

**India Security Survey 2013**

*The heart of the matter 06 | Methodology 08 | An in-depth discussion 10 |  
Industry overview 27 | What this means for your business 31*

# ***Changing the game*** **The State of Information Security Survey India 2013**



[www.pwc.com/india](http://www.pwc.com/india)

# Preface

PricewaterhouseCoopers Pvt. Ltd (PwC) has been publishing the State of the Information Security Survey- India since 1999. This is the fifth edition of the survey. Through these surveys, over the years, we have chronicled the changing nature of risks, created awareness and driven greater understanding of the information security landscape in India.

The technology environment in organisations in India has evolved rapidly in both content and form. Consequently, new challenges have emerged for organisations in managing their information security risks. Today, organisations are striving to manage information security risks systematically through their organisation, in line with larger business objectives, under the active involvement of their leadership.

In this study, conducted by PwC, as part of our global survey titled The Global State of Information Security Survey 2013, we have assessed the status of information security in organisations in India. We have aimed to provide you with an insight and analysis on aspects such as information security behaviors in organisations, security priorities and spending, safeguards and security policies implemented by companies in order to secure their information assets.

We hope this report will play an important role in helping enterprises of all sizes and operations, shape their efforts and strategies towards information security and compliance. We look forward to your comments and feedback.

Happy reading!




*P. v. Krishnan*

**Sivarama Krishnan**

Executive Director

PricewaterhouseCoopers, India

Email: [sivarama.krishnan@in.pwc.com](mailto:sivarama.krishnan@in.pwc.com)



*'The smartest organisations in the country are bringing together strategy, technology and market intelligence in a way that stacks them at the top of the information security league tables. The high stakes game of information security is witnessing unforeseen dynamics wherein both the game and the opponents are ever changing. To win, consummate strategists are focusing on advanced skills, processes and technology.'*

# Executive Summary

## **Key findings from our analysis are**

*Respondents from India are more confident of their organisations' information security capabilities as compared to their global counterparts. They are also way more optimistic of enhanced organisational focus on security compared to global peers.*

45% of respondents rate their organisations highly, saying their companies exhibit the attributes of information security leaders. 80% of the respondents have high confidence levels that their organisations have instilled effective security behaviors in their culture. 82% respondents report confidence in the execution and operationalization of security in their organisations and their partner/supplier organisations and vouched for overall effectiveness.

75% of respondents from India, as compared to 45% of global peers expect an increase in information security spending. Consequently with rise in spending project deferrals are decreasing and overall project budgets are protected. 46% of the respondents reported that both economic environment and business continuity/disaster recovery were primary among the critical factors influencing security budgets. Regulatory compliance is the key justification provided by executives for increase in information security spending.

*Respondents report strong alignment of information security strategies with business goals.*

Nearly 85% respondents claimed that their organisations' security strategy and security spending are aligned with business objectives. Organisations in India have stronger process controls in terms of data privacy and information security safeguards. More than half the respondents from organisations in India report having a well staffed internal information security structure.

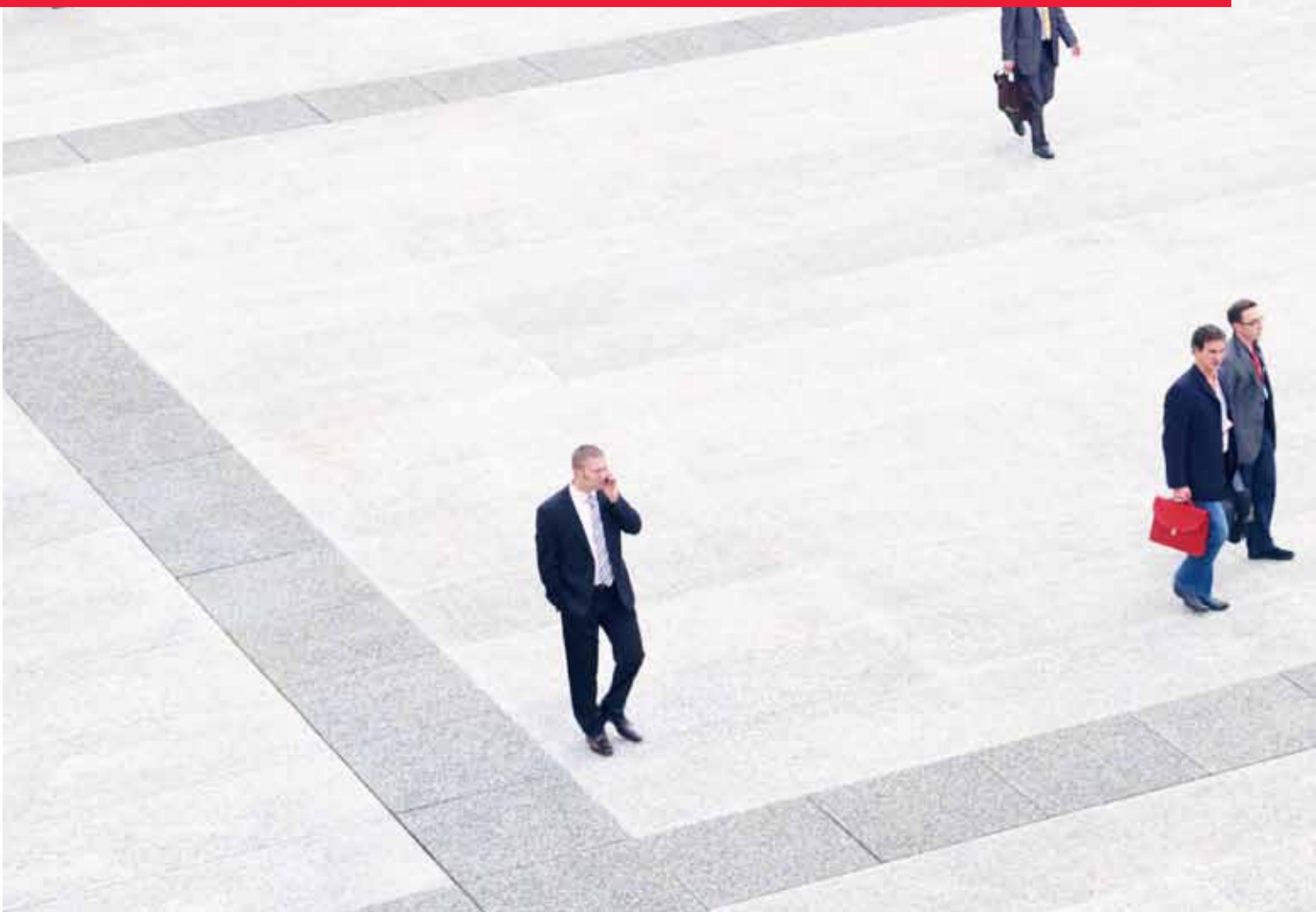
*Respondents concede that there continue to be key areas where information security capabilities need to be improved.*

While security incidents have increased three-folds in India, data avers that respondents do not measure losses completely. Security lags technology adoption in mobile devices, social media, and the cloud environment. Ubiquity of these new technologies has still not translated into effective enterprise strategies focused on them. Over time, there has been a decline in the use of most basic information security detection technologies. Several organisations also report a relaxation of fundamental security principles in their policies. Interestingly, 59% respondents view senior leadership as a significant challenge in improving overall effectiveness of their organisation's information security function.



01

# *The heart of the matter*



*Security has become a critical success factor for businesses in India. Increasingly businesses are discovering that security is a game wherein the rules are ever changing and the opponents ever ready to outsmart. The risks are on the rise.*

The uncertainty in the global as well as the Indian economy in the past few years has made information security an increasingly challenging game whose outcome can have potentially serious consequences for your business. In today's rapidly evolving threat landscape, businesses run the risk of falling behind, their defences weakening and security practices dulling. At the same time, their adversaries are becoming ever more sophisticated, breaching the defences of business ecosystems and leaving reputational, financial, and competitive damage in their wake.

Respondents to The State of Information Security Survey – India, 2013 seem to be playing an entirely different game. Of the 738 executives across 17 industries who responded to the survey, most expressed a high level of confidence in their organisations' information security practices. Indeed, many believe they are winning. Strategies are deemed to be sound. Nearly half (45%) the respondents see their organisation as a "front-runner" in terms of information security strategy and execution. The odds, however, are not in their favor. Too often, and far too many organisations are reporting degradation in security programs. Risks are neither well understood nor addressed. The number of security incidents is on the rise. Senior executives are frequently seen as part of the problem rather than keys to the solution. These are posing significant challenges to the information security environment in organisations. Given today's elevated threat environment, businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win.





02

# *Methodology*



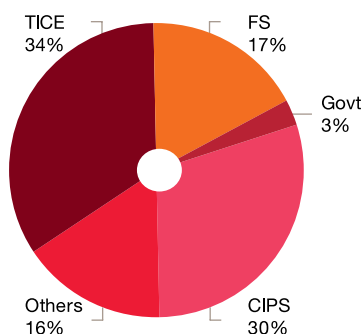


The survey was conducted using a structured questionnaire, administered online. Organisations across the country were invited via email to take the survey. This survey was conducted as part of PwC's global survey titled The Global State of the Information Security Survey 2013. The results discussed in this report are based on responses from more than 730 CEOs, CFOs, CISOs, CIOs, CSOs, vice presidents, and directors of IT and information security from 17 industries in India. The margin of error is less than 1%. All figures and graphics in this report were sourced from survey results.

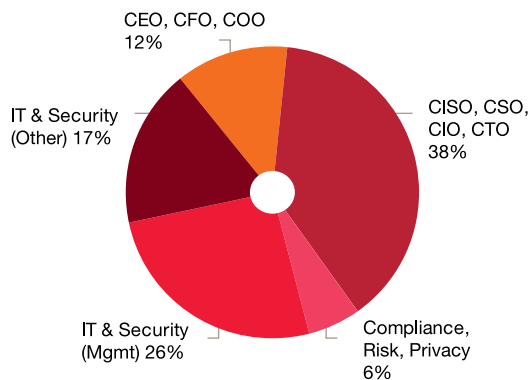
The State of Information Security Survey- India, 2013 is in its fifth edition. The survey was conducted online through a structured questionnaire. Key facts about the respondents:

- Respondents have been clubbed into four major industry verticals – Consumer, Industrial Products and Services(CIPS), Technology, Information, Communications and Entertainment(TICE), Financial Services(FS), Government and Others
- Maximum responses have been received from TICE (34% respondents) followed by CIPS (30%)
- Majority of the respondents (61%) are from medium and large enterprises
- Around 93 % respondents either represent senior management or specialized information security staff

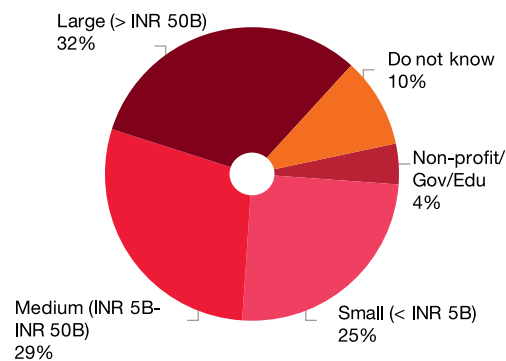
Respondents by industry



Respondents by title



Respondents by company profile



Note: Due to rounding, numbers reported may not reconcile precisely with raw data.



03

## *An in-depth discussion*





*When it comes to their security game plan, the general mood among executives in India is optimistic. Although the data do not always support that sentiment.*

## **A game of confidence** Organisations assess their security practices

---

### **Finding #1**

**45%** of respondents rate their organisations highly, saying their companies exhibit the attributes of information security leaders.

However, analysis reveals that only **15%** of respondents' organisations reflect attributes of true information security leaders.

---

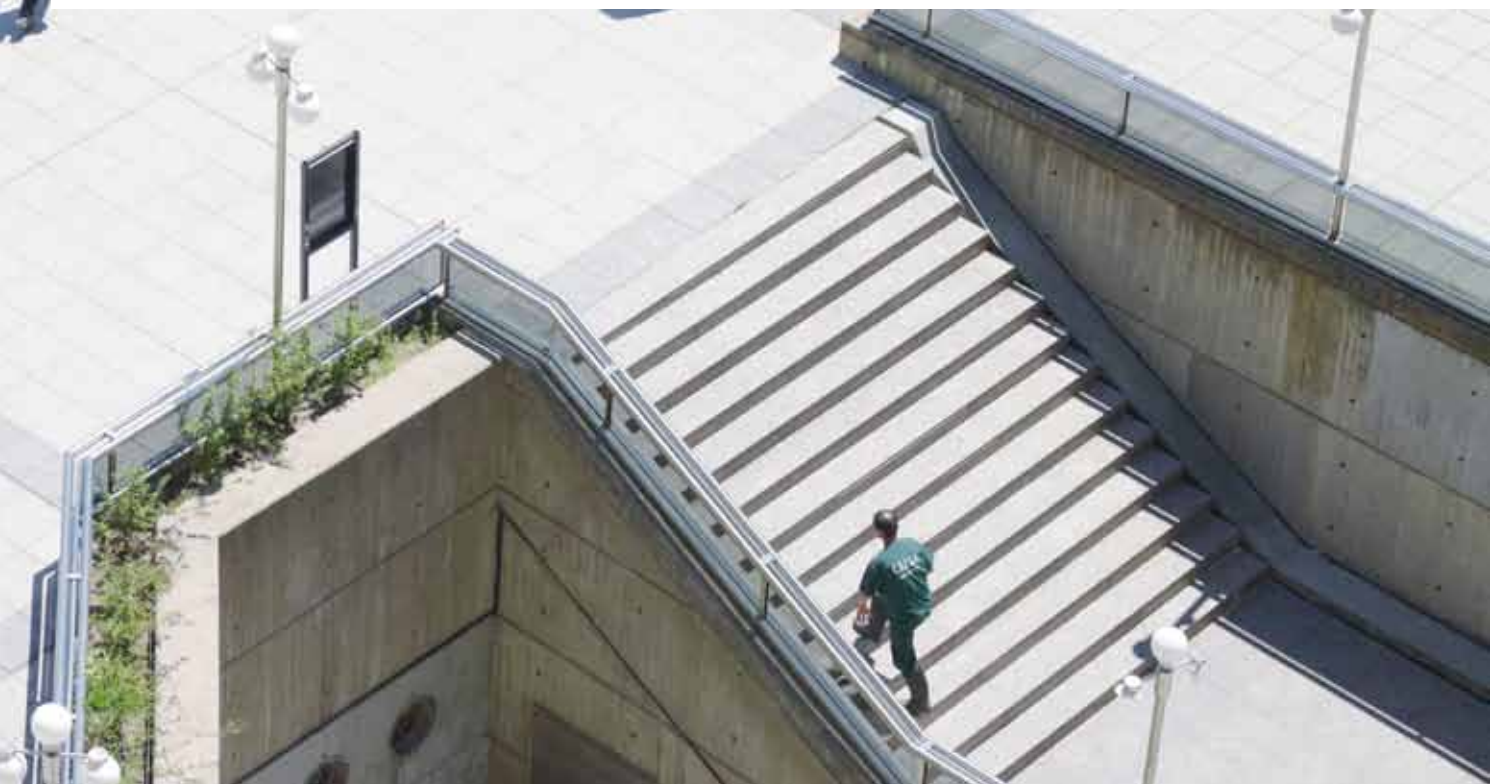
### **Finding #2**

**80%** of the respondents have high confidence levels that their organisations have instilled effective security behaviors in their culture. However, data reflects lack of general commitment to information security on the ground.

---

### **Finding #3**

**82%** respondents report confidence in the execution and operationalization of security in their organisations and their partner and supplier organisations and vouched for overall effectiveness.



---

### Finding #1.

45% of respondents rate their companies highly, saying their organisations exhibit the attributes of information security leaders. However, analysis reveals that only 15% of respondents' organisations reflect attributes of true information security leaders.

A closer look at the data shows that many of these claims are overly optimistic. Our survey includes several questions meant to identify genuine security leadership, along with others that allow organisations to assess their own readiness.

We have categorized respondents according to the way they describe their approaches to security. Frontrunners (45%) say their organisation has “an effective strategy in place and is proactive in executing the plan.” These are key elements of true security leadership. Strategists (28%) say they are “better at getting the strategy right’ than executing the plan,” while tacticians (16%) rate

themselves “better at getting things done’ than at defining an effective strategy.” Firefighters (11%) admit that they “do not have an effective strategy in place and are typically in a reactive mode.”

But are our front-runners actually leaders? We measured respondents’ self-appraisals against the four key criteria used to define leadership. Real leaders must:

- Have an overall information security strategy
- Employ a chief information security officer (CISO) or equivalent who reports to the “top of the house”—e.g., to the chief executive officer (CEO), chief financial officer (CFO), chief operating officer (COO), or 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

The self-assessments tend to be much more positive as against our analysis of these organisations. Based on the qualifications outlined above, our analysis reveals that only 15% of respondents from India rank as true information security leaders. Compare that elite group to the much larger cohort of self-identified front-runners and it seems clear that many organisations overrate their security practices.

---

How survey respondents characterize their organisations’ approach to information security

---



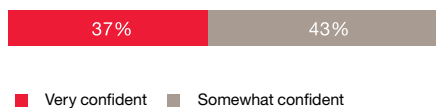
Note: Due to rounding, numbers reported may not reconcile precisely with raw data.

## Finding #2.

80% of the respondents have high confidence levels that their organisations have instilled effective security behaviors in their culture. However, data reflects lack of general commitment to information security on the ground.

To be effective, security must be integral to the way people think and work, not merely an afterthought or another item to be checked off a list. And most respondents tell us they have achieved that kind of buy-in: 37% are very confident they have instilled effective security behaviors into their organisational culture, and another 43% are somewhat confident. Just 14% are either not very confident or not at all confident on the culture question, while 6% say they do not know.

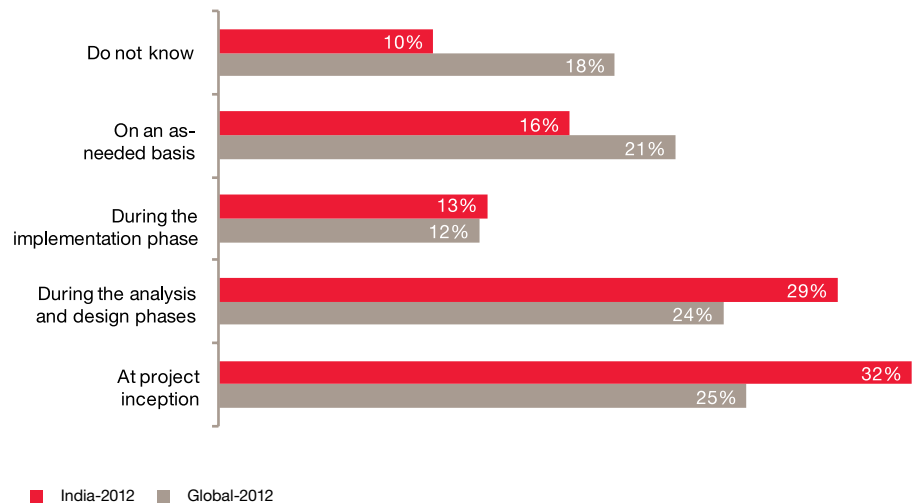
Confidence that organisations have instilled effective information security behaviors into their culture



However less clear, is whether security really has become second nature. A look at the routines and interactions that make up an average workday reveals gaps between perception and reality. For example, nearly one-third (32%) of respondents report that information security becomes involved in major projects at inception, while 29% state that security is looped in during the analysis and design phases and 13% says that it becomes involved during implementation. More than one in six affirm that security gets involved on an as-needed basis, while 10% do not know.

The way people work with others also reflects a general lack of real commitment to security. Most organisations lack an incident-response process to report and handle breaches at third parties that handle data, and fewer than 40% require third parties (including outsourcing vendors) to comply with their privacy policies. Furthermore, fewer than half (47%) of respondents say their firms collect, retain, and access only as much personal customer information as is necessary to conduct their business. The rest, presumably, collect more customer information than they actually use.

When information security becomes involved in major projects

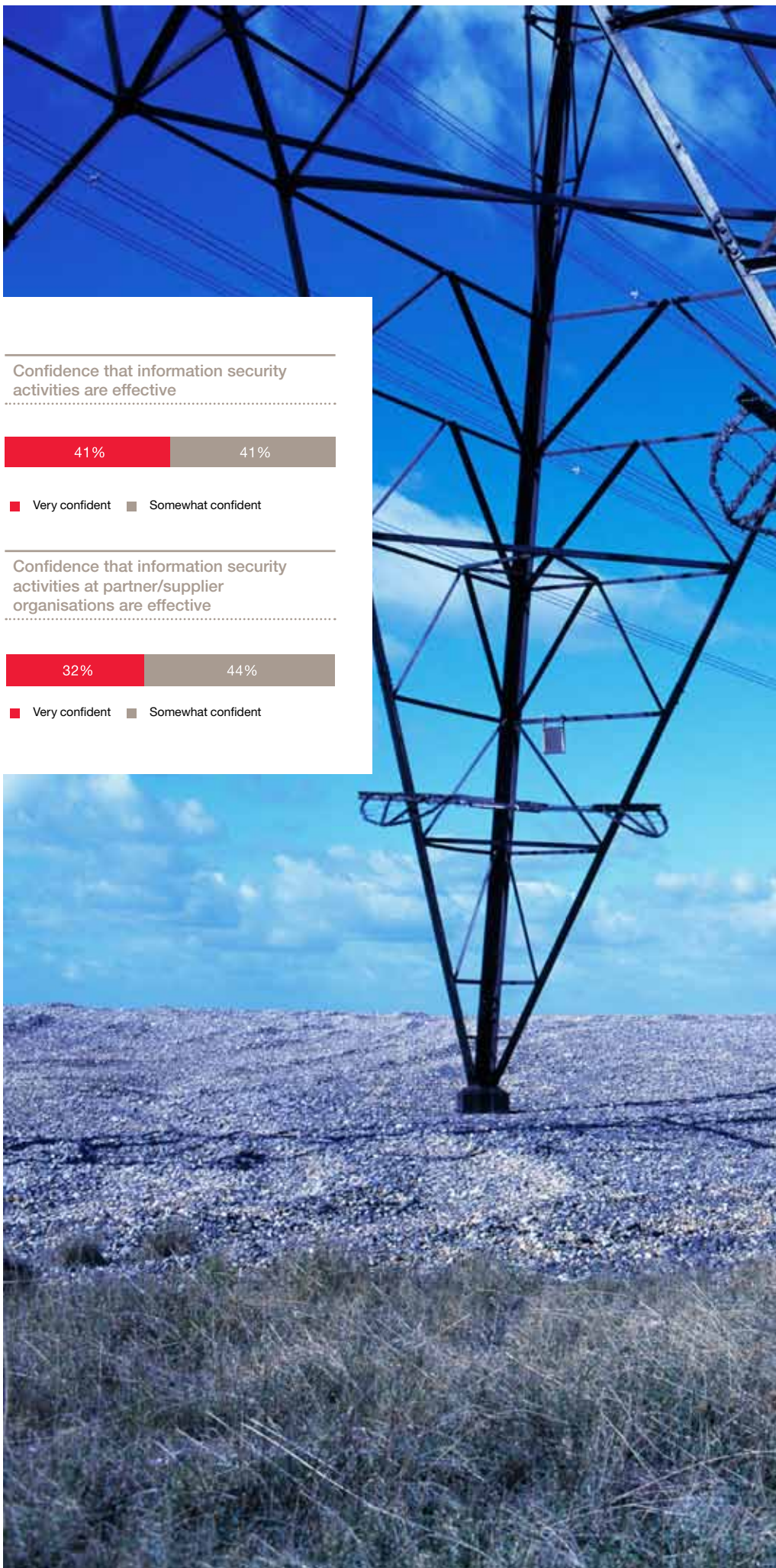


**Finding #3.**

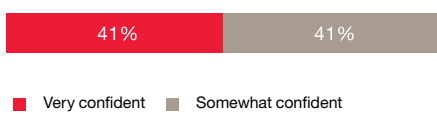
82% respondents report confidence in the execution and operationalization of security in their organisations and their partner or supplier organisations and vouched for overall effectiveness.

Strategy and culture only pay off if execution is strong, and most of the people who took our survey have a strong sense that their security is good at a nuts-and-bolts level. 82% of respondents are very (41%) or somewhat (41%) confident that their organisation's information security activities are effective. The percentage of respondents indicating confidence in their security activities has come down slightly from 85% in 2011. Yet, organisations here continue to be more confident than global counterparts (70%) on overall effectiveness of information security.

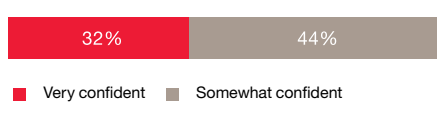
Companies in India are also slightly more confident of the security environment of their suppliers or partners compared to global peers.



Confidence that information security activities are effective



Confidence that information security activities at partner/supplier organisations are effective





## **A game of risk**

### **Enhancement of capabilities**

---

#### **Finding #4**

75% of respondents from India, as compared to 45% of global peers expect an increase in information security spending. Consequently with a rise in spending, project deferrals are decreasing and overall project budgets are protected.

---

#### **Finding #5**

While reported security incidents have increased three-folds in India, financial losses due to security breaches have decreased significantly. Yet, data avers that respondents do not measure losses completely.

---

#### **Finding #6**

46% of the respondents reported that both economic environment and business continuity or disaster recovery were primary among the critical factors influencing security budgets. Regulatory compliance is the key justification provided by executives for increase in information security spending.

---

#### **Finding #7**

There is a decline in the use of most basic information security detection technologies. Several organisations also report a relaxation of fundamental security principles in their policies.

---

#### **Finding #8**

Organisations in India continue to have stronger process controls for data privacy in terms of safeguards. Although, in keeping with the global trend, there is a loosening of tabs on data as compared to the previous year.

---

#### **Finding #9**

Security lags technology adoption in mobile devices, social media, and the cloud environment. Ubiquity of these new technologies has still not translated into effective enterprise strategies focused on them.

**Finding #4.**

75% of respondents from India, as compared to 45% of global peers expect an increase in information security spending. Consequently with a rise in spending project deferrals are decreasing and overall project budgets are protected.

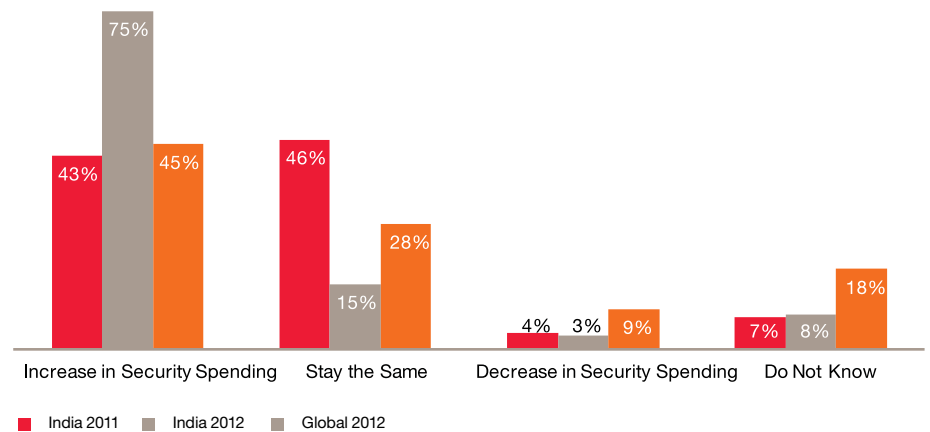
Over 75% of the respondents in India expect to see an increase in security spending over the next 12 months compared to the global average of 45%. Another 15% expect the spending on information security to remain steady, demonstrating that most companies are either increasing or maintaining their spending and consequent focus on information security.

Good news is to be also found in the declining rates of deferrals for both capital and operating expenditures along with fewer budget cutbacks for security initiatives. Nearly 58% of respondents report that their organisation did not defer capital spending for IT security. Another 23% state projects were deferred by less than six months; only 4% saw projects deferred by a year or more. Meanwhile, deferrals on operating expenditures were even less common. Around 66% of respondents report that their organisation did not defer operational spending for IT security, while 21% reported that projects were deferred by less than six months; only 3% saw deferrals beyond a year.

Project budgets were pretty well protected, with no spending cuts seen by almost two-thirds of respondents, and another 16% reporting cuts of less than 10%. Still, almost 7% capital projects saw cost cuts of over 20%. Again, the numbers were similar for IT security operating budgets.

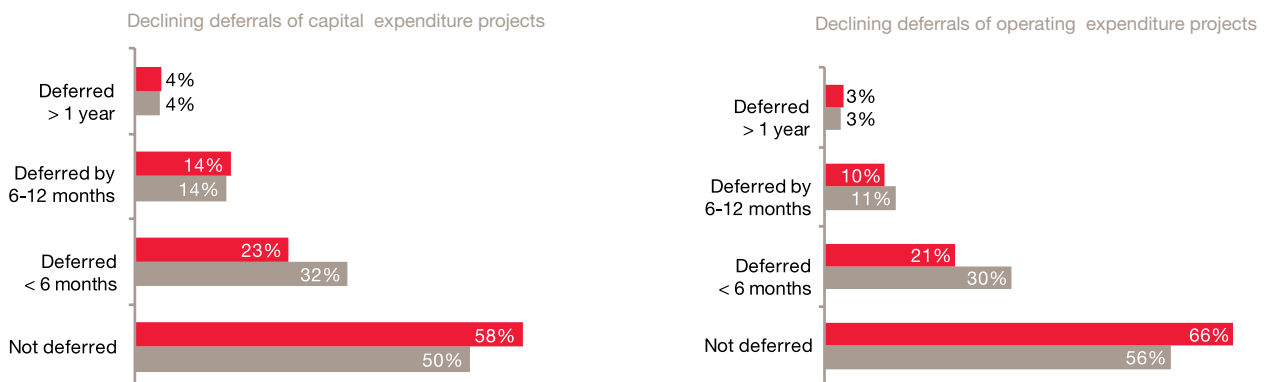
In order to measure effectiveness of security spending, most companies in India rely on professional judgment together with improvement against internal security metrics and reduction in security incidents.

Security spending over next 12 months



Note: Due to rounding, numbers reported may not reconcile precisely with raw data.

Declining deferrals for capital and operating projects



Note: Due to rounding, numbers reported may not reconcile precisely with raw data.



### Finding #5.

While reported security incidents have increased three-folds in India, financial losses due to security breaches have decreased significantly. Yet, data avers that respondents do not measure losses completely.

Reported security incidents are on the rise as compared to last year. The number of respondents reporting 50 or more incidents hit 15%, up from 4% last year. About 23% of respondents affirm that their organisation experienced no incidents, while 9% say they do not know.

Most reported incidents comprised of exploitation of removable storage (35%), data (32%), and mobile devices (28%).

Employees of the firms were reported as the most common source of security incidents. More than half (53%) of the respondents said that current employees expose their organisation to security incidents which is 17% higher compared to global averages. Former employees

were also cited as a major security threat, reported to be responsible for nearly one third of the incidents. This indicates that the companies need to establish greater rigor in their exit related processes. One-fourth of the respondents blamed the competitors for security breaches.

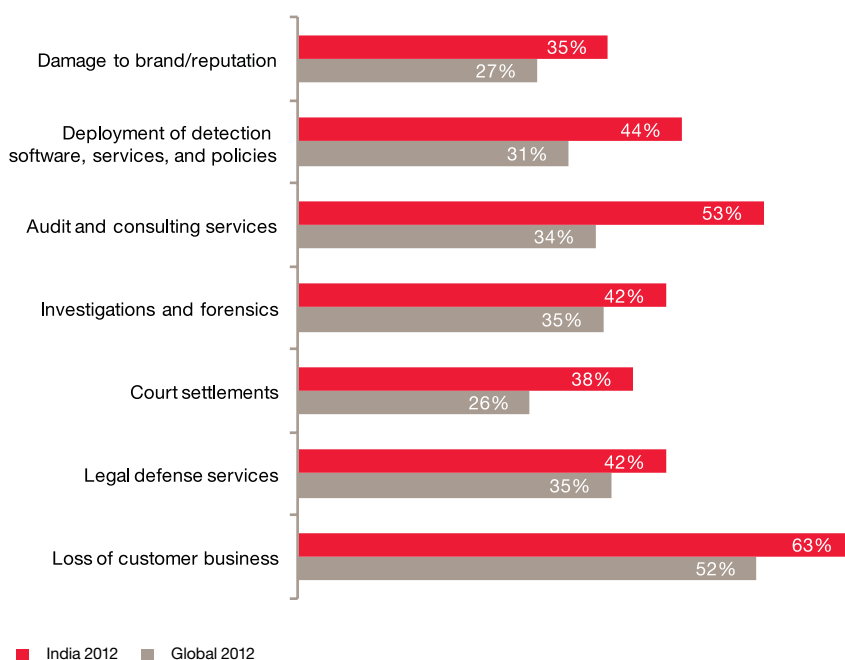
Most companies in India rely on detective controls for identifying security incidents and breaches. 4 out of 10 respondents reported that their organisations detected incidents from analysis of the server and firewall logs. Reporting by customers and colleagues were also important in discovering security incidents.

Among those that did experience a security incident, 35% of respondents reported financial losses due to breaches, down from 52% in 2011. 19% say they experienced a loss in shareholder value this year due to security breaches, down a bit from last year.

Ironically, many organisations do not perform a thorough appraisal of the factors that might contribute to such losses. While a large number of companies (63%) considered loss of customer business while computing adverse impact of incidents barely one-third (35%) considered damage to brand and reputation when estimating the full impact of a security breach.

Not all organisations considered the entire costs in computing their financial losses. Audit and consulting services costs were included by only 53% respondents. Investigations and forensics were included by 42% of respondents, and the same percentage (42%) looked at legal defence services. Only 38% included costs of court settlements.

Factors included in calculation of financial losses from security threats



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

## Finding #6.

46% of the respondents reported that both economic environment and business continuity or disaster recovery were primary among the critical factors influencing security budgets. Regulatory compliance is the key justification provided by executives for increase in information security spending.

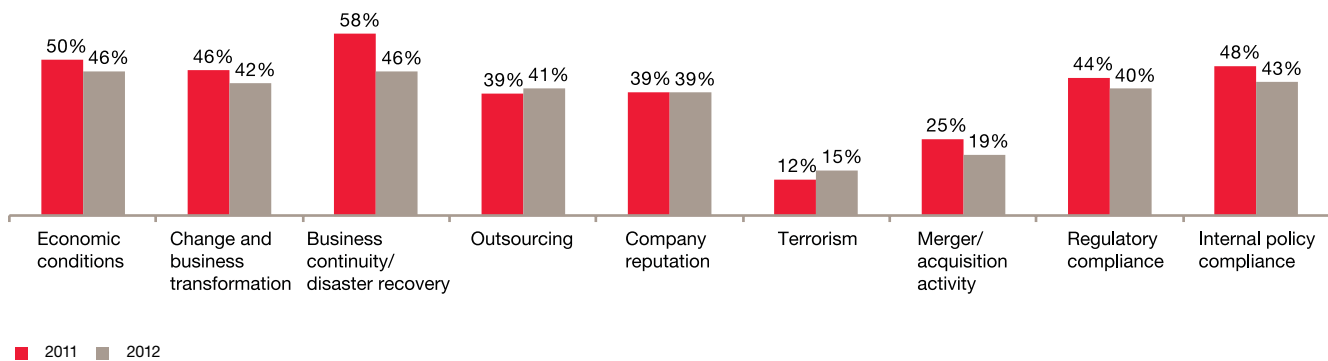
What business issues or factors drive security spending? We saw a wide range of responses on this issue, but the most frequently cited answers did not concern the business value of good information security. In fact, economic conditions and business continuity and disaster recovery are by far the largest drivers of security spending, cited by 46% of respondents.

Compliance requirements (combined total of 73% for internal and regulatory compliance requirements) are also a significant determinant in shaping security budgets.

Change and business transformation, rated as important by 42% respondents, alludes to the evolving organisational dynamics impacting strategic security decisions. 39% respondents also rate company reputation as an important factor driving information security spending.

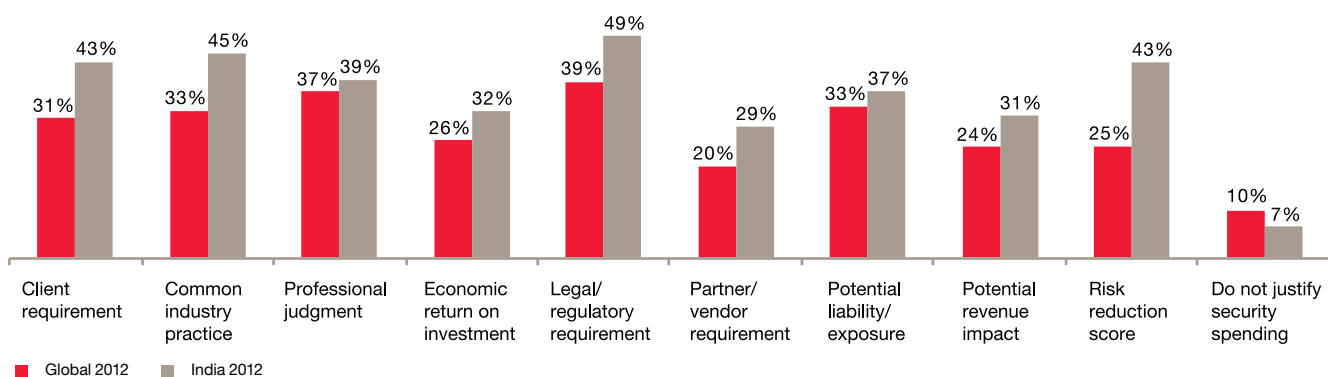
Respondents (49%) cited legal and regulatory compliance requirements as the key justifications for information security spending. This is in line with global trends. Globally, professional judgment is the second most reported justification while it ranks fifth in citation in India. This implies a relative under-confidence in security ranks of companies in India.

Business issues or factors driving organisation's information security spending



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

Justification of information security spending— Global vs. India, 2012



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

## Finding #7.

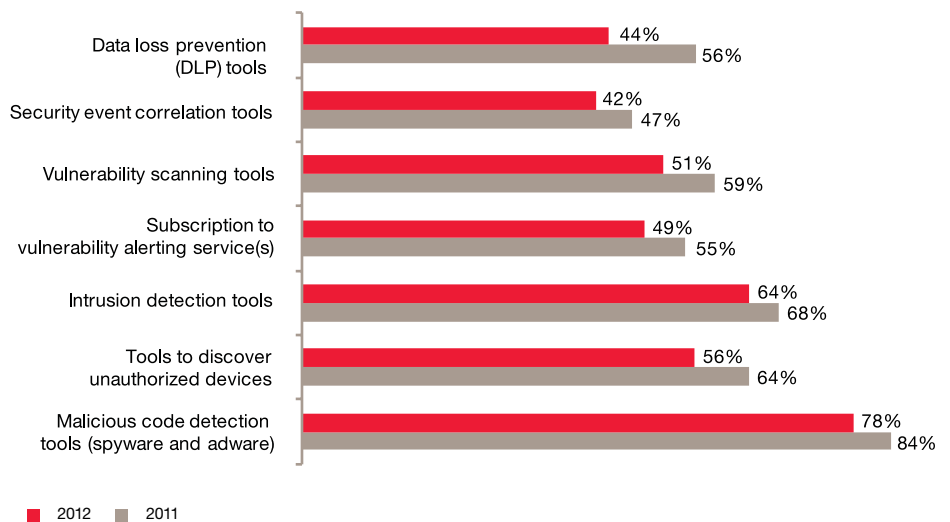
There is a decline in the use of most basic information security detection technologies. Several organisations also report a relaxation of fundamental security principles in their policies.

A counter-intuitive trend during this era of information security confidence has been the decreasing deployment of many basic information security and privacy tools and the watering down of fundamental security components in policies.

What is clear is the diminution of detection technology arsenals in recent years. Among the categories taking a hit are malicious code detection tools for spyware and adware, down to 78% after topping out at 84%, and intrusion detection tools, once in use by nearly 68% of respondents last year and now used by just 64%. Similar slides have occurred with tools for vulnerability scanning, security event correlation, and data loss prevention.

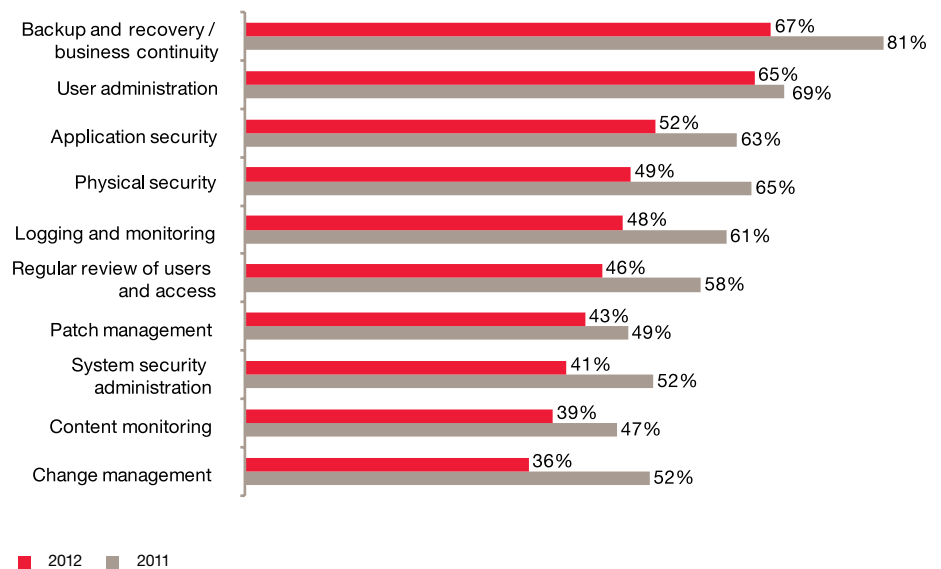
Concurrent with the emptying of information security toolboxes has been a relaxation of the policies that set standards across the enterprise. Many fundamental elements of security policy have dwindled—sometimes sharply—over the past 1 year. Take, for example policies defining backup and recovery / business continuity, which only 67% of respondents say remain in place at their organisations from 81% of respondents claiming the same in 2011. The list goes on: User administration, application security, physical security, and management practices like segregation of duties have all seen declines.

### Technology information security safeguards in place



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

### Elements included in security policies



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

**Finding #8.**

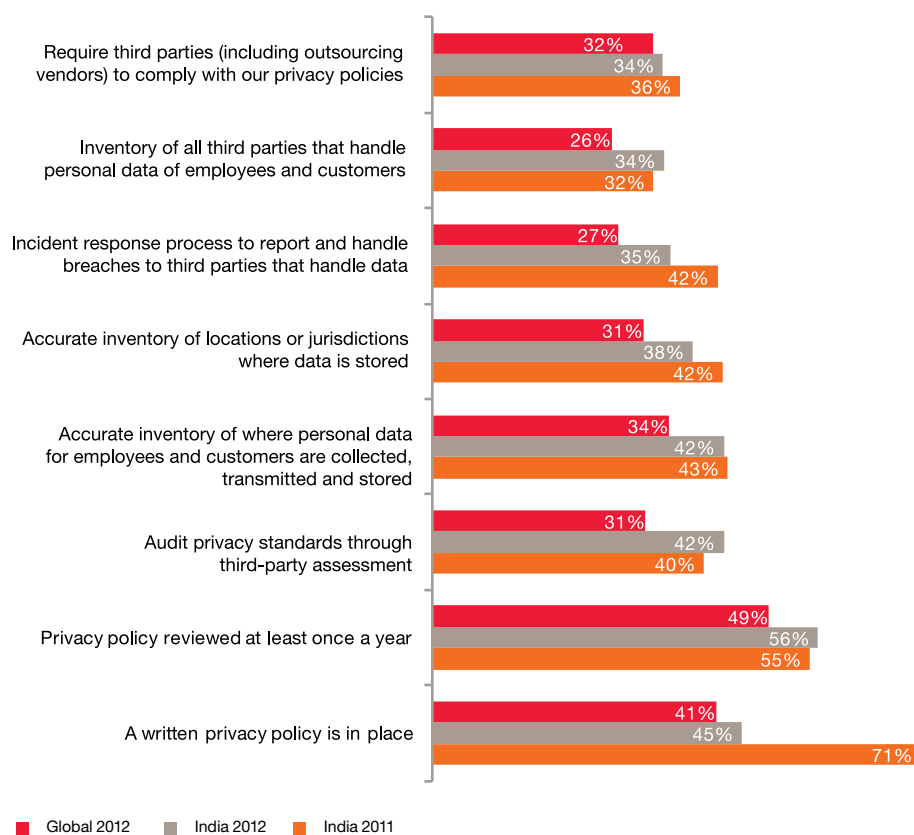
Organisations in India continue to have stronger process controls for data privacy in terms of safeguards. Although, in keeping with the global trend, there is a loosening of tabs on data as compared to the previous year.

Organisations in India continue to report higher data privacy safeguards compared to global peers. These companies show improvement in people related privacy safeguards. More than half (56%) of the respondents report that their companies require them to complete training on privacy policies and 64% claim that they are required to self-certify compliance with privacy policies.

Firewalls and operating system patch management (70%), malware and virus protection software (66%), secure user authentication protocols (63%) and secure access control measures (61%) are the key technology safeguards employed by organisations for privacy management.

Process controls data suggests that as compared to the previous year there is a loosening of process linked safeguards for privacy. The percentage of respondents reporting an accurate inventory of employee and customer personal data decreased slightly from last year at 42%. Accurate accounting of locations and jurisdictions of stored data followed a similar trajectory. Interestingly, more than half the respondents claimed that their companies did not have a published policy on privacy.

Data privacy safeguards in place related to process



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

---

### Finding #9.

Security lags technology adoption in mobile devices, social media, and the cloud environment. Ubiquity of these new technologies has still not translated into effective enterprise strategies focused on them.

India is one of the fastest growing mobile technology markets. Urban Indians are latching onto social media. The cloud may have less cultural cachet, but it, too, has become part of the infrastructure of everyday life and business.

In this context, it comes as no surprise to find an increase in the number of organisations with safeguards in place for mobile, social media, and cloud computing, along with policies covering the use of employee-owned devices. But these numbers remain stubbornly low. Just 46% have a mobile security strategy, while strategies for the cloud (31%) and social media (37%) indicate a lag in adoption rates.

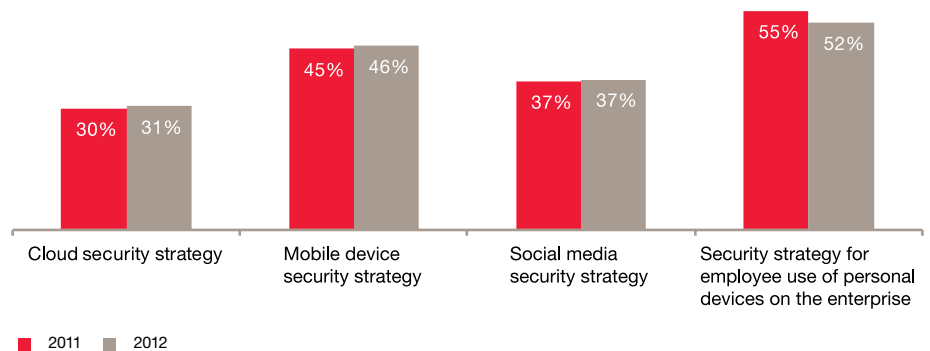
Interestingly, 52% of respondents have a security strategy to address personal devices in the workplace but only 38% have malware protection for mobile devices indicating a lag between strategy and basic execution.

To address mobile device security risks organisations are increasingly undertaking protection of corporate e-mail and calendaring on employee and user owned devices (45%) and deploying mobile device management software (44%) along with strong authentication on devices (41%). Several (36%) also reported ban on user owned devices in the workplace or network access.

---

Information security safeguards currently in place

---



Note: Not all factors shown. Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

## ***It's how you play the game***

Alignment, leadership, counsel and training are key

---

### ***Finding #10***

Nearly **85%** respondents claimed that their organisations' security strategy and security spending are aligned with business objectives.

---

### ***Finding #11***

**59%** respondents view senior leadership as a significant obstacle in improving overall effectiveness of the organisation's information security function.

---

### ***Finding #12***

Unlike global trends, more than half the respondents from organisations in India report having a well staffed internal information security structure.

---

### ***Finding #13***

**75%** respondents report that their companies actively seek external counsel to manage their information security requirements.



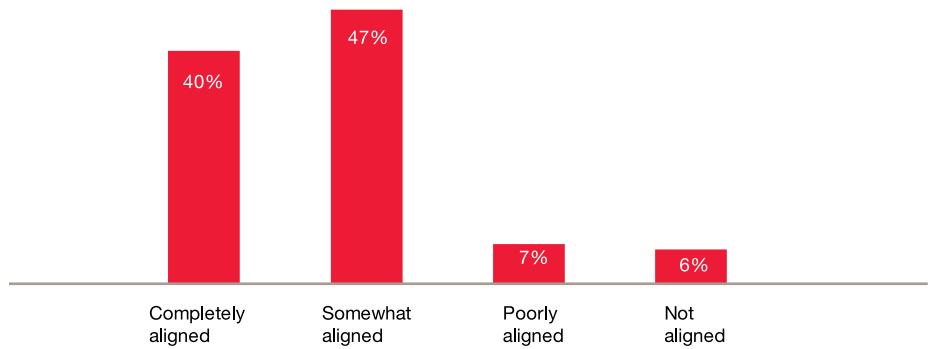
**Finding #10.**

Nearly 85% respondents claimed that their organisations' security strategy and security spending are aligned with business objectives.

Most respondents believe their security efforts are well-targeted and aligned with the goals of the larger organisation, with 40% saying security policies are completely aligned with business goals. Another 47% say they are somewhat aligned. Just 13% respondents say strategies are poorly aligned or not aligned.

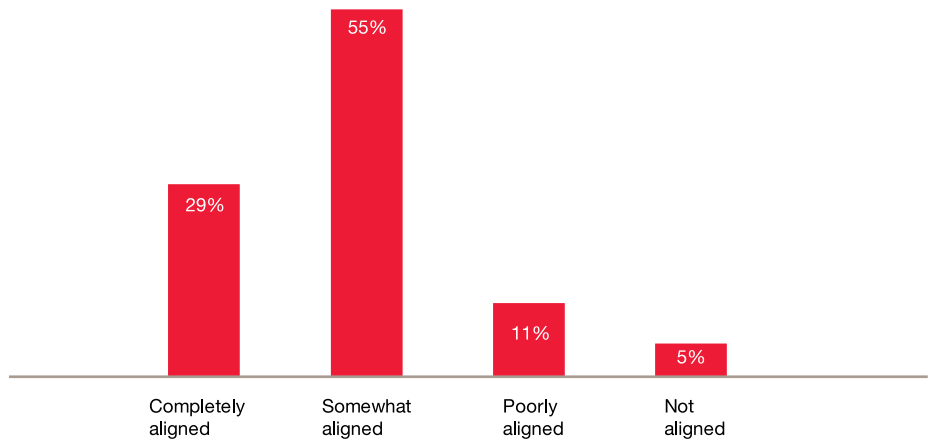
Translating those policies into well targeted spending is the next task, and alignment of security spending with business objectives hits similar marks. 55% of respondents say they are somewhat aligned, 29% claim to be completely aligned, while 11% claim poor alignment and 5% say they are not aligned.

Alignment of security policies with business objectives



Note: Due to rounding, numbers reported may not reconcile precisely with raw data.

Alignment of security spending with business objectives



Note: Due to rounding, numbers reported may not reconcile precisely with raw data.

**Finding # 11.**

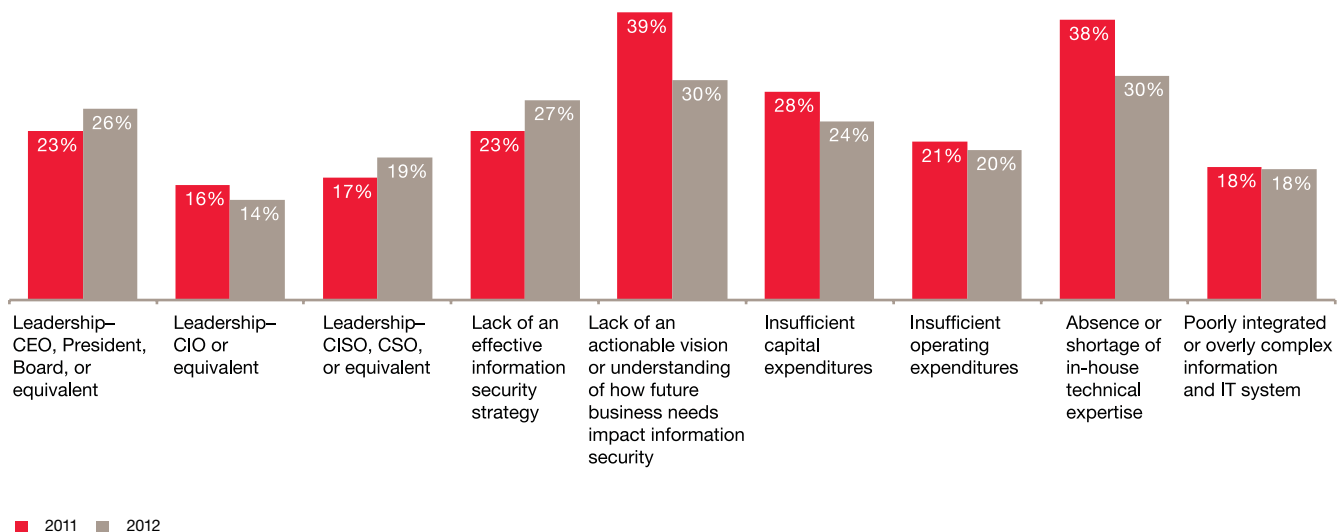
59% respondents view senior leadership as a significant obstacle in improving overall effectiveness of the organisation's information security function.

Respondents were asked to name the most significant barriers to improving the overall strategic effectiveness of the information security function. Many of the respondents point to the top: More than one in four name the CEO, board, or equivalent, while another 14% single out the CIO and 19% cite senior security officers. Added together, more than half of respondents say top-level leadership is the greatest obstacle to improving information security effectiveness—a larger number than any single category, including insufficient capital and operating funds, lack of strategy, and a shortage of skilled workers.

The data pointing to a lack of C-suite leadership in information security makes sense considering that the security function often lacks a direct channel to the real decision-makers. Reporting to the top of the house is a mark of a true security leader, but only 42% of senior information security executives report directly to the CEO greater than 31% in 2011. The percentage reporting to the CFO (11%) increased slightly from last year. Surprisingly, nearly a third reported that the CISO/CSO reports into the CIO. Given that the former often has to audit the activities of the latter there is a clear conflict of interest here.

Absence or shortage of in-house technical expertise together with lack of actionable vision of understanding of how future business needs impact information security has also been cited as a major barrier by 30% of the respondents.

Obstacles to improving the overall strategic effectiveness of the organisation's information security function



Note: Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.



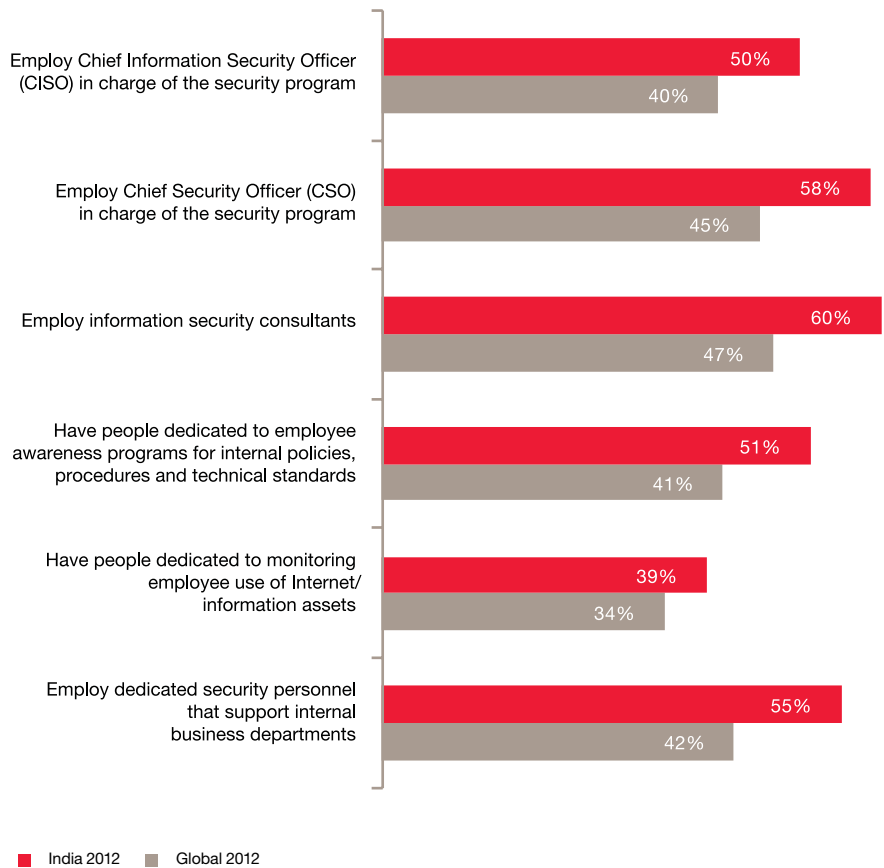
**Finding # 12.**

Unlike global trends, more than half the respondents from organisations in India report having a well staffed internal information security structure.

As compared to global peers, more than half the respondents claimed that their companies employ CISOs/CSOs. Over half the respondents also said that their organisations have depth in their information security structure employing security consultants, dedicated vigilance resources, and dedicated personnel to support internal departments.

Still, the level of personnel deployed on the training front, and the trend in that area, raise serious questions. This year saw a decrease in staff dedicated to employee awareness programmes for internal policies, procedures, and technical standards, from 67% in 2011 to 51% in 2012, and also a slight decline in the employment of information security consultants from 54% in 2011 to 60% in 2012.

Information security safeguards related to people- Global vs. India, 2012



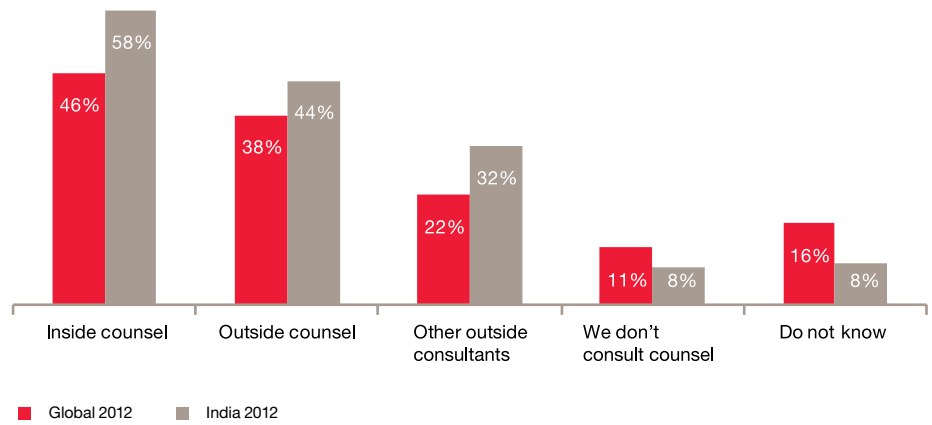
Note: Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.

**Finding #13.**

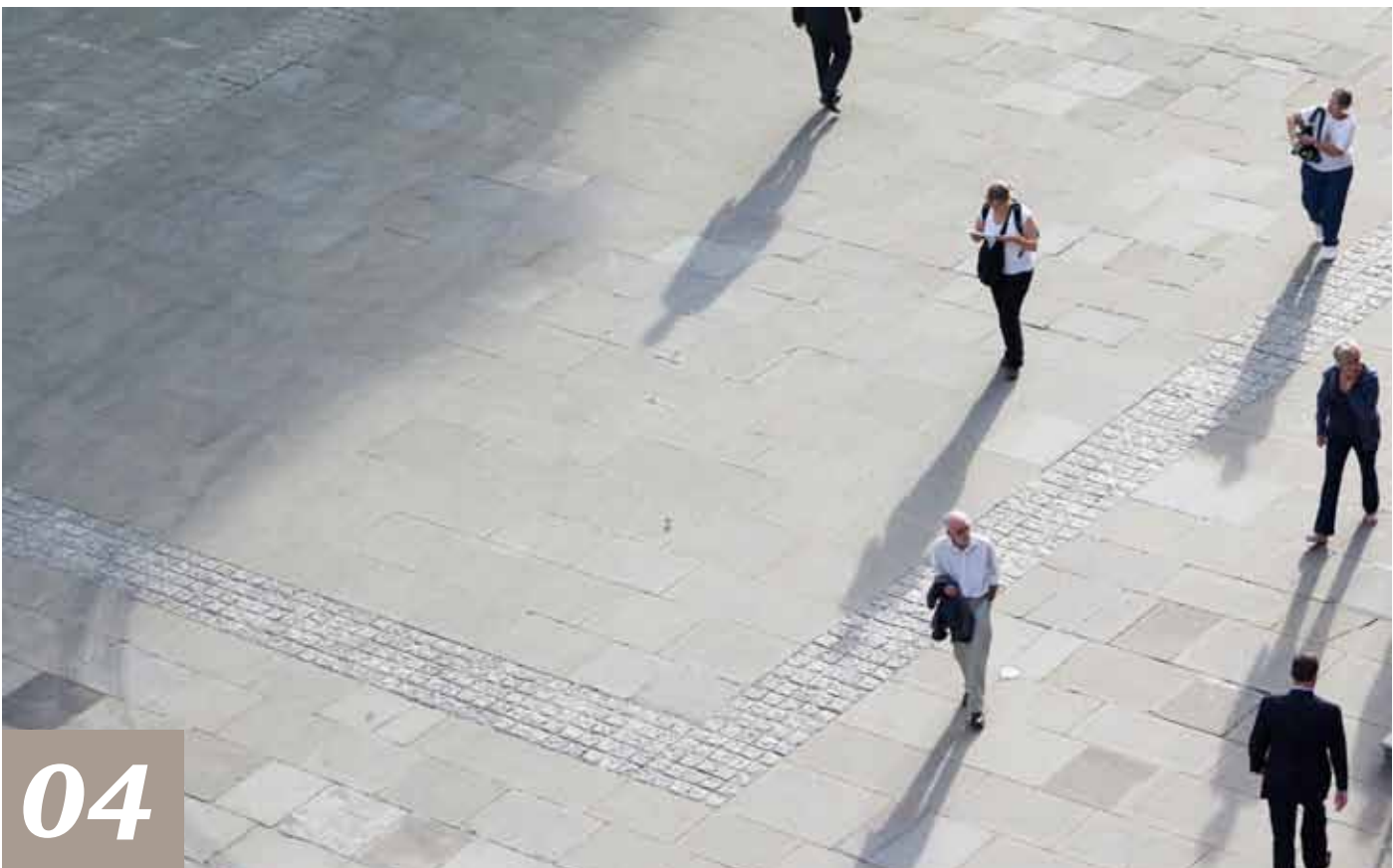
75% respondents report that their companies actively seek external counsel to manage their information security requirements.

Interestingly, in spite of having a relatively larger number of resources deployed for security related activities, the complexities of the security environment is forcing companies in India to seek external help not only to fire-fight incidences but increasingly to manage information security end to end. This is indicative of the constantly evolving nature of information risks that companies in the country are challenged with. Increasing use of external counsel also implies that there is a evolving environment of best practices sharing between companies nurtured through these external resources.

Figure 22: Sources from which companies seek advice for privacy and information security management



Note: Totals do not add up to 100%. Respondents were allowed to indicate multiple factors.



04

# *Industry overview*





## **Technology, information, communications and entertainment (TICE)**

### **Security priorities**

Nearly 43% of respondents from TICE organisations feel that their security policy is completely aligned with their business goals. Another 45% feel that their security policies are somewhat aligned with their business objectives.

Organisations are also confident about their overall security activity. About 46% of TICE respondents are very confident of the effectiveness of their security operations and another 35% are somewhat confident of the same.

### **Security investments and spending**

Respondents from TICE are optimistic about the alignment of spending with their business goals. Most (89%) respondents feel that there is an alignment between the two.

74% respondents believe there will be an increase in security spending in the next 12 months.

### **Safeguards present and future**

Centralized user data store and identity management technology are the primary technology safeguards in TICE companies. In terms of encryption of devices, this sector has focused most on encryption of laptops (68%) followed by encryption of databases and fileshares in the organisation.

64% respondents reported having people dedicated to employee awareness programs for internal policies, procedures and technical standards and similar percentage reported having people dedicated to monitoring employee use of Internet / information assets in their organisation.

The TICE sector leads other sectors in terms of security strategy for employee use of personal devices in the enterprise. Nearly half of the respondents said their key priority for the next 12 months is cloud security strategy.

### **Security breaches**

Around 32% respondents reported 10 or more security incidents in the past 12 months, making TICE the highest segment to report security breaches.

Current and former employees have been identified as the major sources of negative security incidents. 43% respondents also report that hackers are the other major source of security incidents.

Around 62% of respondents say that unavailability or slowed network is the main impact of security breaches followed by 44% reporting unavailability of e-mails and applications.

### **Security barriers**

Leadership and insufficient capital expenditures are the primary barriers to improving information security.



## **Financial services (FS)**

### **Security priorities**

Nearly 44% of respondents from FS organisations feel that their security policy is completely aligned with their business goals. Another 50% feel that their security policies are somewhat aligned with their business objectives.

Financial services organisations are also confident about their overall security activity. About 44% of FS respondents are very confident of the effectiveness of their security operations and another 44% are somewhat confident of the same.

### **Security investments and spending**

Respondents from FS are optimistic about investments in security. According to 89% of the respondents their information security spending is aligned with their business objectives. Most (81%) respondents feel that there will be an increase in security spending in the near future.

### **Safeguards present and future**

Nearly 60% of the organisations in the financial services sector have appointed a Chief Information Security Officer (CISO), which is significantly higher than other industry segments. In addition, nearly 40% of respondents from the financial services sector claim that the CISO reports into CIO. In case a CISO reports to CIO, there might be independence issues and conflict of interest, as a CISO is responsible for evaluating security and controls of the IT Infrastructure and the CIO is responsible for investing, managing and maintaining the same. This is a clear red flag that financial services companies will need to review.

Only 26% of the respondents said that their companies have process related safeguards for cloud security, while only 28% had safeguards related to social media in place. Safeguards around penetration testing and threat and vulnerability assessments continue to hover around 60% considering the external threat perceptions for FS institutions. From a tools perspective 76% of the respondents reported having malicious code detection tools followed by (73%) intrusion detection tools.

### **Security breaches**

Security incidences in the past are either better pre-empted or not reported as only 20% of the respondents indicated having experienced 10 or more security breaches in the past 12 months. Around 28% of the organisations have indicated that they had suffered financial losses due to security incidents.

Current and former employees have been identified as the major sources of negative security incidents. 32% respondents also report that hackers are the other major source of security incidents.

Around 30% of respondents say that brand reputation compromises followed by 28% reporting fraud and financial losses as the key adverse impact of security breaches.

### **Security barriers**

Within the range of the overall response, 35% of the respondents feel that absence or shortage of in-house technical expertise is the primary barrier to information security. 33% feel that lack of actionable vision or understanding of future business needs impact information security is also a critical barrier.

## **Consumer, industrial products and services (CIPS)**

### **Security priorities**

Nearly 42% of respondents from CIPS organisations feel that their security policy is completely aligned with their business goals. Another 47% feel that their security policies are somewhat aligned with their business objectives.

CIPS organisations are also confident about their overall security activity. About 39% of CIPS respondents are very confident of the effectiveness of their security operations and another 45% are somewhat confident of the same.

### **Security investments and spending**

Nearly 36% of CIPS organisations feel that their spending on information security is completely aligned with their business requirements. However, 49% of the respondents feel that their spending is only somewhat aligned. 75% respondents believe there will be an increase in security spending in the next 12 months.

### **Safeguards present and future**

Around 63% of the respondents in CIPS said that they conduct security audits in their organisations to assess gaps and mitigate and a similar percentage claim that they have active monitoring and analysis of information security intelligence in their companies.

Respondents from CIPS companies claim that they have people dedicated to employee awareness programs for internal policies, procedures and technical standards. As a people linked safeguard majority also report that they conduct employee background checks.

84% of the respondents have malicious code detection safeguards followed by 72% with web content filters and another 61% with intrusion detection safeguards in their companies.

### **Security breaches**

Nearly 30% of the respondents indicated that they faced 10 or more incidents in their organisations in the past 12 months.

Current and former employees have been identified as the major sources of negative security incidents. 29% respondents also report that hackers are the other major source of security incidents.

Around 34% of respondents say that financial losses followed by a similar percentage reporting intellectual property theft as the key adverse impact of security breaches.

### **Security barriers**

Leadership and lack of actionable vision or understanding of how future business needs impact information security are the key barriers to improvement in information security in CIPS companies.



05

## *What this means for your business*



*True leaders have distinctive information security practices that help them remain ahead of the game. These are adaptable by the rest.*

Our survey enlisted participation from hundreds of executives in India. These people take information security seriously and it is their job to get their information security strategy right. Interestingly, while most exuded confidence in their security strategies and tactics the data suggested otherwise. Only 15% of the respondents were identified as true leaders in information security. These belong to an elite group with the vision, determination, skills, and support to create the most effective security organisations.

Leaders in India came from both large and medium sized companies that had a focus on security and commanded relatively larger IT and security budgets than their peers.

### **How leaders play the game**

True leaders in information security differentiate themselves through the following:

- Strong alignment of security strategy with organisational objectives and goals
- Employing an organisation wide integrated approach combining compliance, privacy and data usage, security and identity theft best practices. Leaders also deploy frameworks that enable them to establish the best in class processes and response systems for information security management.
- Continued growth in spending on information security to keep up with the ever new challenges posed by the external and internal environment
- Stronger C-suite access of security personnel and stronger integration of the security function with internal departments
- Better understanding of the losses emanating from information security breaches and consequent razor sharp focus on prevention through anticipation and early detection

At an operational level, leaders clearly outshine the rest through the following:

- Clearly defined information security organisation helmed by a CISO /CSO
- On time completion and a no tolerance approach to deferral of information security projects





- Comprehensive policy and process coverage across legacy and new technologies – mobile devices, social media, cloud etc.
- Wide deployment of information security enablement technology suite including tools that cover new technologies and existing processes effectively
- Regular audits for gap identification in security strategy and operations

Most importantly, leaders are high on awareness of their internal organisational environment and the threats emanating in the external environment. Leaders are able to apply themselves in anticipating threats and gear their security strategy and operations to respond with a pre-emption plan.

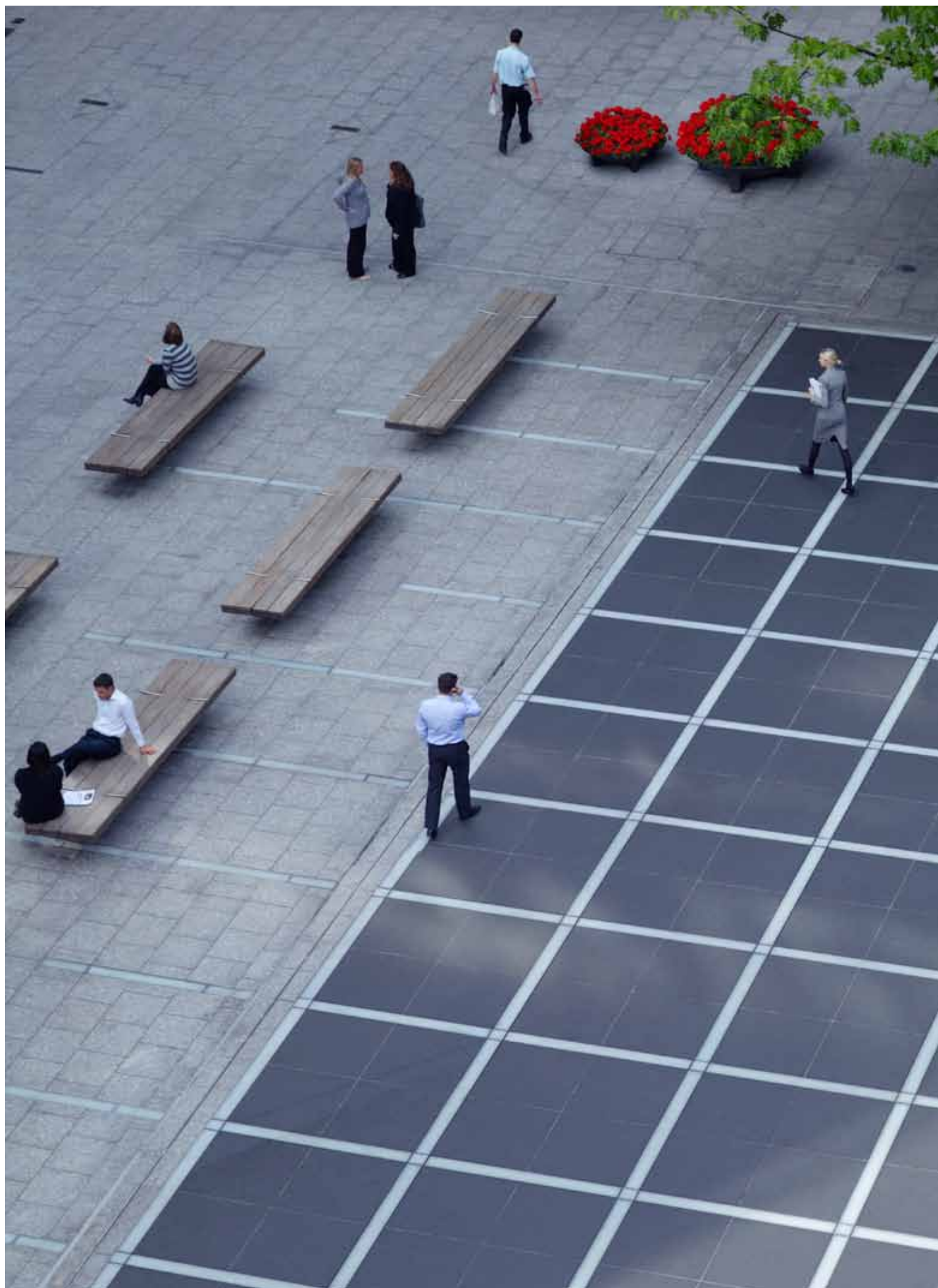
### ***What you can do to improve your performance***

Information security leaders clearly understand that the game to achieve effective security needs a high level of commitment to understanding, preparing and responding to threats with an integrated organisation wide approach. There are clear best practices that businesses seeking to strengthen their security practice can take imbibe from these leaders. These include:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks
- Understand their organisation's information, who wants it, and what tactics adversaries might use to get it
- Understand that information security requirements—and, indeed, overall strategies for doing business—have reached a turning point
- Embrace a new way of thinking in which information security is both a means to protect data and an opportunity to create value to the business

*Ask us, and we can provide you with more details on the way leaders play a better game and how their moves are relevant to your organisation.*





---

# About PwC India

PricewaterhouseCoopers Pvt Ltd is a leading professional services organisation in India. We offer a comprehensive portfolio of Advisory and Tax & Regulatory services; each, in turn, presents a basket of finely defined deliverables, helping organisations and individuals create the value they're looking for. We're a member of the global PwC Network.

Providing organisations with the advice they need, wherever they may be located, PwC India's highly qualified and experienced professionals, who have sound knowledge of the Indian business environment, listen to different points of view to help organisations solve their business issues and identify and maximise the opportunities they seek. Their industry specialisation allows them to help create customised solutions for their clients.

We are located in Ahmedabad, Bangalore, Bhubaneshwar, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune.

Tell us what matters to you and find out more by visiting us at [www.pwc.com/in](http://www.pwc.com/in).

You can connect with us on:

**f** [facebook.com/PwCIndia](https://www.facebook.com/PwCIndia)

**t** [twitter.com/PwC\\_IN](https://twitter.com/PwC_IN)



## Contacts

**Satyavati Berera\***

Tel: +91 124 330 6011

Email: [satyavati.berera@in.pwc.com](mailto:satyavati.berera@in.pwc.com)

**Arup Sen**

Tel: +91 22 6669 1078

Email: [arup.sen@in.pwc.com](mailto:arup.sen@in.pwc.com)

**Harpreet Singh**

Tel: +91 124 330 6012

Email: [harpreet.singh@in.pwc.com](mailto:harpreet.singh@in.pwc.com)

**Kumar Dasgupta**

Tel: +91 22 6669 1341

Email: [kumar.dasgupta@in.pwc.com](mailto:kumar.dasgupta@in.pwc.com)

**Manpreet Singh Ahuja**

Tel: +91 124 330 6021

Email: [manpreet.singh.ahuja@in.pwc.com](mailto:manpreet.singh.ahuja@in.pwc.com)

**Neeraj Gupta**

Tel: +91 124 330 6010

Email: [p.neeraj.gupta@in.pwc.com](mailto:p.neeraj.gupta@in.pwc.com)

**Sanjay Dhawan**

Tel: +91 80 4079 7003

Email: [sanjay.dhawan@in.pwc.com](mailto:sanjay.dhawan@in.pwc.com)

**Sivarama Krishnan**

Tel: +91 124 330 6018

Email: [sivarama.krishnan@in.pwc.com](mailto:sivarama.krishnan@in.pwc.com)

**Siddharth Vishwanath**

Tel: +91 22 6669 1559

Email: [siddharth.vishwanath@in.pwc.com](mailto:siddharth.vishwanath@in.pwc.com)

**Tapan Ray**

Tel: +91 22 6669 1204

Email: [tapan.ray@in.pwc.com](mailto:tapan.ray@in.pwc.com)

*\*National Practice Leader (RAS)*

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwCPL, its members, employees and agents accept no liability, and disclaim all responsibility, for the consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it. Without prior permission of PwCPL, this publication may not be quoted in whole or in part or otherwise referred to in any documents.

© 2012 PricewaterhouseCoopers Private Limited. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Private Limited (a limited liability company in India), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.