Technology risk management

From strength to strength

Raising the benchmark for information security in India

2007 – 2008

certin
enhancing cyber security in India

FICCI
Federation of Indian Chambers
of Commerce and Industry

PRICEWATERHOUSECOOPERS

PricewaterhouseCoopers has taken all reasonable steps to ensure that the information contained herein has been obtained from reliable sources and that this publication is accurate and authoritative in all respects. However, this publication is not intended to give legal, tax, accounting or other professional advice. No reader should act on the basis of any information contained in this publication without considering and, if necessary, taking appropriate advice upon their own particular circumstances. If such advice or other expert assistance is required, the services of a competent professional person should be sought.

Designed by: www.lopezdesign.com

Contents

Message

I am happy to learn that the Indian Computer Emergency Response Team (CERT-In), PricewaterhouseCoopers (PwC) and Federation of Indian Chambers of Commerce and Industry (FICCI) have joined hands to conduct an Information Systems Security Survey in the country.

With the advent of information technology, there is hardly any walk of life that has remained untouched. Leveraging IT, societies, governments and businesses are discovering newer ways of connecting and communicating with each other like never before. In fact, it is now almost impossible for anyone to even imagine social development and economic integration by choosing to remain outside the ambit of IT.

While IT has emerged as a key enabler of growth and development, it has its own share of problems. With the growing use of IT, networking takes the centrestage and thus arises the scope for increased dependency. It is this aspect of dependency that makes all of us vulnerable and we are now witnessing growing instances of fraudulent and criminal exploitation of cyberspace. So, today we find the ghost of cyber security assuming threatening proportions that can disrupt the golden dreams of inclusive growth and overall development. We have a responsibility to create an environment of "trust and confidence" by way of effective collaboration and communication among all parties concerned.

In this context, I find the Information Systems Security Survey quite timely and useful since it serves the twin objective of revealing our current standing in implementing information security in comparison to our global counterparts and at the same time allows us an opportunity to benchmark against the global best practices on information security.

We realise that the battle to contain the information security menace is a long one and we cannot afford to lose it. I am sure these kinds of surveys and similar actions will keep us effectively engaged.

A. Raja
Minister
Communications & Information Technology
Government of India

Foreword

Information technology and the Internet have become omnipresent in the enterprises and businesses of today. And while both of these create a vast array of opportunities for businesses and the common man, it also presents numerous challenges.

Today, Information Systems (IS) Security is one of the most important challenges faced by enterprises globally. It has become vital for every organisation to become thoroughly cognisant of the importance of information security, and to work for managing risk systematically throughout the organisation in line with each situation, under the active involvement of the management. New threats to information and networks arising from e-spionage and hacking make it necessary for a comprehensive and integrated approach and framework for effective information security and protection.

This study, conducted by the Federation of Indian Chambers of Commerce and Industry (FICCI) in association with Indian Computer Emergency Response Team (CERT-In) and PricewaterhouseCoopers (PwC) assesses the status of IS Security across sectors. It gives a deep insight and analysis on aspects like security priorities, security spending, safeguards, business continuity planning, disaster recovery planning policies implemented by companies across Industry sectors to secure their information assets.

I am sure this report will play an important role in helping enterprises of all sizes and operations shape their efforts and strategies towards information and network security and compliance.

Rajeev Chandrasekhar
MP and President, FICCI

Preface

Security in Indian organisations is evolving at a rapid pace. To simply keep up with its promise and potential is difficult for many organisations, particularly because they still deploy significant resources on managing outdated security infrastructure, implemented when security was in its adolescent stage.

What prevents the development of a mature vision of security is the lack of consensus amongst decision-makers on what constitutes the value of security. The value of security is fundamentally based on the relationship between security and what an organisation cherishes – its mission and its performance. Consequently, the benefits from security initiatives depend upon the extent to which they are aligned with the business objectives. Security creates value for an enterprise when appropriately implemented. Conversely, it can harm an organisation when its role is poorly anchored within the operating environment.

In this study, the fourth Information Systems Security Survey, conducted jointly by the Indian Computer Emergency Response Team (CERT-In), PricewaterhouseCoopers (PwC) and the Federation of Indian Chambers of Commerce and Industry (FICCI), we have attempted to assess the preparedness of Indian organisations in facing the challenge of securing their information systems and data.

We trust that these findings and conclusions will form the basis for an increased level of understanding of areas that need to be addressed for creating a robust information security framework in an organisation. We look forward to receiving your comments and feedback to make our future surveys more comprehensive and interesting.

N. Ramesh R

Ramesh Rajan
Chief Executive Officer
PricewaterhouseCoopers, India

Highlights

In the mid-1990s, Indian enterprises first learned the benefits of the internet and the web, and how they could connect with their external partners, suppliers, and customers in dynamic new ways. More than a decade-and-a-half later, they are still coming to terms with the fact that each advance in the ability to communicate and transact business comes with its own security ramifications, such as security breaches.

In the last two years, Indian organisations have experienced a number of security breaches like data leakage and its misuse. These incidents have raised doubts on the environment of security and controls within Indian enterprises.

Indian enterprises can avoid most of these unwanted events and improve information access for their extended user communities if they develop and implement an effective information security strategy and framework. By viewing security as a strategic initiative, and not as a cost centre, Indian companies can strengthen this process.

In this survey, we have attempted to assess the preparedness of Indian organisations in meeting information security challenges. Some of the key trends that emerge from the survey are:

- Information security gets a high priority amongst a majority of the enterprises, as in all previous surveys.[1]

- Our previous surveys showed an increasing trend of information security breaches: 60% of the organisations had suffered breaches in 2000-01, 80% in 2002-03 and 83% in Previous Survey*. However, it is encouraging to note that in the current survey, only 54% of the organisations have suffered security breaches. Here, one must keep in mind that in many cases, organisations were found to be unaware that a breach had occurred.

- Indian organisations have deployed a variety of controls, spread across people, process and technology domains, and have fared better than their Global+ counterparts did.

- Viruses, like in the previous surveys, continue to be the single largest source of breach, affecting 68% of the respondents, even though relatively newer forms of attack, such as phishing, pharming and botnets, are on the rise.

[1] Current Year @ : CERT-In – FICCI – PwC Information Systems Security Survey, 2007-08 titled *From Strength to Strength*.
Previous Survey* : CII – PwC Information Systems Security Survey, 2004.
Global+ : The Global State of Information Security 2007, Study conducted by CIO magazine, CSO magazine and PwC.

Top 10 recommendations

- View security as an enterprise-wide strategic imperative and not as a cost-centre.
- Perform risk assessment on a regular basis to ensure alignment of policies and practices with the ever-changing business environment.
- Integrate security responsibilities as part of job definitions.
- Define Key Performance Indicators (KPIs) for information security and measure its effectiveness on an ongoing basis.
- Develop an enterprise-wide Business Continuity Plan and continuously test it.
- Conduct security assessment of third parties handling critical information.
- Give more emphasis on incident management and incident reporting. Have a close relationship with CERT-In.
- Identify and adhere to relevant regulatory and compliance requirements.
- Market information security to make it visible to stakeholders.
- Proactively monitor security compliance.

- A major initiative taken by the Government of India was the setting up of CERT-In to act as the nodal agency for information security. It is disappointing to note that many organisations are not even aware of CERT-In. More than 53% of the respondents did not have any form of interaction with CERT-In.

- Lack of dedicated resources and adequate training are identified as the primary barriers to strong information security. Universities and colleges will need to come up with specialised courses to develop skilled information security professionals equipped with the necessary knowledge and knowhow to address security related issues.

- The financial services sector has traditionally been at the top in terms of having security that is more effective. However, in this survey, the ITeS sector has gained the leadership position.

In today’s inter-networked business environment, any static approach to security is inadequate. Good security is a dynamic process, fully integrated with other business processes. Confronting a host of vulnerabilities makes it imperative that comprehensive, end-to-end security solutions are implemented and reviewed periodically.

The primary benefit of such an integrated approach is that it addresses the dual purpose of protection and enablement, thereby creating a way to improve security while simultaneously managing, the people, processes and technologies of an enterprise.

P. V. Krishnan

Sivarama Krishnan
Executive Director
PricewaterhouseCoopers, India

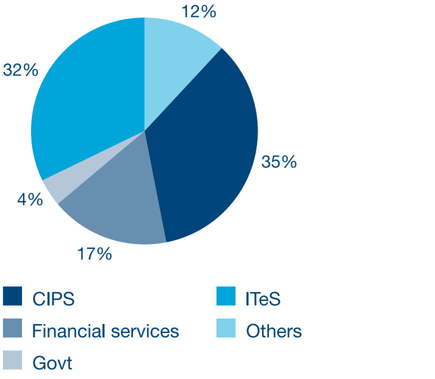
01

Methodology and respondents' profile

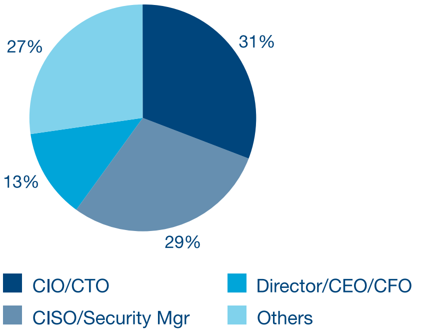
The Information Systems Security Survey 2007-08 titled *From Strength to Strength*, conducted by CERT-In, FICCI and PwC, is a detailed assessment of the status of and trends in information security practices followed by enterprises in India. This is the fourth such survey carried out exclusively for the Indian industry.

The results of this year's survey have been benchmarked with the Information Systems Security Survey 2004 and with the 'The Global State of Information Security 2007' study conducted by CIO magazine, CSO magazine and PricewaterhouseCoopers.

Respondent organisation profile – industry



Respondent profile



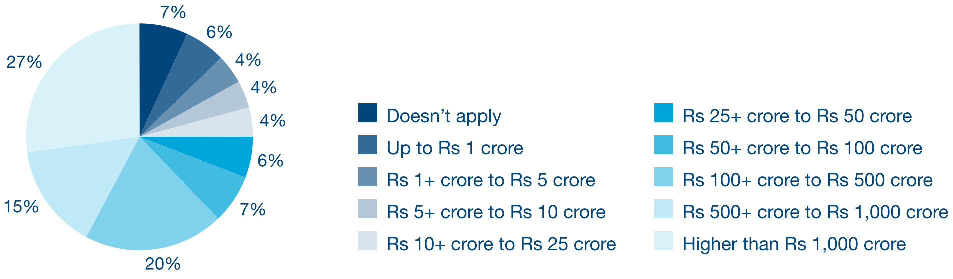
The survey was conducted using a structured questionnaire, which was administered through mailers and online. More than 140 organisations from a broad range of industries took part in the survey. In order to avoid biased responses, it was ensured that the respondents represented the senior management of their respective organisations.

The survey results have been benchmarked with the Previous Survey* and the Global+. One must, however, keep in mind that the respondents' profile varies across these surveys, which might have some influence on benchmarking of the results.

Some facts on the participating organisations are as follows:

- The respondents to this survey represent a wide variety of organisations, spread across various industry verticals. The industry verticals have been grouped as CIPS (Consumer, Industrial Products and Services), FS (Financial Services), ITeS (IT enabled Services) and others.
- The maximum responses have been from the CIPS segment, followed by the ITeS sector.
- Nearly 90% of the organisations have a strength of over 100 employees' while 50% of the organisations have more than 1,000 employees.
- Around 42% of the organisations have a gross annual turnover exceeding Rs 500 crore.
- Unlike previous surveys, India's public sector is fairly represented in this survey. It demonstrates the fact that government and public sector undertakings are also gearing up towards securing their information assets.
- Around 73% of the respondents either represent senior management (CEO, CIO, CTO, CFO and Director) or specialised information security staff (CISO, CSO, Security Manager, etc).

Respondent organisation profile by revenue



02

Prioritising security: on the road ahead

Given the environment in which we live, security is very high in the priority list of most organisations. Considering that data and information flow is at the heart of almost every core business activity, business leaders are today taking a hard look at the associated risks and developing risk mitigation strategies.

No longer is security merely a line item in the overheads budget, nor is it a technical issue easily addressed by an off-the-shelf technology product. Over the last few years, it has become an important item in corporate agenda and is a strategic initiative that affects business objectives, performance and accountability to stakeholders.

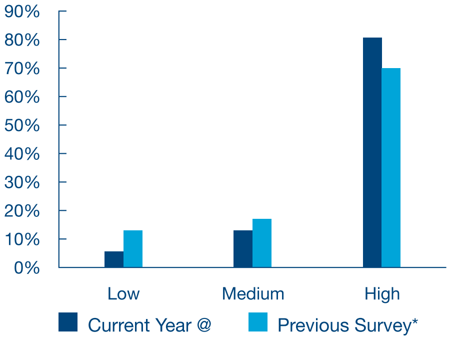
With increased awareness of the business value of data and significant increase in automation of business processes, organisations today are more sensitive about the confidentiality, integrity and availability requirements of their data. There is a marked improvement across all industry sectors in terms of according high priority to security.

All respondents indicated that they hold business critical information in the electronic form. More than 65% of the respondents identified electronic information as highly confidential. Hence, it is not surprising to find that more than 81% of the respondents identified information security priority as high in comparison to 70% in Previous Survey*.

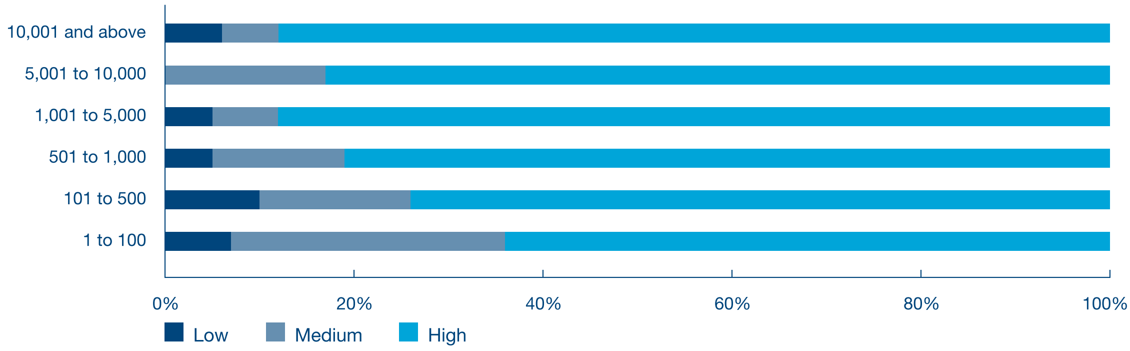
Only 6% of the organisations accorded low priority to information security this time unlike 13% in Previous Survey*. This clearly demonstrates that organisations are increasingly becoming aware of the business value of data and the need to protect it.

Of the organisations having more than 10,000 employees, 89% accorded high priority to information security as compared to 64% of small organisations employing less than 100 employees, thus demonstrating that the larger the organisation, the greater is the security need. Since larger organisations extensively leverage available technology, inter-networking and telecommunications networking for enhanced business productivity, they need to accord high priority to information security.

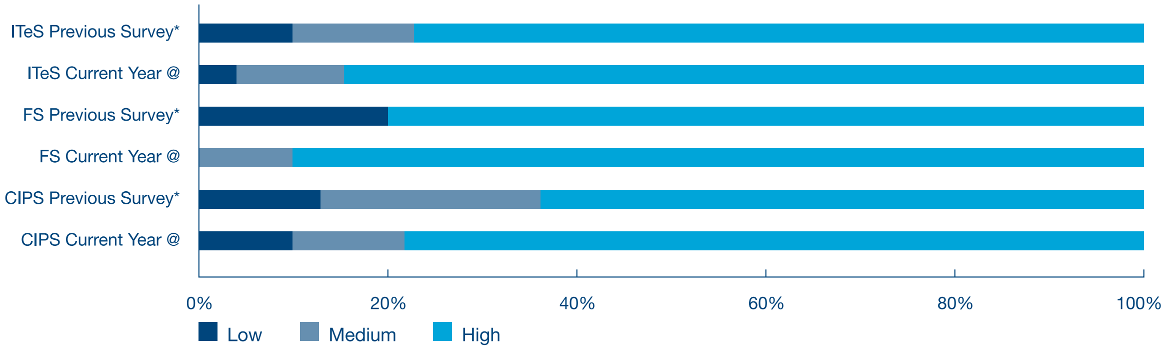
Information security priority

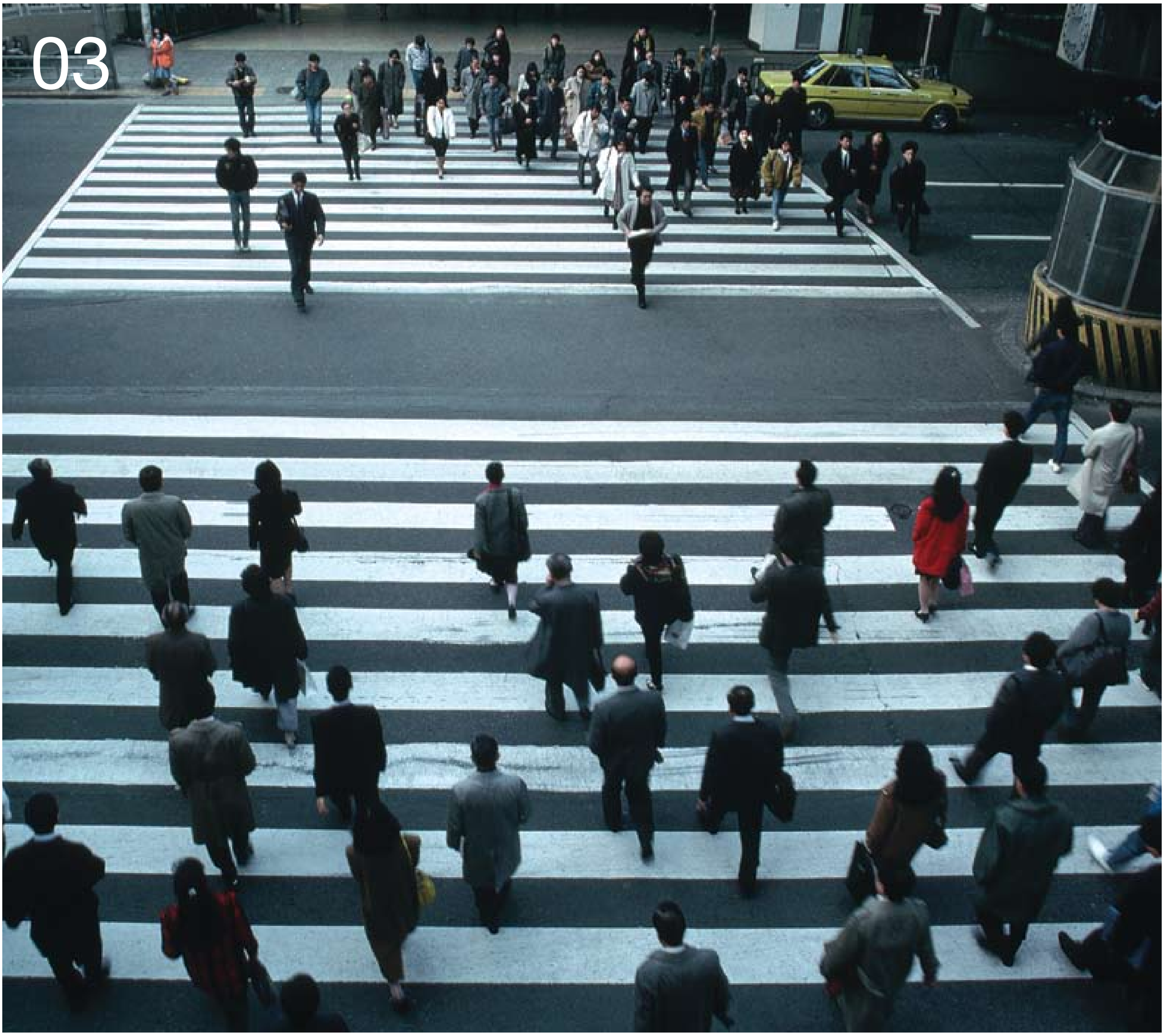


Information security priority – by organisation size



Information security priority – industry-wise





Implementing safeguards: securing ourselves along the way

To effectively secure their IT infrastructure from malicious users and attackers, and facilitate closer working relationships with suppliers, customers and other business partners, an organisation requires committed people participation, implementation of best practice processes and investments in the latest appropriate technologies.

Existing controls

People

Traditionally, organisations tend to rely on technological controls for information security. However, even the strongest technical security can be breached if users are not aware of security basics. Employees must be made aware of security measures within an organisation and the importance that the management attaches to them.

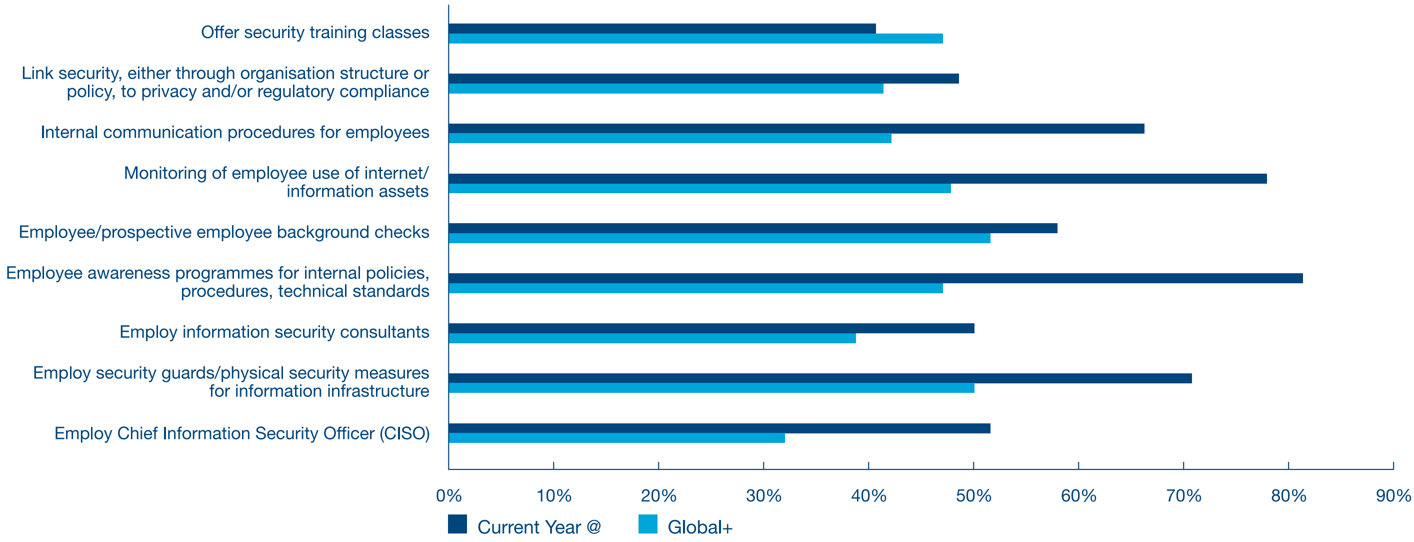
The Previous Survey* highlighted a significant gap in the implementation of ‘people’ related controls. The scenario appears to have improved since, as in this survey, organisations identified enhancement of security awareness as a top strategic priority for the coming year.

Today, more than 80% of the organisations focus on employee awareness programmes as compared to 47% as per Global+. Monitoring of employee use of the internet and information use is the latest trend, with more than 78% of the organisations focusing on this, as compared to the Global+ figure of 48%.

As had been predicted in Previous Survey*, India Inc. is increasingly hiring specialised security staff. Thus, 51% of the organisations in India, as against 32% as per Global+, have employed Chief Information Security Officers. While this trend started with companies in the ITeS and financial sectors, organisations across industry verticals have now adopted this practice.

A string of security scandals in the BPO industry might have helped Indian corporates realise the importance of the ‘people’ element in information security. Indian organisations, in general, are tightening security procedures to a point that goes far beyond security controls practised in the West, e.g. BPO workers (agents) are required to surrender everything that could facilitate data compromise, like mobile phones, PDAs, pens and notebooks. Similarly, all respondents from the ITeS segment indicated that they verify the background of prospective employees.

Existing controls – people



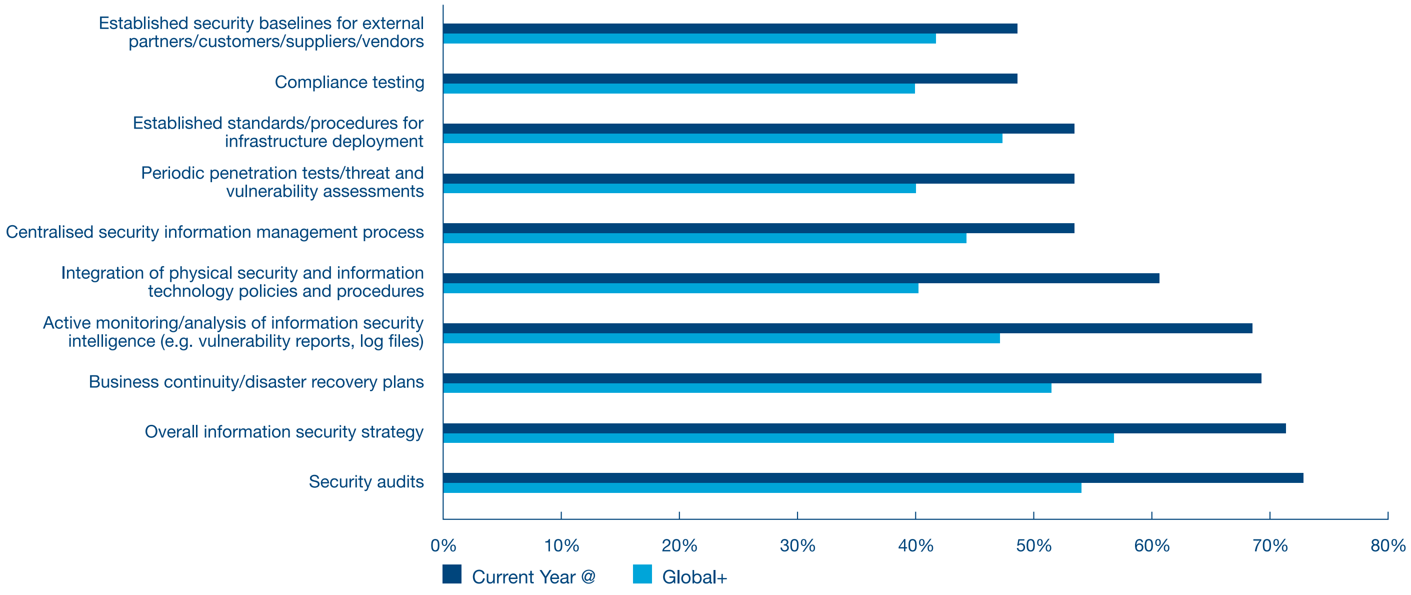
Process

Here too, India Inc. has moved faster as compared to their counterparts around the world. About 73% of the organisations, as compared to 54% globally, have established processes for conducting periodic security audits. Similarly, about 71% of the Indian organisations, as against 57% globally, have an overall information security strategy in place.

Active monitoring/analysis of information security intelligence and business continuity/disaster recovery plans are also areas of focus for most organisations.

India Inc., however, lags behind in outsourcing of security, as compared to Global+. Outsourcing of security is still a nascent concept in India and its activities are typically managed internally.

Top 10 existing controls – process



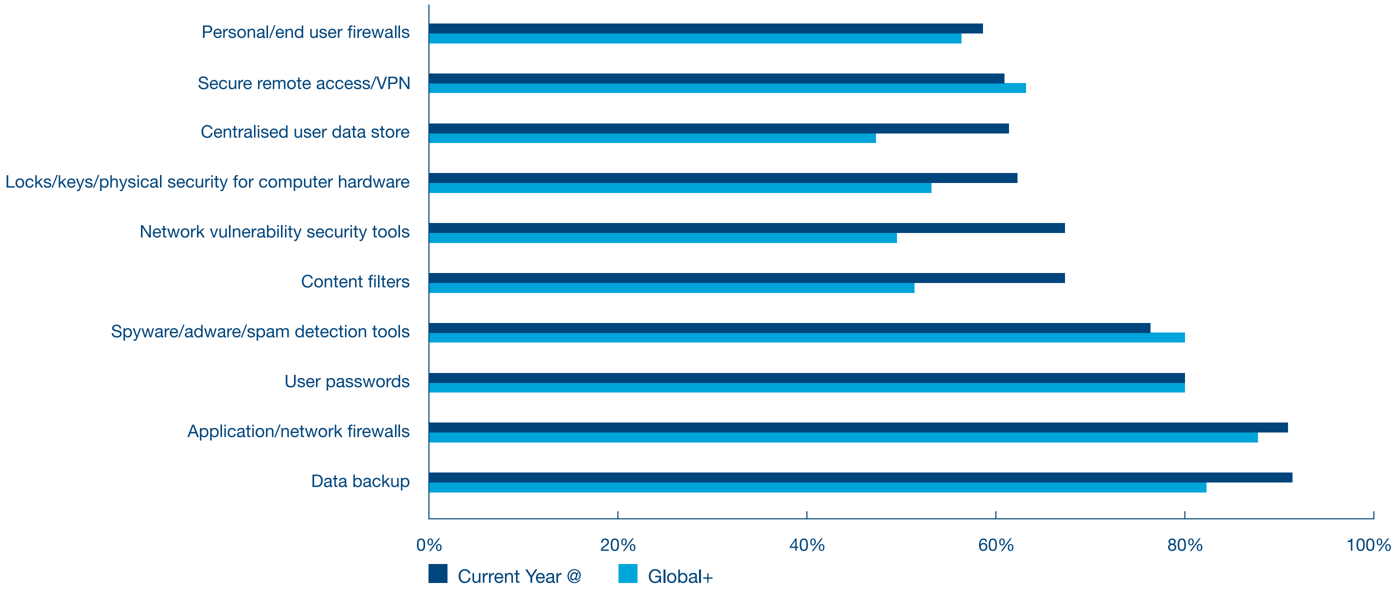
Technology

In terms of deploying technology safeguards, organisations in India are again ahead of their peers overseas. As more and more organisations are focusing on their business continuity and disaster recovery plans, usage of data backup solutions has gained prominence. More than 91% of the respondents indicated having data backup mechanisms in place, as against 82% as per Global+.

For many businesses, the traditional boundary of their network has been their internet gateway. In the Previous Survey*, it was observed that organisations focused on defending the periphery, and did less to secure computers within the network. Firewalls continue to be the dominant mode of securing and monitoring boundaries, with more than 91% of the organisations using application/network firewalls, as compared to 75% in the Previous Survey*.

It is very encouraging to note that the use of intrusion detection and prevention systems is on the rise. In our 2002-03 survey, only 21% of the organisations had deployed intrusion detection systems. In the Previous Survey*, this figure increased significantly to 58%. As per this survey results, more than 54% of the respondents now use intrusion detection tools while 44% use intrusion prevention tools, as against the Global+ figures of 59% and 52%, respectively. The proliferation of intrusion detection and intrusion prevention tools signifies the gradual progress of focus on information security in India from adolescence to a fair bit of maturity.

Top 10 existing controls – technology



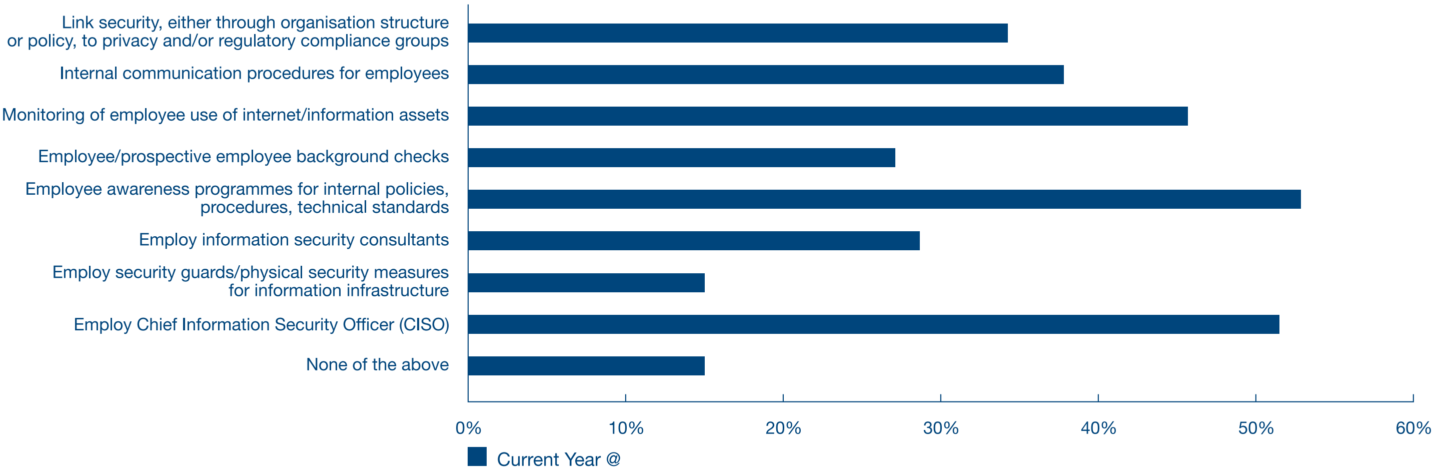
Future initiatives

People

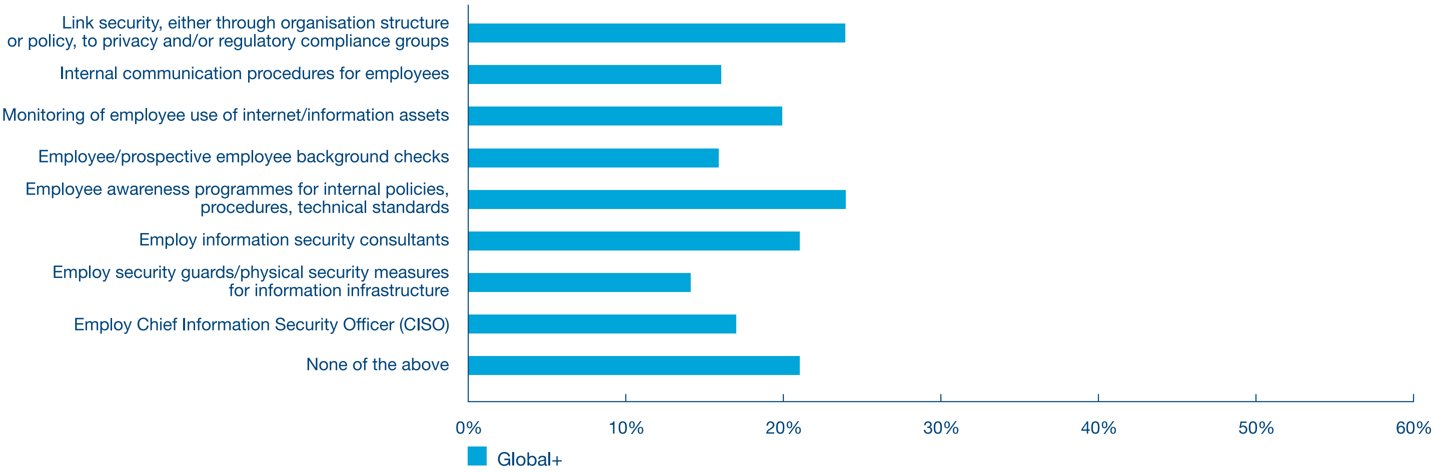
About 53% of the respondents indicated that they want to focus on employee awareness programmes for internal policies, procedures and technical standards, while 46% indicated that they intend to monitor employee use of internet and information assets. These are twice as compared to Global+ figures of 24% and 20%, respectively.

Only 27% of the respondents in India intend to conduct background checks. Due to the high employee attrition rates in India and the prominence of the service industries, we predict that conducting background checks will become more prevalent in the days to come.

People initiatives – India



People initiatives – Global+

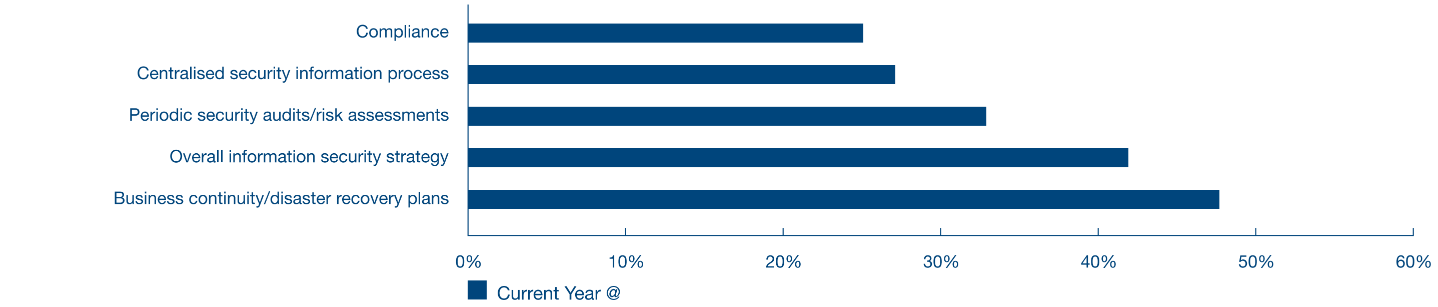


Process

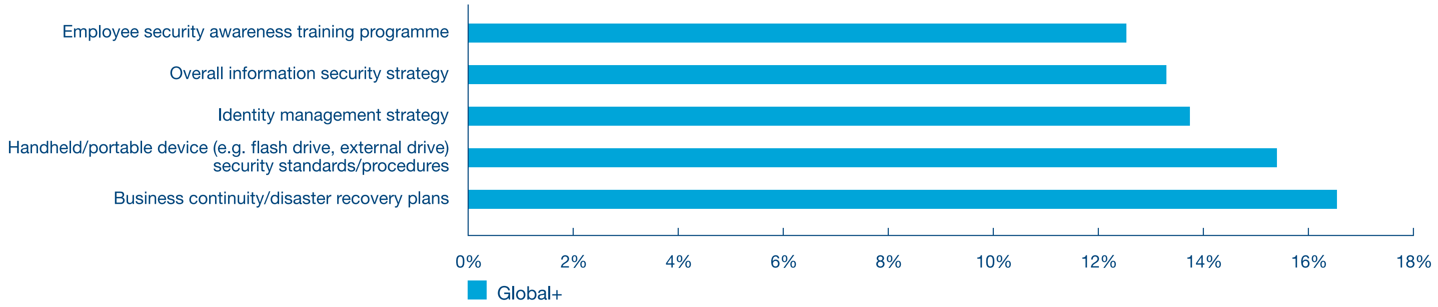
About 42% of the respondents said they want to develop an overall information security strategy while 48% wanted to prepare business continuity/disaster recovery plans. Again, 63% of the organisations in the FS segment and about 50% in the CIPS sector indicated that developing plans for business continuity/disaster recovery will be a strategic initiative for them in the current year.

It is interesting to note that security standards/procedures for handheld and portable devices is one of the top process initiatives as per Global+. However, this does not find a place amongst the top process initiatives of Indian organisations.

Top 5 process initiatives – India



Top 5 process initiatives – Global+

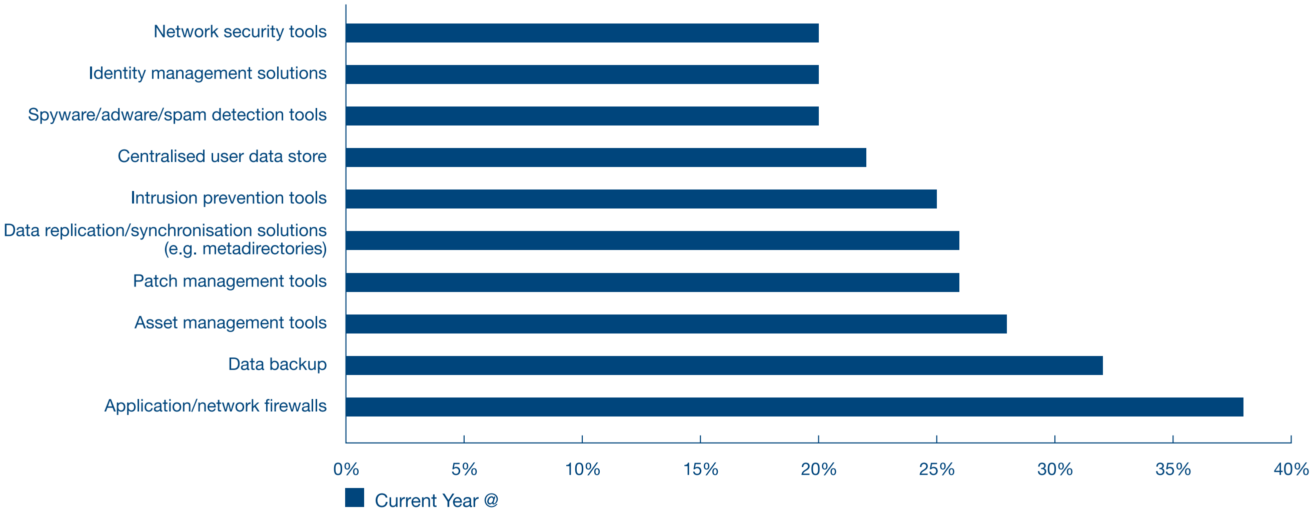


Technology

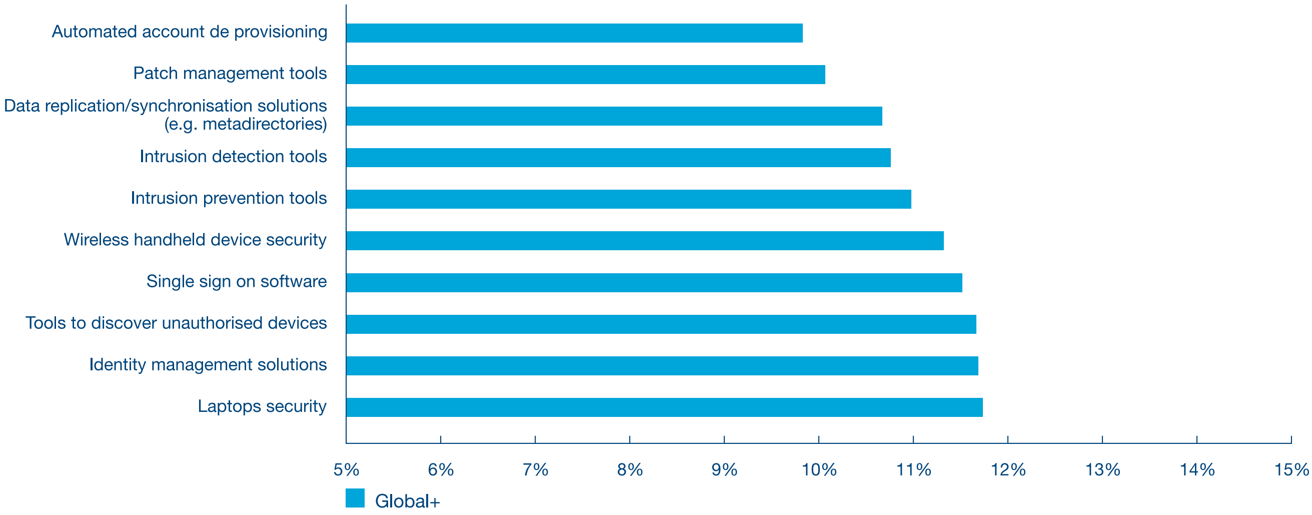
A large number of respondents, like in the previous survey, expressed interest in deploying application/network firewalls and personal/end-user firewalls. It is interesting to note that organisations are no longer only bothered with perimeter security. The security of desktops, the source of a number of security breaches/lapses, has also assumed importance amongst Indian organisations. More than 25% of the respondents expressed their intention to deploy asset management and patch management solutions.

Securing mobile devices, such as laptops are also not in the priority list of Indian organisations, while it is one of the top technology initiatives as per Global+.

Top 10 technology initiatives – India



Top 10 technology initiatives – Global+



Security policies: following the roadmap

Security policies and procedures form the backbone of an organisation's security framework. A formal security policy document is critical for establishing and communicating the basic security standards and requirements in an organisation.

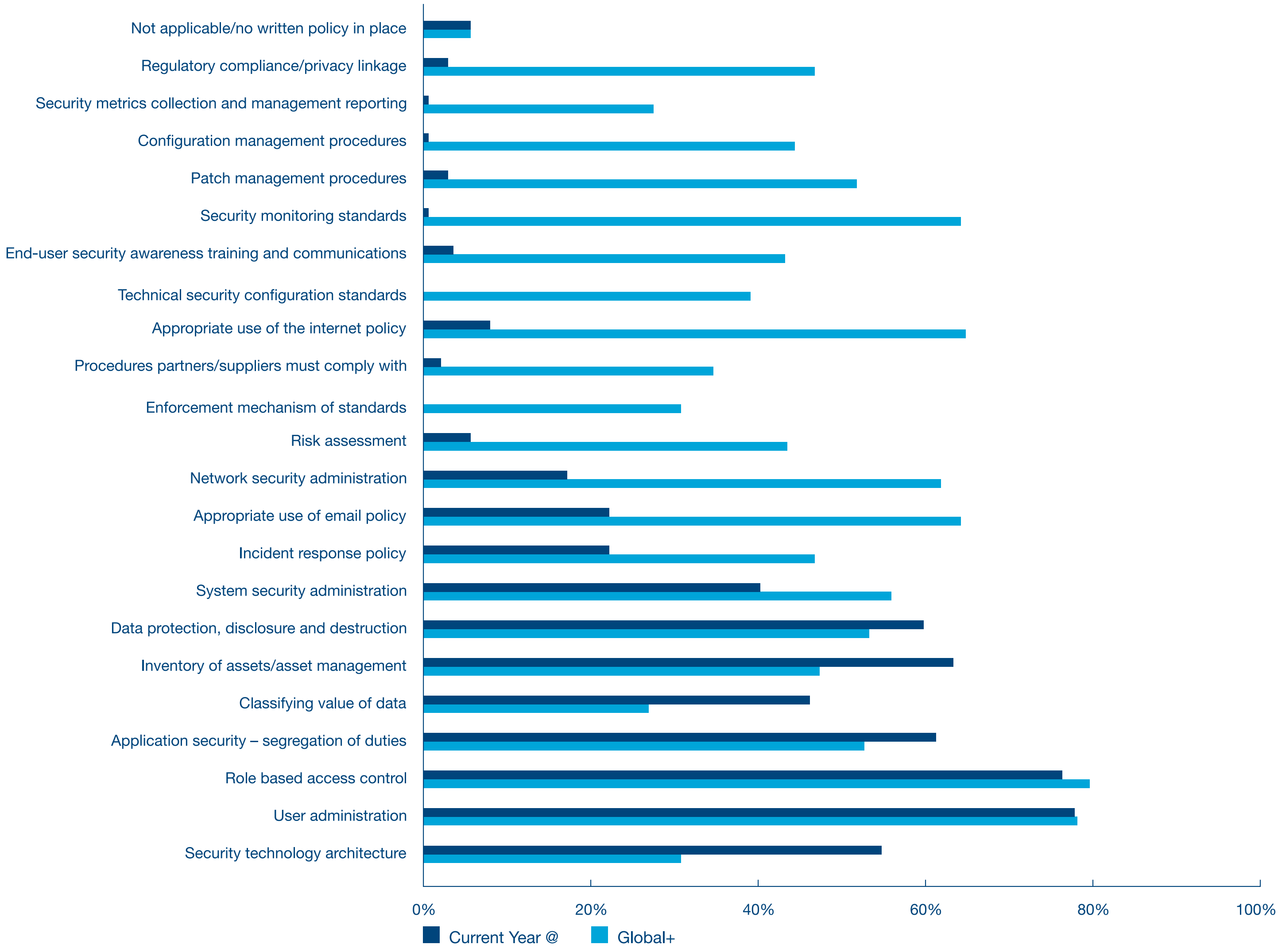
Security Policies

It is obvious that without rules, responsibilities and formal procedures, an information security framework can never be effective. It is the first step towards aligning information technology with business objectives.

In the Previous Survey*, 39% of the organisations either did not have or operated without an information security policy. This was almost four times greater than the then global average of 10%.

As predicted in the Previous Survey*, there is a significant reduction in the number of such organisations and now only 6% of the surveyed respondents do not have a written security policy, something which is similar to the Global+ average. However, it is important to note that key security policy and procedure elements, e.g., linkages with privacy/regulatory compliance requirements, configuration management procedures, etc., have not been defined by most of the organisations.

Elements of security policy

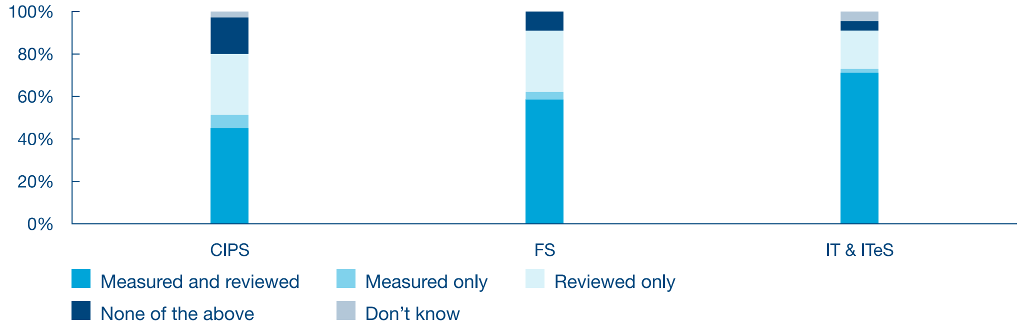


Effectiveness of security policy

Security policies and procedures need to be regularly reviewed and updated in order for them to remain effective and able to address the changing business requirements. More than 10% of the respondents do not review and measure the effectiveness of their security policy as against 33% as per Global+.

Further, 54% of the respondents stated that they have measured as well as reviewed the same during the past year, as against the Global+ average of 48%. The ITeS vertical is the leader amongst industry segments when it comes to having reviewed and updated security policies over the past one year, with over 71% of them giving a positive response. At the same time, 16% of the organisations from CIPS and 8% from the FS segments do not review or measure the effectiveness of their policies and procedures periodically.

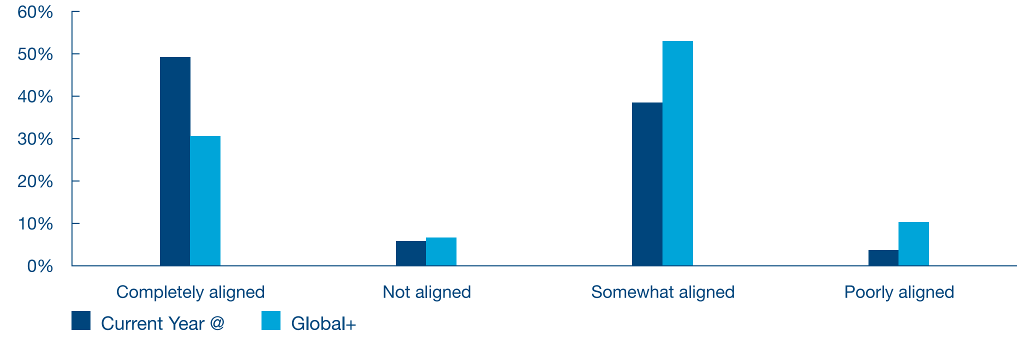
Measurement and review of information security policies



Alignment of security policy with business objective

While 49% of the organisations believe that their security policies are completely aligned with their business objectives (30% globally), 39% believed that they are somewhat aligned (53% globally). Only 6% organisations in India thought that information security policies are not aligned with business objectives, which is same as the Global+ figure.

Alignment of security policies with business objectives



Business Continuity (BCP)/Disaster Recovery Plans (DRP)

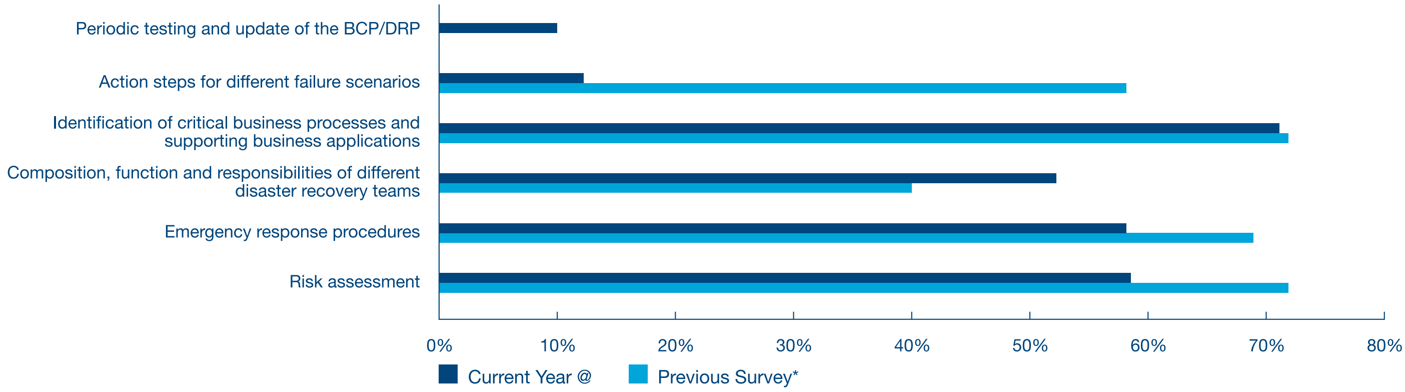
Almost 83% of the respondents have a business continuity/disaster recovery plan. However, more than 90% of the organisations do not conduct regular testing of their plans. In the event of a service disruption or disaster, these organisations might not be able to effectively resume operations.

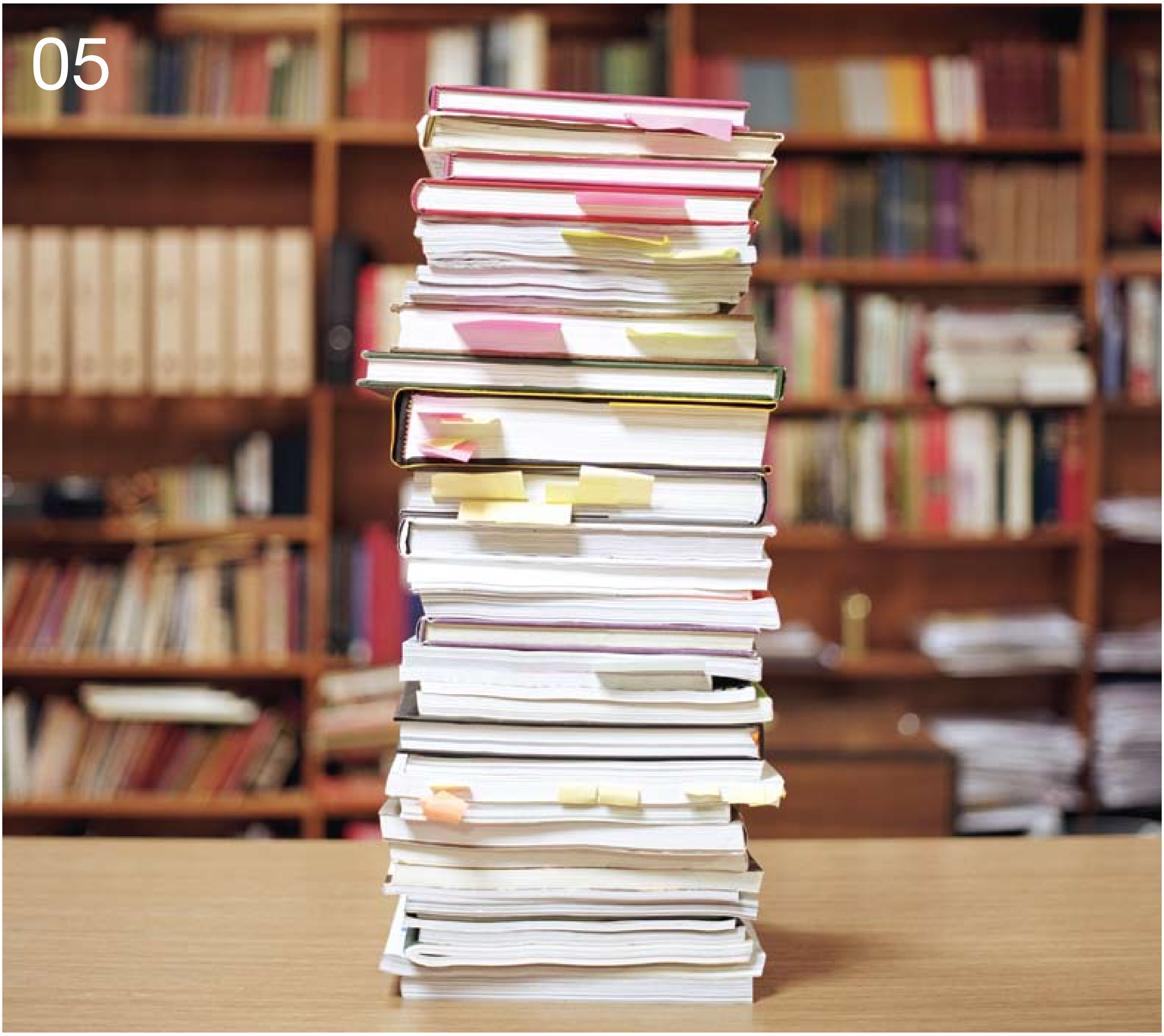
Similarly, risk assessment, another critical component of building an effective disaster recovery plan, has been conducted by only 59% of the respondents. Only 12% of the organisations have taken action steps for different DR scenarios as compared to 58% in the Previous Survey*.

About 71% of the organisations having DCP/DR plans identified critical business processes and applications as part of their plan. However, the effectiveness of these plans is questionable, as action steps for various failure scenarios have not been defined by majority of them.

Major events, such as the 1993 Mumbai blasts (mainly the explosion at BSE), Bhuj earthquake, 2005 Mumbai and Chennai flooding, 7/11 Mumbai blasts and the Asian tsunami, immediately come to mind when one thinks of a disaster. In the light of these incidents, organisations need to re-look at their BCP/DRP strategies in a holistic manner to ensure effective recovery in the event of a major disaster.

Which of the following form part of your BCP/DRP?





05

Compliance: abiding by the rules

Organisations today are facing increased compliance obligations and are exposed to reputation risks. The risks associated with non-compliance are increasing day by day.

Indian organisations are gearing up compliance with security/privacy laws that directly apply to them (like Reserve Bank of India directives, Basel II, HIPAA, GLBA, EU Data Privacy directives, UK Data Protection Act, etc). The RBI has asked banks to move in the direction of implementing the Basel II norms. It has specified that the migration to Basel II will be effective from March 31, 2008, for banks with substantial overseas operations and by March 31, 2009, for others. Our survey results indicate that more than 60% of banks are yet to comply with Basel II norms.

Indian organisations are increasingly becoming aware of the local regulatory requirements in comparison to Previous Survey*; however, a lot remains to be done in order to comply with these norms.

It augurs well to note that ISO 27001 is still the most coveted standard amongst all Indian industry segments (not only the ITeS sector) with more than 60% of the respondents intending to achieve compliance. A significant 32% indicated that they are already in compliance with ISO 27001. India, therefore, looks strong to retain its position to be amongst the top two countries with the maximum number of ISO 27001 certifications.

While a large number of organisations, across industries, are looking for adherence to CERT-In guidelines and meeting the IT Act 2000 requirements, the compliance figures suggest a need for greater attention in this regard.

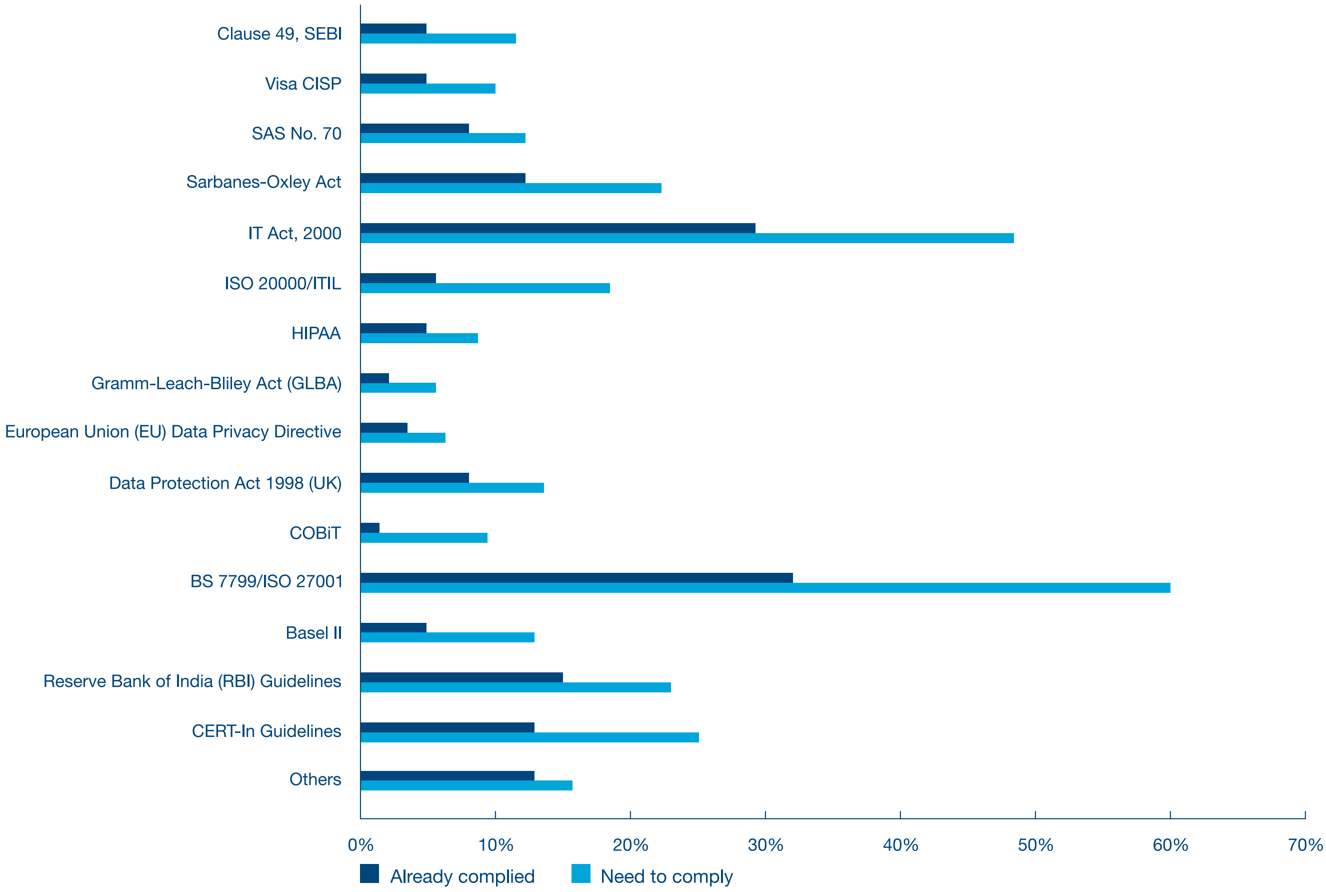
A number of organisations, primarily involved in offshore software development, are now focusing on complying with ISO 20000 and Information Technology Infrastructure Library (ITIL) practices. These may be due to increased attention on IT service delivery and management in an outsourcing environment. Around 16% of the ITeS organisations are moving toward ISO 20000/ITIL compliance.

Sarbanes-Oxley and SEBI Clause 49 Compliance has been much talked about in recent times. More than 39% of the organisations have deployed or plan to deploy an enterprise-wide security strategy as a direct or indirect result of these regulations. Within this group, more than 35% have adopted or have decided to adopt a security standard, e.g. ISO 27001, ITIL or COBIT.

Today, for CIOs of India Inc., the challenge lies not only in achieving compliance but also in sustaining them with limited IT resources, skill sets and budgets. They also have the daunting task of ensuring that the compliance efforts evolve from being ad-hoc IT projects to specific, cost-effective, efficient, robust and sustainable processes that can be applied across various compliance requirements.

Compliance is often identified as a major driver of information security. A large number of organisations, specifically in the ITeS and FS sector, justify their security investments for complying with legal and regulatory requirements. Organisations in India must realise that there are significant advantages in achieving compliance. It can result in more cost-effective and efficient processes, and ensure more top management support and commitment towards information security.

Compliance status



06

Security breaches: enroute to a risk-free environment

Security breaches are on the rise the world over because of the growth of distributed computing environments, web services, grid computing, shared storage systems and peer-to-peer applications, which make it easier to launch large-scale remote and anonymous attacks. These technology trends, along with mobile computing, add complexity to and enhance the problem of security management. Consequently, a comprehensive security strategy, engineering, operations and response become even more essential to prevent security incidents and breaches.

Statistically, India seems to have fared better in preventing security related incidents as compared to those globally.

In the last one year, only 17% of the respondents were unaware of any security incidents and breaches as against a Global+ benchmark of 40%.

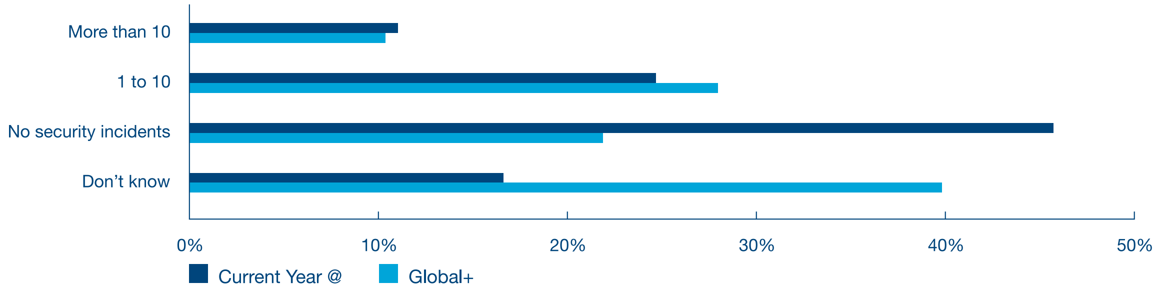
It is encouraging to note that 46% of the Indian organisations reported that there have not been any security incidents in the last one year against 22% as per Global+ and 17% as per the Previous Survey*.

However, this should not be a reason for complacency, as organisations reporting no negative security incidents may not have adequate processes or awareness for detecting or reporting incidents.

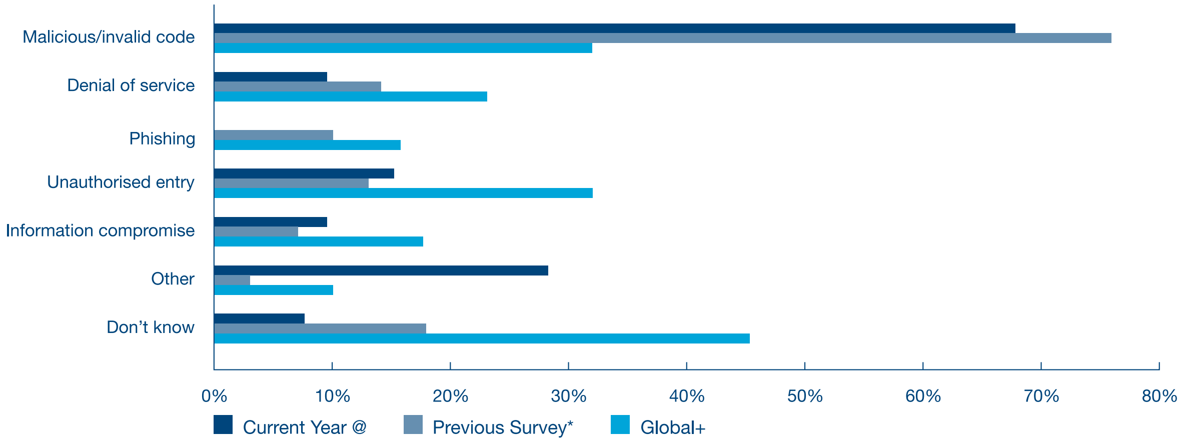
A closer look at the kind of incidents reported in the last year indicates that malicious code, i.e., worms or viruses, account for 68% of the cases, which is slightly lower than 75%, as reported in the Previous Survey*.

The more publicised form of security breaches, consisting of denial of service and unauthorised entry, seem to be much lower than the Global+ averages.

Number of negative security incidents in the past 12 months



Nature of events



Impact of incidents

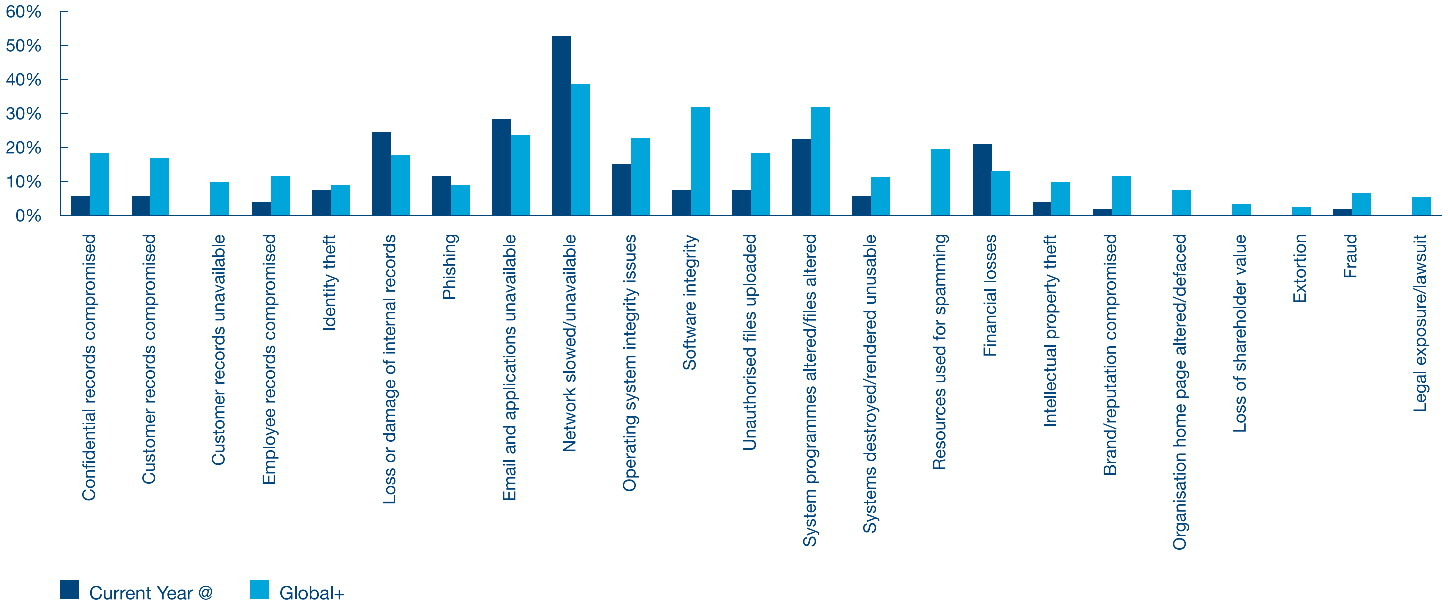
Most organisations felt that the impact of negative security events was largely on network performance or availability. The second most affected component was the email system. Compromise of confidential records and customer records had occurred only in 6% of the organisations, which is less than half of the Global+ average of 18% and 17%, respectively.

Financial impact due to security incidents has been reported by 21% of the organisations. Only 2% believe that their brand image was impacted due to the incidents.

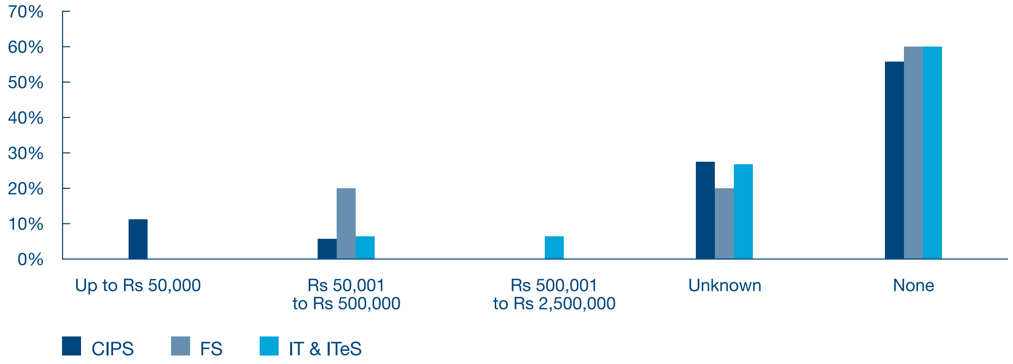
Of the many influences a security incident may have, system or network downtime affects a large number of organisations, as it directly impacts productivity. In India, 40% of the companies reported that they have not faced a downtime due to negative security incidents. More than 23% of the organisations reported a downtime of less than four hours. No organisation reported a downtime of more than 10 days.

Amongst the industry segments, CIPS and IT/ITeS sectors have been largely impacted due to loss of internal records. CIPS is the only sector to have reported compromise of employee records. Almost 10% of the organisations in the FS sector reported compromise of customer records. Phishing was reported to have affected all sectors, with the FS sector being the worst hit. This is similar to what was published in the CERT-In report, which stated that phishing incidents have increased multi-fold, primarily affecting the FS sector. The growing number of phishing attacks emphasises the paramount importance of promoting end-user awareness.

Impact of breaches



Financial losses as a result of negative security incident

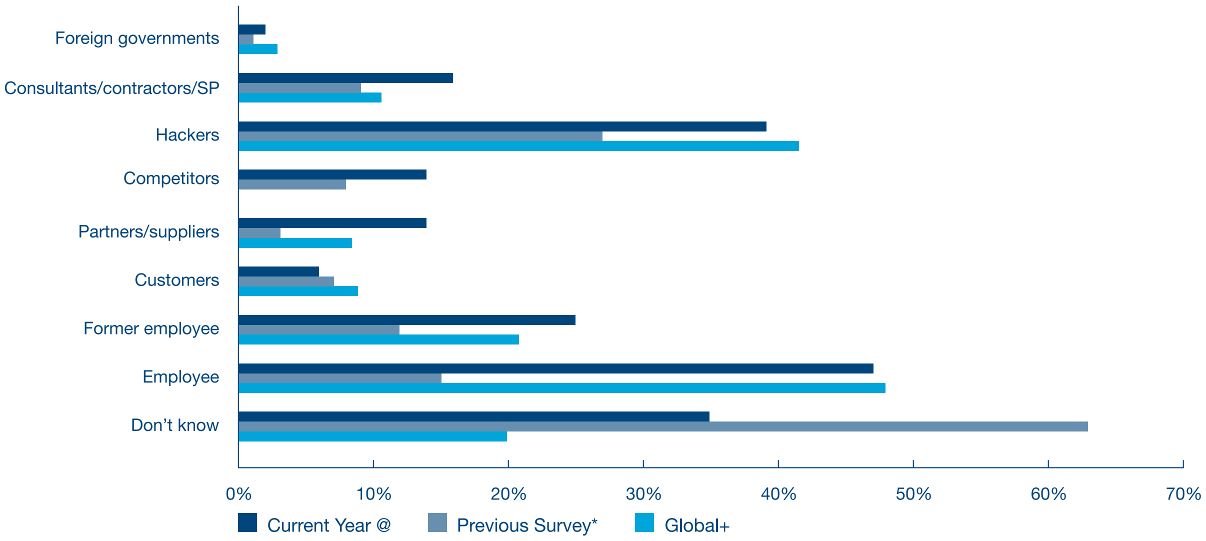


Source of attack

Email virus was reported as the most common source of security incidents, with 68% of the respondents attributing security incidents to email worms and viruses. Known operating system vulnerabilities can be eliminated by timely application of vendor patches. However, in India, as well as globally, exploitation of these vulnerabilities account for a large number of attacks. These were reported as the second most common method of attack by 23% respondents, not very far from the Global+ average of 16%. Abuse of account permissions remains an area of concern for most organisations, with 19% classifying it as a primary source of attack.

Sources of attacks are as important as their impact, if not more. Majority of the organisations believed that employees or former employees are a major source of security threat. Almost 47% of the organisations believe that the employees were responsible for security incidents and 25% attributed them to former employees. Only 39% companies attributed negative security events to external hackers. This again establishes the fact that more attacks are likely from within an organisation (employees and former employees) than from outside.

Security breach – who is the culprit?



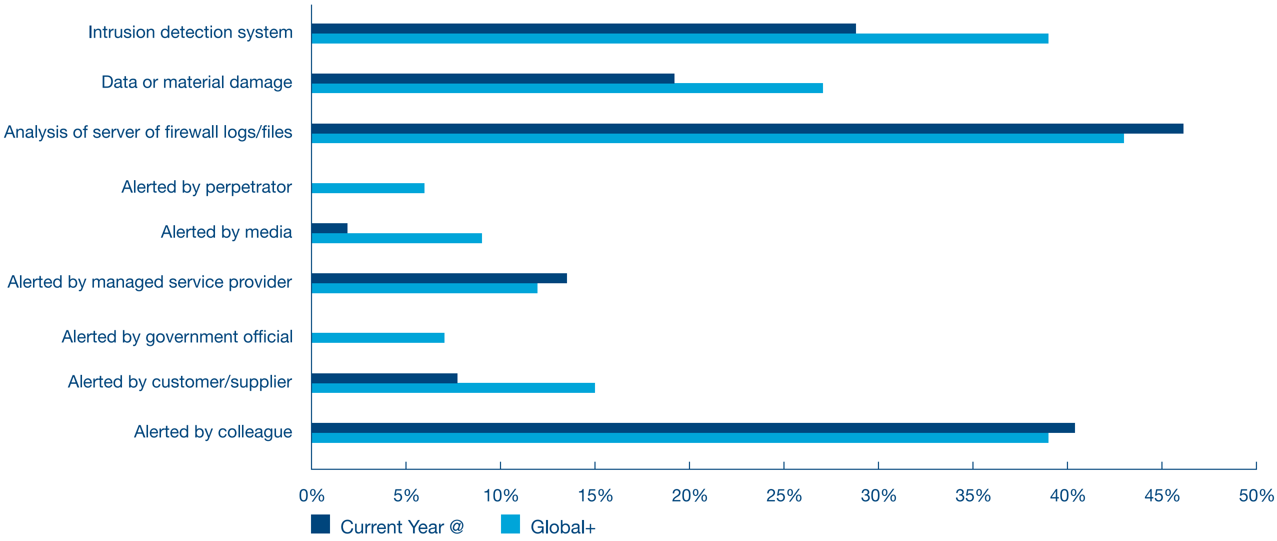
More than 35% of the organisations in India were not aware of the likely sources of attack. This indicates that in many cases, organisations were not able to track the source from whom or where the attack originated.

Corporate espionage has emerged as one of the leading threats, with 14% of the organisations attributing security incidents to competitors.

Incident information

Most organisations (46%) detected incidents from server or firewall logs. Incidents reported by colleagues or employees were the second-most common way of unearthing an incident. In contrast, automated tools, such as intrusion detection systems, came only third. This highlights the fact that security awareness plays an important role in not only preventing but also detecting security incidents.

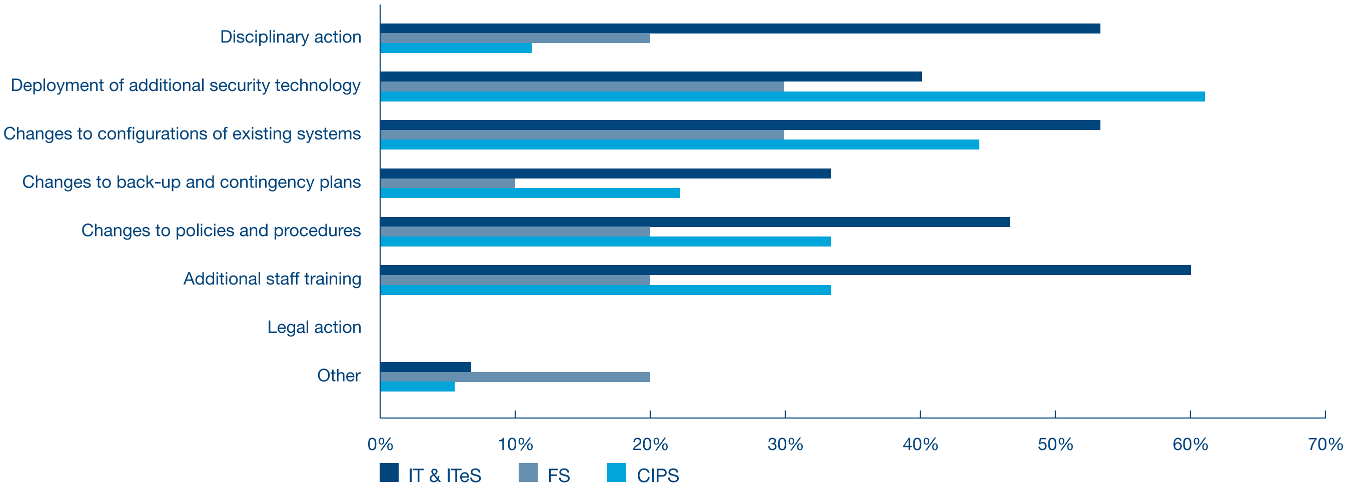
How were the breaches detected?



Post-incident activity

Interestingly, the survey reveals that only 22% of Indian organisations have documented an incident response policy. However, all organisations claimed to have taken action based on negative security events. Although no organisation reported taking any legal action, a large number of ITeS organisations (53%) have taken disciplinary action. Only 20% of FS and 11% of CIPS organisations have taken disciplinary action in response to negative security events. More than 60% of the companies in CIPS sector reported to have invested in security related technologies. All sectors reported training additional staff in response to security incidents, with the maximum number (60%) being from the ITeS sector.

After the event which of the following action was taken?



Changes to policies, procedures, configuration and contingency plans have been made by organisations across sectors. However, the response from the FS sector was the least in terms of measures that they have taken post such incidents, with only 10% having updated their backup and contingency plans.

None of the organisations informed their investors/shareholders of such incidents. In addition, none of the organisations sought guidance from CERT-In or from industry bodies such as FICCI or NASSCOM.

49% of the organisations had not reported/informed any other organisation or authorities about an incident. Nevertheless, 40% of the ITeS companies informed their business partners/vendor or suppliers of the security breaches, followed by 30% in FS and 22% in CIPS sectors. No FS organisation informed its customers about security incidents. However, 27% of ITeS organisations and 17% of CIPS organisations informed their customers of the security incident.

Only about 9% of the organisations informed law enforcement agencies. FS leads the industry sector in this regard, with 20% companies reporting incidents to the police or other law enforcement agencies, followed by 13% in the ITeS and 6% in the CIPS sector.

CERT-In was set up by the Ministry of Information Technology as a referral agency for responding to computer security incidents as and when they occur. CERT-In also helps organisations to proactively implement measures to reduce risks of computer security incidents. It was expected that Indian organisations would leverage CERT-In to report security incidents and seek advice on security from time to time. However, over 53% of the organisations have not engaged CERT-In in any manner and only 5% proactively contacted CERT-In. As many as 10% of the organisations have not even heard about CERT-In!

07

Security budgets: reaping the benefits

The security focus in an organisation is often measured by the size and growth of its information security budgets.

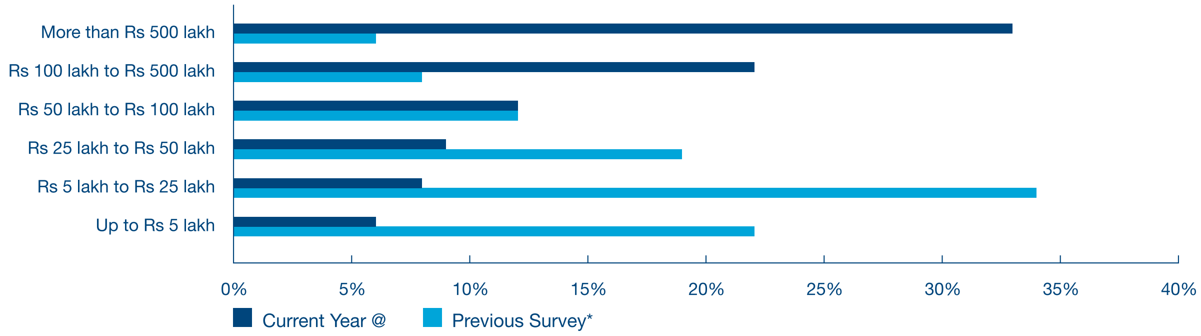
In line with its growing priority, organisations have started investing more on information security. The number of organisations, having low budgets (less than Rs 25 lakh) as per Current Year @ has been reduced as compared to Previous Survey*, whereas the number of organisations having high budgets (more than Rs 50 lakh) increased. Security spending increased during the year, as 33% spent more than Rs 500 lakh as compared to just 6% in Previous Survey*.

As expected, the FS sector, in general, has the highest budget for information security amongst industry segments.

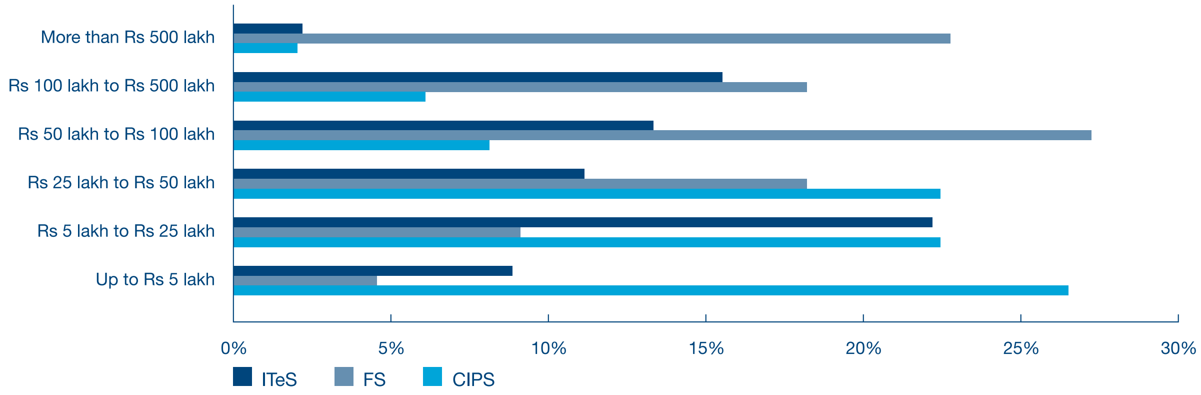
Approximately 71% respondents indicated that their information security budgets are likely to increase in the coming year, with more than 47% saying that the rate of increase will be in double digits!

This clearly portrays that information security is gaining prominence and such initiatives are being supported by increased allocations.

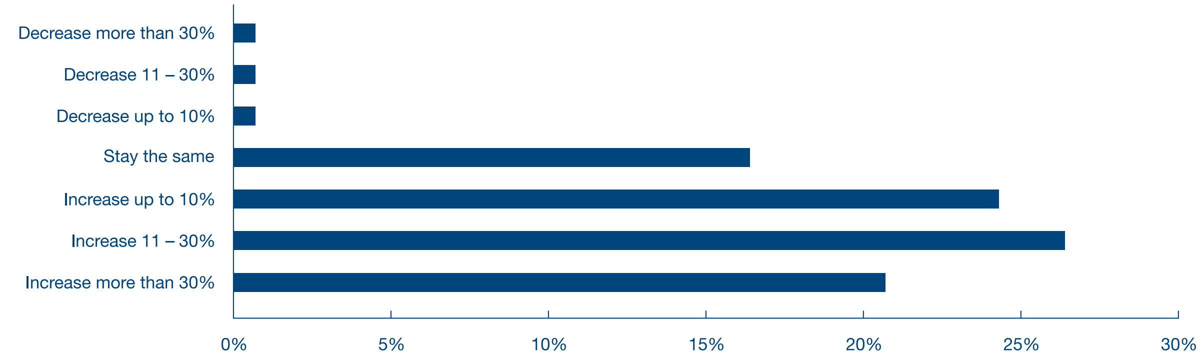
Annual information security budget



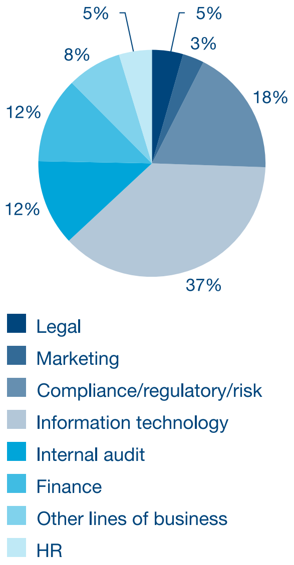
Annual information security budget – industry



Security spending in current year as compared to previous year



Source of IS funds besides IS budget

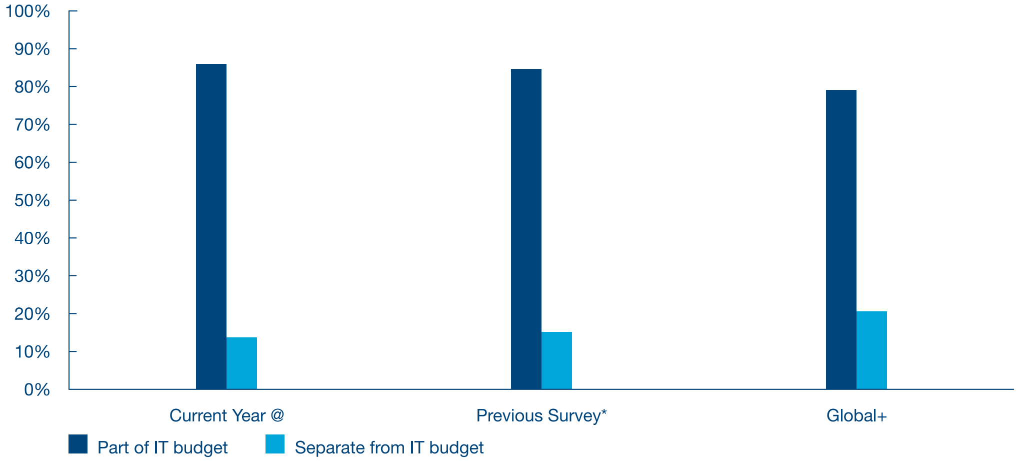


As expected, IT remains the primary source of information security budgets. However, a significant portion of the budget has started flowing from internal audit and compliance/regulatory heads. This demonstrates the increasing importance of complying with regulatory standards, such as Sarbanes Oxley, SAS 70, Basel II, HIPAA, GLBA, Data Privacy Acts, among others. It is also worthwhile to mention that more than 80% of the organisations said that their information security budget was within the IT budget. The trend is similar to Previous Survey* results.

As indicated by the respondents, information security budget, on an average, is around 13% of the overall IT budget. This is more or less in line with the Global+ spends. In case of the ITeS sector, this spend is the highest, with an average of 17%, which clearly indicates that safeguarding customer data is a key business imperative.

The external and internal drivers in terms of regulatory compliance, market requirements, and corporate governance best practices have driven the increasing investment towards information security.

Information security budget

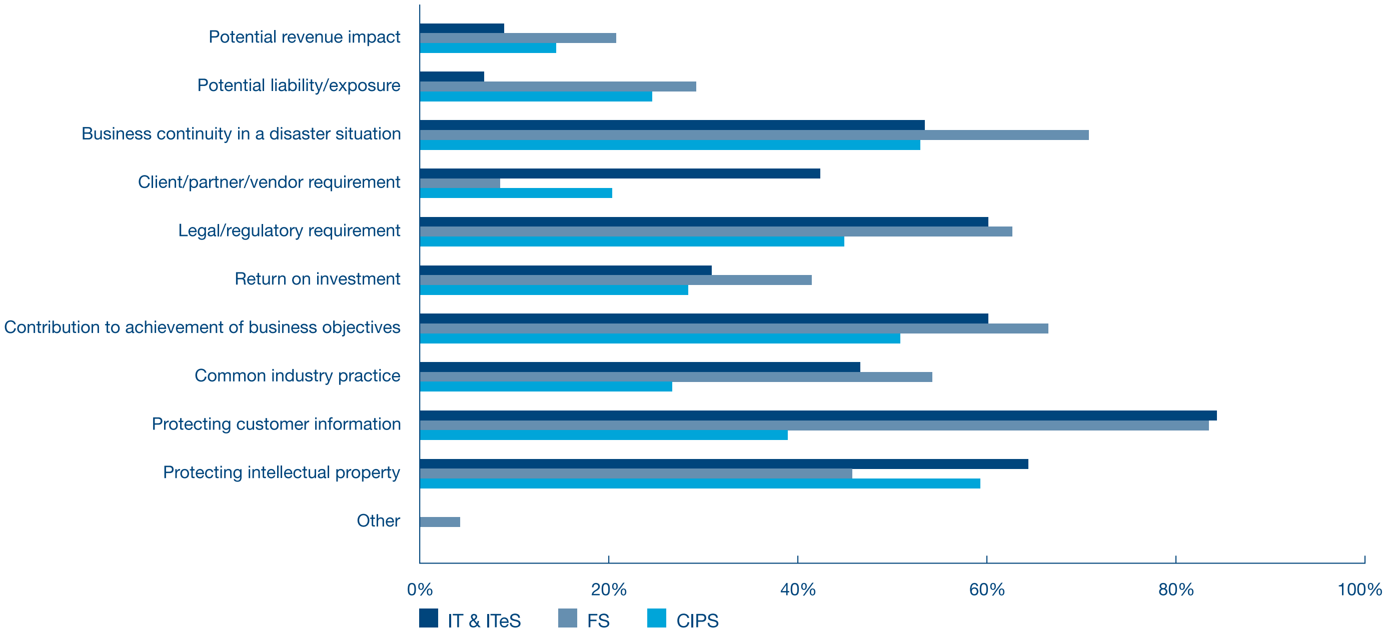


Drivers for security investment

Protecting customer information has emerged as the most important driver for spending money on IT security in an organisation. More than 83% of FS and ITeS organisations justify their security investments on grounds of protecting customer information. Against this, protecting intellectual property is the major justification for security investments in the CIPS sector.

For more than 60% of the organisations in the ITeS and FS sectors, complying with legal and regulatory requirements was another major reason for increased investments in information security. Contribution towards achievement of business objectives and contingency planning are also two very common factors for increased security investments.

How are security investments justified?



Information security should be seen as an investment rather than an expense. Surprisingly, only 42% organisations in the FS sector and 31% and 29% in ITeS and CIPS sectors, respectively, compute the payback on their IT security investments.

Alignment with business objective

Only 26% of the organisations feel that their spending is completely aligned with their business objectives while 50% believe that it is somewhat aligned. 7% organisations believe that the security spending is poorly aligned and another 9% feel that the security spending is not at all aligned with their business objectives.

Organisations in India have started investing in relatively new technologies and solutions, such as patch management, managed security services and identity management. However, it is too soon to assess whether such investments have helped them accomplish their stated business objectives.

08

Security barriers: removing the obstacles

An organisation faces a number of barriers while practising and promoting information security. It is very important for us to understand these barriers so that organisations can take constructive steps to overcome them.

In our previous surveys, in India, capital expenditure restrictions and limited budgets were considered as the most important barriers to information security enhancement. Globally too, most organisations believed that limited allocations was the biggest barrier to implementing good security measures.

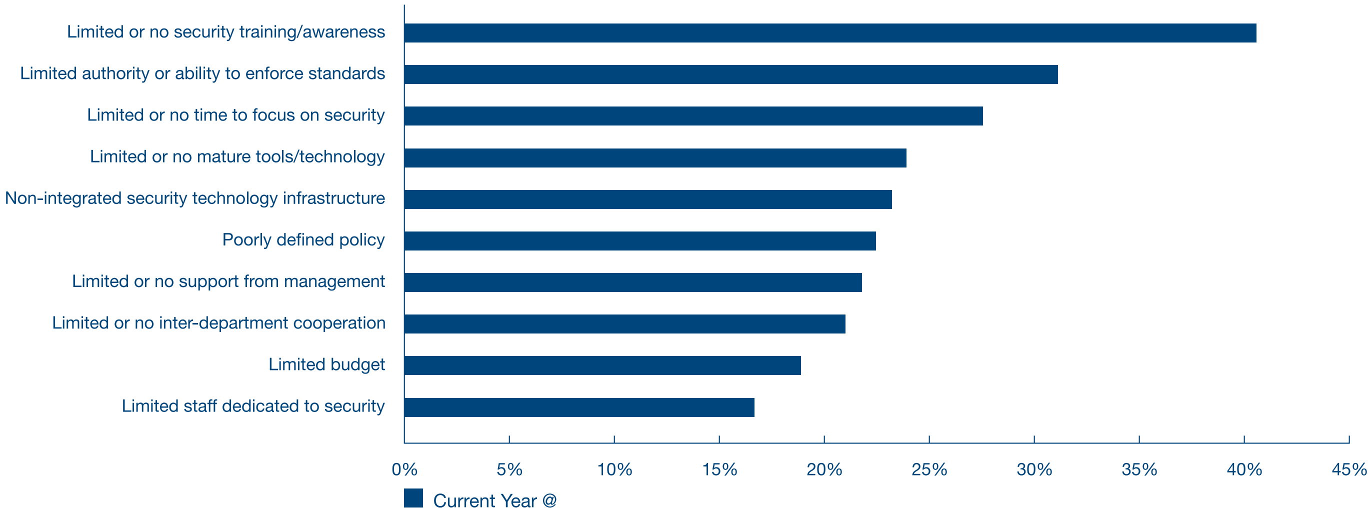
Significantly however, in this survey, most organisations indicated that limited or no security training and awareness is the biggest barrier to good security measures.

Limited authority or ability to enforce standards is the second most significant obstacle, followed by limited or no time to focus on security.

Only 7% of the Indian organisations believed that poor technology infrastructure is a hindrance to implementing security controls.

Thus, due to increased management concern on security and the challenges to data privacy, security budgets in Indian organisations have increased. However, it seems that a large part of these budgets are utilised in deploying tools and techniques, and implementing policies and procedures, rather than hiring staff who can be dedicated to security. Acute shortage of candidates with suitable skill sets can be a major reason for the same, something that has also been indicated as a significant barrier for implementing good security measures.

Top 10 barriers to good security measures



09

Industry-wise analysis

Information security is a concern for all organisations across all industry verticals. However, the nature and form of information security concerns manifest with varying levels of urgency across different industry verticals.

ITeS

Highlights

84% have accorded high priority to security compared to 77% in 2004.

47% are very confident about their organisation's security policy.

60% of the ITeS organisations comply with ISO 27001 requirements.

84% organisations feel that protecting customer data is the primary motivation for information security investment.

More than 75% ITeS organisations continuously or periodically perform prioritisation of their data and information assets according to their risk level.

Security priorities

Most ITeS organisations accord high priority to security and they are confident about their security initiatives.

Security investments and spending

Information security budgets in the ITeS segment have increased significantly. More than 16% of the ITeS organisations have a security budget of more than Rs 100 lakh. On an average, the information security budget is 17% of the overall IT budget for the ITeS sector, the highest as compared to other industry segments.

Expenditure on security in a large number of ITeS companies is driven by client demands – companies are willing to spend more to meet client expectations/requirements. There is, therefore, a change in the philosophy towards spending in this area. Security is no longer deployed on an ad-hoc basis – clients are now charged for the extra security they demand. This results in companies providing services with high quality security.

Compliance

As expected, ISO 27001 certification is most sought after by organisations in the ITeS segment. More than 84% of the ITeS organisations identified ISO 27001 as a guideline/standard, they want to comply with. Of them, 60% already comply with this standard.

There are tremendous pressures on ITeS companies to meet regulatory norms/standards. Thus, it is not surprising to learn that in case of 23% of ITeS organisations, expenditure towards IT security comes from the regulatory/compliance/risk management head.

Safeguards present and future

User administration and role-based access control is the primary focus area.

ITeS sector leads other industry sectors in terms of security strategy initiatives and what it wants to deploy in the days to come. Periodic security audits/risk assessment is one of the key initiatives in the ITeS sector.

Over 80% of the ITeS organisations have invested in patch management solutions – well ahead of other industry segments.

Employee training and awareness has been identified as the primary privacy safeguard by a majority (60%) of ITeS organisations.

Security breaches

Malicious codes (viruses/worms/trojans) remain one of the major sources of negative security incidents.

More than 60% of the responding ITeS organisations identified their employees as one of the sources of threat. This is not surprising considering that some recent security incidents, involving data theft, were supposedly done with the involvement of a company's staff.

Security barriers

42% of the respondents feel that limited or no time to focus on security is the major barrier to good security measures. 38% of the respondents feel that lack of security awareness is the next barrier to good security measures.

BCP and DRP

Most ITeS organisations have identified critical business processes and supporting enablers for developing their business continuity/disaster recovery plans. 73% of the ITeS organisations have formal emergency response procedures in place.

Financial Services

Highlights

90% organisations in FS sector have accorded high priority to security.

None of the FS organisations have accorded low priority to security.

83% of the organisations feel that their security investments are driven by customer data protection need.

71% of the FS organisations perform periodic security checks.

67% of the FS perform employee background verification.

Security priorities

Compared to other sectors, companies in the financial services sector are more confident that their security policy and expenditure are aligned with their business goals. More than 79% of such organisations feel that their security policy is completely aligned with their business goals.

Financial services organisations are also confident about their overall security activity. About 63% of respondents are very confident whereas the average response across all sectors was only 41%.

Security investments and spending

Financial services organisations are the highest spenders on information security. Even then, the ratio of information security spending to the total IT spending is less for the financial sector in comparison to other industry segments.

Compliance

More than 50% of the organisations in the financial services sector are not meeting their compliance requirements.

ISO 27001 is the most sought after information security standard amongst organisations in the financial services sector.

Safeguards present and future

Nearly 58% 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, 26% of organisations in the financial services sector have a security committee to whom the CISO reports. This is different in case of other industry segments where the CISO usually reports to the 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. Thus, practices followed by financial sector companies are better than those adopted by other industry segments in this regard.

Currently, only 4% of the financial services organisations use identity management solutions. However, implementation of such solutions is on the top priority for a large number of organisations in this sector. Thus, 17% organisations intend to deploy identity management solutions next year.

In line with the overall trend, financial services organisations also focus on employee awareness programmes.

Security breaches

Not unexpectedly, financial services organisations have suffered a large number of breaches in the last 12 months, with 13% of the respondents indicating having experienced more than 20 security breaches. Around 20% of the organisations have indicated that they had suffered financial losses ranging from Rs 50,000 to Rs 5 lakh, due to such incidents.

Malicious codes (viruses/worms/trojans) remain one of the major sources of negative security incidents. Amongst them, email virus is the most common method of attack. Around 40% of the financial services organisations feel that internal employees can be one of the primary sources of attack.

Interestingly none of the financial services organisations had come across any security incident resulting in loss or damage of internal record. On the contrary, 22% of the organisations in other industry segments experienced loss or damage of internal records due to security breaches.

It is interesting to note that the financial services organisations are in more frequent touch with CERT-In in comparison with other industry segments with 35% respondents saying that they receive advisories published by the CERT-In.

Security barriers

Within the range of the overall response, 55% of the respondents feel that limited or lack of dedicated security training is the primary barrier to information security.

BCP and DRP

According to 95% of respondents, identification of critical and supporting business processes is one of the core components of their overall BCP strategy.

CIPS

Highlights

Unlike other industry segments, which have identified internal employee as the most likely source of attack, CIPS organisations feel that external hackers are the most likely source.

35% of organisations are very confident about effectiveness of their information security programme. This is significantly low when compared with other industry segments.

Security priorities

This industry segment accords high priority to information security; however, security budgets are significantly lower when compared with ITeS or finance sectors.

About 22% of CIPS organisations stated their intent to comply with the ISO 27001 standard.

Security investments and spending

Similarly, 22% of CISP organisations feel that their spending on information security is completely aligned with their business requirements. However, 45% of the respondents feel that their spending is only somewhat aligned.

The information security budget, in comparison to the overall IT budget, is less than 10% for more than 70% of the organisations. This is the lowest in comparison to organisations in ITeS and financial services segments.

Compliance

For CIPS organisations, the IT Act 2000 is the most sought after compliance requirement instead of ISO 27001. Only 16% of the organisations comply with the ISO 27001 standard.

Safeguards present and future

Around 51% of the CISP organisations feel the need for an information security strategy in future. Again 86% of the CISP organisations have deployed application/network firewalls. More than 27% of the CIPS organisations conduct security audits and risk assessment on a regular basis which is higher in comparison to other industries.

Security breaches

The number of security incidents in this segment is lower than that in other industry segments. More than 41% of the respondents indicated that they did not face any security incidents, while 33% faced between 1 and 10 incidents. However, it does not necessarily indicate that CIPS organisations have better protection, as many were unaware of the security breaches that had occurred.

Also, 33% respondents admitted that they had suffered loss or damage of internal records due to such attacks.

CIPS organisations are also not really well connected with CERT-In. Majority of the organisations are not involved with CERT-In. More than 56% organisations say that they had not reported security events to any external party.

Security barriers

Lack of dedicated resource and appropriate training are the primary barriers for information security for CIPS organisations. This is in line with the overall trend.

BCP and DRP

Similar to the overall industry trend, CIPS organisations intend to focus on BCP in the days to come. As per Current Year @, 26% of the CISP organisations reported not having a business continuity/disaster recovery plan in place.

About CERT-In

The Indian Computer Emergency Response Team (CERT-In) is a national initiative to tackle emerging challenges in the area of information security and country level security risks and vulnerabilities.

CERT-In is coordinated by the Department of Information Technology, Ministry of Communication and Information Technology, Government of India in cooperation with several agencies in the Government, Academia and Industry. The mission of CERT-In is to enhance the security of India's communications and information infrastructure through proactive action and effective collaboration.

The activities at CERT-In are the joint efforts within its partner network. In all of its endeavours, CERT-In depends on its system, network and staff, but most importantly, as professional, CERT-In depends on each other, and that's why information sharing is one key word for achieving success in our endeavours. The motto is to build trusted relationship right across the various sectors and enhance this work by conducting our own research and actively looking for problems before they arise.

For more information, please visit **http://www.cert-in.org.in/**

About FICCI

The Federation of Indian Chambers of Commerce and Industry (FICCI), set up in 1927 is the largest and oldest apex business organisation of Indian business. With a nationwide membership of over 1500 corporates and over 500 chambers of commerce, FICCI espouses Indian businesses and speaks directly and indirectly for over 2,50,000 business units. FICCI maintains the lead as the proactive business solutions provider through research, interactions at the highest political level and global networking.

FICCI organises a large number of exhibitions, conferences, seminars and business meets for promoting business.

For more information, please visit **http://ficci.com**

About PwC

PricewaterhouseCoopers Pvt. Ltd. **(www.pwc.com/india)** provides industry – focused tax and advisory services to build public trust and enhance value for its clients and their stakeholders. PwC professionals work collaboratively using connected thinking to develop fresh perspectives and practical advice.

Complementing our depth of industry expertise and breadth of skills is our sound knowledge of the local business environment in India. PricewaterhouseCoopers is committed to working with our clients to deliver the solutions that help them take on the challenges of the ever-changing business environment.

PwC has offices in Ahmedabad, Bangalore, Bhubaneshwar, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune.

PricewaterhouseCoopers contacts:

Bangalore
Mayurakshi Ray
mayurakshi.ray@in.pwc.com
+91-99026 88200

Chennai
Sucindran R
Sucindran.r@in.pwc.com
+91-98401 73025

Delhi
Siddharth Vishwanath
siddharth.vishwanath@in.pwc.com
+91-98734 34609

Hyderabad
Juzer Soni
juzer.soni@in.pwc.com
+91-98490 51265

Kolkata
Priti Ray
priti.ray@in.pwc.com
+91-99030 90100

Kasturi Bhattacharjee
kasturi.bhattacharjee@in.pwc.com
+91-98304 23286

Mumbai
Sivarama Krishnan
sivarama.krishnan@in.pwc.com
+91-98331 73610

pwc.com/india