DATA SECURITY COUNCIL OF INDIA

State of Data Security and Privacy in the Indian Industry

DSCI- KPMG Survey 2009



Under the

DIT - NASSCOM Cyber Security Awareness Project

In association with CERT-IN

DSCI
PROMOTING DATA PROTECTION

certin
Handling Computer Security Incidents

KPMG

Foreword

Data Protection is important for Indian Service Providers not only because India is a destination of choice for Global IT and Business Process Sourcing, but also for the domestic industry which is beginning to provide more and more services over the internet. With the passage of Information Technology (Amendment) Act, 2008, India has demonstrated its willingness and commitment to create a strong data protection regime in the country. This amendment now mandates all body corporate to implement reasonable security practices to protect sensitive personal information of customers.

It is recognized that legislative requirements drive compliance and discipline of compliance drive policy level changes. Under these circumstances, it is important for us to understand the existing level of implementation of information security in the country to determine the course of supportive actions and policy directions. In this context, it is heartening to see that an information security survey has been conducted by DSCI through KPMG in the partnership with CERT-In. The survey has a highly representative sample of over 150 organizations from various sectors including IT/BPO service providers, banks and public sector enterprises. Besides the efforts to know the status of information security in the country, the survey has also focused on assessment of privacy practices independent of security and general understanding of organizations about Information Technology Act and its amendments, in relation to data protection and need for interface with CERT-In in the event of security incidents.

I believe the information security survey serves the twin objectives of revealing the current status of information security in the country and at the same time allowing us an opportunity to benchmark against the global best practices. The survey results are very interesting. It is highly gratifying to see that as a country, the information security practices of Indian service providers match very well with that of their global counterparts. I am sure these kinds of surveys and similar actions can keep us effectively engaged. It gives me great pleasure to release the survey findings.

R. Chandrashekhar
Secretary, DIT

Messages

MESSAGE FROM CERT-IN

The Data Security Council of India (DSCI) and KPMG have jointly conducted Information Systems Security Survey. This is an attempt to assess the preparedness of Indian Organizations in IT and IT enabled services facing the challenge of securing their IT infrastructure. The report also provides industry specific trends.

In today's context, ensuring safety & security of the cyber space throws up new challenges and opportunities. It is quite an involved task to simultaneously ensure IT enabled growth & development and at the same time prevent criminal & fraudulent exploitation of the weaknesses in IT systems & networks. Seen from this angle, the results of the survey are quite informative. It is heartening to note that information security is getting its due priority among majority of enterprises in the country. Deployment of security controls & technology by the Indian companies has been found to be comparable to that in similar organizations globally.

These kinds of surveys help us to map the requirements and generate accurate data that can support more focused actions. In future, we hope to step up and increase our efforts.

Gulshan Rai
Director General, Cert-In

MESSAGE FROM DSCI

We are happy to present the second DSCI – KPMG Security Survey. It is much more diverse in its base of surveyed organizations – IT/BPO, Banks, Telecom, Public Sector, E-commerce – and the number of respondents. Over 150 organizations were surveyed. Other important elements that have been included for the first time are data privacy trends and Information Technology Act awareness along with CERT-In interface. Security technology adoption trends to mitigate threats and vulnerabilities have been analyzed in reasonable depth. It is gratifying to find that the organizations are focused on technology adoption and implementation of latest tools such as DLP. They are also well prepared to meet the challenges posed by mobile and wireless devices at endpoints. Security preparedness of organizations continues to enhance. Once again it is the IT/BPO companies, banks and telecom service providers which are at the frontier of using cutting edge technology and standards to enhance their security. While compliance regulations continue to be a driver for security, the latter is seen as a differentiator too.

Kamlesh Bajaj
CEO, DSCI

MESSAGE FROM KPMG

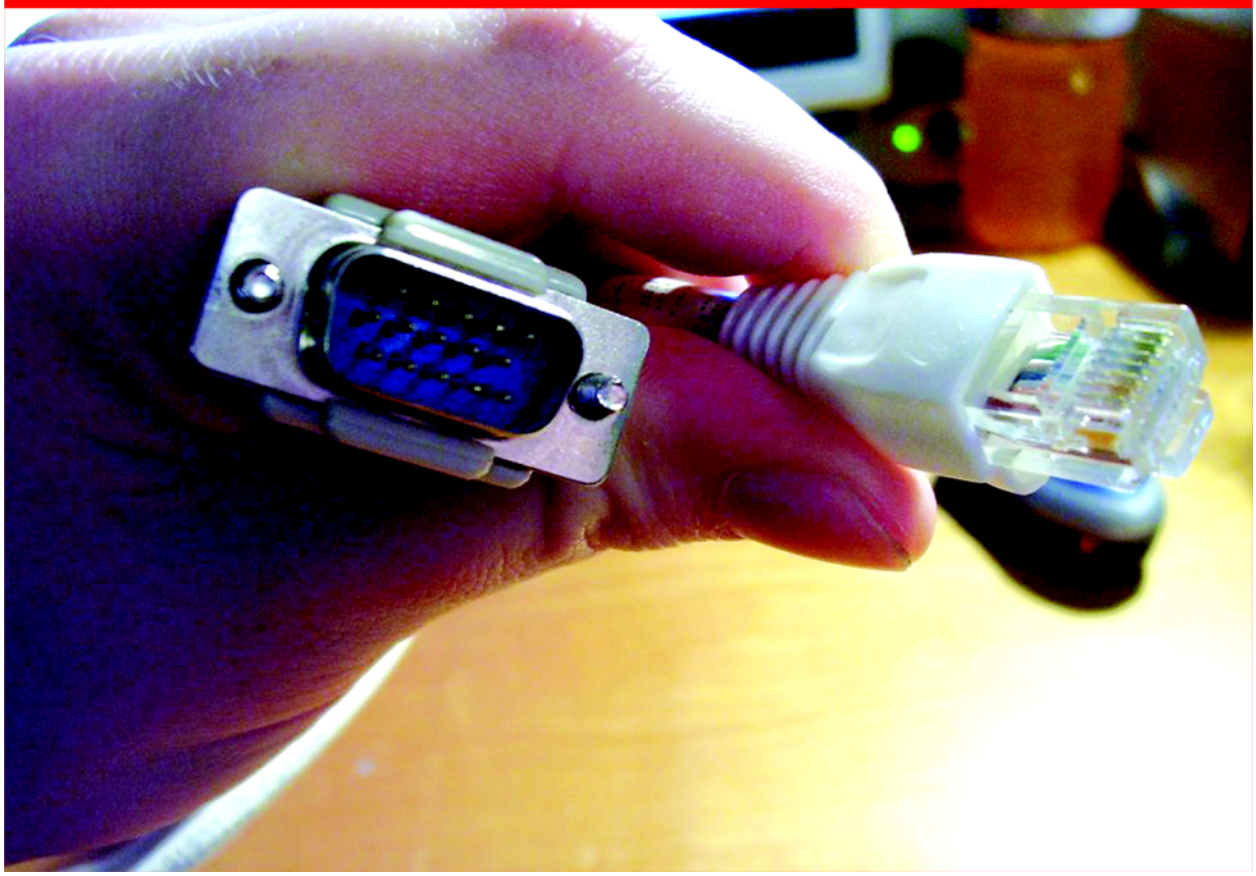
Information security, both conceptually and practically is not a new phenomenon. Organizations have over the years understood its importance and initiated measures. However the threats today have re-aligned and are far grave than before. While organizations continue to demonstrate maturity in dealing with them, there are contradictions on intent versus implementation effectiveness. Furthermore, these threats cannot be overcome by point solutions but a long-term security governance and sustenance plan. This is also essential as over a period of time, physical and information security controls will converge, thereby mandating the need for a comprehensive framework.

KPMG is pleased to be associated with DSCI and CERT-IN on this initiative. KPMG has worked on many such initiatives that help highlight information security challenges. The objective of this survey has not only been to carry out an assessment of the industry but also to sensitize organizations on best practices. We hope the readers find the analysis insightful and can initiate measures to enhance the security posture their organizations.

Akhilesh Tuteja
Executive Director, KPMG

CONTENTS

Introduction



Highlights

The survey provides insights into the information security and data privacy environment in India. There is evidence that validates general perceptions and then there are some outliners that do not align to the seemingly obvious.

- Information security is a "Top Priority" or is "Critical" to **87%** of respondents
- Data privacy is as much of a concern across the industry. More so amongst participants from the **Telecom** segment where it is perceived more critical than information security
- **82%** of respondents perceive top management focus on information security as adequate; yet 64% have concerns regarding employees not attributing enough importance to the same
- More than **80%** of respondents, irrespective of organization size, are earmarking budget for information security
- There is a growing interest in **endpoint** and **virtualization security**
- The adage "one-size-fits-all" may not work well across industry segments as each seems to have **unique challenges** that need to be addressed

Summary

Indian service providers are global sourcing partners to large clients in North America, Europe and other countries of the world. They handle important corporate and sensitive personal information of consumers. Further, domestic industry is more proactively using Information Technology for their business transactions, gathering and processing the information.

When such information is business critical and sensitive, it is pertinent to ask – is it safe? Data Security Council of India (DSCI) and KPMG jointly conducted a survey to assess the trends in the area of information security and data privacy in the Indian industry and to gain insights into how the Indian industry is addressing such concerns.

150 organizations were surveyed with the following objectives:

- Assessing the importance attributed to information security and data privacy;
- Obtaining insight into the concerns and challenges that need to be addressed;
- Identifying the leading practices and/or standards adopted for information security and data privacy; and
- Assessing awareness in the industry on how the Indian Government (Department of IT), through legislation, and entrusted bodies such as CERT-In are working towards creating an environment conducive to enhancing information security and data privacy.

In order to ensure that the survey results represent the Indian industry at large, we reached out to CISOs and their equivalents in organizations across industry segments and sizes.

The survey results highlight trends and insights into the state of information security and data privacy in the Indian industry – many "generally known" practices are validated, yet certain unexpected insights are revealed.

Importance

There is unanimous acknowledgement of the importance of information security amongst the participants across industry segments and sizes. Further, an encouraging fact is that data privacy is not as low on the agenda of India Inc., considering this is a concern that has only recently come to the fore. The first section of the report – 'Importance' – reveals these and other such trends in detail.

Challenges & Concerns

The findings reveal that that top management, across industries, are still finding it challenging to drive the importance of security and privacy of information down to every level of the organization. The report, in its second section – 'Challenges and Concerns' – highlights this and other significant concerns that are ailing the industry. Though, on the brighter side, it seems that the first step towards addressing a 'problem' – acknowledging the fact that there is one – seems to have been done.

Industry Preparedness

In the last section – 'Industry Preparedness' – the report highlights how the participants have prepared themselves to address their challenges and concerns and what the leading security practices and technologies which are being adopted to do the same.

India Inc. has prepared itself well to deal with the known and unknown with widespread implementation and frequent updates to Business Continuity Plans (BCP) and Disaster Recovery (DR) plans.

The findings that have been reported indicate the progress that is being made in the Indian industry with regards to information security and data privacy. The findings underscore the direction that the early adopters, along with solution providers, are defining for rest of the industry to follow.

It is envisaged that the results of this survey along with the emerging trends and indicators will help DSCI and CERT-In in the following way:

- Create a visibility on the state of security and privacy at Indian industry: outsourcing service providers, industry verticals and public sector organizations
- Understand key security challenges faced by the Indian industry, their level of preparedness and maturity of their initiatives
- Judge awareness of Indian industry towards policy initiatives: IT (Amendment) Act 2008
- Serve an information source to the national programs initiated by industry — DSCI- NASSCOM and by government—CERT-In (DIT)

Methodology

The survey was conducted using a structured questionnaire, which was administered through mailers, telephonic and in-person meetings. 150 organizations from a broad range of industries took part in the survey.

In order to get holistic perception of information security measures deployed, it was ensured that the respondents represented relevant personnel in the organization's information security team – typically the senior management such as Chief Information Security Officers (CISO) or equivalents and IT Security Managers.

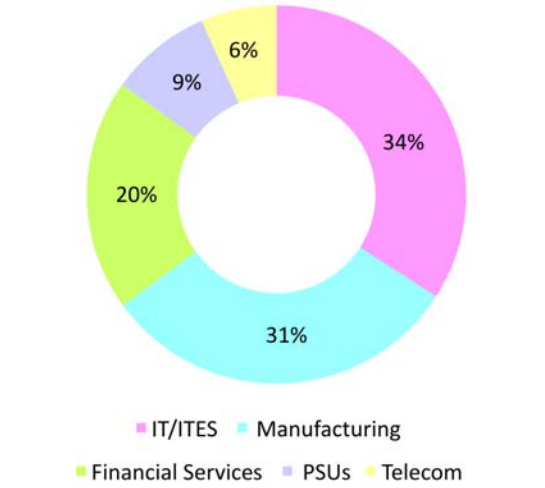
Some facts on the participating organizations are as follows: The respondents to this survey represent a wide variety of organizations, spread across various industry segments. The industry segments have been grouped as under:

- Information Technology (IT) and IT enabled Services (ITeS)
- Financial Services (FS)
- Manufacturing
- Telecom
- Public Sector Undertakings (PSU)

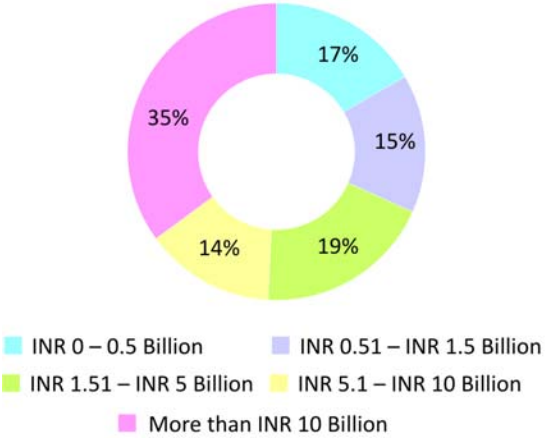
India's public sector has a fair representation, which demonstrates the fact that government and public sector undertakings are also gearing up to securing their information assets.

"It must, however, be kept in mind that the respondents' profile varies across the surveys, which might have some influence on the results."

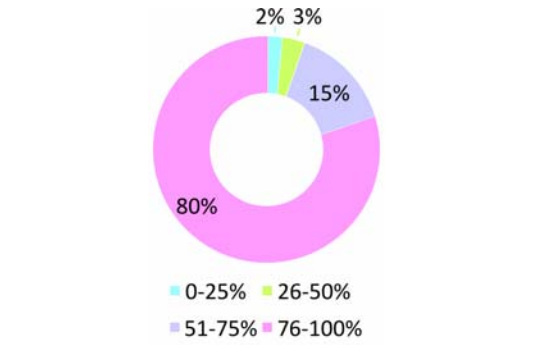
INDUSTRY DISTRIBUTION



DISTRIBUTION OF TURNOVER FOR PARTICIPANTS



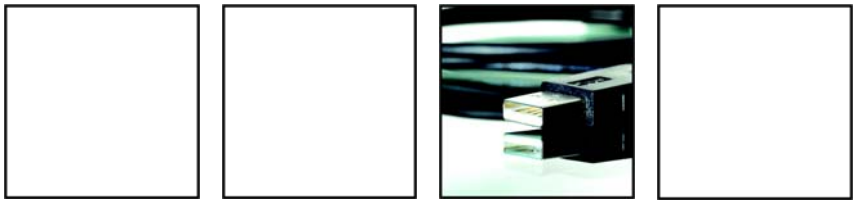
DISTRIBUTION OF COMPANIES AS PER EMPLOYEES ACCESS TO COMPUTER SYSTEMS



Importance

Importance

Information security and data privacy are the current watchwords in the context of Indian organizations. No longer are these restricted to specific industry domains or to a handful of “interested” people, but these have assumed importance that are a CxO level concern for the organizations. This is substantiated by our findings in this section.



Key findings

- Majority of the survey participants attribute information security and data privacy as either a “Top Priority” or “Critical” to their organization
- Organizations with an independent management structure for information security outnumber those that have a shared structure
- Organizations have dedicated teams to address information security
- Majority of organizations have updated their business continuity plans in the last 12 months and have formal disaster recovery plan in place

Establishing Importance

Survey reveals that majority of the Indian Organizations perceive the importance of Information Security and Data Privacy as either "Top Priority" or "Critical" for Indian Organization business operations is an important factor that reflects the management intent - an absolute must for the success of information security.

Significance of Information Security and Data Privacy in the Indian Context

The survey results indicate that the Indian industry attributes due importance to information security. IT/ ITeS and Financial Services organizations give greater importance to information security as compared to their Telecom, Manufacturing and PSU counterparts. Data privacy also emerges as a steadily growing trend - 99% of participants from telecom and 96% from financial services attributed 'Critical' or 'Top Priority' to the importance of data privacy (refer Figure 1 and 2). It is evident that organizations that process personal information attribute greater importance to information security and data privacy controls.

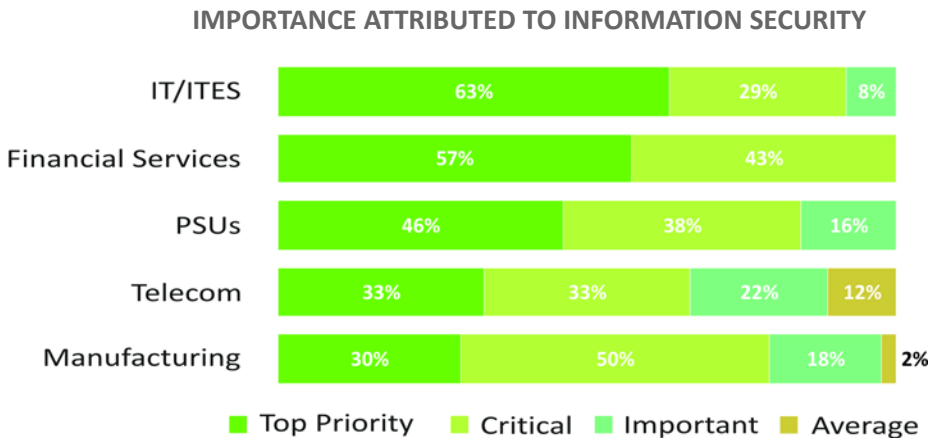


Figure 1

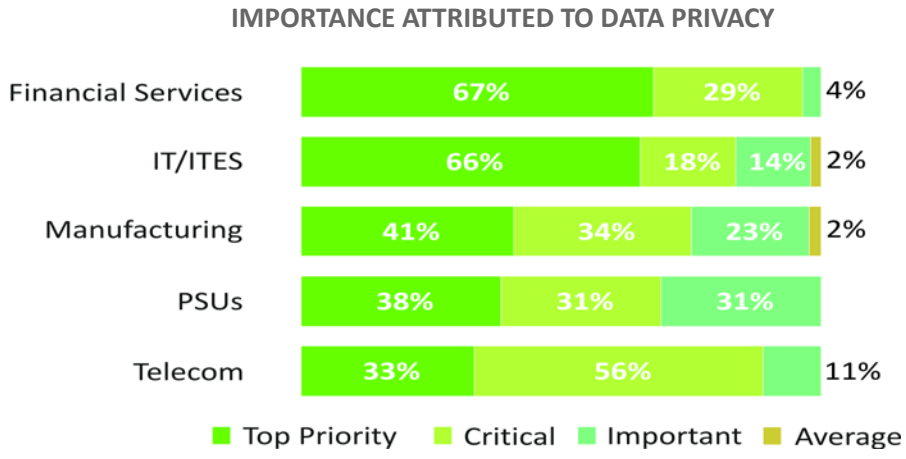


Figure 2

A “CxO” level concern

The survey highlights the fact that more than 95% participants, across industries, have a CxO level or equivalent oversight on either the approval and/ or implementation of information security initiatives. Information security is indeed a “CxO” level concern within the Indian industry.

The survey results also emphasize the management’s commitment to ensure that information security function is not undermined by business imperatives. This is evident from the fact that two out of every three organization have an IT Security Management structure independent of other IT support teams (refer Figure 3).

INFORMATION SECURITY FUNCTION HAVING AN INDEPENDENT MANAGEMENT STRUCTURE

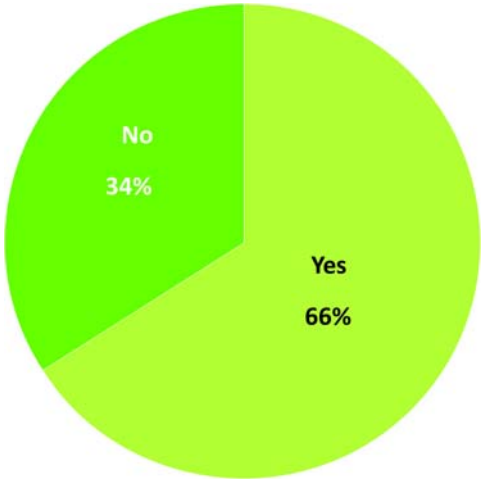


Figure 3

People, Process and Technology Initiatives

Information Security Spending - A Snapshot							
% of IT Budget	> 10%	8-10%	6-7%	3-5%	1-3%	<1%	No separate Budget
% Response	11	16	10	20	10	5	18

Figure 4

Information Security Spend

Survey results show that there is a definite percentage of IT budget allocated to information security (refer Figure 4). The next few sections details the information security and data privacy initiatives that the management of Indian organization is investing in.

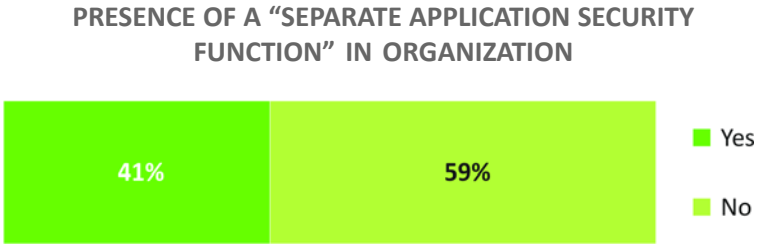


Figure 5

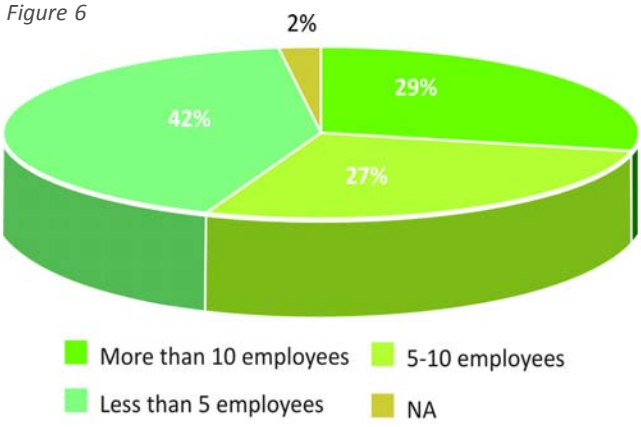
People Initiatives

Organizations have dedicated teams that address their information security requirements. The results also show that 56% respondents have five or more people in their information security team (refer Figure 6).

Apart from the size of the team, management is also investing in development of skills. Forty one percent of the respondents have a separate application security function with IT/ITeS and financial

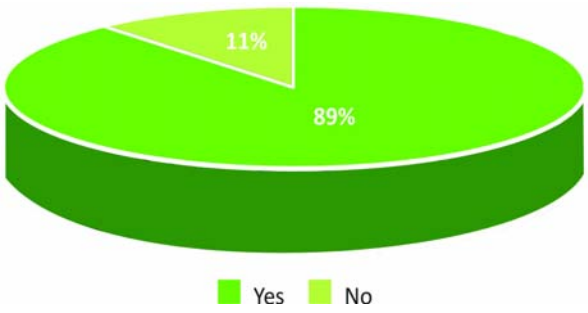
SIZE OF INFORMATION SECURITY TEAM

Figure 6



AUDITS ON INFORMATION SECURITY FUNCTION

Figure 7



services organizations leading such investments (refer Figure 5). This highlights that some of the areas - that require special focus, attention and skills - are being established as separate disciplines of information security function.

Processes Initiatives

Organizations seem to be keen on validating their investments in information security through internal/ external audits of information security function. Eighty nine percent of respondents have conducted such audits (refer Figure 7) of which close to 69% have conducted process audits while 53% have conducted vulnerability assessment and penetration testing.

The Indian industry is also investing in adopting industry-accepted standards such as ISO 27001. Almost two third participants have already adopted the standard or are looking at doing so in the near future. Further, IT/ITeS (Health Insurance Portability and Accounting Act - HIPAA) and financial services (Payment Card Industry - PCI) organizations, are most concerned about compliance requirements.

Technology Initiatives

Implementation of tools and technology controls for information security and data protection continues to be a strong trend. IT/ITeS and financial services organizations displayed a greater propensity towards adopting tools including newer technologies such as end-point encryption and virtualization security (refer Figure 9). While participants from other industry segments may be adopting new technologies at a slower pace, it is evident that they have already implemented basic IT security controls such as Anti-Virus/ Malware, Firewalls, Content Monitoring and Filtering.

5 MOST "IMPLEMENTED" TOOLS BY INDIAN INDUSTRY

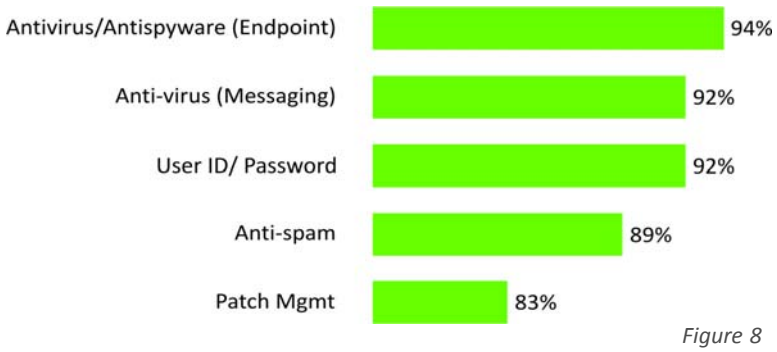


Figure 8

TOP 3 TECHNOLOGY SOLUTIONS BEING CONSIDERED FOR IMPLEMENTATION

Rank	IT/ITeS	Financial Services
1	End-point Encryption	Virtualization Security
2	Governance Risk & Compliance	Network Access Control
3	Virtualization Security	End-point Encryption

Figure 9

Presence of Disaster Recovery Plan

Continuity and Recovery

Survey results show that more than 80% of respondents have both – a business continuity plan (BCP) and a disaster recovery plan (DRP) (refer Figure 10). The results also indicate that these plans are maintained and updated on a regular basis (refer Figure 11). However, the survey results also indicate that these plans are not tested regularly.

There seems to be a sense of caution that is driving proactive measures to address threats to business continuity, be it natural disasters or geo-political events.

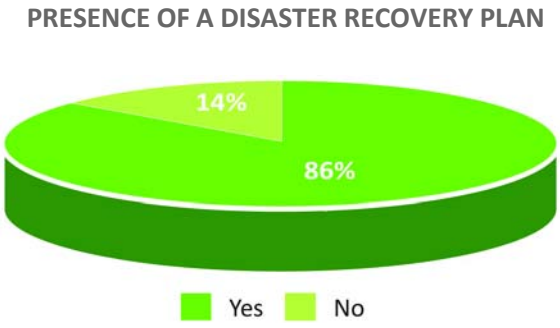


Figure 10

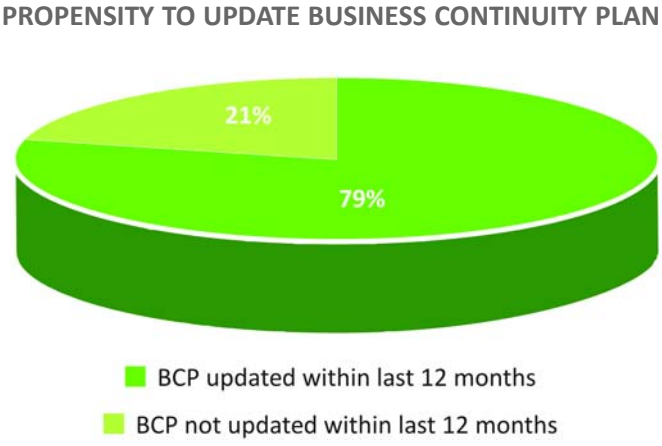
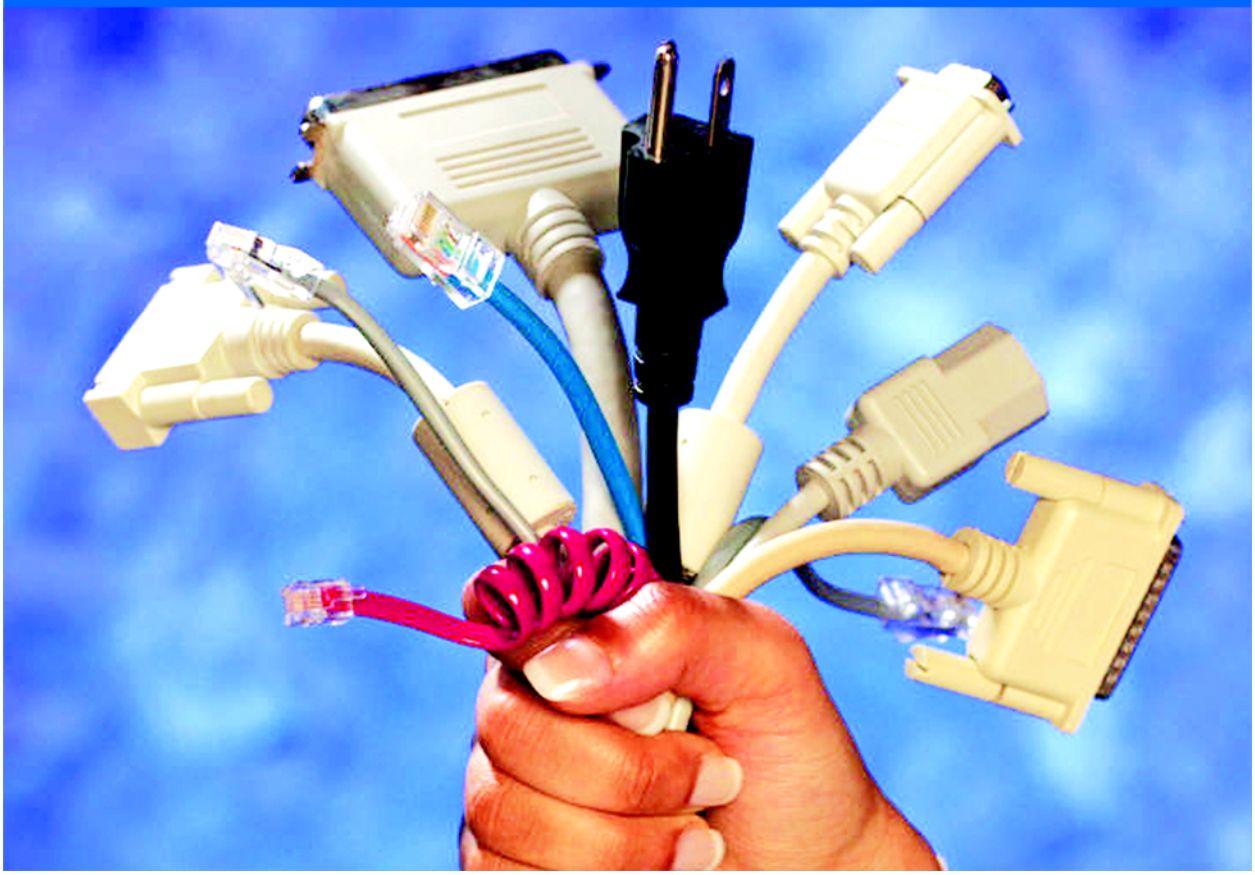


Figure 11

Challenges and Concerns



Challenges & Concerns

What impels the importance of security and privacy in the Indian industry? Is it a need that is borne out of "competitive pressure" in a global world? Or are there concerns and challenges that arise from within that drive the security and privacy initiatives?

Key findings

- Client/ customer concerns about privacy of their sensitive information is the prime driver for newer initiatives on data privacy
- "Employees underestimating importance of security" is the biggest challenge that respondents face in implementing an effective information security paradigm
- People aspects of security is still a major concern as "compromised user account" is observed as the most frequently observed incident.
- Email without encryption is voted as the most prevalent data leakage scenario, which is following by printing of information and use of USBs and CDs

Factors of Impetus

The survey results provide insight into the factors that influence information security and data privacy initiatives amongst the respondents. A number of these factors are focused on overcoming challenges in maintaining a minimum level of security. At the same time factors, previously considered insignificant, such as data privacy concerns over personally identifiable information (PII), are also beginning to give shape to security initiatives.

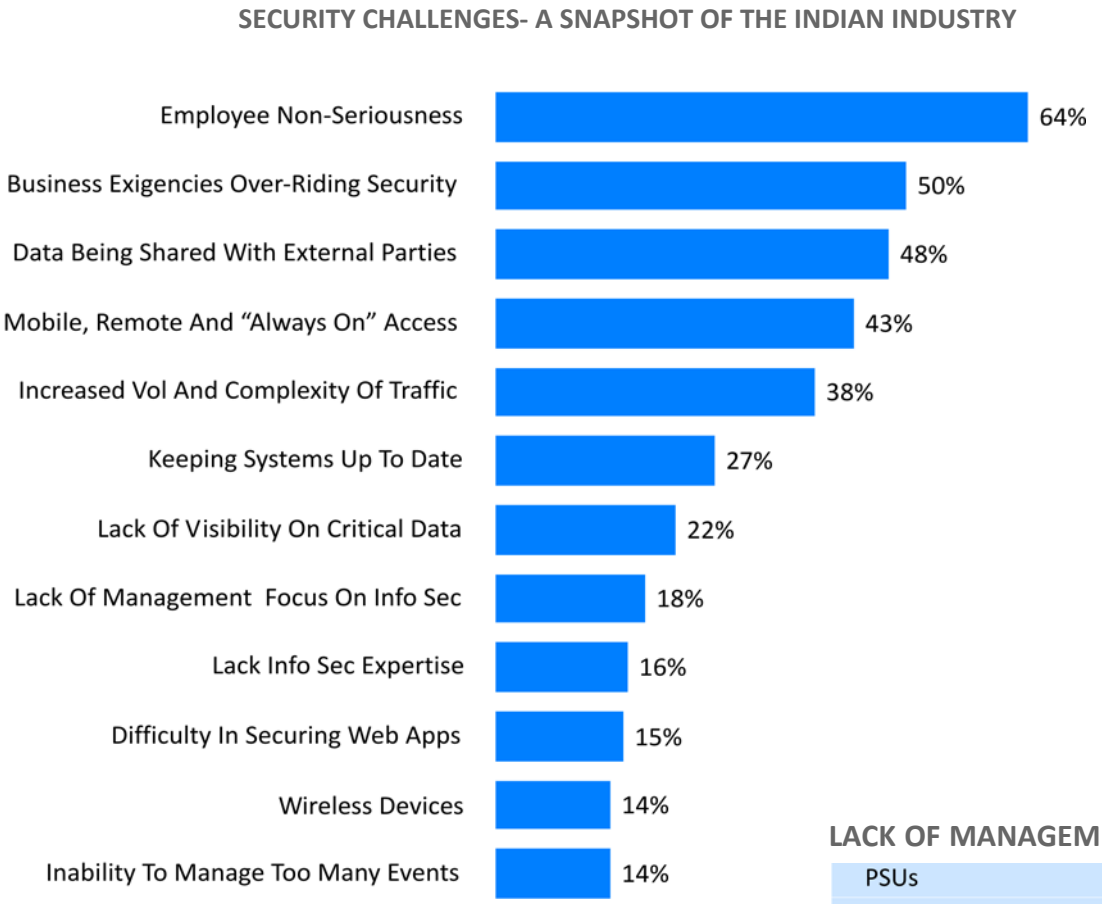


Figure 12

LACK OF MANAGEMENT FOCUS

PSUs	46%
Manufacturing	18%
IT/ITeS	14%
Telecom	11%
Financial Services	4%

Figure 13

Challenges

"Employees underestimating the importance of following the security policies" is the biggest challenge the Indian organization faces in effectively enforcing information security controls (refer Figure 12). This, along with the fact that there is unanimous cognizance of security and privacy as a top priority at a strategic level may imply that there is scope for improvement in driving the importance of security to the operational level - specifically in the manufacturing and PSU organizations (refer Figure 14).

Further, this survey confirms the fact that the concept of "extended organization" is a significant security concern amongst the participants.

ANALYSIS OF THREATS ASSOCIATED WITH "EMPLOYEE- NON SERIOUSNESS" ACROSS INDUSTRIES

Figure 14

Information Security Incidents

Information Security Incidents

Identification and analysis of information security incidents enables improvement in controls to prevent future reoccurrences. Reporting of these incidents, however is not perceived, to be without associated hazards since as many as 13% respondents choose not to comment on the incident experienced in the past. It may indicate that the organizations do not feel the need to disclose such information or just that they may not have insight into such incidents.

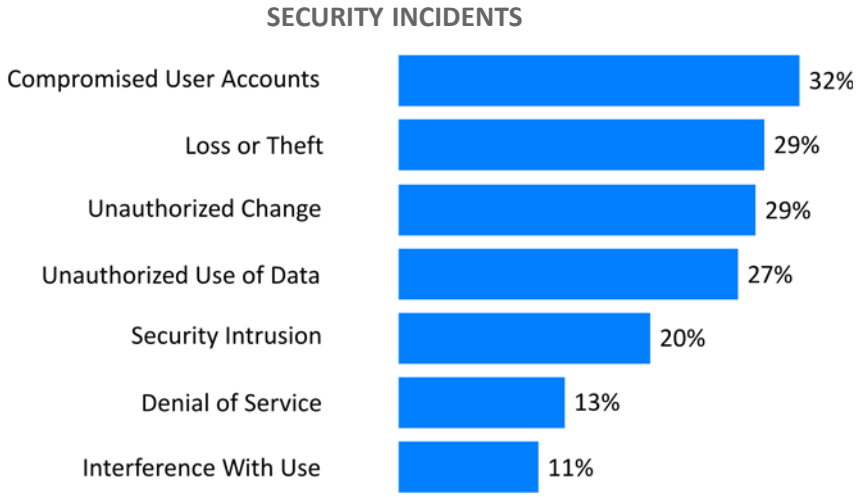


Figure 15

"Compromised User Account (Sharing of sensitive data within and/or outside the organization)" emerged as the most frequently occurring incident with 32% respondents reporting having experienced the same (refer Figure 15). This category indicates that the '*people*' aspect of security is still a major concern – an awareness issue or employees underestimating the importance of adhering to security policies?

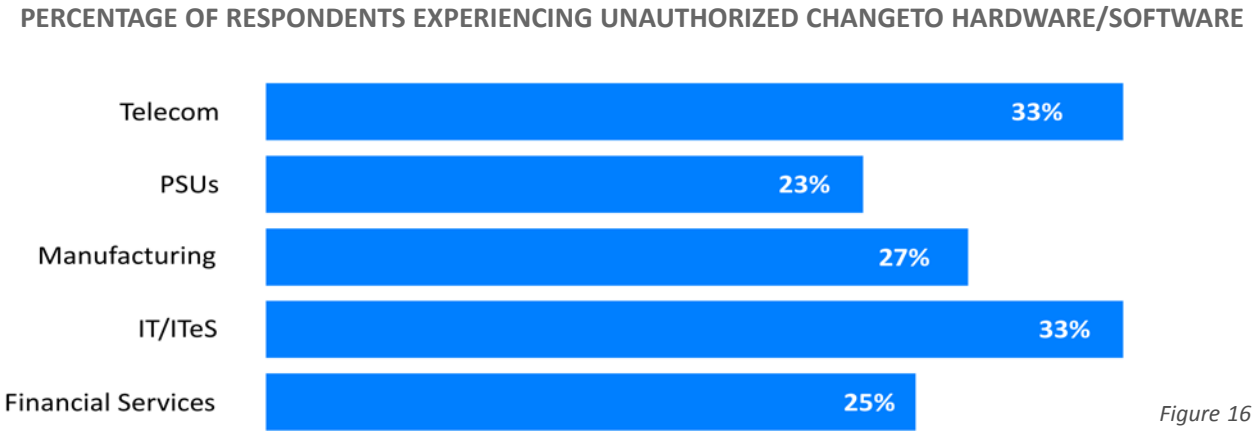


Figure 16

An analysis of the other two most frequently reported incidents (refer Figure 16 and 17) reveals that loss or theft of devices storing sensitive information is a concern with almost 50% of the participants from telecom and financial services. With such incidents being rampant, it is imperative that organizations dealing with sensitive electronic records consider use of end-point encryption and protection tools that can offer higher levels of protection to the information stored on such devices.

PERCENTAGE OF RESPONDENTS EXPERIENCING THEFT OR LOSS OF EQUIPMENT WITH POTENTIALLY SENSITIVE INFORMATION

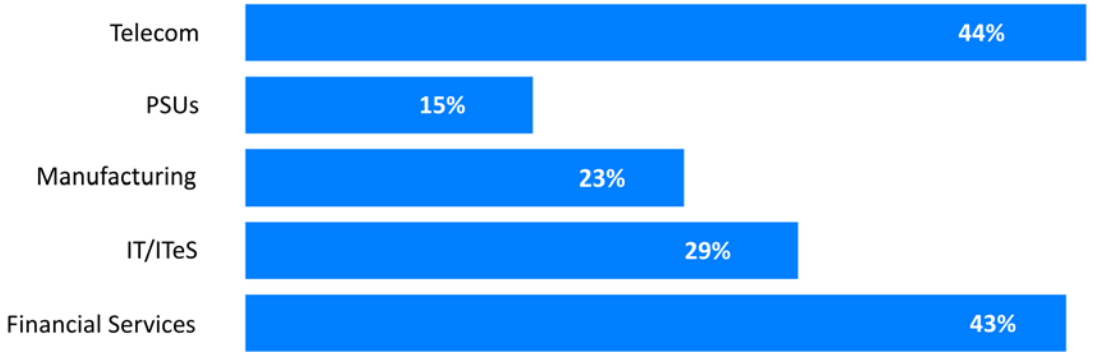


Figure 17

Drivers for Corporate-wide Information Security Certification

- The survey results show that IT/ITeS organizations acknowledge competitive pressure as a driver for corporate wide information security certification.
- "Compliance" is the prime driver for the corporate wide information security certification.
- Even though 63% organizations recognize certification as a "Business Enabler" only 26% go in for certification due to competitive pressure.
  (refer Figure 18)

DRIVERS FOR CORPORATE-WIDE INFORMATION SECURITY CERTIFICATION

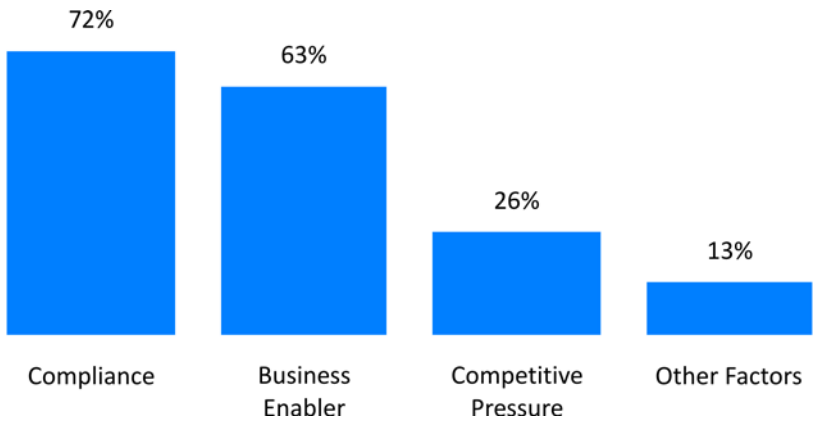


Figure 18

Drivers of Data Privacy

Drivers for Data Privacy

One of the reasons for the growing focus on data privacy could be the increased inflow of critical data and processes to outsourcing service providers. Legal, contractual and compliance requirements are resulting in clients, from various geographies demanding greater assurance on data privacy by the outsourcing service providers (refer Figure 19).

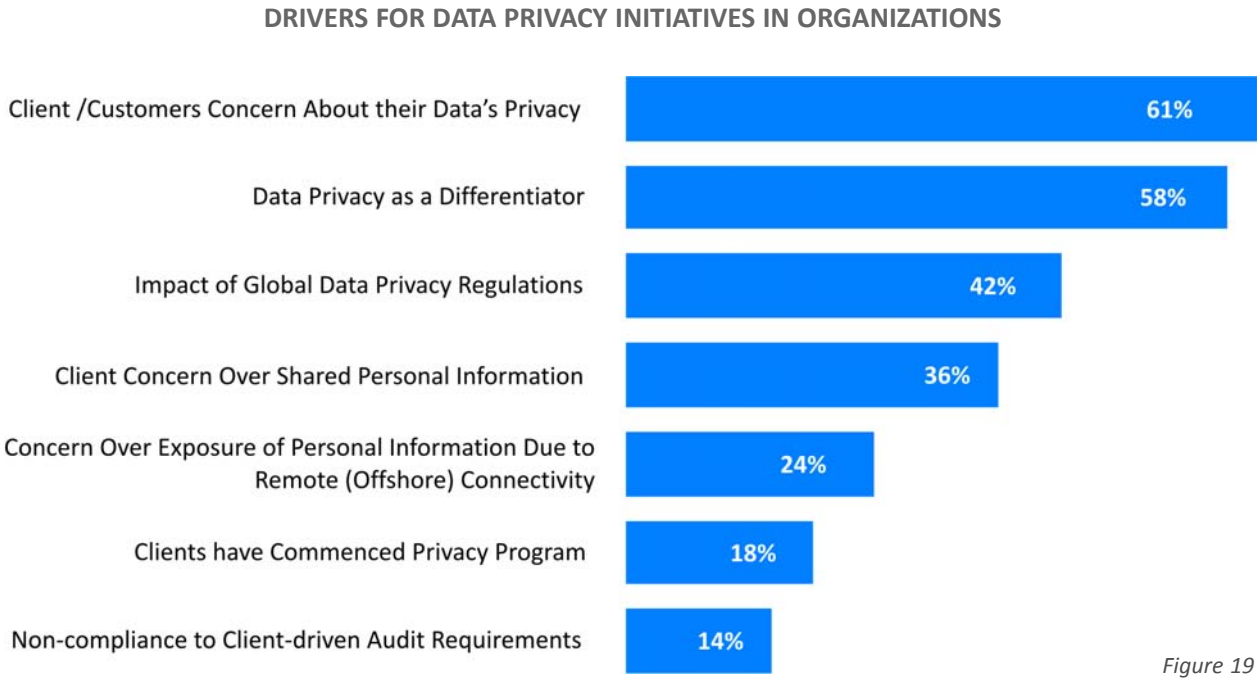


Figure 19

The survey reveals that each industry segment experiences a different degree of pressure to drive data privacy initiatives (refer Figure 20). Understandably, IT/ITeS and Financial services perceive the greatest pressure but the fact that the Telecom organizations perceive such pressures much more than any other highlight growing awareness and demand for data privacy from within the domestic market.

"Client /Customers Concern About their Data Privacy" was observed as one of the prime drivers that is pushing organizations towards greater control over sensitive data (refer Figure 21). The survey further reveals that 55% of the IT/ITeS and 67% of Telecom organizations, agree to having client/ customer concern about privacy driving their privacy initiatives.

Figure 20 and 21 also reveals that while data privacy is a concern in general for organizations from the Manufacturing section, these concerns are not due to client/customer concerns. These may be arising due to internal factors such as lack of capability to secure business critical information.

PRESSURE EXPERIENCED FOR INCREASED DATA PRIVACY INITIATIVES

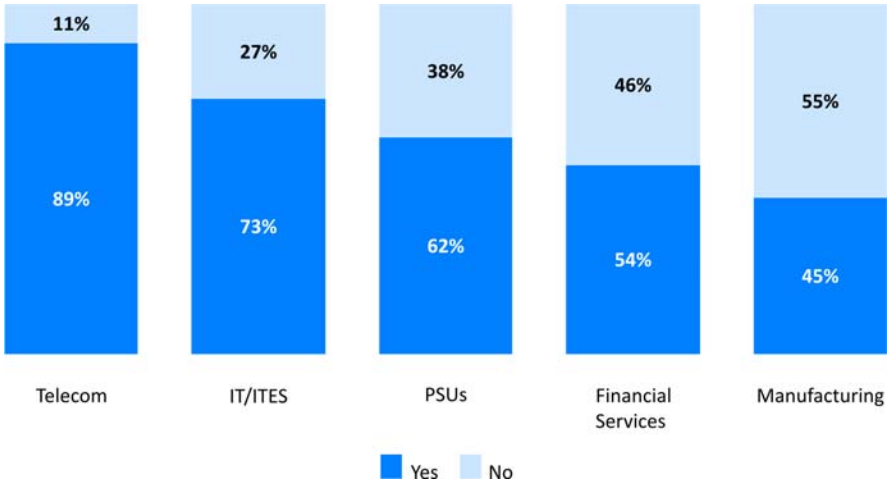


Figure 20

CLIENT/CUSTOMER CONCERN ABOUT PRIVACY

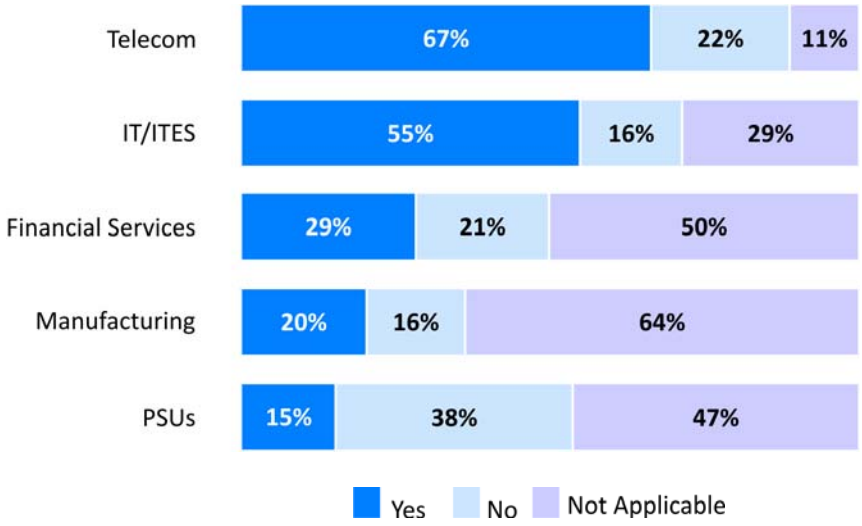


Figure 21

Access to Sensitive Information

Organizations, and in turn the employees, are responsible for security of information that is generated or processed within an organization. More than 98% of organizations that responded to the survey, provide a majority of their employees access to electronic records and thus it becomes imperative for such organizations to maintain visibility over the critical information that is being accessed. Understandably, highly sensitive information such as credit card data remains limited to the financial services organizations (refer Figure 22); however business critical information assets such as IPR, business plans, etc. exist in electronic as well as physical form in almost all organizations and need to be suitably protected. This data clearly establishes the fact that irrespective of the industry segment, there is a need to adopt a comprehensive approach to protecting such sensitive data.

	Financial Services	IT/ITES	Manu-facturing	PSUs	Telecom
Critical or IPR-based Information (Figures in %)					
Credit Card Numbers and its authorization informaiton	50	24	2	15	22
Personally Identifiable Information	71	35	23	38	44
Critical design, images, and diagrams	50	51	52	62	22
Business strategy documents, board presentations, MoMs etc	79	65	68	85	89
Business plan, proposals, RFPs, presentations etc	86	78	73	85	89
Project plans, project reports etc	71	69	68	77	56
Source code, libraries and reusable components etc	71	61	27	62	22
Financial information- payroll,receipts and expenditure, transaction logs and reports	82	73	70	92	67
Knowledge assets, research and market analysis reports	68	57	52	62	44

Figure 22

Data Leakage Scenarios

An attempt was made, through the survey, to identify significant threats to data privacy, as perceived by the respondents. The results reveal that scenarios such as emails without encryption (63%) printing of information (60%), use of CDs and USBs (57%), employees retaining critical information (51%) are being given serious thought (refer Figure 23). Such concerns reinforce the need for automation and strong governance practices to address data leakage.

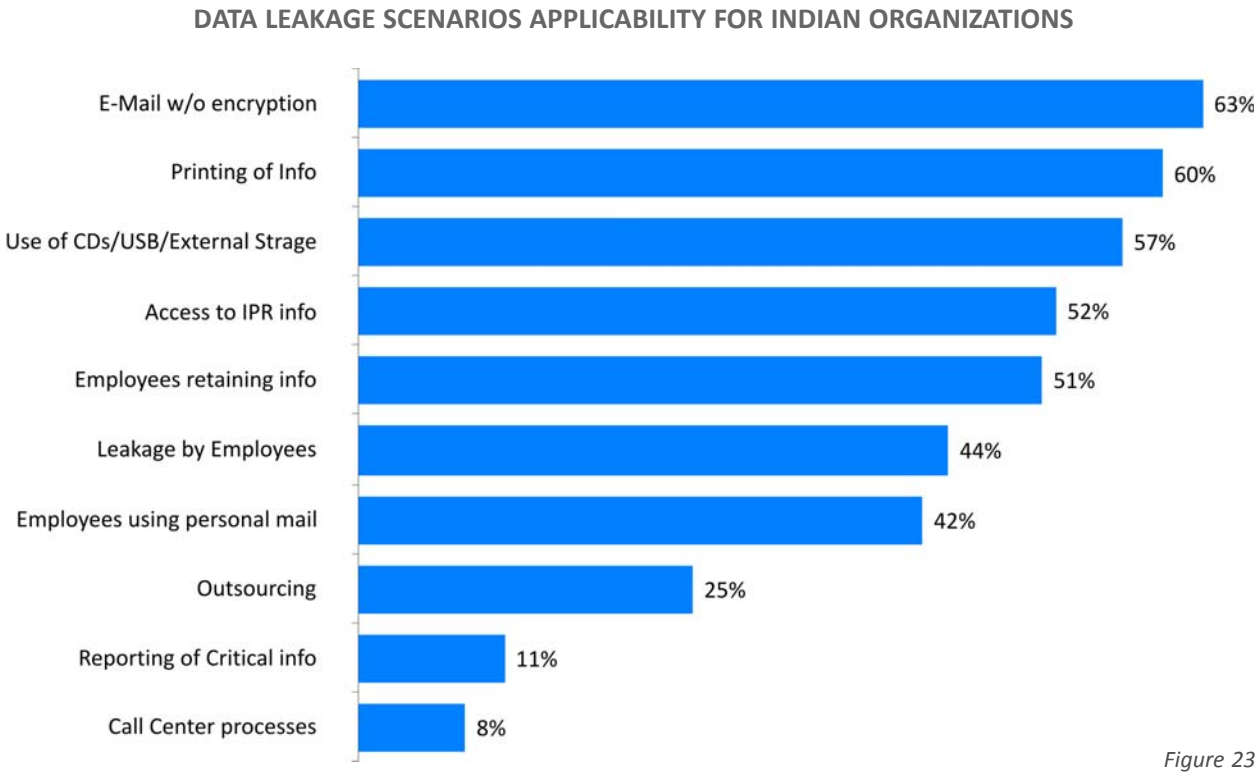
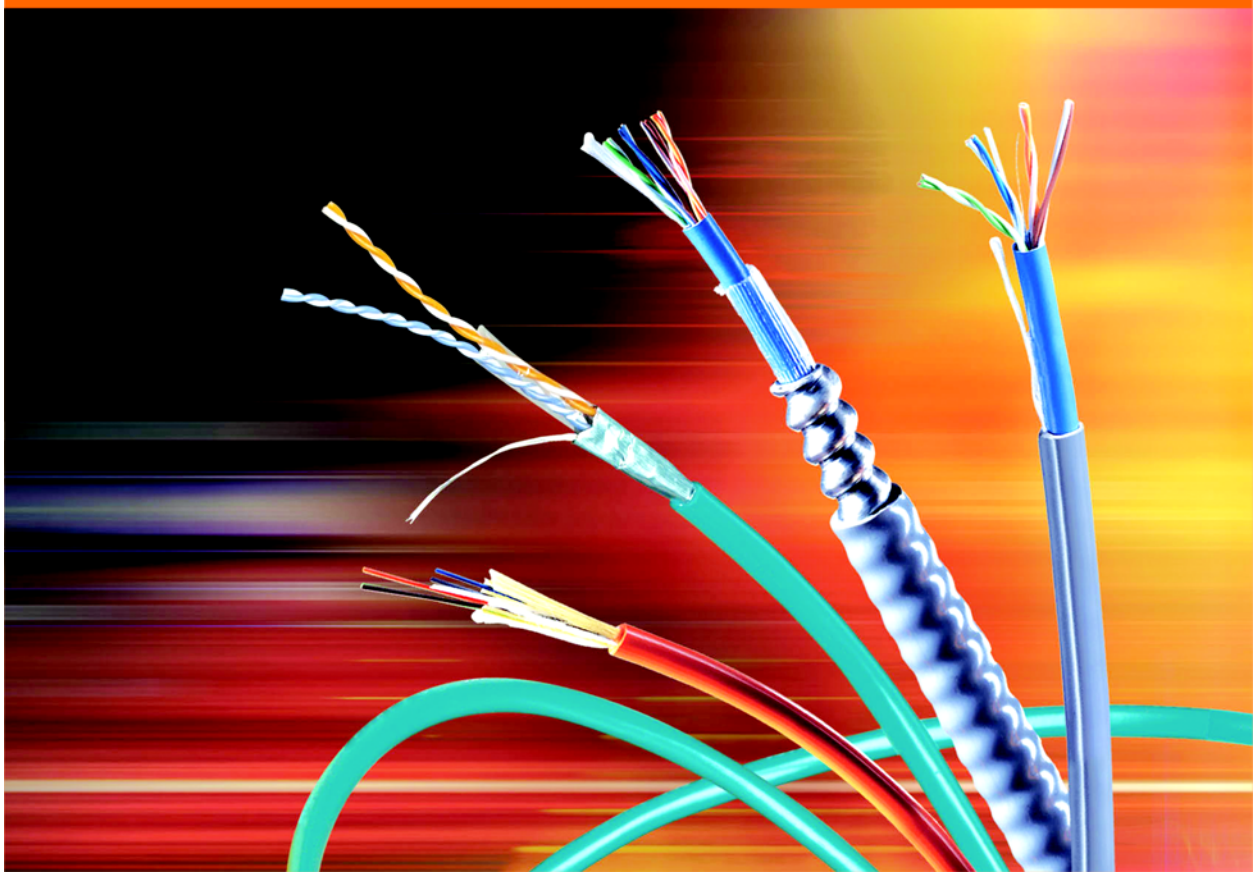


Figure 23

Industry Preparedness



Industry Preparedness

How does India Inc. react to the imperatives and substantiate its claim of being a secure outsourcing destination? What are the strategic and tactical practices that are being relied upon to address the ever increasing security and privacy challenges?

Key findings

- More respondents have “Centralized” Information Security function.
- Privacy initiatives are still seen as a part of the information security function of an organization
- Organizations seem to find merit in outsourcing select skill-oriented security processes such as application security
- Although data security technology is increasingly being adopted, classification of data is still figuring as an important challenge
- Physical and information security functions are converging
- There is keen interest in adoption of newer technologies such as virtualization security and Data Loss Prevention (DLP). It seems organizations are pro-actively deploying controls and are undeterred by risks associated with adopting leading technology platforms

Security Governance

Governance of the information security function facilitates efficient management control over implementation of policies, processes and technologies aimed at securing the organization's information assets. The Indian industry appears to be well positioned to govern information security program.

Characteristics of Information Security Function

- There is CxO oversight in more than 95% of organizations that responded to the survey;
- The information security function has been segregated from IT operations in close to two third of respondents;
- It has been established as a centralized function in 81% of respondents (refer Figure 24); and
- Two thirds of participants prefer centrally driven, enterprise-wide roll-outs of security initiatives.

NATURE OF INFORMATION SECURITY FUNCTION

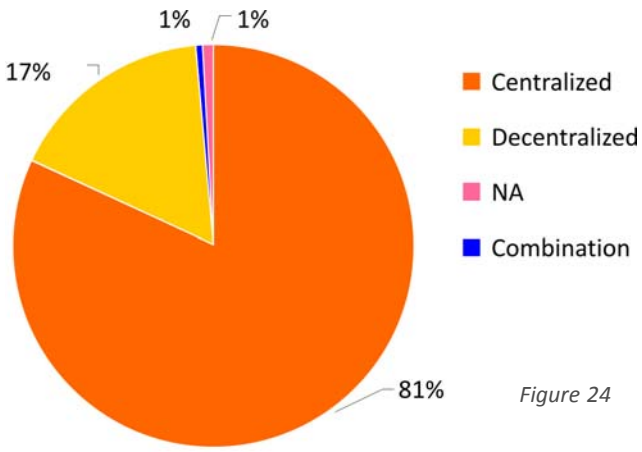


Figure 24

Annual Turnover vs. Information Security Team Size

The presence of a dedicated information security team reflects the organization's commitment towards security and privacy. An analysis of variation of the size of information security function over annual

SIZE OF INFORMATION SECURITY TEAM VIS-À-VIS ANNUAL TURNOVER

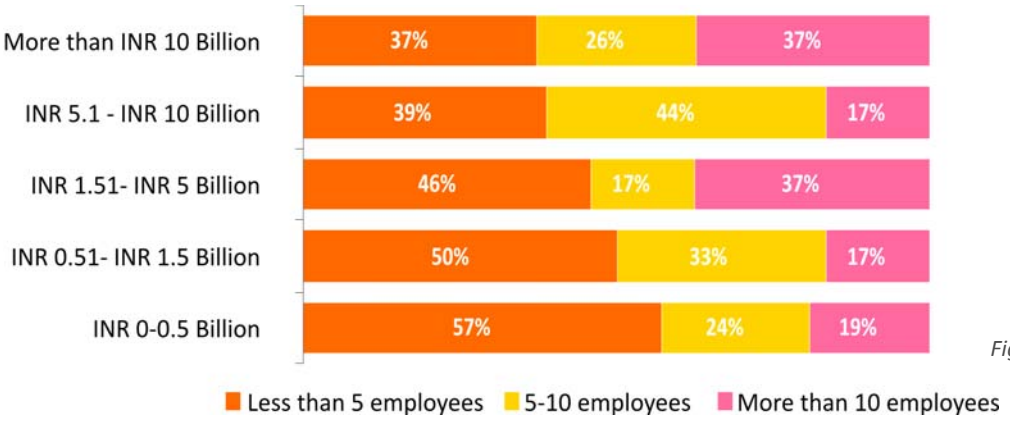


Figure 25

turnover (refer Figure 25) shows that there is no 'drastic' drop in the team size even in smaller organizations. This trend highlights that even smaller organizations acknowledge the importance of security and make investments commensurate to their requirements.

Segregation of Information Security and Data Privacy

Growing data privacy concerns are resulting in organization undertaking initiatives that go beyond IT security and focus on data privacy controls. The survey reveals that this global trend is yet to catch up with a large section of the participants as 89% of organizations are not planning to segregate data privacy and information security functions in the near future.

SEGREGATION OF INFORMATION SECURITY AND DATA PRIVACY FUNCTIONS

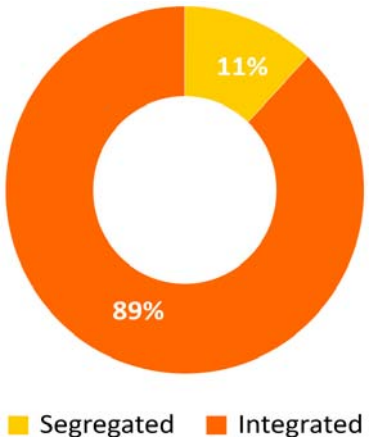


Figure 26

Key Performance Indices (KPIs)

The survey results show that many participants have established indicators for measuring the performance of Information Security function.

It is observed that respondents who have established "Somewhat" defined KPIs are almost as many as those who have established "Strong KPIs" (refer Figure 27). Nevertheless, considering the challenges involved in defining strong KPIs for information security, the fact that 87% of respondents have KPIs in place does emphasize the maturity of information security functions in the Indian industry.

It is also noteworthy that close to 67% of organizations that have implemented a decentralized information security function have "somewhat defined" KPIs or have not defined any.

STATUS OF KEY PERFORMANCE INDICES

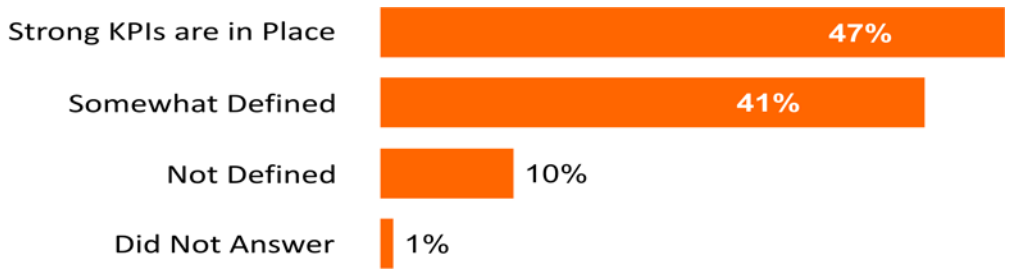


Figure 27

Security Practices

The security of electronic information is dependent on the policies and even more on the practices being followed. The survey results tabulated below (refer Figure 28) show the following key trends with regards to adoption of good practices amongst the participants.

- **Need-based-access:** Financial Services and IT/ITeS organizations are more cognizant of the risks related to providing unrestricted access to information assets.

Activities	Financial Services	IT/ITeS	Manu-facturing	PSUs	Telecom
Standard operating environment (Figures in %)					
Only non-administrative privileges granted	68	57	45	54	67
Standard operating environment	100	98	91	92	100
Hardware inventory	96	92	89	77	89
Authorized software	93	92	84	54	89
No access to non-official personal mail	71	41	36	38	44
No Access to public instant messaging	96	63	64	69	56
No Access to public social networking sites	96	67	61	62	67
Updated regularly with security patches	93	98	93	77	100
Updated anti virus definitions covering all computer systems	96	100	93	85	100
Secure browser settings that cannot be changed by the user	82	63	55	46	67
Filters for inappropriate web content	93	92	91	85	89
Only safe attachments to be sent through emails	86	94	86	85	78
Policies related to authorized programs/ applications either integrated to the system or communicated to the user	89	90	82	85	78

Figure 28

- **Non-business Applications & Web access:** Organizations are actively restricting access to web and messaging sources to mitigate risks such as information leakage, exposure to malware, etc.
- **Email Security:** Organizations unanimously look at implementing solutions that classify the attachments, based on their safety that can be circulated through mail.
- **End-User Security Controls:** PSUs seem to be laggards in implementing security controls in the end-user security such as application of latest patches on the systems, verifying authorization of software in use.
- **Online Access:** While respondents from the financial services segment seem to be leading in implementation of security controls, very few of them have implemented controls to restrict access to personal mails, public instant messaging or social networking sites.

Maturity of Security Program

PROMINENT TRENDS IN APPLICATION SECURITY INITIATIVES

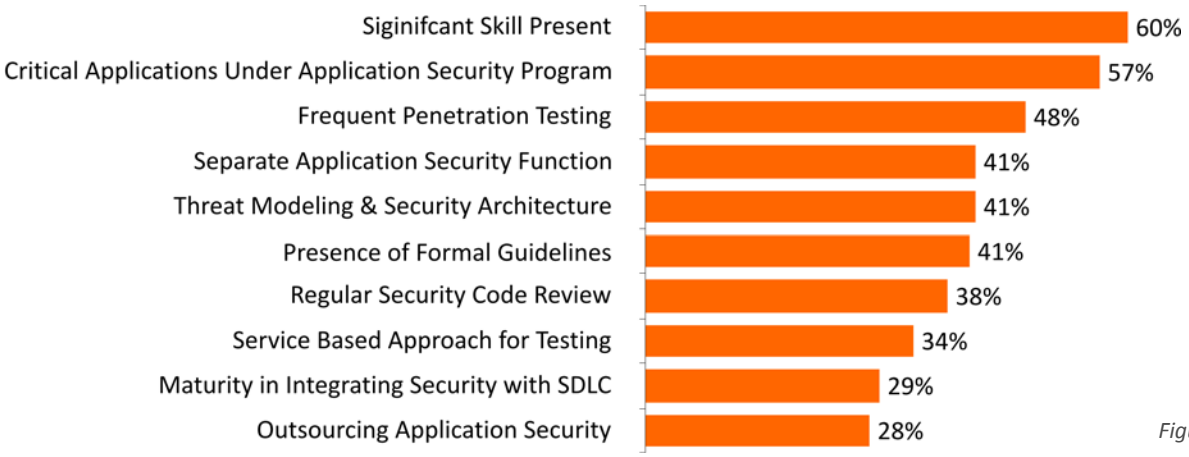


Figure 29

Application Security Initiatives

The survey results reveal that participants, specially from IT/ITeS, financial services and telecom, have established measures to secure their critical applications against vulnerabilities. Across industry segments, it is observed that 57% respondents have covered their critical application under their application security program (refer Figure 29), and 48% of them carry out frequent penetration testing. Significant number of organizations also adopt measures such as separate function for application security, architectural treatment to security at application layer and establishment of formal guidelines for secure application development and deployment. This indicates that application security function is maturing at Indian organizations

MATURITY IN INTEGRATING SECURITY WITH SDLC OF APPLICATION

Financial Services	43%
Telecom	33%
IT/ITeS	31%
Manufacturing	23%
PSUs	15%

Figure 30

Participants from Financial Service segments employ specialized skills for application security, 75% of them have developed in house skills in this area.

APPLICATION SECURITY PROGRAM MANAGEMENT

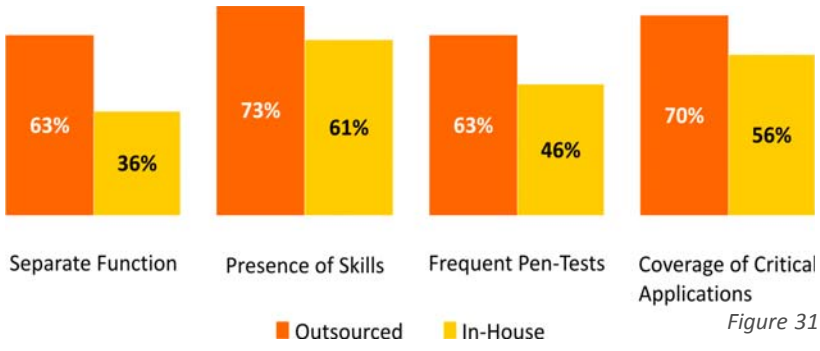


Figure 31

The Indian industry needs stronger emphasis on

integrating security in the application SDLC. Though there has been some focus on this, (refer Figure 30) more work still needs to be done in this area .

The survey also reveals that organizations are adopting "Outsourcing of the Application Security Tasks". Key application security initiatives showed a higher effectiveness in environments where related tasks were outsourced (refer Figure 31).

Data Security Initiatives

The more commonly implemented data security initiatives include controls such as appropriate policies, classification of information and securing access to data from privileged users. Survey results revealed that these have already been implemented by organizations across industry sectors. It is also evident that less than half of the respondents seem to have significant visibility over data (refer Figure 32).

One conclusion that may be drawn from these results is that while the basic policy-level control on classification of data may be in place, the effectiveness of such controls only improve when all information get classified according to its importance and criticality; as treated accordingly. However, the practical challenges in achieving this clearly highlight the need for adoption of automation and standardization of security practices.

Organizations from the IT / ITeS industry understandably lead when it comes to classification of information over respondents from other industry segments. This is largely driven straight by the need to isolate and securely manage information pertaining to different clients.

The results highlight that manufacturing organizations are laggards in terms of classifying information

PROMINENT TRENDS FOR DATA SECURITY INITIATIVES

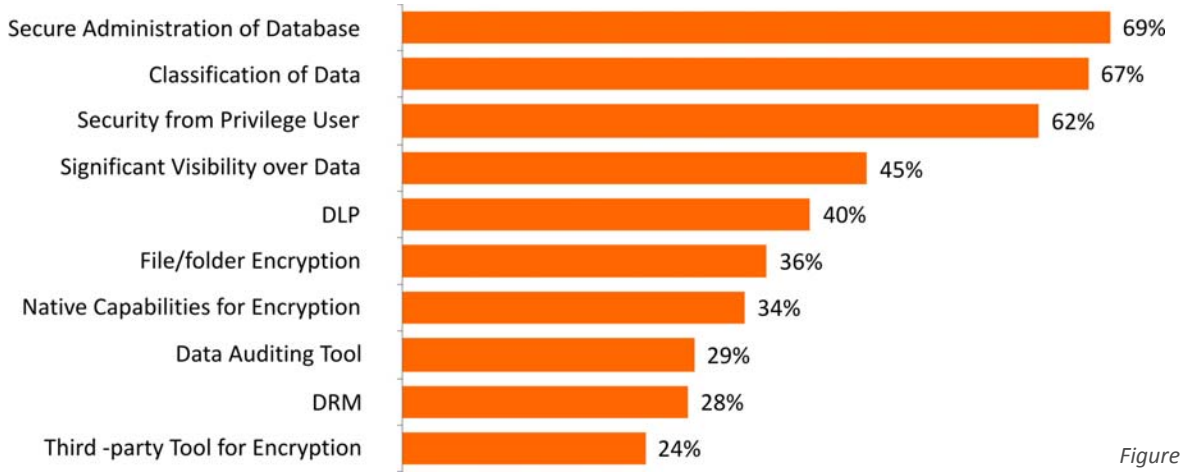


Figure 32

and secure administration of databases. This leaves them prone to risks of exposure of critical information residing in the databases of Enterprise Resource Planning (ERP) systems. (refer Figure 33 and 34)

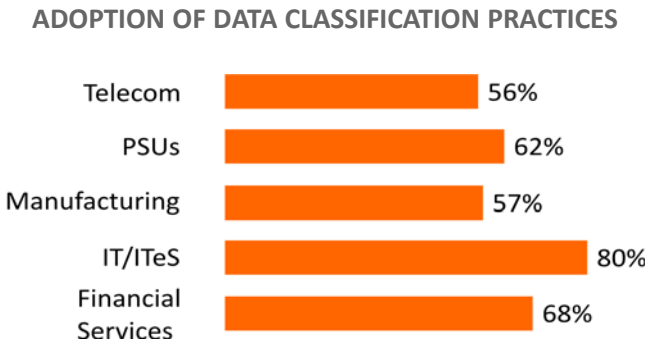


Figure 33

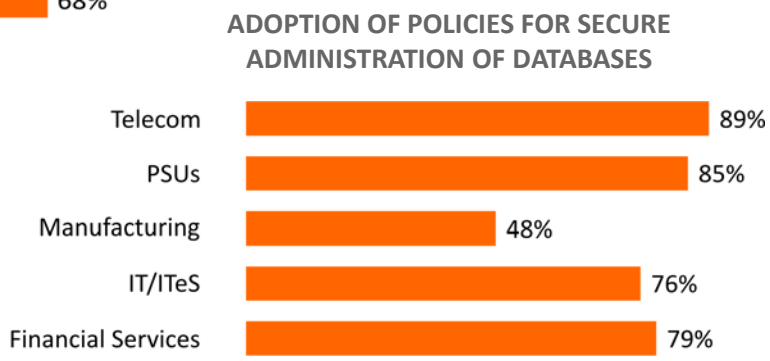


Figure 34

Disaster Recovery Practices

Eighty six percent of the survey respondents indicate that they have implemented a formal disaster recovery plan (DRP). However, there are organizations that have implemented only certain aspects of the recovery instead of having a comprehensive disaster recovery plan.

The survey also reveals that "Regular backup of critical information" is the most important activity covered under disaster recovery planning (refer Figure 35).

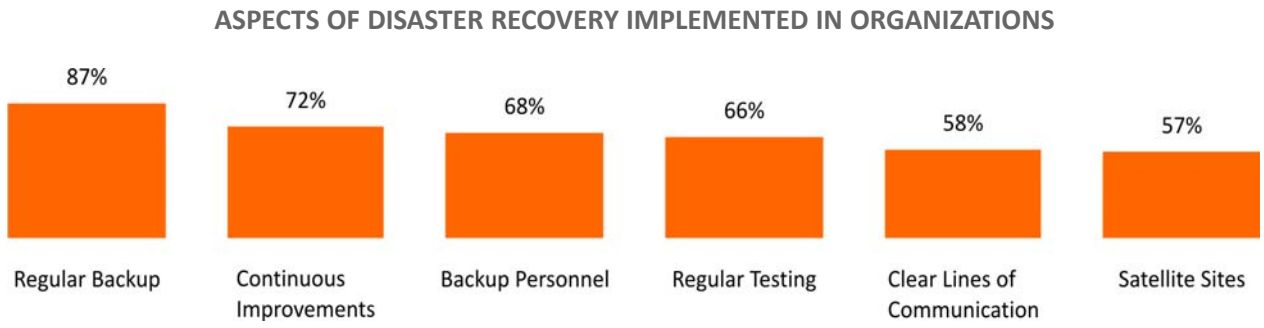


Figure 35

Integrating Business Continuity Planning with Human Capital

The survey results reveal that business continuity plans of a large majority of respondents give due importance to human capital. Several aspects including health and safety, communications, succession planning and training are already implemented as part of the continuity plans in such organizations.

An important factor in the success of any BCP is communication, and participants from manufacturing and PSU segments did not fair as well as others in this regard. (refer Figure 36).

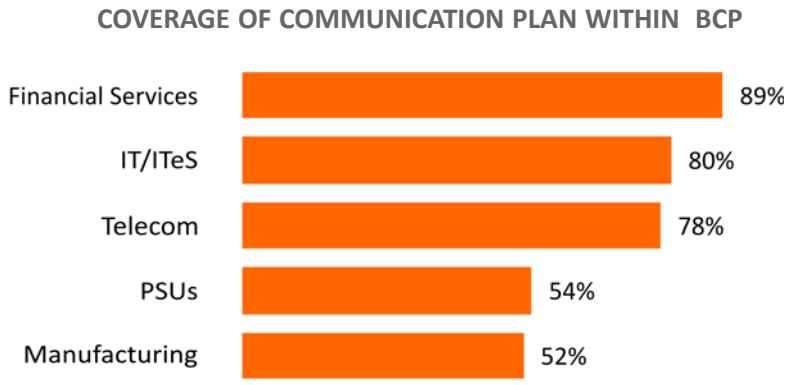


Figure 36

Convergence of Physical and Information Security

The survey results show that 2 in every 3 organizations are converging their Information and physical security functions. (refer Figure 37)

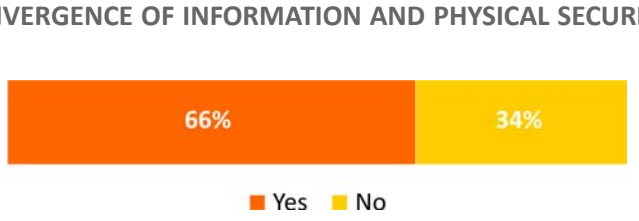


Figure 37

Security Technologies

The survey results indicate that the Indian industry has moved beyond just securing its perimeter and is considering leading technologies to protect end-points and data.

An analysis of the most widely-implemented tools in the Indian industry shows that while anti-virus and patch management are the most deployed tools. Security information and Event Management (SIEM), network security solutions such as SSL-VPN and data recovery capabilities are also widely accepted. (refer Figure 38).

A closer analysis of the security solutions being considered by the participants from IT/ITeS and financial services reveals that these two segments of the industry follow quite similar trends. Participants from both these industry segments are considering virtualization security and end-point security for implementation in the near future.

Public Key Infrastructure (PKI), SMS based authentication and Federated Identity Management solutions find few takers.

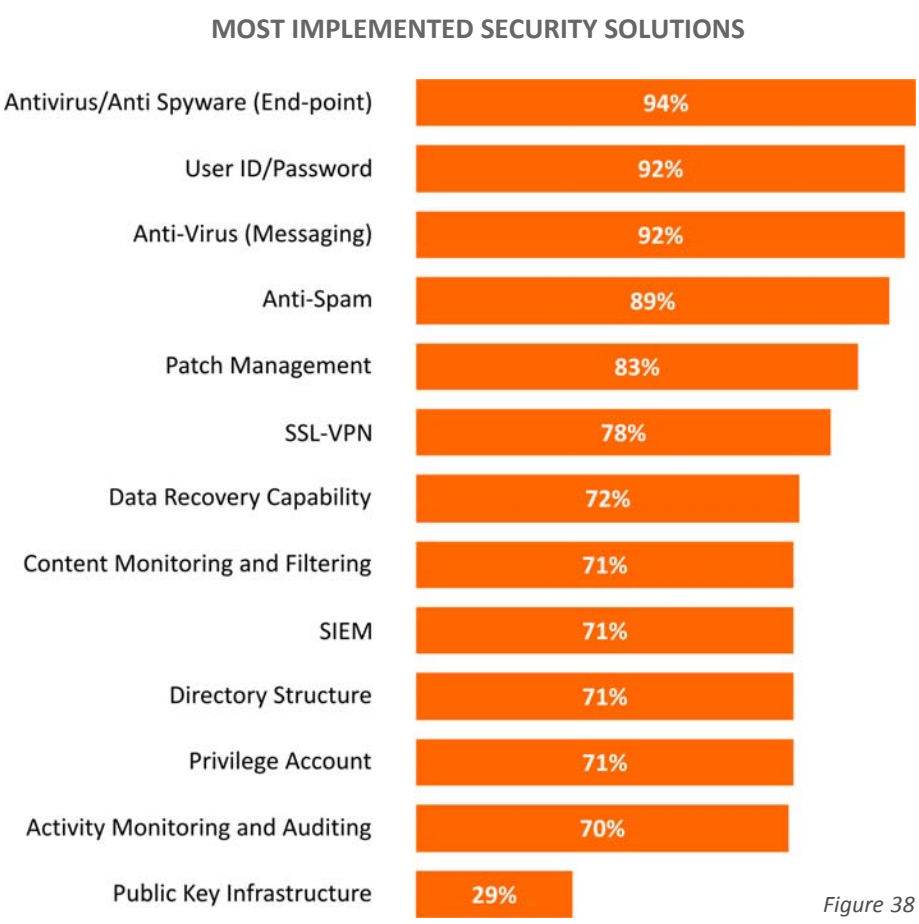


Figure 38

It was also observed that the industry is keenly following the developments in virtualization security, governance risk and compliance, Unified Threat Management solution and DLP.

The radar diagram on the next page depicts the level of industry acceptance of the various security solutions.

TECHNOLOGY ADOPTION TRENDS

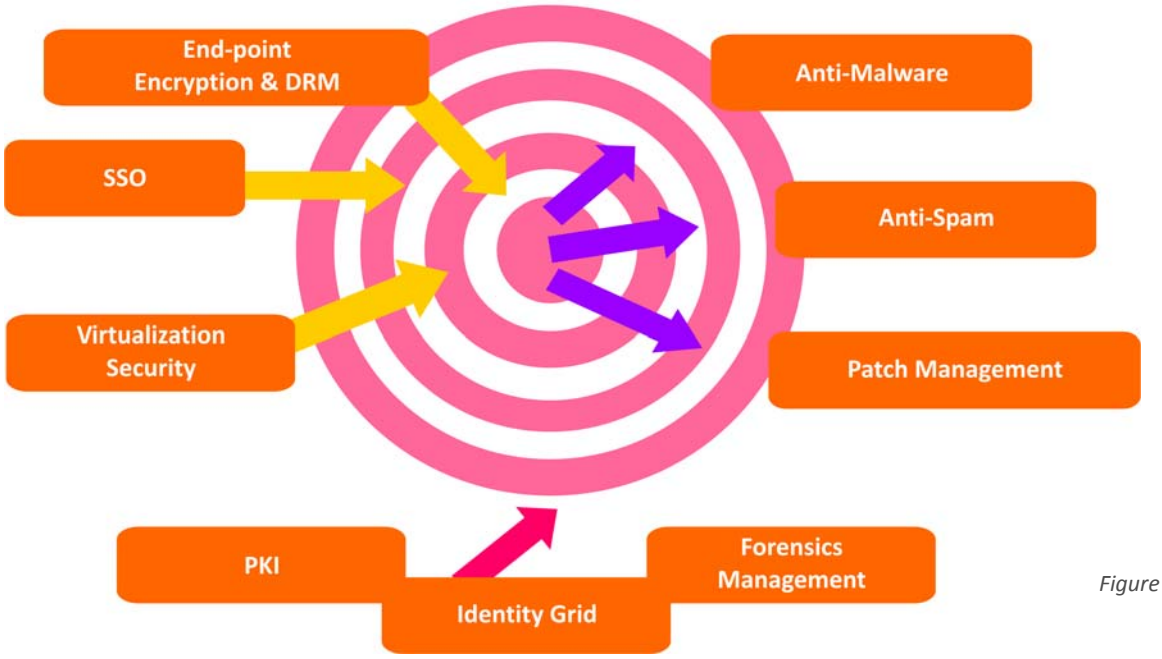


Figure 39

- ***Arrows pointing toward* the *center are active, approaching, and strengthening:*** *This includes tools that are being considered for implementation such as endpoint protection and virtualization security. The comparative proximity of the arrow to the center of the diagram indicates that it is already witnessing a high degree of adoption as compared to others.*
- ***Outward-facing arrows indicate already prevalent trends that will grow weaker in the future:*** *These include traditional security solutions including Anti-virus, Anti-Spam etc that have already been deployed and in future may only be a basic requirement for building further controls.*
- ***Arrows on the perimeter indicate weak trends:*** *This includes solutions that are yet to generate interest in the industry. Public Key Infrastructure (PKI), Identity Grid and Forensics Management may just be tools that have arrived a bit ahead of time for the industry to take full advantage of.*

Legal and Regulatory Ecosystem for Information Security

The survey results have unequivocally established that there is a concerted effort to address information security and data privacy concerns – be it at an organizational level or at a wider level through bodies such as DSCI and CERT-In. But a significant factor that is critical to the success of such initiatives is the overarching legal and regulatory ecosystem in which these organizations operate.

The Indian government has undertaken significant initiatives to strengthen the cause of information security and data privacy in the industry. IT Act 2000 and IT (Amendment) Act, 2008 establish the foundation that is imperative to creating an environment conducive to the security of information in business transactions. Empowerment of CERT-In through the amendment is another crucial step that will have far-reaching impact on ensuring effective implementation of the rules and guidelines established through the act. Through the survey we collected data on how the Indian regulatory environment is perceived by the Indian industry.

IT (Amendment) Act, 2008

Survey participants' perception about the influence of IT (Amendment) Act, 2008, on the information security and data privacy is positive. The industry is reasonably convinced about its effectiveness towards establishing a baseline for reasonable security practices within organizations. This perception is not plain optimism but is rooted in awareness of the compliance requirements that the IT (Amendment)

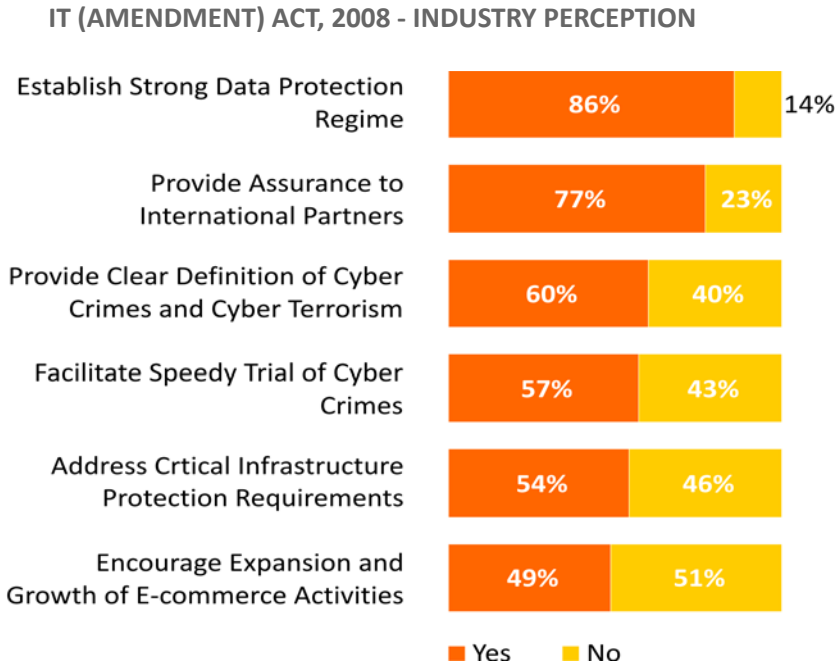


Figure 40

Act 2008 will mandate (refer Figure 41). This awareness may also be the reason behind the belief that the legislation will have a positive impact on the global perception of the Indian legal framework for data protection (refer Figure 40)

On the other hand, many participants expressed that the act itself may not be enough and had divided opinion on whether it can address operational issues such as providing protection to critical infrastructure, expediting trials and may not also have significant impact on the growth of eCommerce in India.

AWARENESS OF IT (AMENDMENT) ACT, 2008 COMPLIANCE REQUIREMENTS

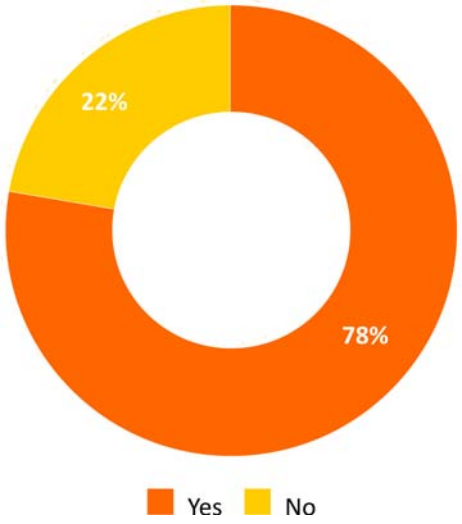


Figure 41

Significance of CERT-In in the Indian Information Security Ecosystem

CERT-In is a body that is widely recognized as an agency that can provide direction and guidance to the Indian industry for responding to computer security incidents and providing assistance in implementing proactive measures to reduce associated risks. This recognition is evident from participant's awareness of the same (refer Figure 42).

AWARENESS ABOUT CERT-IN

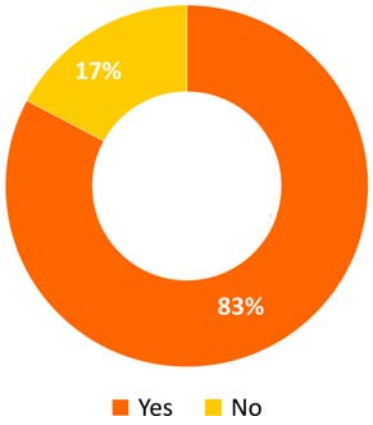


Figure 42

While CERT-In has been influencing the information security and data privacy initiatives in the Indian industry for some time now, the enactment of the recent amendment implies that it has an even bigger role to play (refer Figure 43).

AWARENESS OF THE ROLES AND RESPONSIBILITES OF CERT-IN AS PER IT ACT AMENDMENT

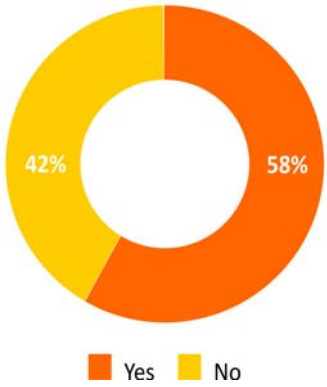


Figure 43

As per the survey results, the initiatives undertaken by CERT-In to assist organizations in addressing security challenges proactively, seem to be succeeding through its mailing list, which is widely subscribed by the industry.

More than seventy percent of the respondents subscribe to CERT-In mailing list and regularly visit the CERT-In site. This clearly indicates that organizations interact with CERT-In for advisory and guidance for responding to computer security incidents.

The survey revealed that most of the respondents perceive that key take-away from reporting such incidents is generating better understanding about the incident (refer Figure 45).

On the other hand only one third of respondents plan to interact with CERT-In to report incidents that they may encounter (refer Figure 46).

It is evident from the results that while organizations regularly interact with CERT-In for advisory however

there are concerns deterring organizations from reporting incidents. This may be due to perception about negative publicity.

In order to assist the industry better, CERT-In will have to address concerns and create better awareness in the industry on its role.

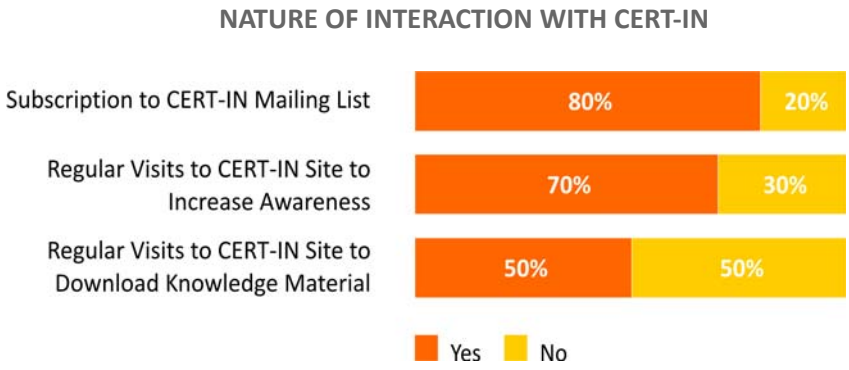


Figure 44

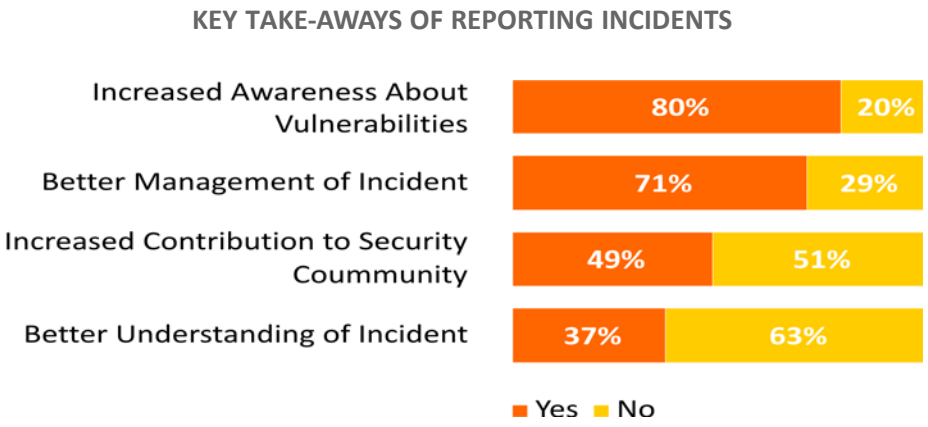


Figure 45

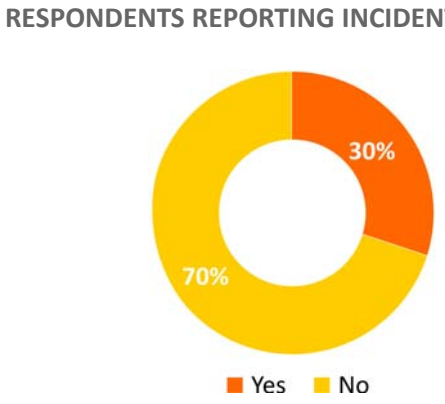


Figure 46

Epilogue

Conclusion

India is increasingly recognized as an important player in the field of IT, not only because of its leadership in providing IT services organizations across the globe, but also because of increasing adoption of IT by Indian organizations and by various government departments. For availing complete benefits of IT, both in the case of outsourcing industry and domestic industry, IT requires fine balancing of the risks associated with it. This survey captures how Indian industry is prepared to address emerging data security and privacy challenges. As it covers industry segments like IT/ITES, Financial Services, Manufacturing, Telecom and Public Sector Undertakings, it gives a fair insight into the state of data security and privacy in the Indian industry as a whole. Along with assessing industry initiatives, the survey also captures Government of India's initiatives to establish an appropriate legal framework. This survey, thus, helps understand the ecosystem as it obtains in India; led by industry on the one hand, and supported by the government, on the other hand, for enhancing security and privacy culture.

Security is now an important function of an organization's ecosystem, becoming a top priority across all Industry verticals. Privacy is also attracting attention of organizations, reflecting increasing concern of end users, be it Indian nationals or end customers of organizations that are outsourcing their operations to India. While facing the evolving challenges, the industry is seen adhering to leading practices and acquiring newer technology options. Industry does not appear to be restrained in adoption of trends like mobile computing, wireless technologies and virtualization, because of security concerns. They tend to adopt appropriate security solutions to address the security challenges that arise out of the changed IT ecosystem. In comparison to the global trend, Indian industry is seen to be in the process of maturing their programs in application and data security. The survey specifically selected these two areas as we witness current momentum of security concentration at application and data layers. Although key industry verticals like IT/ITES, Financial Institutions and Telecom are taking leadership positions as compared to others, the overall position is improving in terms of enhanced level of preparedness.

The survey also captures the positive perception of the Indian industry about recently enacted IT (Amendment) Act, 2008 and its importance of establishing strong data protection and cyber security regime in the country.

The results of the survey will help organizations understand the trends to benchmark their security and privacy initiatives and may also help in articulating the current state of Indian industry, and in perceiving the national level picture of the current level of preparedness. The survey results will be of particular interest to national level initiatives. On the one hand, it gives critical inputs to DSCI and NASSCOM to formulate their strategy and programs; while on the other hand, it gives key information to CERT-In (DIT) that may help the government formulate policies that ensure a high level of assurance.

Key Messages

The survey results provide insight into the information security and data privacy environment within the Indian context. There is evidence that validates general perceptions and there are some eye-openers as well.

- Information security has taken a prominent position in hierarchy of participating organizations.
- Respondents seem to have implemented basic information security solutions and are keenly following the progress of technology that will enable securing data
- Extended business environment including mobile workforce, third-party vendors, partners and other stakeholders is posing a significant challenge in securing of information assets
- Respondents from the IT/ITeS and financial services seem to be better prepared to address information security and data privacy challenges
- Respondents from the above two segments also show greater propensity to adopt new solutions and practices whereas participants from Manufacturing and PSUs appear to be laggards
- There is evident trend towards greater maturity in application security function in participating organization
- Information security controls and physical security controls are converging

DATA SECURITY COUNCIL OF INDIA

A **NASSCOM®** Initiative

L: Niryat Bhawan, 3rd Floor, Rao Tula Ram Marg, New Delhi - 110057, India

P: +91-11-26155071 | **F**: +91-11-26155070 | **E**: info@dsci.in | **W**: www.dsci.in

Designed & Printed by Swati Communications 9213132174