www.pwc.in

Managing cyber risks in an interconnected world

Key findings from The State of Information Security Survey 2015, India

pwc

Contents

"The future of security is here; at its heart is the 'human parameter.' Organisations in India need to work harder as well as faster, and align with it."

Sivarama Krishnan
Executive Director
PwC India

Foreword

Cyber security threats today have become increasingly sophisticated and complex. Organisations, however, have not been able evolve at the same pace. As organisations move ahead and embrace new technologies without fully comprehending the implications these have on the entire enterprise, they are rendering themselves susceptible to an array of cyber-security threats.

The conventional 'technology-centric' approach has now become outdated and a more comprehensive and strategic approach to tackle these evolving threats is essential. As the enterprise network boundaries are getting blurred, a new approach, rooted in technology, but one that also includes other key aspects such as people and processes is needed. In fact, it is time to focus on the human parameter.

An efficient and executable strategy is one that is agile and can adapt to the changing threat landscape. Through our report, we were able to assess the cyber-security outlook of Indian organisations and compare it with their global peers. This helped us identify the attributes of security leaders, whose practices in other organisations can enhance cyber-security posture.

We are certain that this report depicts the cyber security stance of organisations in India with accuracy and look forward to hearing from you, so that we can make our future surveys even more engaging.

#01

Cyber risks
Endangering the present

Cyber security: Rising concern

Cyber security is no longer an issue that concerns only IT and security professionals. The impact has extended to the C-suite as well as the boardroom. It is now a persistent business risk. Awareness and concern about such security incidents and threats are a priority for the consumers as well. To sum it up, few risk issues are as all-encompassing as cyber security.

Media reports of security incidents have become as common as the weather forecast, and over the past 12 months, virtually every industry sector across the globe has been confronted by some kind of cyber threat.

As incidents proliferate, governments are becoming proactive in helping organisations fight cyber crime. A recent report by FireEye Labs and CyberSquared Inc's Threat Connect Intelligence Research Team (TCIRT) uncovered cyber espionage activities by an Islamabad based group targeting Indian companies. It appears that the group initiated the `Bitterbug' malware that spread through documents, compromising organisations in India.

In North America, the US Department of Justice (DOJ) charged five Chinese military hackers with conducting cyber economic espionage against American companies in the nuclear power, metals, and solar energy sectors. This was the first time that the US charged state officials with economic espionage using external cyber attacks under section 1831 of the Economic Espionage Act.

In Verden, Germany, city officials announced the theft of 18 million email addresses, passwords as well as other information.

Closer home, huge heists of consumer data were reported in South Korea, where 105 million payment card accounts were exposed in a security breach. On similar lines, cyber thieves plundered more than 45 million USD from worldwide ATM accounts of two banks in the Middle East.

Instances of state-sponsored espionage were uncovered by security firm Symantec, which discovered attacks against major European governments that have been underway for at least four years. Geopolitical discord, most notably between Russia and Ukraine, resulted in a volley of cyber attacks between the two nations that took down and defaced government websites on both sides of the conflict, as well as spread malware to the embassies' computers.

Recently, computer systems at the Eastern Naval Command in Visakhapatnam, where the indigenous nuclear submarine Arihant has been undergoing sea trials, were breached by Chinese hackers. Reports of breaches of DRDO computer systems resulting in the leak of sensitive files also surfaced in the recent past.

Financial service companies continue to be primary targets. A survey of 46 global securities exchanges conducted by the International Organisation of Securities Commissions (IOSCO) and the World Federation of Exchanges found that 53% had experienced a cyber attack. According to a report by Arbor Networks, there has been a significant increase in attacks on financial organisations in India, up from last year's 15% to 34% this year.

Other critical infrastructure providers are also prone. In India, an NTRO analysis revealed that in recent years, the Stuxnet worm had infected computers at critical infrastructure facilities such as the Gujarat and Haryana electricity boards and an ONGC offshore oil rig.

On similar lines, a hacker group successfully infiltrated a US public utility via the internet and compromised its control system network. The intrusion was halted before any damage was done. Sophisticated state-backed cyber adversaries employed powerful malware to infect the industrial control systems of hundreds of energy companies across the US and Europe.

One of the year's most far-reaching incidents was the Heartbleed defect, which impacted almost two-thirds of the web servers around the world, including some of the most popular email and social networking sites. It is believed to have compromised millions of websites, online shopping destinations, security applications, as well as software such as instant messaging, remote access tools and networking devices.

The Computer Emergency Response Team of India (CERT-In), the nodal agency for combating hacking and phishing as well as fortifying security-related defences of the country's internet domain, has categorised the severity of the Heartbleed virus as high, fearing it can compromise personal data in India as well.

While telcos in India are advocating faster adoption of the 'internet of things' (IOT), they are also besieged with the challenge of securing an ecosystem of devices that interconnects information, operational and consumer technologies.

Increased focus among regulators around the world

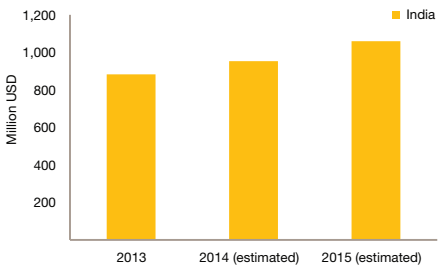
In an indication of how the regulatory landscape is evolving, the US Securities and Exchange Commission (SEC) Office of Compliance Inspections and Examinations (OCIE) recently announced that it plans to examine the cyber security preparedness of more than 50 registered broker-dealers and investment advisors.

Executives from multinational organisations are keeping track of the European Union Data Protection Regulation, scheduled to be finalised in 2015. The regulation is expected to add new requirements for breach notification to individuals and will require organisations that handle personal data to conduct risk assessments and audits, as well as increase the fines for compromised businesses.

The Singapore Personal Data Protection Act establishes new standards for the collection, use and disclosure of personal data. The new guidance highlights several unique requirements, such as suggesting that organisations have cyber insurance and are able to produce a comprehensive inventory of all security incidents and breaches.

The Indian government is strengthening cyber security both in the private and public space. Besides existing initiatives and legislations such as the Information Technology Act 2008, it is actively considering the Data Privacy and Protection Act, which will spell out stringent requirements for data privacy and protection. The government also launched the National Critical Information Infrastructure, the National Cyber Coordination Centre of India (NCCC) besides creating the Triservice Cyber Command for Armed Forces of India. These oversight bodies are expected to establish relevant cyber security postures for their respective domains.

India's security market size



Cyber security services: Expanding market

In the wake of increased incidents and heightened regulations, corporations and government agencies are struggling to safeguard their data and networks; a push that is catalysing the growth of cyber security solutions and technologies.

Following are the four key drivers for information security market growth in India:

- Increasing sophistication and frequency of attacks
- Increasing number of financially and politically motivated attacks
- Slew of legislations focused on security and privacy
- Increasing IT expenditure

Gartner predicts that the global IT security spending will increase 7.9% to reach 71.1 billion USD in 2014, and grow an additional 8.2% to reach 76.9 billion USD in 2015. It estimates that India's security market size will jump to 1 billion USD in 2015. In India, consulting, implementation, support and managed security services comprise 55% of the market.

#02

Cyber attacks
Financial impact

Rising year-on-year incident cost

Given the nature and number of prominent security breaches over the past year, it comes as no surprise that the cost of incidents reported in the State of Information Security® Survey, India 2015 has risen, year-on-year.

The annual survey of security, IT and business executives in India found that the total number of security incidents detected by our respondents was over 1 million this year, which translates to 2,800 attacks per day, every day.

Interestingly, these numbers represent only the total incidents detected and reported by the respondents to our survey. Many organisations in India continue to be unaware of such attacks, while some others do not report detected incidents for strategic reasons or because the attack is being investigated as a matter of national security.

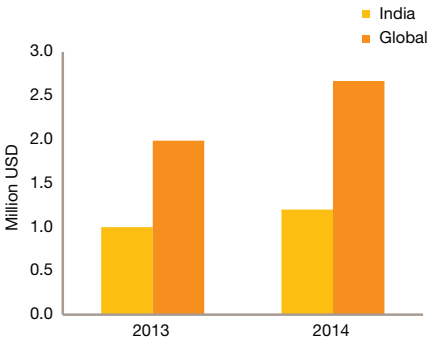
It seems certain, given the technical sophistication of today's well-funded threats, that a substantial number of successful incidents go undiscovered.

Financial losses increase apace

As security incidents become more frequent, the costs of managing and mitigating breaches also rise.

The global annual estimated reported average financial loss attributed to cyber security incidents was 2.7 million USD, 34% more than in 2013. In India, it rose to 1.2 million USD, almost 20% more than the previous year.

Average financial loss attributed to security incidents

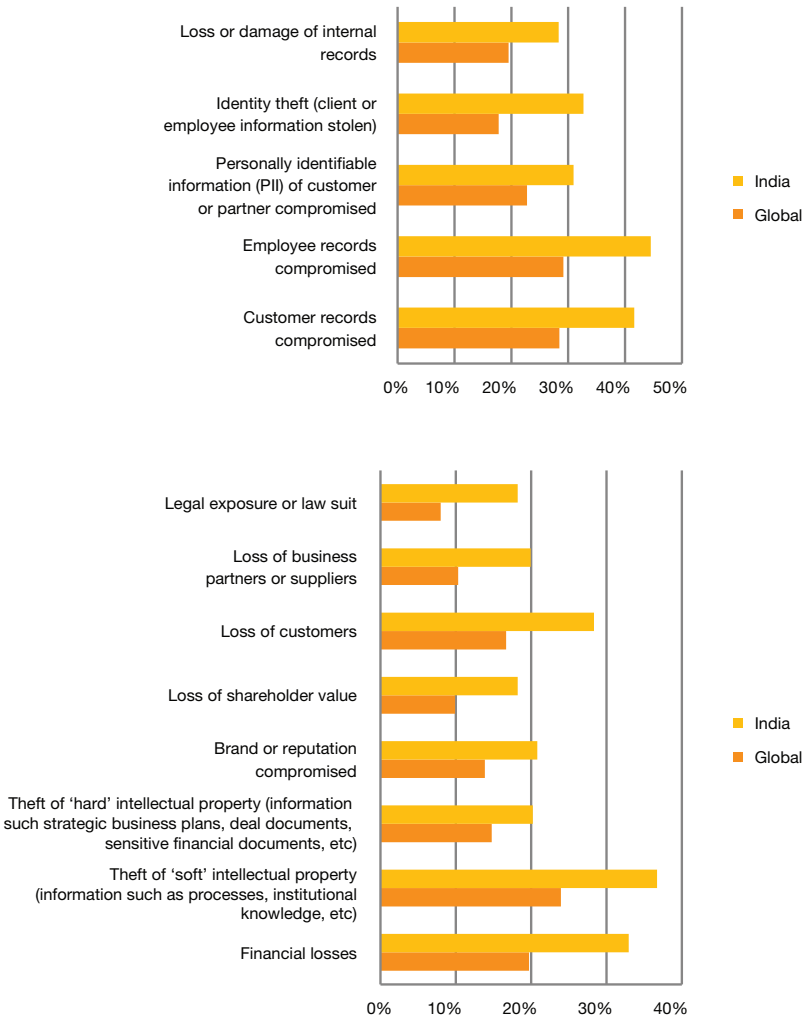


Rise in the average cost of incidents is primarily a consequence of today's more sophisticated compromises, often extending beyond IT to other areas of the business.

As with the total number of incidents, the global loss due to cyber crime cannot be calculated as many attacks do not get reported and the value of certain types of information, intellectual property in particular, is difficult to ascertain. A recent study by the Centre for Strategic and International Studies noted the difficulties in estimating financial impact but stated that the annual cost of cyber crime to the global economy ranges from 375 billion USD to as much as 575 billion USD.

However, these figures seem small when compared with the estimates of losses that can result from the theft of trade secrets and intellectual property. The impact of this type of information loss can be measured by financial as well as non-financial indicators. Financial impact may include decreased revenues, disruption of business systems, regulatory penalties and the erosion of customers. Non-financial impact may include reputational damage, product piracy, diversion of R&D information, impacts to innovation, stolen product designs or prototypes, theft of business and manufacturing processes as well as loss of sensitive information such as M&A plans and corporate strategy.

Impact of security incidents



While risk has become universal, our security survey found that financial losses due to security incidents vary widely as per organisational size. To understand these discrepancies, we looked into how organisations measure the financial impact of security incidents.

Large companies typically spend more on information security and have more mature programmes. They are, consequently, more likely to have the processes and knowledge to accurately calculate financial losses. They can consider a full range of possible impacts, including costs associated with loss of customer business, legal defence fees, court settlements, forensics and reputational damage. Larger organisations also adopt a more strategic approach towards security by identifying sensitive assets and allocating spending to their most valuable data. They are likely to understand third-party risks through the use of security baselines for partners.

Large companies tend to have processes and technologies to actively monitor and analyse security intelligence. Should anomalies be detected, they are in a better position to have an incident response process ready. They cultivate a culture of security through employee awareness and training programmes, as well as by ensuring that senior executives emphasise the importance of cyber security across the enterprise.

#03

Cyber incidents
Sources

Employee caution is important

Nation-states, hackers and organised crime groups are not the only culprits of cyber crime.While there is no doubt that these actors are a force to be reckoned with; current as well as former employees have also been found engaging in such activities. This does not imply that all employees exhibit malicious behavior. However, they may unwittingly compromise data through loss of mobile devices or targeted phishing schemes.

Growth in high-profile crimes

Cyber incidents that garner the most attention are compromises caused by nation states, organised crime and competitors and are among the least frequent. That's of little comfort, however, considering that our survey results show that these attacks are also among the fastest growing threats.

In-line with global trends, this year in India, we found a two-fold increase in the number of respondents who say they have been compromised by nation-states. Given the ability of nation-state adversaries to carry out attacks without detection, we believe the volume of compromises is, in all probability, under-reported.

The battle against nation-state crimes is compounded by the fact that timely sharing of cyber-threat intelligence is a challenge for most countries, including ours. Only a few countries, such as the US, Canada, the UK, Australia and New Zealand, have the ability to effectively share cyber-attack information with companies headquartered in their respective countries.

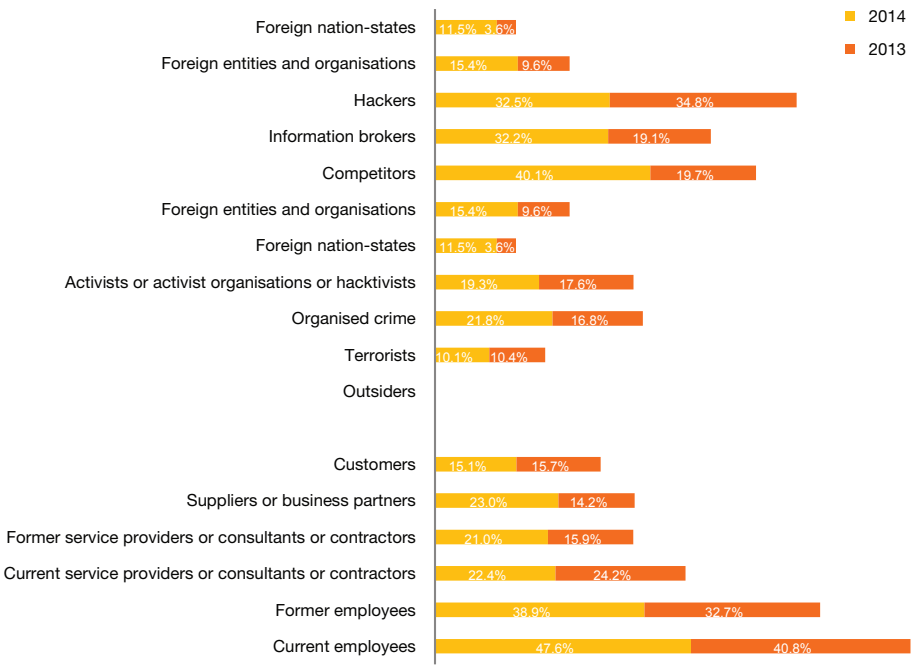
The security incidents attributed to competitors, some of whom may be backed by nation-states, doubled from last year's figure to a whopping 40%. The reason for this increase may be that companies are discovering that, as information is increasingly being stored in digital formats, it is easier, cheaper, and quicker to steal IP and trade secrets than to develop capabilities themselves.

The rise in cyber-crimes attributed to nation-states and competitors is concurrent with an increase in theft of intellectual property and other types of sensitive information. This year saw a 46% jump in cases of theft of 'soft' intellectual property, which includes information on processes and institutional knowledge. However, fewer than 19% said that 'hard' intellectual property, such as strategic business plans, deal documents and sensitive financial documents were stolen.

Increased instances of compromises caused by organised crime

One in five (22%) respondents in India claims to have experienced security breaches caused by organised crime groups, much higher than the global average of 15%. Organised crime groups are typically motivated by financial gain. A successful cyber-attack can get millions of payment card records that can be quickly monetised.

Likely sources of incidents



#04

Cyber security
Measures and programmes

Lack of top-level participation

Our survey reveals the lack of board level involvement in key areas of security; only 49% respondents believe that their board is involved in defining the security budget, moreover, only 39% believe that their board actively participates in reviewing current security and privacy risks.

Over 50% believe that their boards are actively involved in formulating the overall information security strategy and allocating an adequate budget to execute the strategy, which is significantly higher than the global average of 42%. Yet, this indicates that organisations have not elevated information security to a board level issue.

Our survey found that Indian IS budgets actually decreased by 17% in 2014. It seems counter-intuitive that, even though threats have become more frequent and damaging, organisations have not increased their security spending. We also believe that many organisations struggle to understand how much to spend on security and how to determine the RoI of their security outlay. In part, that's because there is no definitive data on current security risks to help inform a security spending strategy.

Although 86% respondents believe that their security expenditure will increase in the next 12 months, almost 25% cited a shortage of capital and operating expenditure as a major hindrance to information security. This, coupled with the limited involvement of the board, only represents the tip of the iceberg.

Respondents with safeguards already in place

	India	Global
Centralised user data store	63%	57%
Behavioural profiling and monitoring	55%	47%
Encryption of smartphones	53%	55%
Intrusion detection tools	55%	55%
Vulnerability scanning tools	57%	54%
Asset management tools	61%	54%
Use of virtual desktop interface	53%	51%
Protection or detection management solution for APTs	54%	49%
Security information and event management (SIEM) technologies	61%	62%

Dynamic security practices: Need of the hour

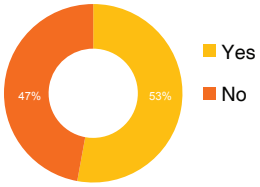
Investments need to be made in the right processes and technologies to prevent, protect, detect and respond to risks in order to have dynamic security practices in place. Many organisations, however, are failing to do so.

Given today's interconnected business ecosystem, where the amount of data generated and shared with business partners and suppliers is exponentially greater, due diligence of third parties has become a concern. It is worrisome that the focus on third-party security weakened in the past year in some very key areas; even as the number of incidents attributed to 'insiders' increased.

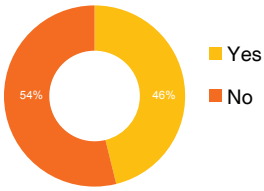
It is striking that although 86% respondents displayed confidence in their partners' or suppliers' information security practices, less than 49% have a formal policy requiring third parties to comply with their privacy policies.

Our survey evaluates the third-party due diligence competencies of organisations on the following three activities:

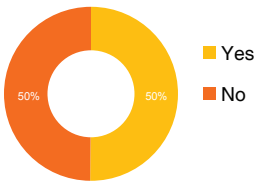
- Whether organisations appropriately inspect vendors to ensure that they have the ability to safeguard information
- Whether organisations have a robust contractual protection
- Whether organisations monitor ongoing processes to ensure that the third party is protecting the data



Compliance audits

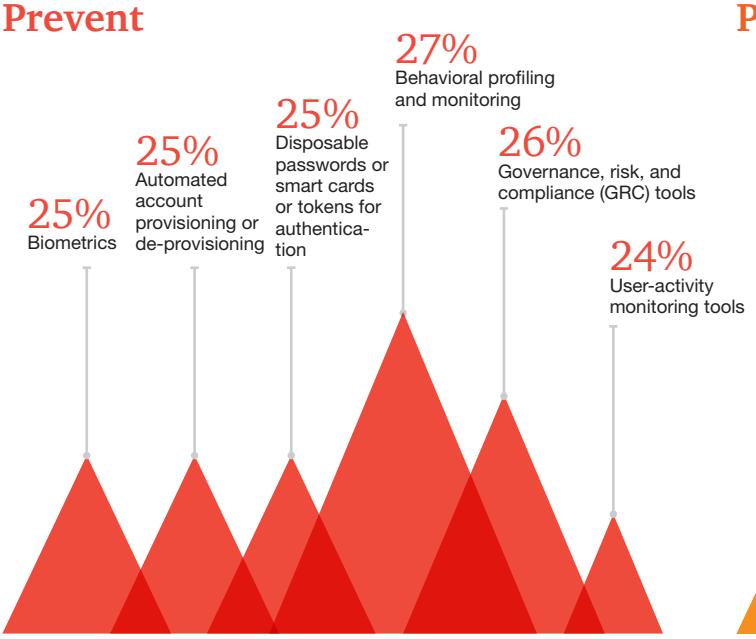


Appropriate protection

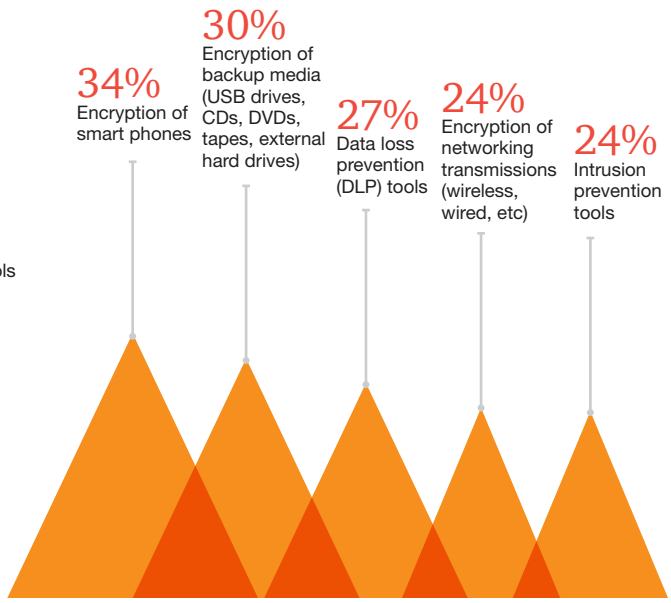


Robust contracts

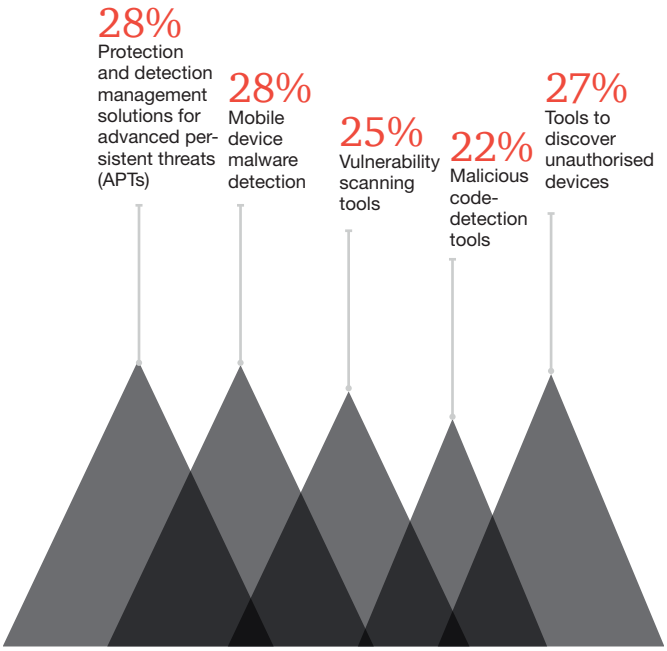
Prevent



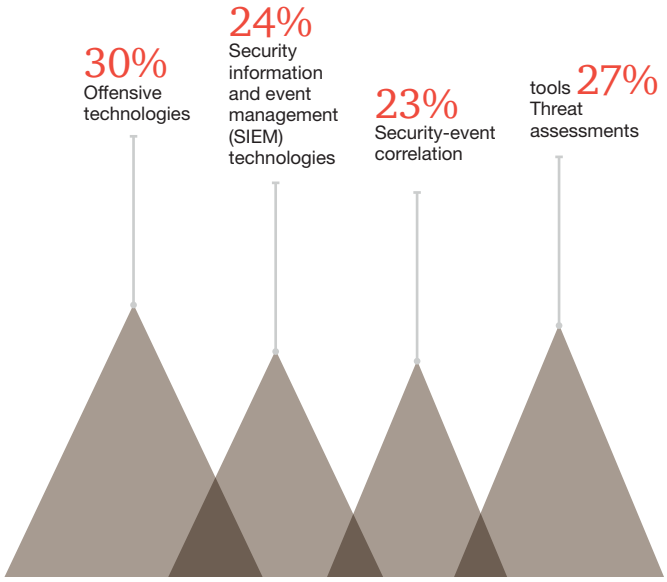
Protect



Detect



Respond



Percentage of respondents with security controls

Only 48% say that they have performed risk assessments on third party vendors and just 50% have an inventory of all third parties that handle personal data of employees and customers.

Moreover, only 15% considered outsourcing and vendor oversight to be a major security challenge in the foreseeable future. This indicates a need for greater rigour in managing information security risks stemming from partners and suppliers, and a thorough risk assessment of relationships with suppliers.

Employee training and awareness

Employee training and awareness is a fundamental component of every programme, as the weakest link in the security chain is often the human resource. The problem mostly lies in the way organisations engage with their employees and the communication programmes they employ to generate awareness.

Effective security awareness requires top to down commitment and communication, a tactic that is often lacking. Only 50% respondents say that they have a cross-organisational team that regularly convenes to discuss, coordinate and communicate information security issues. Further, only 54% have an employee security awareness training programme, down from last year's 56%.

Compared to last year's 61%, fewer respondents (56%) require their employees to complete training on privacy policy and practices.

Prevent	Protect	Detect	Respond
65% Secure access control measures	61% Encryption of e-mail messages	54% Intrusion detection tools	56% Security event correlation tools
63% Privileged user access	58% Intrusion prevention tools	56% Malicious code detection tools	61% Business continuity or disaster recovery plans
54% Employee security awareness training program	57% Data loss prevention (DLP) tools	58% Unauthorised use or access monitoring tools	54% Incident response process to report and handle breaches to third parties that handle data
49% Require third parties to comply with our privacy policies	56% Patch management tools	62% Active monitoring or analysis of information security intelligence	
55% Conduct personnel background checks	54% Protection or detection solutions for advanced persistent threats (APTs)	57% Vulnerability scanning tools	

#05

Security initiatives

It's about time that Indian companies started harnessing the complementarities of SMAC (social, mobile, analytics and cloud) technologies. Their applications, though previously debated, are now being utilised to maximise operational efficiencies and boost revenues.

Social media

Social media is no longer optional for enterprises. The ambiguity in calculating the return on social media investments, coupled with the difficulty in understanding the applications of social media in business and leveraging them to generate a profit stream has led to a slow adoption. However, more and more Indian companies are now adopting them, albeit cautiously.

Over 58% of Indian respondents already have a social media security strategy in place and another 27% have identified it as a top priority for the next 12 months. The fact that over 27% of respondents understand that social media is a major security challenge, highlights that business have taken cognisance of the threats linked with a hasty adoption of social media.

Mobility

One area that organisations are increasingly focusing on is enterprise mobility, which enables employees, partners and customers to access and work on the organisation's technology platforms through any secure enabler (laptops, tablets or smartphones).

The following are some elements of enterprise mobility infrastructure:

- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Network Access Control (NAC)
- Support

MDM and MAM solutions help in device control and are essential safeguards to counter threats to the individual's or the organisation's mobile devices.

Although, globally there has been a decline in the deployment of MDM, India has seen an 11% increase in the use of such solutions, which is in line with the growing smartphone penetration in the country and the BYOD trend.

Indian companies are taking measures to tackle threats from mobility. For instance, over 54% respondents already have a security strategy for mobile devices and more than 57% have a security strategy for BYOD. However, there is plenty of room for improvement.

Enterprise mobility challenges

Calculating returns on mobility solutions is difficult and involves too many variables that can affect the outcome; one approach can be to analyse the organisation's performance based on financial and operational parameters, before as well as after the roll-out of the enterprise mobility strategy. The lack of a single accurate method to calculate returns might deter further investment in mobility.

The ascent of mobility in the enterprise has far reaching ramifications for all aspects including people, processes and technology. This furthers the need for a closer alignment between the overarching IT and IS strategies, without which the organisation will be unable to completely leverage the benefits of mobility.

Analytics and big data

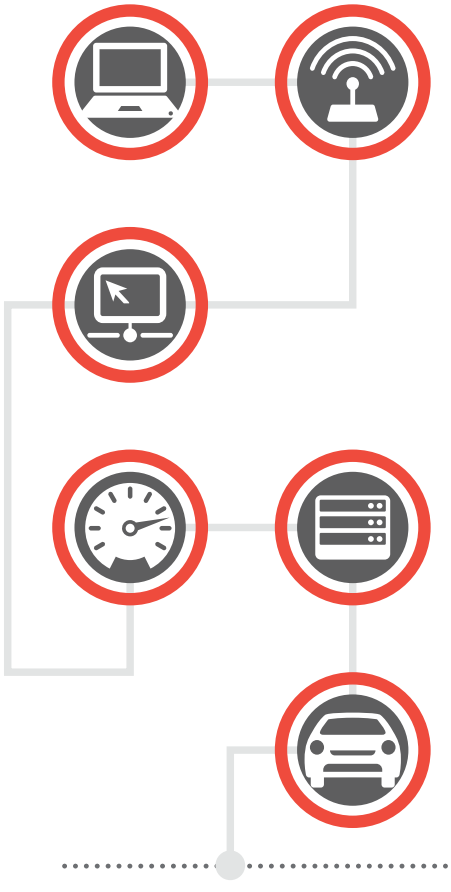
As the digital footprints of consumers increase, data-led insights pave the way for organisations to make informed business decisions about organisation-wide issues, ranging from product design and development to competitive pricing. Although there are threats linked to the adoption of analytics for decision-making, as long as organisations understand the value of collected data and ensure that the sanctity of data is maintained, they can combine the collected data to reveal trends as well as the causal relationships between business drivers.

Further, big data analytics can be used to strengthen the existing security monitoring tools. Over 47% of our respondents have utilised big data analytics to model for and identify information security incidents and over 57% of those who have employed big data analytics, claim that it has helped them detect more incidents.

Cloud services

Cloud services, with the ability to reduce the burden of investing huge capital in IT infrastructure and reducing the time to market for organisations, are clearly on the ascendency. Although almost 68% of our respondents use cloud services in the form of Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), organisations have largely been skeptical of migrating to the cloud. The concerns over data security and privacy, compliance to regulations and the difficulty in calculating actual profits earned by using cloud services have prevented organisations from leveraging cloud services.

Developing a cloud security strategy seems to be a top priority for majority of our respondents, but even with the best intentions, most organisations fail to implement the required multi-dimensional approach. The strategy should envision not only the migration of existing technology and processes but also the integration of legacy systems with the cloud.



#06

Cyber risk management

Organisations in India have been focused on perimeter security. It is only now that there are visible signs of organisations moving from the asset and technology centered paradigm for information security to comprehensive cyber-risk management. This is a result of the growing realisation that the erstwhile approach is incapable of keeping up with the cyber-threats of today and that the costs of cyber-incidents can be prohibitive.

Several multinationals in India are working to align their security strategies with the NIST Cyber Security Framework that has been advanced by the US government. This framework highlights the correct mix of people, processes and technologies for an effective model for risk based security for organisations.

The future of cyber-security in India will involve a tripartite model wherein the government, the organisation and the individual work in tandem to secure information and information assets in a concerted unified manner. This will require enhanced collaboration and communication of security posture among individuals, executives and industry organisations, as well as potential future improvements in legal exposure and assistance in regulatory compliance.

The first step for all organisations will be to align security spending with the organisation's strategic assets. In India, 12% respondents do not allocate security spending to the most profitable lines of business. Currently, only 56% report that they have a programme to identify sensitive assets, and about 65% have taken the effort to inventory the collection, transmission, and storage of sensitive data for employees as well as customers.

Strategic security spending also demands that businesses identify and invest in cyber-security practices that are most relevant to today's advanced attacks. It is essential to fund processes that fully integrate predictive, preventive, detective, and incident-response capabilities to minimise impacts.

Minimising losses caused by cyber security incidents

Businesses with adequate security awareness, have reported significantly lower average financial losses from cyber security incidents.

Effective security will also require a certain amount of knowledge about the existing as well as potential adversaries, including their motives, resources and methods of attack. This will not happen without a budget for threat analysis and monitoring, as well as a commitment of time and resources for collaborating with government agencies, peers, law enforcement, and other third parties to gain an understanding of the leading cyber-security practices. In the current environment of proliferating threats, risk-based security practices should be the primary component of an organisation's overall enterprise risk management framework.

While a well-designed cyber-risk management programme will not totally eliminate risk, it will enable organisations to manage threats through an informed decision-making process, increase efficiencies in security practices, and create a more resilient security practice.

In the coming years, we believe that advances in computer science will help organisations manage the risks and repercussions of cyber-threats better. Technology breakthroughs will help organisations reduce the complexity of cyber-security, detect and remediate incidents faster, as well as improve their abilities to monitor and analyse digital activity. Until then, it is imperative that organisations, both large and small, commit to understanding and managing the cyber security risks that have become primary concerns for executive leaders, boards, as well as consumers across the globe.

#07

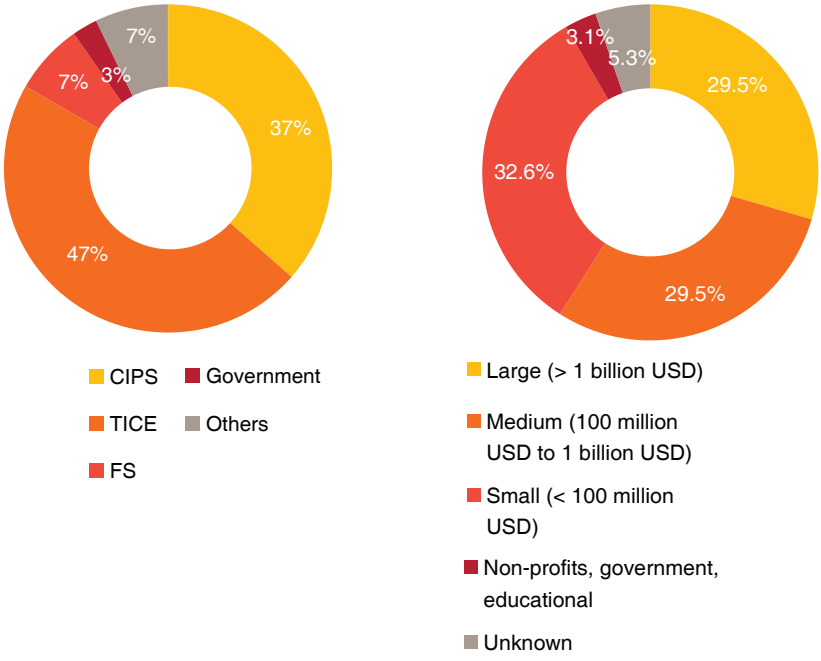
Methodology

This survey was conducted as part of PwC's Global State of Information Security Survey © 2015. The Indian edition of this survey is based on the responses from over 350 C-suite executives, vice presidents and directors of IT and information security, across 17 industries. The margin of error is less than 1% and all figures and graphics in this report have been sourced from survey results.

Respondents can be clubbed into the following four major industry verticals:

- CIPS (consumer, industrial products and services)
- TICE (technology, information, communications and entertainment)
- FS (financial services)
- Government and others

Around 30% of our respondents had annual gross revenues of over 1 billion USD, and another 30% (approx.) had revenues between 100 million USD and 1 billion USD. Almost a third of our respondents were small enterprises with annual gross revenues of less than 100 million USD, making it an inclusive survey with a distributed respondent base.



About PwC

PwC helps organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with more than 184,000 people who are committed to delivering quality in Assurance, Tax and Advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.in

PwC refers to the PwC network and / or one or more of its member firms, each of which 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

Sivarama Krishnan
Leader, India Cyber Security, Governance Risk and Compliance Services
sivarama.krishnan@in.pwc.com

Siddharth Vishwanath
Executive Director, Cyber Security Services
siddharth.vishwanath@in.pwc.com

Anirban Sengupta
Associate Director, Cyber Security Services
anirban.sengupta@in.pwc.com

Tarun Kumar
Associate Director, Cyber Security Services
tarun.k@in.pwc.com

Priti Ray
Associate Director, Cyber Security Services
priti.ray@in.pwc.com

Manu Dwivedi
Associate Director, Cyber Security Services
manu.dwivedi@in.pwc.com

Sundareshwar Krishnamurthy
Associate Director, Cyber Security Services
sundareshwar.krishnamurthy@in.pwc.com

Rahul Aggarwal
Associate Director, Cyber Security Services
rahul2.aggarwal@in.pwc.com

pwc.in

Data Classification: DC0

NJ 268 - October 2014 GSISS.indd
Designed by Corporate Communications, India