Before tomorrow dawns
Key findings from the State of Information Security Survey-India

pwc

www.pwc.in

Foreword

Sivarama Krishnan
Executive Director
PwC India

Siddharth Vishwanath
Executive Director
PwC India

It is heartening to note that information security is finding its way to the Board agenda. An increasing number of organisations in India are moving beyond information security basics and exploring new paradigms and models of information security to meet the evolving threat land-scape.

The litmus test for a truly exceptional strategy is to make organisations responsive to the needs of today and become better prepared for the challenges of tomorrow. So is the case with information security strategy wherein both knowledge and agility are key. In this report, we study the current status of information security in Indian organisations. We analyse information security behaviours, security priorities, security spending, safeguards and security policies implemented by companies to secure their information assets. We also assess and expound on the preparation that organisations in India need have in order to become information security leaders.

As always, while information security has its roots in technology, the key drivers of any security culture continue to be the people. This survey explores the key issues and challenges with regards to this critical aspect of information security culture.

we are sure this report will play an important role in helping enterprises strengthen their information security posture. We look forward to your feedback to make our future surveys even more comprehensive and interesting.

Information security threats are complicated, complex and damaging. Organizations need to prepare by continuously assessing and evaluating security strategies and practices.

Executive summary

- Confidence is high but true leaders in security are few: While 89% of respondents repose confidence in the effectiveness of their information security activities and 57% consider themselves 'front-runners' in strategy and security practices, our analysis reveals that only 38% organisations are real information security leaders.
    - Security loopholes result in failures: The number of security related incidents detected in the past 12 months has increased by 98%, an indication of the elevated threat environment today. It is troubling that over one-third of the respondents claim to have learnt of these from external sources, such as customers or service providers. This may be due to continued investment of organisations in traditional information security products or safeguards rather than on new ones.
    - Spending may not be in right direction: Over 90% respondents claim that their security policies and security spending are aligned with business objectives, with 25% reporting security budgets of more than five million USD. There is a sharp increase in the number of security incidents and resultant financial losses are on the rise. This contradicts the belief that organisations are becoming more adept at detecting intrusions. It, in fact, suggests that the security models in use may either be broken or ineffective.
    - New technologies are implemented without security: Enterprise mobility and cloud services are gaining greater traction within organisations in India. Information security for mobile devices and cloud services, however, lags behind adoption rates. Less than 50% of respondents claim fundamental information security controls for mobile security and even less than 20% have policies addressing the use of mobile phones.
    - Information security lacks management support: Nearly 30% of respondents report that leadership and strategy are the two most common obstacles in effecting a strong information security function within their organisations. Thus, information security in many organisations is still not a foundational component of the business strategy, one that is championed by senior management, the CEO and the Board.
    - Lack of focus on the 'real' intruders: Insider threats are rising. Insiders, particularly current or former employees, are cited as security threats by almost 75% of respondents. Lack of solutions around behavioural profiling and event management adds to the problem. Many organisations do not yet have plans for responding to insider threats. The information security spending is still more focussed on external factors, such as client and regulatory requirements.

The heart of the matter

Indian businesses are confident about their security posture, but are ill-prepared for the future. While traditional concepts of security help establish rudimentary foundations, everchanging threats necessitate that businesses look beyond.

Indian companies have been focussing on compliance based and perimeter oriented security strategies. While they have proved to be useful in the past, these strategies alone will not be able to meet challenges posed by adversaries leveraging the threats and technologies of tomorrow.

The intruders have become more sophisticated: by moving on from dated perimeter attackes to ones which are highly targeted and difficult to pre-empt. Interestingly, the attack surface (partners, suppliers, customers and others) has expanded with the ease of staying connected. Adversaries are breaching the defences of business ecosystems and are leaving reputational, financial and competitive damages in their wake.

Respondents to The State of Information Security® Survey – India, 2014 appear to be distant from ground reality. More than 620 executives across 17 industries who responded to the survey, were confident about their organisation's information security practices, some even believing that they're leading. More than half (57%) of the respondents see their organisation as a 'front-runner'.

While organisations have raised the bar in security, their adversaries have made sure they are a step ahead. This year's survey shows that there is a 98% jump in the number of incidents reported this year and average financial losses have gone up by 26% in India compared to the global average of 18%.

A majority of organisations are clearly underprepared to deal with the vulnerabilities and threats around new technologies and business models. Security, which needs to be a foundational component of business strategy, particularly in an elevated threat environment, still goes begging for top management's sponsorship in most organisations.

It is clear that organisations have not been able to keep pace with today's escalating risks and there is a long way to go before they are able to manage impending threats.

Methodology

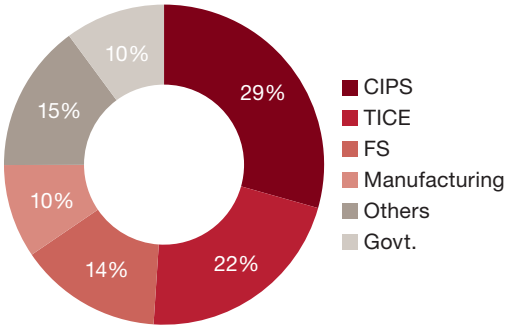
The survey was conducted using a structured questionnaire, administered online. PwC clients from across the country were invited via email to take the survey. This survey was conducted parallely with PwC's global survey titled The Global State of the Information Security Survey 2014. The results discussed in this report are based on responses from more than 620 CEOs, CFOs, CISOs, CIOs, CSOs, vice presidents, and directors of IT and information security across 17 industries. The margin of error is less than 1%. All figures and graphics in this report were sourced from survey results.

The State of Information Security Survey 2014, India is in its sixth edition. Key attributes of the survey are:

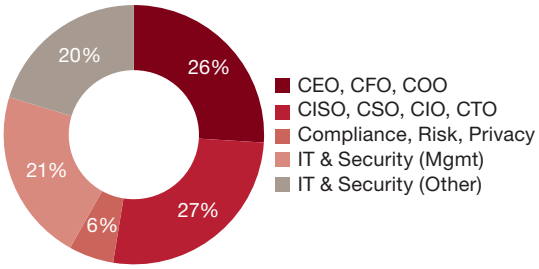
Respondents have been clubbed into four major industry verticals: CIPS (consumer, industrial products and services), TICE (technology, information, communications and entertainment), FS (financial services), the government and others.

- Maximum responses have been received from CIPS (29% respondents) followed by the TICE (22%) group.
- Majority of the respondents (75%) are from medium and large enterprises.
- Around 80% respondents represent senior management from business and IT.

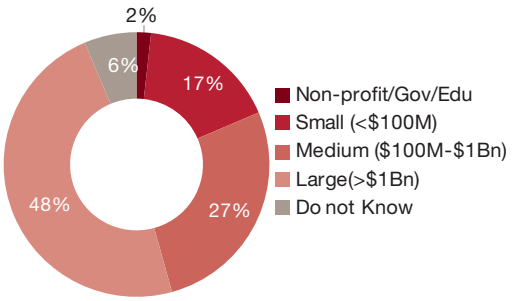
Respondents: Industry wise



Respondents: Title wise



Respondents: Size of company wise



An in-depth discussion

Indian executives rate the effectiveness of their information security strategies very highly. But, closer scrutiny reveals that they lack preparedness in meeting impending security threats

Confidence is high but true leaders in security are few

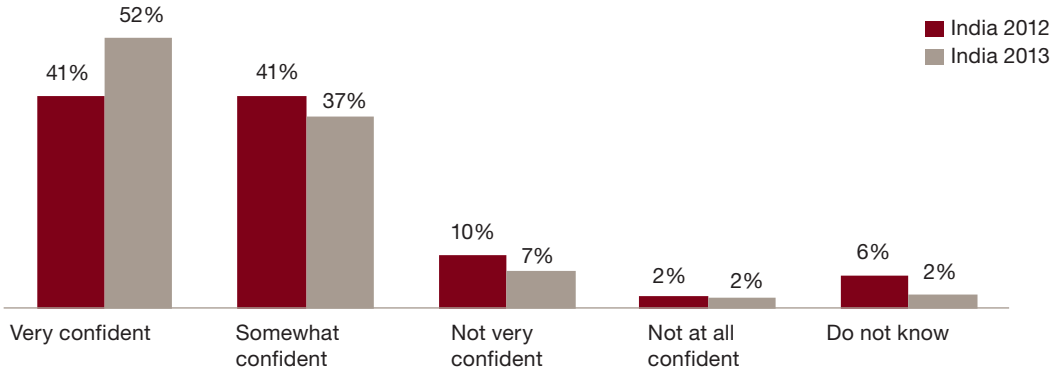
While 89% of respondents repose confidence in the effectiveness of their information security activities and 57% consider themselves 'front-runners' , our analysis reveals that only 38% of the organisations can be called information security leaders.

The State of Information Security Survey-India, 2014 reveals that the overall confidence in information security practices in India has jumped from the previous year with more than 89% respondents claiming to be confident about their organisation's security. This is striking considering the climate of escalating and evolving risks. A similar trend has been observed globally with nearly 74% respondents claiming to be confident of their security practices, a significant increase from the previous year. Interestingly, among the executives, both business (CEOs) and security leaders (CISOs), repose high confidence in their organisations' security practices.

Confidence in the information security practices is also palpable with more and more executives claiming that their information security program is aligned with business objectives both in terms of policies and spending. 94% respondents this year compared to 87% respondents last year claim that they have either fully or partially completed the alignment of security policies with the business objectives. Similarly, 91% compared to 86% respondents from the previous year claim that their security spending is aligned with business objectives. This indicates that the respondents clearly understand that security is integral to the business agenda and can add immense value to business goals.

This positivity around security posture also gets reflected in the way respondents assess their approach to information security. It is encouraging to note that a large number of executives claim that their organisations have crossed the chasm between having an effective information security strategy in place and proactively executing the strategy. This year's respondents that say they have the attributes of a 'front-runner', have risen 25% from the previous year. About one in three (28%) say they have the strategy right but may not have been able to successfully execute the plan. These we call the 'strategists'. Those who consider themselves better at 'getting things done' than defining an effective strategy are the 'Tacticians' which account for 9% of the respondents. And the group that can be aptly described as 'firefighters', the ones who do not have a strategy in place and are typically in a reactive mode, constitute 6% of the respondents.

Confidence in organisations' security



How respondents characterize their approach to information security

Front-runners
We have an effective strategy in place and are proactive in executing the plan

Strategists
We are better at "getting the strategy right" than we are at executing the plan

Tacticians
We are better at "getting things done" than we are at defining an effective strategy

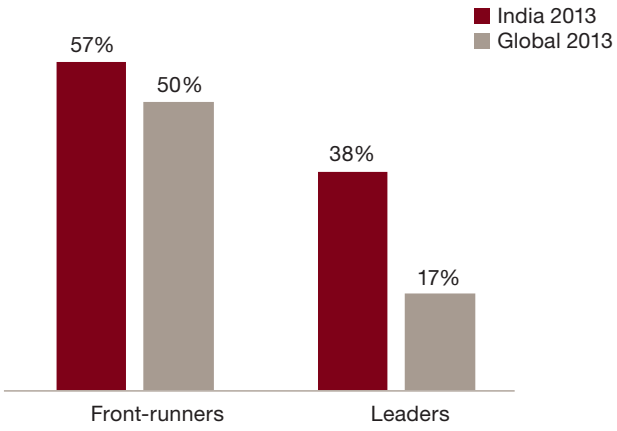
Firefighters
We do not have an effective strategy in place and are typically in a reactive mode

A closer look at the data through the lens of a series of requirements that define 'true leaders' on the basis of reported capabilities rather than self perception reveals that there are far fewer real leaders than 'front-runners'. To qualify as leaders, the respondents must:

- Have an overall information security strategy
- Employ a chief information security officer (CISO) or an equivalent who reports to top leadership: the CEO, CFO, COO, CRO, or the legal counsel
- Have measured and reviewed the effectiveness of their security measures within the past year
- Understand exactly what type of security events have occurred in the past year

Based on these requirements, we understand that those who claim to be 'front-runners' are not necessarily leaders. Filtering on the basis of this criteria, only 38% of all survey respondents rank as security leaders. This compares favorably with 17% of the respondents globally. Compared with the front-runners, these leaders have a significantly better understanding and control over information security risks. They detect more security problems; have a better understanding of what types of security issues occur and the source of those issues and report lower average financial losses as a result of security incidents.

Front-runners vs. leaders



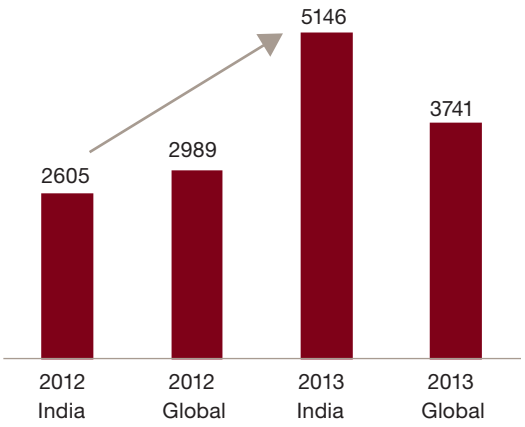
Security loopholes result in failure

We define a security incident as any adverse incident that threatens some aspect of computer security. The number of incidents detected in the past 12 months has increased by 98%, which is perhaps an indication of today's elevated threat environment. It is troubling that over one-third of the respondents claim to have learnt of the security problems from external sources, such as customers or service providers. This may be due to the organisation's continued investments in the traditional information security products or safeguards rather than focusing on new ones.

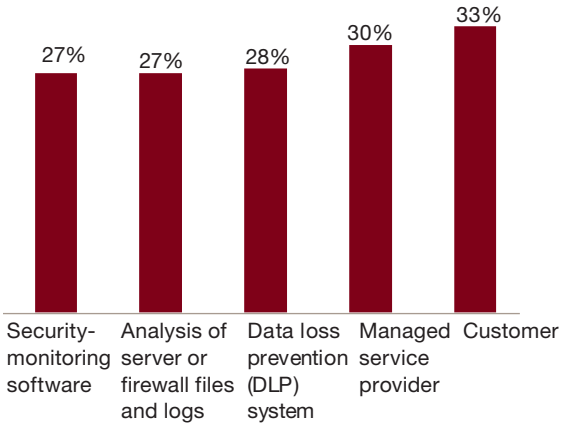
This year's survey results reveal that there is 98% rise in the number of security issues reported by the respondents for the past 12 months. This is significantly higher than the 25% jump reported globally in the number of security incidents for the same period.

This increase could also imply that organisations are getting better at identifying incidents. But the fact that one-third of the respondents claim that they have learnt of incidences from external sources, such as customers and service providers, raises questions on the effectiveness of internal intrusion detection platforms and processes with the organisations. This implies that companies need to deploy more robust internal system led controls for an early detection of such incidents.

Average number of security incidents

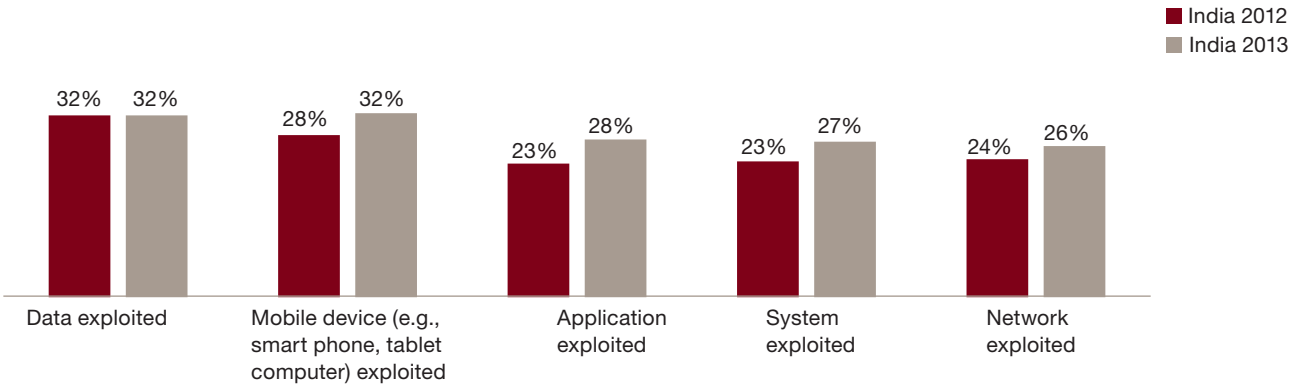


Sources of information on security incidents



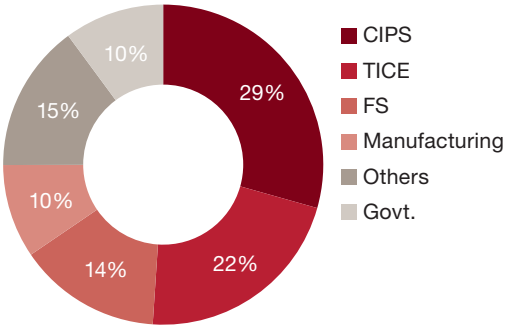
Reported security incidents involve exploits across all platforms. While companies report lesser number of exploits in removable storage, social engineering and paper based information, it is likely these may be going un-reported or un-detected. There is in an increase in the number of respondents reporting the incidents involving exploits of mobile devices.

Types of security incidents



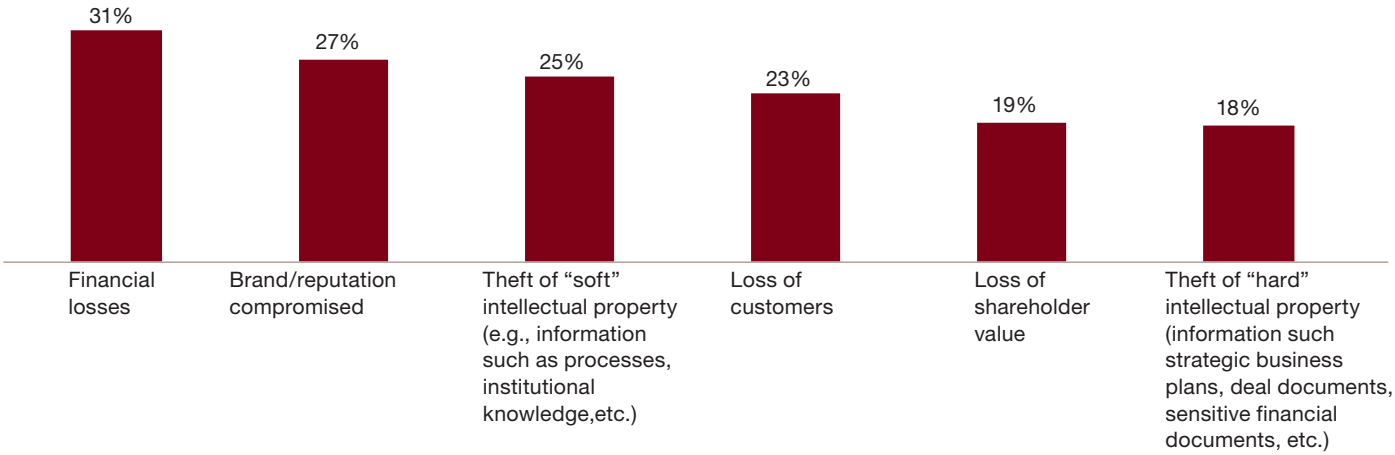
It is interesting to note that a majority of respondents report that compromising data involving employee and customer records is significant when compared to the company IP theft. Every year, respondents claim that the employee and customer data is the most valuable information for them. With the increasing number of breaches however, it appears that these are not as integral to their information security plans as they claim them to be. This suggests that the current data protection efforts are not focused in the right direction.

Data loss on account of security incidents



The business impact of such security incidents is manifold. Most respondents believe that the impact of these incidents extends beyond financial and reputational losses and more often than not results in the loss of customers.

Business impact of security incidents

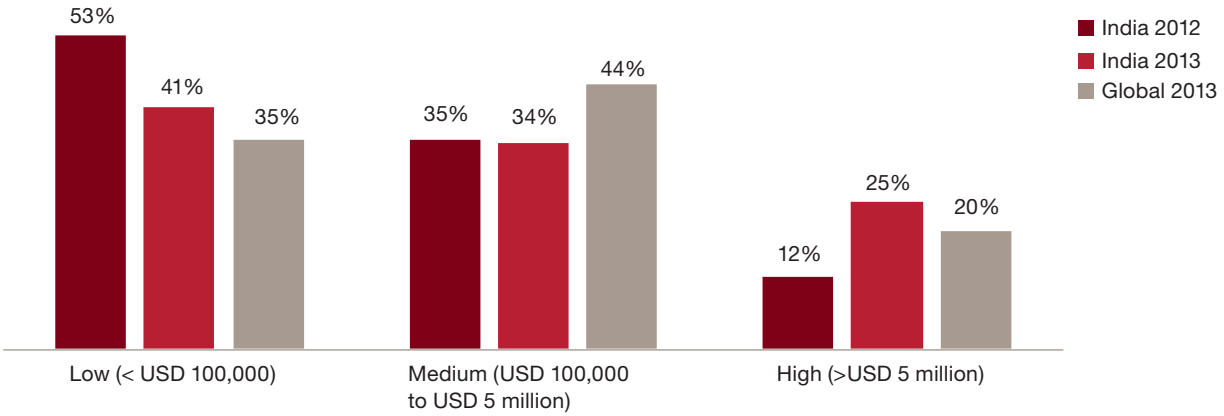


Spending may not be in right direction

Over 90% of the respondents claim that their security policies and their security spending are aligned with the business objectives. 25% of the respondents report security budgets of more than of five million USD. There is a sharp increase in the number of security incidents and the resultant financial losses are also on the rise. This contradicts the belief that organisations are becoming more adept at detecting intrusions. It in fact suggests that the old security models that are still in use may be broken or ineffective.

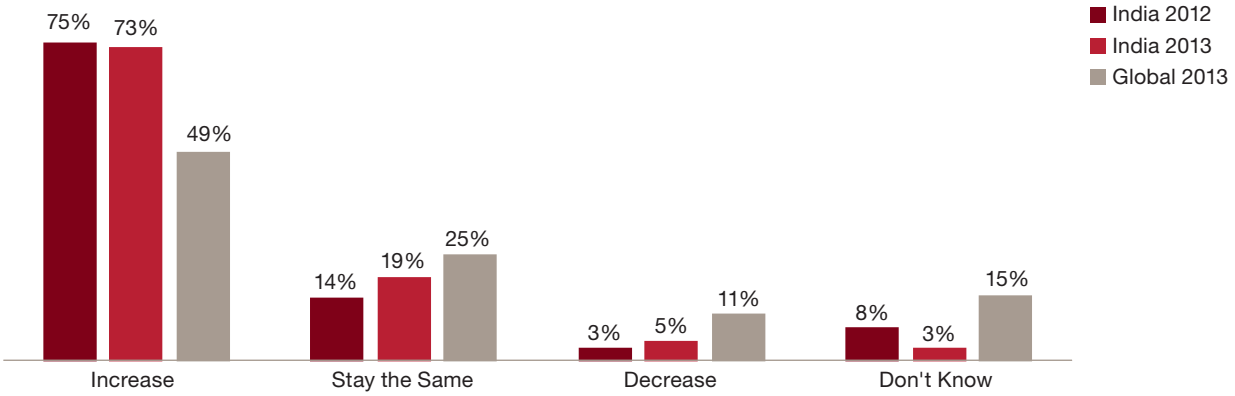
The substantial increase in security spending argues well for the security efforts. Irrespective of the company size, industry and risk profile there is an overall increase in investments for security. Interestingly, there has been a 100% increase in the number of respondents reporting security spending of more than five million USD. This is particularly significant as the number of large and medium enterprises surveyed is not very different from the previous year, which means that more organisations are making greater capital and operational expenditure for security.

Total information security budget, 2013



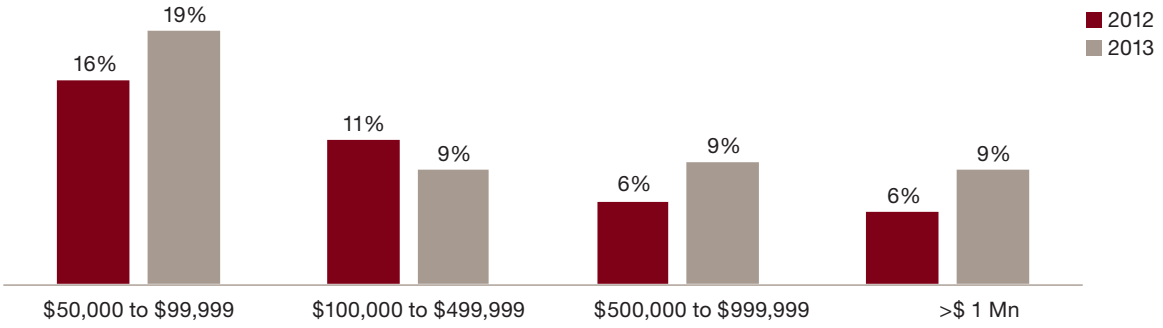
Organisations are optimistic about to the future. In spite of a difficult economic environment, 73% of the respondents expect their information security spending to increase over the next 12 months. However, 19% still expect it to remain the same. Only 5% of respondents from India indicate a cut down in information security spending.

Security spending over the next 12 months



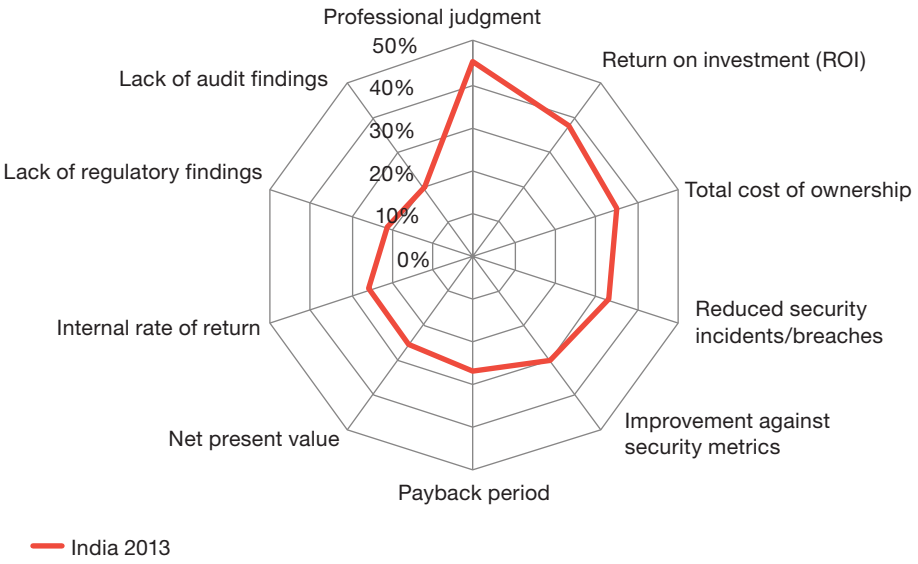
While most respondents claim high spends on securing information security assets, a significant gap appears in the investments made and the outcomes achieved. There is a whopping 26% jump in the average losses on account of security incidents in India in the past 12 months. This is significantly higher than 18% increase in losses reported globally for the same time period. This is indicative of priorities gone wrong or adversaries getting smarter to break into traditional defenses.

Financial losses of 50,000 USD or more



Interestingly, over-reliance on professional judgment rather than hard facts to arrive at a focussed plan based on measurement of effectiveness of information security spending may be clouding or directing spends into less beneficial avenues. Very few respondents claim to use scientific and or objective measures to arrive at spending plans.

Factors for measuring effectiveness of security spending



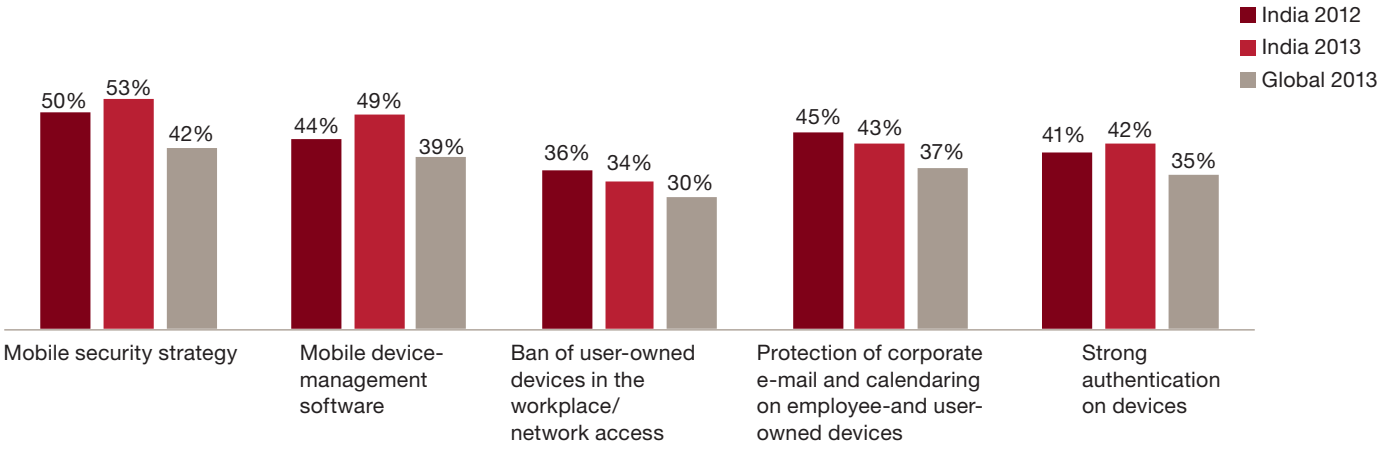
New technologies implemented without security

Enterprise mobility and cloud services are gaining greater traction with organisations in India. Yet, information security for mobile devices and cloud services lags behind adoption rates. Less than 50% of the respondents claim that their organisations have fundamental information security controls for mobile security and even less than 20% have policies addressing use of mobile phones.

A key risk to data security is the surge in the use of mobile devices such as smartphones and tablets, as well as the 'bring your own device' (BYOD) trend. India ranks fifth among the top countries for smartphone users with an estimated 67 million subscribers in 2013, after China, the US, Japan and Brazil. With the increasing penetration of smartphones in the country, there has been a significant rise in the adoption of enterprise mobility. This growth trend in BYOD adoption is expected to become stronger in the coming years. It is reported that adoption of BYOD is deepest in India, where over 38% of workers in 2013 are using personal devices up from 34% in 2011.

It is clear that are lagging of security practices is covering enterprise mobility adoption in the country. Only 53% respondents claim to have a mobile security strategy and less than half the respondents report having mobile device management (MDM) software and authentication of devices.

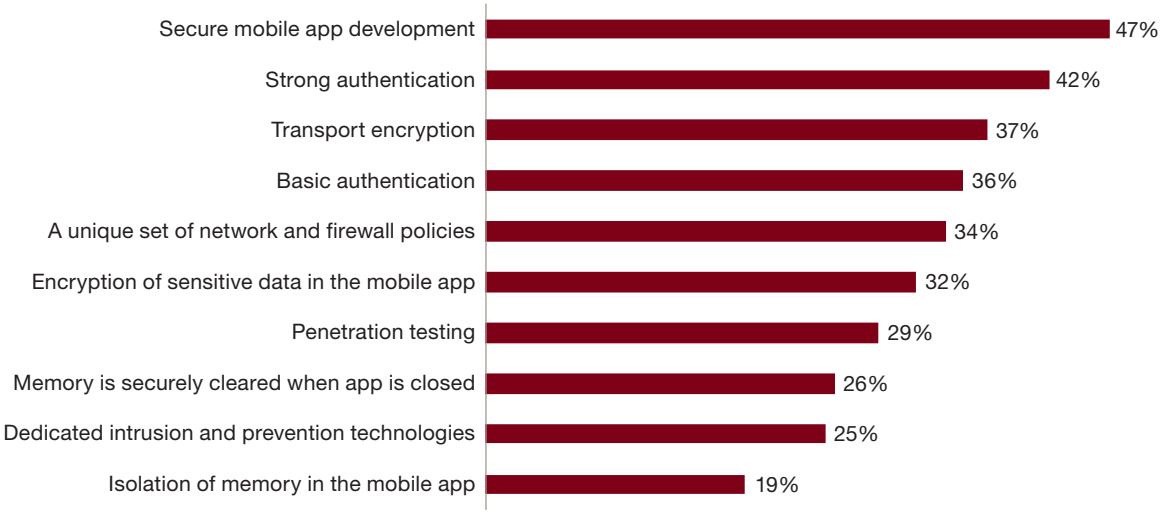
Initiatives to address mobile security risks



While the use of mobile devices to share and transmit data continues to increase, deployment of information security controls lags behind the growing usage of smartphones and tablets. For customers facing mobility applications, respondents report having secured mobile application development and advanced authentication related controls.

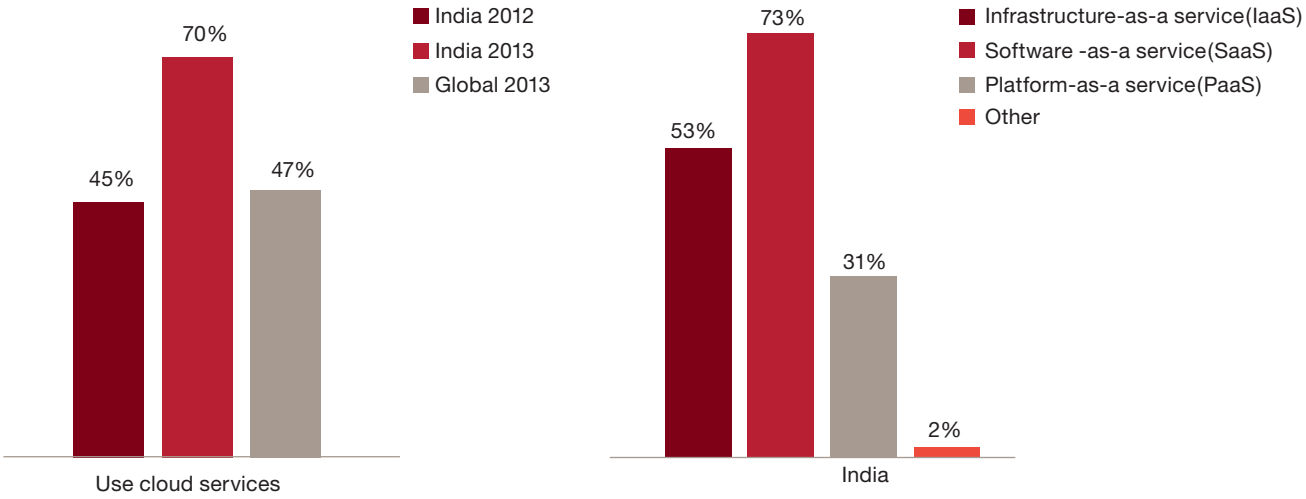
However, few respondents have used penetration testing and dedicated intrusion and prevention technologies. This signifies that externally exposed applications could be vulnerable to threats not contemplated as part of the security strategy.

Security controls for customer facing mobility applications



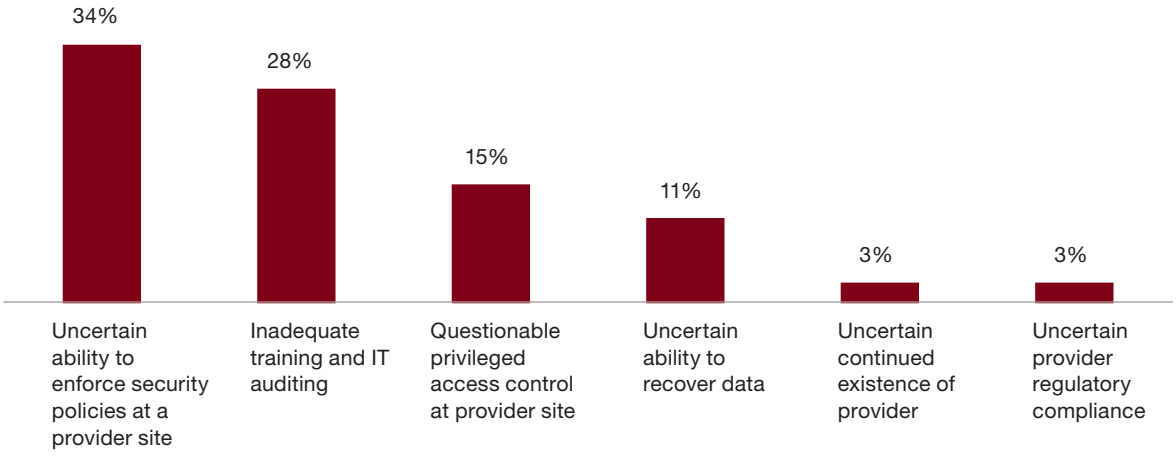
Cloud services adoption in India is on the rise. There has been a 57% rise in the number of respondents reporting to have used cloud services in their organisation. Organisations in India are ahead of their global peers in the use of cloud services. Seventy-three per cent respondents using cloud services have access to SaaS (Software as a Service) platform.

Use of cloud service and type of cloud services



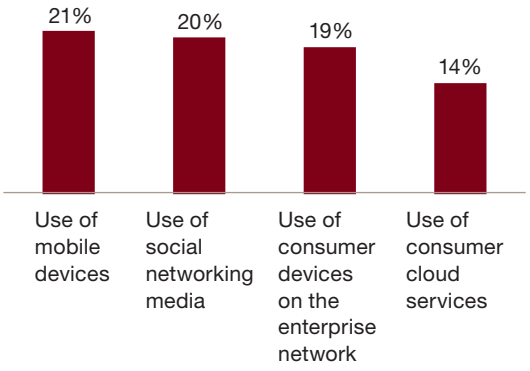
Respondents believe that inability to enforce security policies at the provider's end is the single biggest challenge for cloud security. They also make indirect reference to the lack of training and auditing as a risk for cloud security.

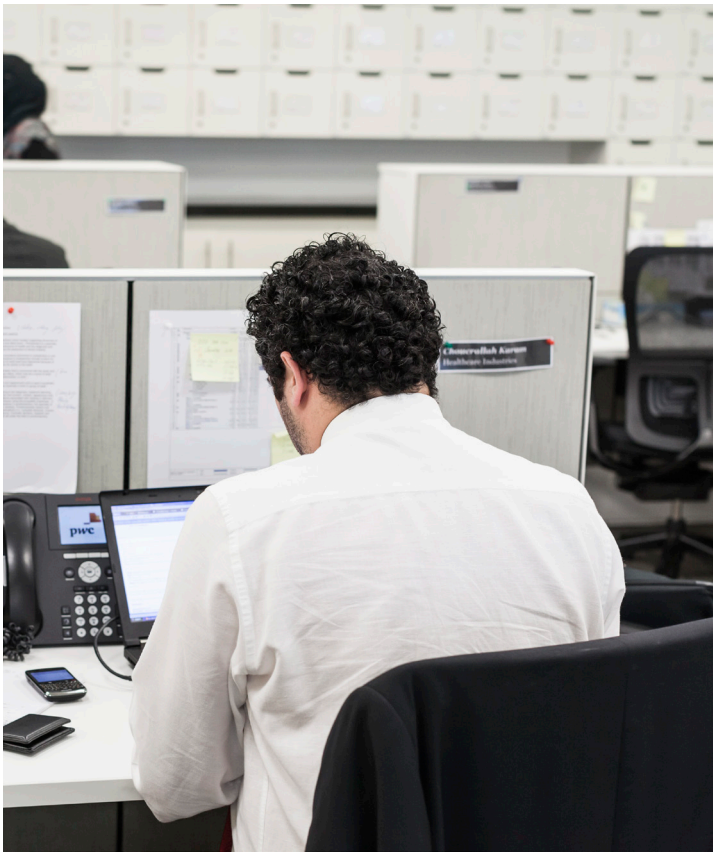
Greatest risks to cloud security



Alarmingly, despite the awareness around security threats to mobility and cloud technologies only a small percentage of organisations have incorporated these in their security policies. This is also telling of the fact that while only 14% organisations in India have policies governing cloud services, nearly double the number expect to be able to enforce policies at partner end to mitigate risks, losing sight of the adage that 'service starts at one's own doorstep'. Globally again only 18% of organisations have covered cloud security as part of their information security policies.

Inclusions in security policy





Information security lacks management support

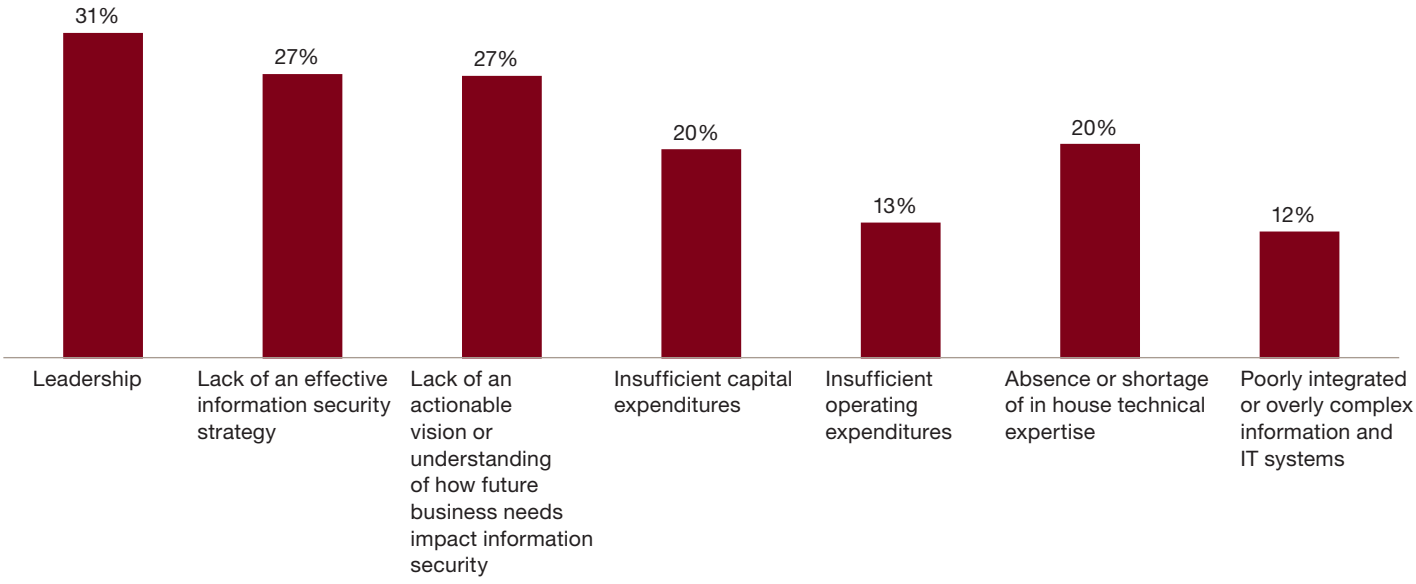
Nearly 30% of respondents report that leadership and strategy are the two most common obstacles in establishing a strong information security function within their organisations. Thus, information security in many organisations is still not a foundational component of the business strategy, one that is initiated by senior management, the CEO and the board.

While most security stakeholders agree that action needs to be taken to improve information security, there appears to be little consensus about the challenges of doing so. Nevertheless, the most significant challenges to improving information security are centred around the lack of adequate leadership focus, well-designed information security strategy and an actionable vision of how future business needs impact information security. As stated earlier, the litmus test for an effective strategy is to be able to cater to the needs of the future while addressing the requirements of today. Currently, information security strategies if any, are focussed on countering today's threats and that too through traditional practices of ring-fencing.

Organisations in India do not report being challenged with funding, both capital expenditure and operating expenditure, for information security. Globally, organisations cite this as one of the major hindrances to information security effectiveness.

Nearly 82% of the respondents in India claimed that their organisations had a senior executive in a CEO, CFO, COO, etc. who proactively communicated the importance of information security to the entire organisation. This is indicative of the fact that while there is significant understanding of the issues around information security by the top management, there are concerns in terms of senior leadership backing the implementation of information security plans.

Obstacles to improving information security

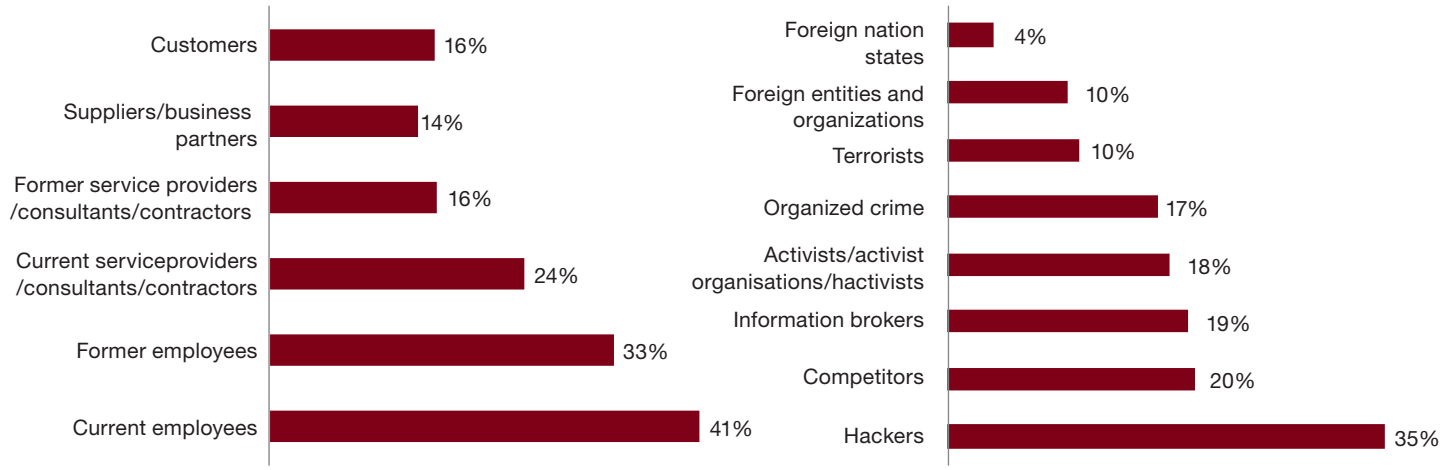


Lack of focus on the 'real' intruders: Insider threats are on the increase

Insiders, particularly current or former employees, are cited as a source of security incidents by almost 75% of the respondents. Lack of solutions around behavioural profiling and event management adds to the problem. Yet, many organisations do not have plans for responding to insider threats. Even today, justification for information security spending is more focussed on external factors, such as client and regulatory requirements.

Most respondents attribute security incidents to every day insiders like current employees (41%) and former employees (33%). Many see these insider threats as far more significant than external threats. Of the external threats, while attacks backed by nation-states make headlines, organisations are more likely to be hit by hackers. Only 4% of respondents report security incidents committed by foreign nation states. Hackers at 35% represent a much more likely danger.

Likely internal and external sources of incidents



**Respondents could select more than one source of incidents*

In order to be responsive to the threats posed by intruders, companies in India need to devise strategies and tactics keeping in mind the real motivators and the impact of each of these actors.

Motivation, vector and impact of threat actors

Lines between the threats are blurring

	Motivators	Threat vectors	Impact
Nation-states	• Global competition • National security • Fraud	• Targeted, long-term cyber campaigns with strategic focus • Insider • Third-party service providers	• Loss of intellectual property • Disruption to critical infrastructure • Monetary loss • Regulatory
Cyber criminals	• Illicit profit • Fraud • Identify theft	• Individual identity theft • Data breaches and intellectual property theft • Insider • Third-party service providers	• Loss of identity • Monetary loss • Intellectual property loss • Privacy • Regulatory
Cyber terrorists/ individual hackers	• Ideological • Political • Disenfranchised • Malicious havoc	• Opportunistic vulnerabilities • Insider • Third-party service providers	• Destabilize, disrupt and destroy cyber assets of financial institutions • Regulatory
Hacktivists	• Political cause rather than personal gain • Ideological	• Targeted organizations that stand in the way of their cause • Insider • Third-party service provider	• Disruption of operations • Destabilization • Embarrassment • Public relations • Regulatory

India seems to be losing its focus on real intruders. It is lagging in its adoption of certain key safeguards that will enable it to meet the threats of today and tomorrow. Less than half the respondents perform behavioural profiling and monitoring, deploy security information and event management technologies and have protection/detection management solutions for advanced persistent threats (APTs). These technologies are focused on real internal and external intruders.

	India
Centralized user data store	61%
Behavioral profiling and monitoring	48%
Intrusion detection tools	68%
Asset management tools	62%
Use of virtual desktop interface	52%
Security information and event management (SIEM) technologies	48%

Insights from industries

FS, CIPS and TICE behaving distinctly

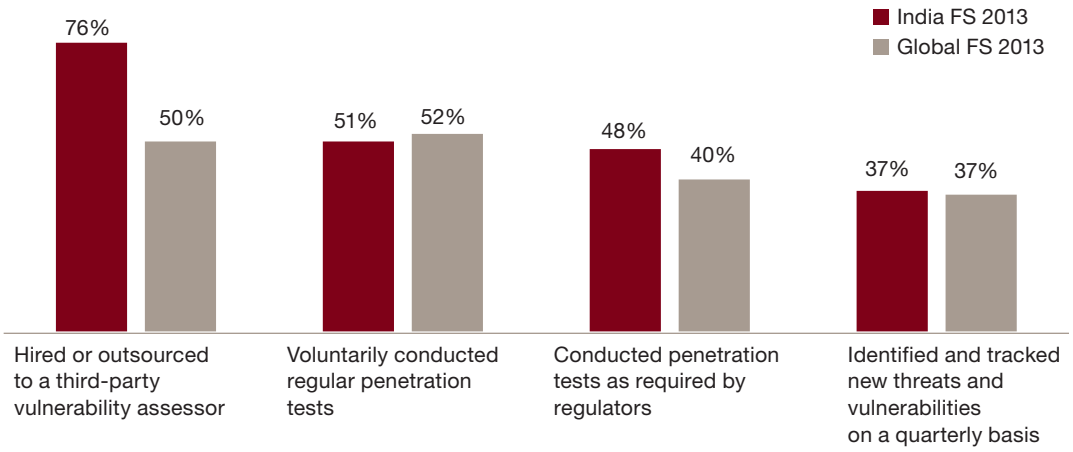
FS companies, regular front-runners in security management practices, continue to focus on maintaining security leadership

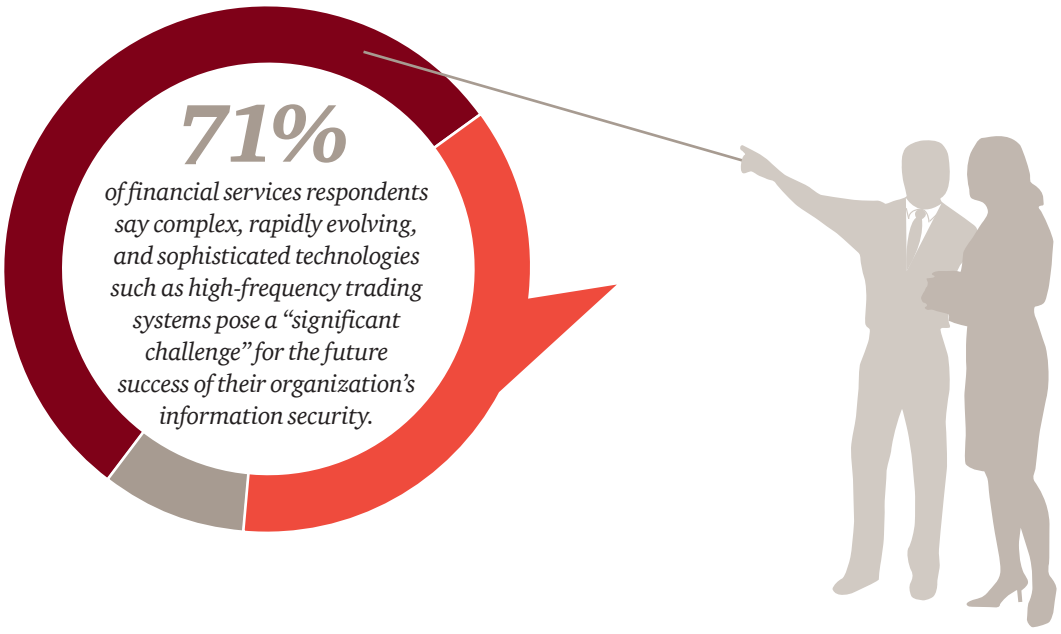
FS companies lead in deployment of security tools and integrating security right from the project inception stage. This gets reflected in the lesser downtime experienced by these companies overall. However, FS companies need to focus on security strategies for new technologies like mobile phones etc.

Financial services companies are spending more on information security than ever before and have improved many of their security practices. Our research indicates that regulatory compliance is still a significant driver of security spend in the industry. Yet incidents continue to occur as a result of unprecedented attacks, ranging from distributed denial of service to APTs

A significant number of financial institutions are seeking external help for risk assessments. Compared to global peers more Indian financial services organisations are using third party vulnerability assessors to help them in identification of gaps and consequent strengthening of information security.

Actions taken to strengthen security in past 12 months





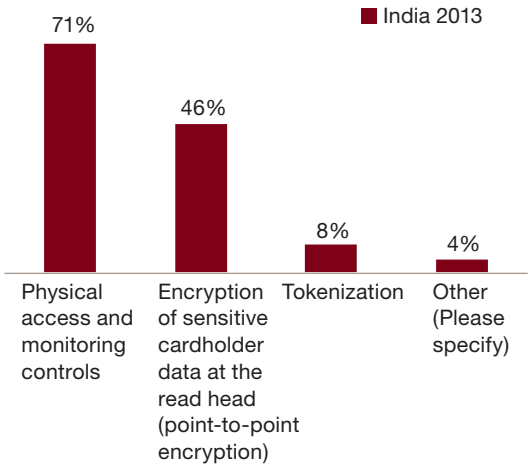
CIPS companies are working at enhancing their capabilities in security strategies and practices

CIPS companies are increasingly adopting security best practices. Most continue to make investments and establish practices around well defined strategies, structures and safe guards. Data privacy is an area that on needs enhanced focus.

57% respondents from CIPS companies claim that they are either prepared or somewhat prepared for data protection in cloud and third party environments. 73% respondents claim that they either have or are planning to implement a secured supply chain solution.

71% of CIPS respondents have physical access and monitoring controls for securing point of sales (POS) systems.

Means to secure POS systems



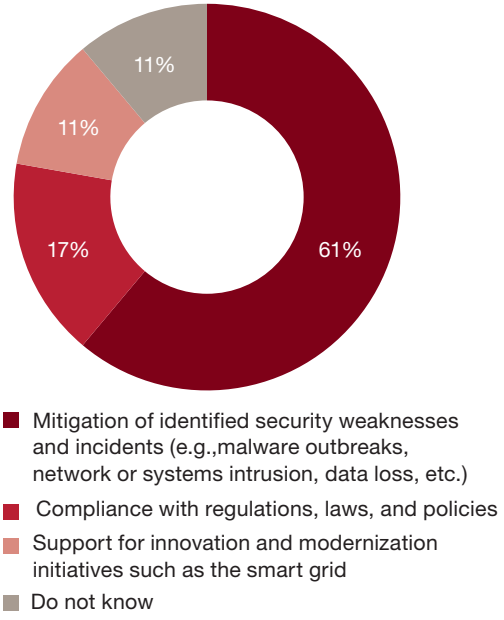
Interestingly only 1/3rd of CIPS respondents have implemented business continuity and disaster recovery plans. An equal number confirm that information security becomes involved in major initiatives at project inception stage. This implies immense scope for improvement for these companies. 70% are optimistic of increases in information security spending in the coming year. This forebodes well for the sector.

TICE industries exhibit emerging leadership in information security management

TICE industries report a strong alignment and continuing investments in information security areas. TICE industries also lead other sectors in establishment of security safeguards, including new technology related safeguards. This is in keeping with India's pre-eminent position as the world's leader in information technology services.

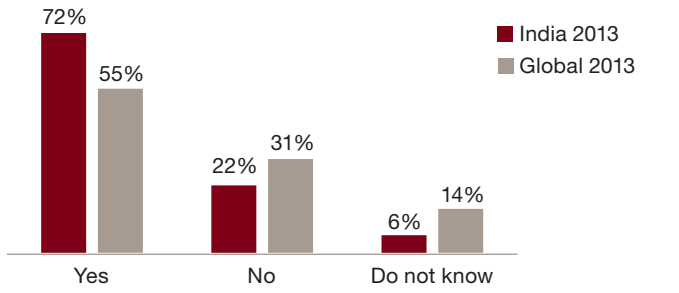
The primary driver of security spending for TICE industries is mitigation of identified weaknesses implying higher self direction. TICE industries clearly understand that need to stay ahead of the curve to maintain their pre-eminence as the country's flagship growth sector.

Primary drivers of spending



More Indian TICE companies (72%) have a unified control or enterprise risk management framework addressing cyber security risks. This compares favorably with 55% globally. TICE companies in India are proactive in establishing and imbibing global practices to counter any information security risks. In fact, a large swathe of TICE companies report having advanced protection against APTs.

Presence of unified control or enterprise risk management framework



What this means for your business?

Yesterday's security defenses are not effective against today's rapidly evolving threats. And the risks of tomorrow- uncertain at best and perilous at worst – will demand a completely new model of information security.

We suggest an evolved approach to what security can be, one that is driven by knowledge of threats, assets and adversaries. One in which security incidents are seen as a critical business risk that may not always be preventable, but can be managed to acceptable levels. We call this model Awareness to Action. At its most basic, this approach comprises four key precepts:

- ***Security is a business imperative:*** Effective security requires that you understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem. An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge.
- ***Security threats are business risks:*** You should view security risks as organisational threats. It is critical to anticipate these threats, know your vulnerabilities, and be able to identify and manage the associated risks. Ensure that suppliers, partners and other third parties knowand agree to adhere toyour security policies and practices.
- ***Protect the information that really matters:*** Effective security requires that you understand and adapt to changes in the threat environment by identifying your most valuable information. Know where these "crown jewels" are located and who has access to them at all times, and proficiently allocate and prioritise your organisation's resources to protect its most valuable information.
- ***Gain advantage from Awareness to Action:*** In this new model of information security, all activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring. You should create a culture of security that starts with commitment of top executives and cascades to all employees and third parties. Engage in public-private collaboration with others for enhanced threat intelligence.

Security is a board-level business imperative	
Advance your security strategy and capabilities.	• An integrated security strategy should be a pivotal part of your business model; security is no longer simply an IT challenge. • You should understand the exposure and potential business impact associated with operating in an interconnected global business ecosystem.
Board and CEO drive security governance.	• Security risks are operational risks and should be reviewed regularly by the board. • Strong support and communication from the board and CEO can break down traditional silos, leading to more collaboration and partnerships.
Strong multi-party governance group should manage security risk.	• An executive with direct interaction with the CEO, General Counsel and Chief Risk Officer should lead security governance. • Security governance group should include representatives from legal, HR, risk, technology, security, communications, and the lines of business. • The cybersecurity governance group should meet regularly (monthly or quarterly) to discuss the current threat landscape, changes within the organization that impact risk levels, and updates to remediation programs and initiatives.

Security threats are business risks	
Security program is threat-driven and assumes a continuous state of compromise.	• Security risks are among the top 10 operational risks. • Adopt the philosophy of an assumed state of compromise, focusing on continuous detection and crisis response in addition to traditional IT security focus of protection and mitigation. • Security risks include theft of intellectual property, attacks on brand, and social media. • You should anticipate threats, know your vulnerabilities, and be able to identify and manage the associated risks. • Focus on your adversaries: who might attack the business and their motivations.
Ensure cooperation among third parties.	• Proactively make certain that suppliers, partners, and other third parties know—and agree to adhere to—your security practices.

Protect the information that really matters	
Identify your most valuable information.	• Know where these "crown jewels" are located and who has access to them. • Allocate and prioritize resources to protect your valuable information.

Establish and test incident-response plans	
Incident response should be aligned at all levels within the organization.	• Incident response should integrate technical and business responses. • Response is aligned at all levels by integrating the technical response (led by IT) and business response (led by business with input from legal, communications, the senior leadership team, and HR).
Security incident response should be tested using real-world scenarios.	• Improve planning and preparedness through table-top simulations of recent industry events and likely attack scenarios. • Frequently conduct table-top simulations. • Response to various attack scenarios and crisis should be pre-scripted in a "play book" format.

Gain advantage through Awareness to Action	
Security program is threat-driven and assumes a continuous state of compromise.	• All activities and investments should be driven by the best-available knowledge about information assets, ecosystem threats and vulnerabilities, and business-activity monitoring. • Organizations should create a culture of security that starts with commitment of top executives and cascades to all employees. • Organizations should engage in public-private collaboration with others for enhanced threat intelligence.

We can help you understand the implications of this new approach to information security and apply the concepts to the unique needs of your business, your industry and your threat environment. Let us show you how to effectively combat the security threats of today and plan for those of tomorrow.

About PwC

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

Sivarama Krishnan
Executive Director
sivarama.krishnan@in.pwc.com

Siddharth Vishwanath
Executive Director
siddharth.vishwanath@in.pwc.com

Anirban Sengupta
Associate Director
anirban.sengupta@in.pwc.com

Sundareshwar Krishnamurthy
Associate Director
sundareshwar.krishnamurthy@in.pwc.com

Priti Ray
Associate Director
priti.ray@in.pwc.com

Manu Dwivedi
Associate Director
manu.dwivedi@in.pwc.com

www.pwc.in

PD 101 - October 2013 Before tomorrow dawns.indd
Designed by Brand and Communication, India