopt proactive steps to ensure that cyber threats do not result in erosion of business value. Organisations need to adopt an effective cyber crime strategy that balances preventive, detective and response measures.

Overall as a first step, organisations must get senior management involved in addressing high priority cyber issues, as well as creating a sustainable programme and culture to remediate security issues on an ongoing basis. Information security and the protection of customer information should be treated from a cultural perspective and senior management should be involved in the same way other industry safety regulations are treated at the company.

Preventive measures:

1 ***Providing proactive and ongoing education and training:*** Security policies, risks, etc. for customers and employees as well as new technologies such as new devices, social media, software as a service, cloud computing, advancement in e-businesses, etc. will help mitigate cyber incidents. These are as follows:

- Stakeholder workshops with industry SMEs and enhanced employee training are important to mitigate the risk of cyber crime within the organisations. Face-to-face training should be given to employees and it is the most effective form when it comes to cyber crime awareness.
- Customers should be well-informed about emerging cyber attacks through messages, mails and social media.

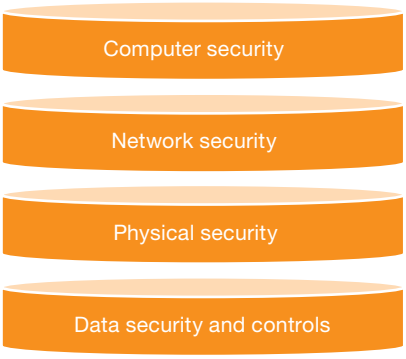


360 - degree situational awareness

2 ***Cyber intelligence team:*** Setting up a cyber intelligence team will help companies to analyse situational awareness and provide warnings of cyber threats in advance. It will also assist companies in discovering, tracking and reporting on global network events of interest that are identified by the team and/or systems, utilising available cyber intelligence analysis data and methods.

3 ***Companies need to carry out risk assessments:*** Organisations should prepare themselves for cyber threats, by focussing on understanding the risks their organisation faces, identify vulnerabilities in existing IT infrastructure, prioritise the impact of those vulnerabilities based on the value of affected information and technology assets, and then identify, implement and continually assess the necessary controls and countermeasures required to mitigate those vulnerabilities.

4 ***Organisations need to deploy comprehensive policies:*** Organisations need to cover network security,device security, physicalsecurity, data privacy andsecurity, BYOD strategy, cloudstrategy, social media security,etc. and align them with technical and corporate culture changes,company's people processesand other key internal controls. These are as follows:



- **Computer security**
  - Full disk encryption
  - Encryption training
  - Identity management or single sign on
- **Network security**
  - Web application testing
  - Network penetration testing
- **Physical security and controls**
  - GPS tracking devices on laptops
  - Access control changes
- **Data security and controls**
  - Risk assessment
  - Revised incident response procedures

Detective measures

1 As far as hacking and intrusion into computer systems is concerned organisations should preserve computers used by web administrators responsible for its website and regularly analyse the server logs to identify unauthorised logins and file transfers to the web server. Apart from these, organisations should adopt the following remedial measures:

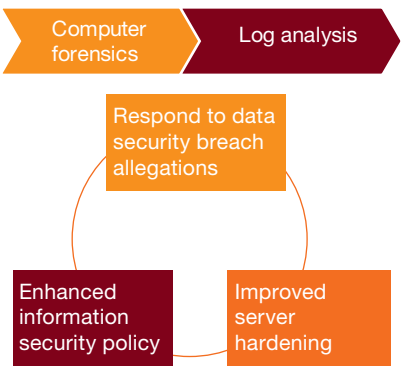
- **Respond to data breach allegations:**

  Knowing the facts about the compromised website, the company will be in a position to effectively respond to the data breach allegations.

- **Server hardening:**

  Web application development and improved server hardening technologies should be developed to help prevent a future computer intrusion.

- **Enhanced information security policy:**Implementation of enhanced information security policy regarding use of remote access technologies can help mitigate the risk of cyber attack.



2 Other security technologies will help companies detect cyber crime and take a proper response measure to mitigate the risk. These are as follows:

- **Intrusion detection system** will help organisations to inspect all of the inbound and outbound network activities and identify suspicious patterns that indicate an attack that might compromise a system.

- **Honeypot** is a device intended to be compromised and to detect cyber crime companies can have the system probed, attacked and potentially exploited.

Response measures

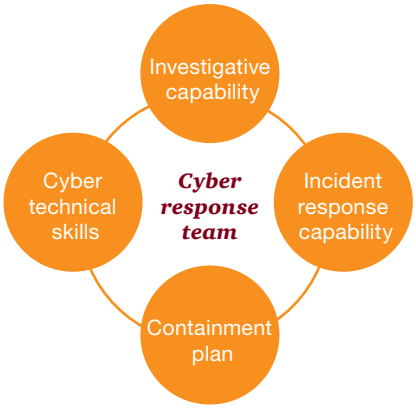
1 Companies need to create a cyber incident response team through which an incident spotted anywhere in the business cab be tracked, risk-assessed and escalated. They need to execute the following:

- Companies need to develop a customised internal incident response capability for the client to investigate complex cyber incidents.

- There is a need to identify technical and human resources to deploy to respond to both an internal or external cyber crime incident.

- Development of a consistent approach will help contain an advanced cyber threat.

- Employing technically skilled resources will help in responding to future cyber intrusions.



2 Organisations need to take a tougher and clearer stance on cyber crime the organisation should take legal action against cyber criminals andannounce what it's doing about threats and incidents.

Conclusion

Since rapid and dynamic changes in the technology space are throwing open new ways of doing business, organisations have to find out appropriate ways to tackle the 'new age' sophisticated cyber crimes emerging in India. Increasing use of mobile and online banking, smart phones and personal devices, social media and cloud computing offer a wealth of attractive business solutions and opportunities to organisations but at the same time they can also pose a plethora of information security risks.

With the increasing number and diversity of cyber crimes in India, it is of paramount importance for organisations to develop a response mechanism that enables them to understand and embrace the risks and opportunities of the cyber world on an ongoing basis. Despite implementing various internal controls, cyber crimes continue to rise at an increasing rate.

Today, more and more organisations in all sectors are seizing the opportunities created by the internet. In our PwC's view, organisations that incorporate cyber awareness and responsiveness in every employee, every decision and every interaction and are aware of the current and emerging cyber environment will be the ones to gain competitive advantage in today's technology-driven environment.

Notes

About PwC India

PwC* helps organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with more than 180,000 people who are committed to delivering quality in assurance, tax and advisory services.

PwC India refers to the network of PwC firms in India, having offices in: Ahmedabad, Bangalore, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, please visit www.pwc.in.

*PwC refers to PwC India and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

You can connect with us on:

facebook.com/PwCIndia

twitter.com/PwC_IN

linkedin.com/company/pwc-india

youtube.com/pwc

Contacts

Satyavati Berera
Tel: +91 124 330 6011
Email: satyavati.berera@in.pwc.com

Sivarama Krishnan
Tel: +91 124 330 6018
Email: sivarama.krishnan@in.pwc.com

Siddharth Vishwanath
Tel: +91 22 6669 1559
Email: siddharth.vishwanath@in.pwc.com

Arup Sen
Tel: +91 22 6669 1078
Email: arup.sen@in.pwc.com

Harpreet Singh
Tel: +91 124 330 6012
Email: harpreet.singh@in.pwc.com

Kumar Dasgupta
Tel: +91 22 6669 1341
Email: kumar.dasgupta@in.pwc.com

Manpreet Singh Ahuja
Tel: +91 124 330 6021
Email: manpreet.singh.ahuja@in.pwc.com

Neeraj Gupta
Tel: +91 124 330 6010
Email: p.neeraj.gupta@in.pwc.com

Sanjay Dhawan
Tel: +91 80 4079 7003
Email: sanjay.dhawan@in.pwc.com

Tapan Ray
Tel: +91 22 6669 1204
Email: tapan.ray@in.pwc.com
**National Practice Leader (RAS)*

www.pwc.in

PD 485 - April 2013 Invading privacy: Cyber crimes on the rise.indd
Designed by: PwC Brand and Communications, India