The threat within

A study on insider threat by DSCI in collaboration with PwC

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

pwc

About Data Security Council of India (DSCI)

Data Security Council of India (DSCI) is a focal body on data protection in India, setup as an independent Self-Regulatory Organisation (SRO) by NASSCOM®, to promote data protection, develop security and privacy best practices & standards and encourage the Indian industries to implement the same. DSCI is engaged with the Indian IT/BPO industry, their clients worldwide, Banking and Telecom sectors, industry associations, Data Protection Authorities and other Government agencies in different countries. It conducts industry wide surveys and publishes reports, organizes data protection awareness seminars, workshops, projects, interactions and other necessary initiatives for outreach and public advocacy. DSCI is focused on capacity building of Law Enforcement Agencies for combating cyber crimes in the country and towards this, it operates several Cyber labs across India to train police officers, prosecutors and judicial officers in cyber forensics.

Public Advocacy, Thought Leadership, Awareness and Outreach and Capacity Building are the key words to continue to promote and enhance trust in India as a secure global sourcing hub, and also to promote data protection in the country.

For more information about DSCI or this report, please contact:

Data Security Council of India
Niryat Bhawan, 3rd Floor
Rao Tula Ram Marg
New Delhi – 110057
India

Phone: +91-11-26155070
Fax: +91-11-26155072
Email: info@dsci.in

Foreword

Insider threats originate from within the organisation. The trusted employees, contractors, partners and suppliers are the source of these attacks. Some of them are as trusted as privileged users. Hence, they can cause more damage. Verizon 2010 Data Breach Investigation Report attributes 48% data breaches to insiders. Privilege misuse was found to be responsible for half of all the insider attacks.

Why are insider threats of interest to us in the IT/BPO industry? This is because as service providers, we process vast amounts of data of clients, from different parts of the world, that crosses borders as part of business process outsourcing. A small data breach attracts wide adverse publicity. Hence, the industry has to be on guard. Likewise, banks and financial institutions are a target of frauds caused more and more by insiders. The number of insider frauds may be small, but their value is significantly higher than that caused by external attacks.

It is generally thought that while the external threats can be handled by deploying appropriate technology solutions, controls, and by developing the required processes, the internal threats are difficult to track. But this is only partially true since there are behavioral indicators that companies can look for in the people who work there. This can be supplemented by tracking their footprints in the logs, to develop added insight. However, all parts of the organisation such as HR, Administration, Legal, Technology Operations, Finance, and Lines of Business must work together to identify the suspects and monitor their behavior. It requires planning ahead and addressing legal issues, policy issues, and employee privacy issues. This clearly implies that best practices for addressing insider threats must be used on a regular basis.

It is with this in view that DSCI partnered with PricewaterhouseCoopers (PwC) in this study. The report is based on a survey of service provider organisations and client organisations and highlights some interesting findings, reflecting the perspectives of both the service providers and clients.

I would like to acknowledge the team effort of DSCI and PwC in conducting this study, and creating a useful analysis. I hope this report will generate interest among service providers and clients and will provide inputs and direction for managing insider threats.

Dr. Kamlesh Bajaj
CEO, DSCI

Message

The IT/BPO industry in India has proven itself beyond any measure of doubt by providing significant cost savings, higher quality products and processes and improved operational performance. At the same time, it also deals with challenges relating to data security and protection from insider threats. This, when combined with increasing regulatory pressures, make insider threat a key challenge for the IT/BPO industry in India.

The insider threat is real and very likely, substantial. Insiders have a significant advantage over others who might want to harm an organisation. They can more easily bypass physical and technical security measures designed to prevent unauthorised access. They are not only aware of the policies, procedures and technology used, but are often aware of the vulnerabilities in their organisation.

This study, conducted jointly by Data Security Council of India (DSCI) and PricewaterhouseCoopers (PwC), assesses the various aspects of insider threats such as insider profile, motivation factors, modus operandi, roadblocks and some best practices which can be deployed to mitigate these incidents.

We trust that this report will help in creating better understanding of the challenges and areas that need to be addressed in order to handle insider threats. We look forward to receiving your comments and feedback to make our future studies more comprehensive and interesting.

Sivarama Krishnan
Executive Director, PwC

Contents

Highlights

The report provides insights into the insider threat environment of the IT/BPO industry in India and the efforts taken by service providers and their clients for mitigating insider risks.

Some of the key findings of the report are as follows:

- All service provider organisations believe that current employees are the primary source of insider incidents.
- More than 50% of the service provider organisations revealed that insiders who do not work in IT department and consequently do not have privileged access have carried out insider incidents at their organisations.
- All the client organisations have mandated their service providers to conduct background check of their employees but employee verification processes are not standardised as service providers are subject to client-driven criteria.
- Service provider organisations are exploring new and innovative methods for employee screening such as social networking and credit card history check.

- As per 89% of the service provider organisations, behavioural motivation to break existing norms is the primary motive that leads to insider threat. However, 75% of the client organisations believe that personal financial gain is the prime motive for insiders at service provider organisations.
- All the client organisations believe that lack of education & awareness is a major barrier in addressing insider threats in service provider organisations. However, only 33% of the service provider organisations agree with the same.
- More than half of the respondents from the service provider and client organisations believe that social engineering and 'someone else's computer account' is used by insiders to commit a breach in service provider organisations.
- As per the survey, 89% of service provider organisations resolved the cases of insider incidents internally, without involving a legal agency. Only 22% service providers initiated legal action against perpetrators.
- Almost 67% service provider organisations have experienced that insider incidents carried out in their organisations were due to unintentional exposure of private and sensitive information. This has been strongly supported by the client organisations (75%).
- Audit and review is still the primary source of identification and learning about insider incidents with around 89% service provider organisations and 75% client organisations being alerted about insider incidents at service provider organisations through this method.
- More than 88% of the service providers have defined the insider incident response plan to manage insider incidents in their organisations.
- All client organisations mandate periodic security awareness and risk assessment on their service providers.
- Seventy five percent client organisations have signed individual non-disclosure agreements with the service provider employees.

Introduction

Background

Security breaches and the compromise of sensitive information are very real concerns for any organisation today. Studies have shown that though the likelihood of the attack from insiders may be very low as compared to external threats, the magnitude of the impact is at least 10 times more than that of the total impact an external attacker can cause. This is because an insider attack is committed by people who know the organisation's most sensitive secrets and vulnerabilities and have access to its systems. In most cases, breaches by insiders are committed by individuals who have no intention of doing anything wrong and then there are some who are motivated by greed, selfishness, or antagonism towards the management.

Data Security Council of India (DSCI) and PricewaterhouseCoopers (PwC) have jointly conducted a study to understand the challenges and risks associated with insider threats.

Objective

The study has been conducted to understand the security posture of the Indian IT/BPO industry from an insider threat perspective and the perceptions of the client organisations on the same. The detailed objectives of the study are as follows:

- Provide better understanding of insider threats and an enhanced ability to manage associated risks
- Assist organisations to plan, prioritise and manage the unknown insider threat incidents
- Understand the modalities of insider threats, find means to detect these threats and plan preventive measures to deal with such threats
- Help staff, management and human resource personnel understand the social, behavioural and motivational factors underlying insider threats
- Provide insight to the technology, procedures and other safeguards, to thwart any attempt of insider threats

Approach

The study was conducted for the IT/BPO industry with a three-pronged approach:

1. ***Industry survey and inputs:*** A structured questionnaire was shared with the senior management who are primarily responsible for their organisations' information security initiative. This was followed by an interview, face-to-face or telephonic, to further collate their inputs and experience.

   The respondents to this survey were identified from IT/BPO service providers and their client organisations. Two survey questionnaires were prepared to understand their respective perspectives and experiences on the circumstances which lead to insider threat and the current level of protection or mitigating controls that are deployed. A total of 13 respondents (nine service providers and four client organisations) were surveyed and their responses analysed. The report is based on the following definitions:

   - Client organisations: Organisations that have outsourced some of their core or support processes to IT/BPO service providers in India

   - Service provider organisations: IT/BPO organisations that provide outsourcing as a service and support a part or a complete process of the client organisation

2. ***Analysis of insider theft cases:*** An analysis of various insider cases available in the public domain or reported by Law Enforcement Agencies in India was carried out in order to correlate with the survey findings. In all, more than 20 such cases pertaining to insider threats or attacks were analysed.[1]

3. ***Insider threat secondary research***: Secondary research was conducted by studying various surveys and research reports to understand the insider threat landscape.

Interpreting the data

The graphs in this report have data for the two respondents viz. client organisations and service providers organisations.

- The data points marked as ***service provider organisations*** are the responses of the IT/BPO organisations surveyed. The numbers from service providers represent their interpretation about their own organisations with respect to insider threat.
- The data points which refer to ***client organisations*** interpret what the client companies surveyed feel or know about their service providers.

Disclaimer

The study provides an understanding of the contextual factors that influence the insider threat landscape. However, findings from this study cannot be generalised with any degree of confidence to a larger universe due to limited information available in the public domain and the limited number of respondents. We tried to reach out to several companies, inviting them to participate in this survey but got limited response because of the sensitivity and confidentiality of the issue.

[1] The case studies were analysed based on the Insider Threat Analysis Framework, covering the following aspects:

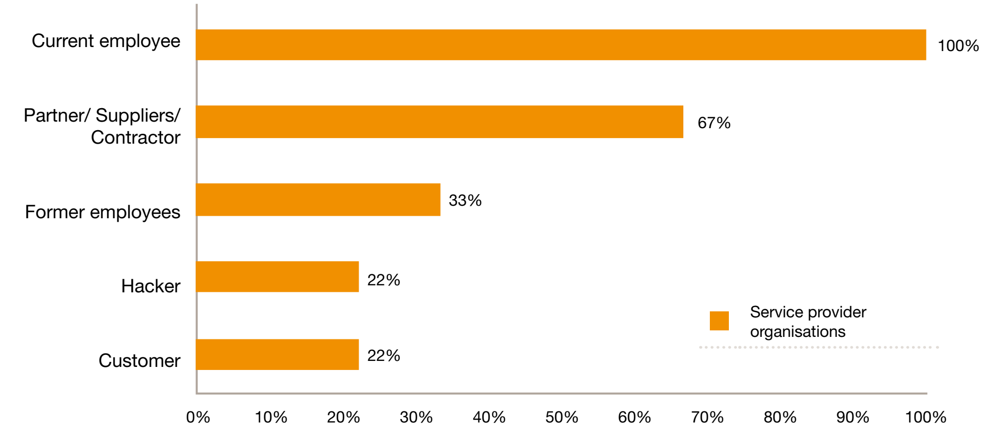
- **Why:** The underlying psychology behind the insider attack
- **When:** Period or phase during which the insider is most active
- **What:** The knowledge assets targeted by insiders
- **How:** Strategy or mechanism used to carry out such theft
- **Who:** The suspect or perpetrator

Profiling the insider

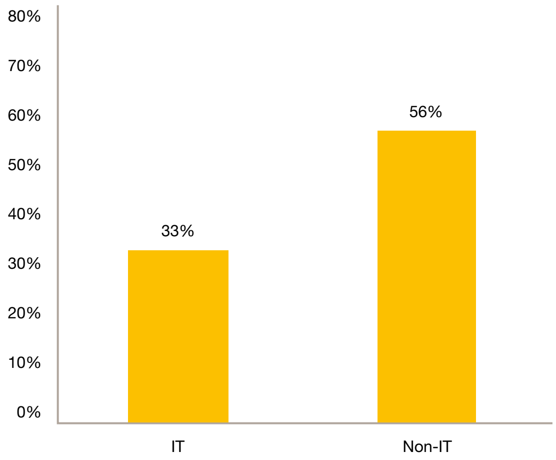
The 'real' threats

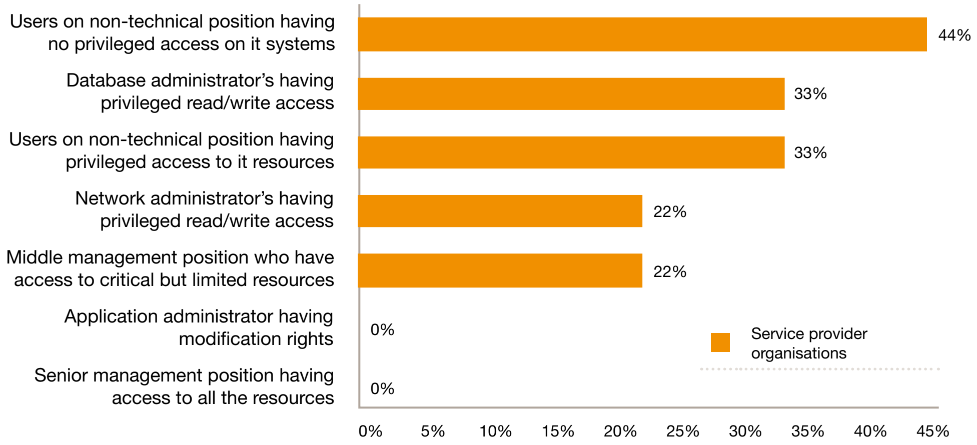
It is important to understand the profile of the people involved in the incidents related to insider threats. All respondents at service provider organisations believe that current employees are the primary source of insider incidents. This is primarily because existing employees are privy to confidential/sensitive information and have legitimate access to internal systems. The same holds true for the organisation's partners/suppliers/ contractors--the extended organisation, who by virtue of their day-to-day business interactions with their clients have privileged access. They have therefore been identified by 67% of the respondents as the likely source of security incidents in the organisation.

It is interesting to note that 56% of the respondents revealed that insiders who do not work in IT department and consequently do not have privileged access to the operating systems, databases, or the business applications, have carried out insider incidents at their organisations.



Insider Types





Surprisingly, not even a single incident was attributed to the senior management of the organisation. This was in contrast to our findings from secondary research, where senior management was found to be involved in a number of such incidents.

Almost 22% of the respondents believe that such incidents can be attributed to middle management which has access to critical but limited resources.

Case | Financial theft | Insider position: Financial functionary[2]

A CA joined the internal finance department of a leading Indian IT company. His role was that of a financial controller with the responsibility of maintaining the organisation's financial books with an additional charge of authorising external payments. His job profile gave him exclusive access to the company bank accounts.

Under the financial controller's responsibility, a large number of external payments were regularly done through online transactions. The CA misused this privilege and started to transfer funds for himself in small amounts along with other payment transactions. For every transaction made to external vendors, he transferred a small percentage to his personal (and his relatives') accounts all across the country. This continued for three years (till the fraud was detected). The transactions done within this period were so many that the total money siphoned off was close to US$ four million!! The fraud was detected due to a bank overdraft notice and investigations led to the arrest of the CA. The company was able to recover about US$ two million, with the help of Law Enforcement Agencies.

[2] Source: www.business-standard.com

Keeping a sharp eye

Background screening

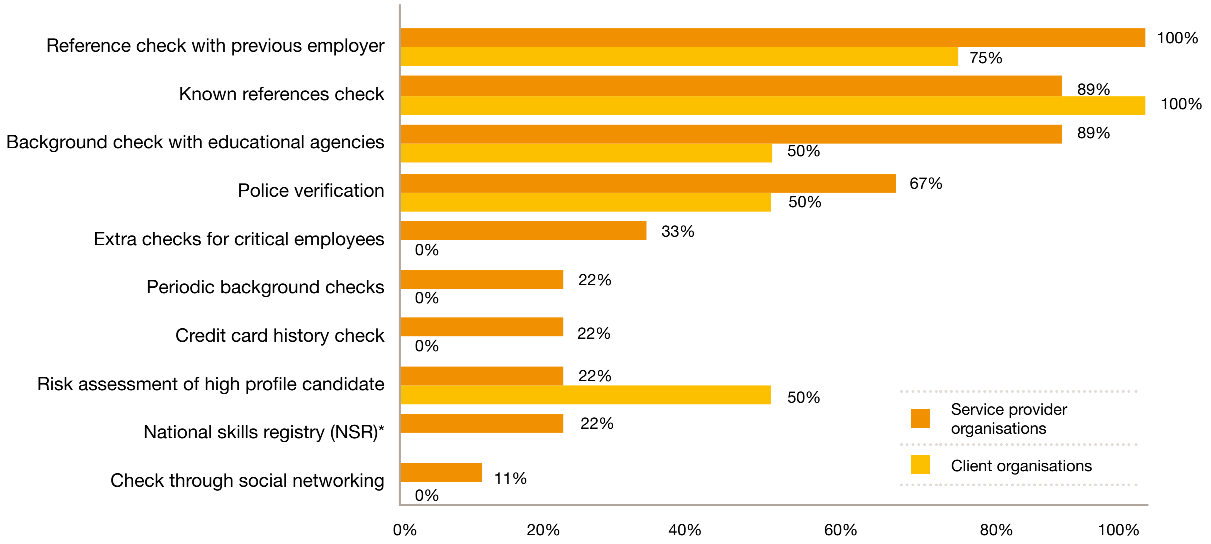
Employee verification processes are not standardised as they are subject to client-driven criteria. The concept of background screening has been in practice in the IT/BPO industry for some time. As per the survey, all client organisations firmly believe that background screening is one of the most critical factors towards preventing insider threats. They have mandated their service providers to conduct background checks for all their employees deployed on their processes. In almost all the cases, background screening is conducted primarily by reference check, education verification or with previous employers.

100%

client organisation have mandated their service providers to conduct background check of their employees

Service providers are sometimes required to follow the processes that are aligned to their clients' policies and contractual requirements. Hence, the background screening processes in service organisations often vary from one client process to another.

Employee verification processes are not standardized as they are subject to client-driven criteria



* Not applicable for client organisations

It is encouraging to note that 22% of the service provider respondents use the National Skill Registry (NSR) to conduct employee screening. To date, more than 8.5 lakh professionals have already registered in NSR and 100 leading IT/ BPO companies representing more than 60% of the employee strength of the industry are participating in the NSR system.[3]

Although client organisations are enforcing tried-and-tested screening methods such as known reference check, background check with educational agencies and reference check with previous employers, it is encouraging to note that service provider organisations are also exploring new and innovative methods for employee screening such as social networking or credit card history check.

Most of the service providers interviewed said that they relied on third-party agencies for conducting background checks.

Some critical hurdles identified in the background screening process are as follows:

- There are no centralised police records/databases available for a comprehensive search on criminal inclinations or antecedents of a recruit/employee.
- Several organisations in India do not share information with third parties (verification companies) for screening purposes, as a matter of internal policy.

There is no doubt that the employee screening process has matured over time. However, to ensure that it continues to do so, it is imperative that service provider organisations treat this process as a risk assurance measure and not compromise it to meet recruitment numbers.

33%

service provider organisations are using new and innovative techniques such as social networking or credit history check for employee screening

[3] https://www.nationalskillsregistry.com/

The driving force

Motivational factors

The survey revealed that an insider can be motivated to commit a crime due to a number of reasons, viz. information gain, personal financial gain, a new job, unsatisfactory appraisal or unmet professional expectations, an urge to prove oneself, feeling of entitlement, dissatisfaction with supervisor, etc.

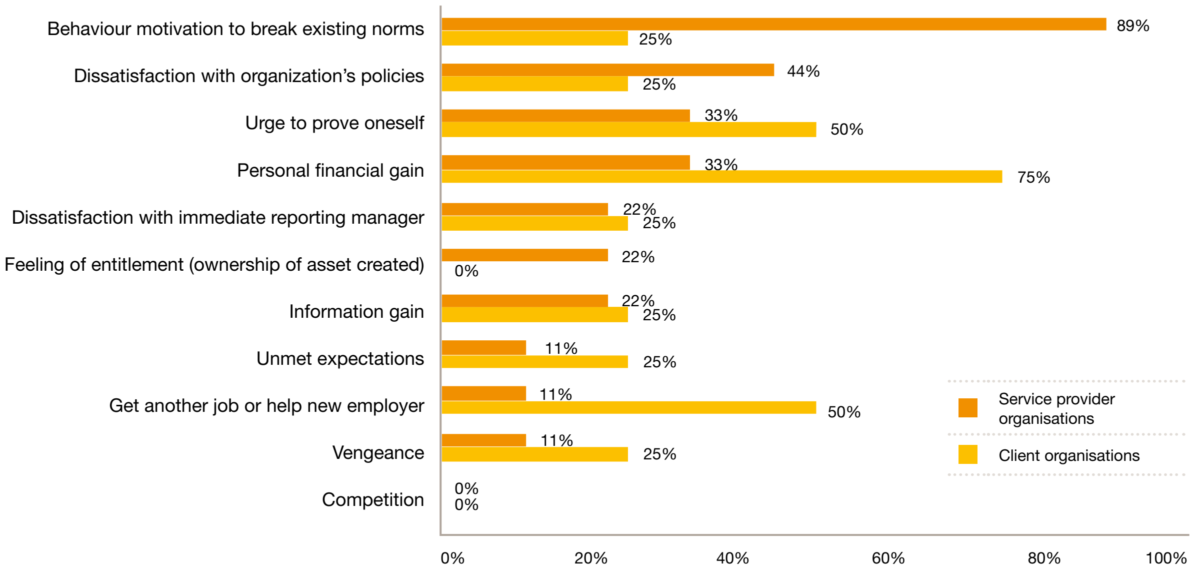
As per 89% of the service provider organisations, behavioural motivation to break existing norms is the primary motive that leads to insider threat. This might be due to the predominant youth mix in the IT/BPO industry.

On the other hand, 75% of the respondents in the client organisations believe that personal financial gain is the prime motive for insiders at service provider organisations to carry out illicit activities.

89%

service provider organisations have revealed that the urge to break existing norms is a single biggest factor leading to insider threat

Motivational factors



Dissatisfaction with organisation policies was rated as the second-most probable reason that leads to insider threat as 44% service provider organisations highlighted this as a concern. However, in contrast, 25% of client organisations believe this to be a reason for insider threat at service provider organisations.

It is encouraging to note that not even a single respondent in service provider organisations considers competition as a driving force for insider threat. This observation is supported by client organisations.

Interestingly, most of the factors such as dissatisfaction with organisational policy, dissatisfaction with immediate supervisor, feeling of entitlement, urge to prove oneself, breaking existing norms and unmet expectations, that lead to insider threats can be controlled. This means that by understanding such (controllable) motivational factors, an organisation can tune its policies to contain insider incidents.

60% motivational factors leading to insider threat are controllable

Case | Credit card fraud[4] | Motivation: Personal financial gain

Ecommerce transactions on the internet require validation of the authenticity of the credit card purchase. These activities are usually done by third-party organisations. In order to achieve this, there are multiple authenticity checks that have to be done in order to allow a transaction e.g. mapping of names, addresses, Personal Identification Numbers (PIN), credit card numbers (VISA/MasterCard, etc), etc. In this particular case[5], an organisation was engaged in the verification of the internet-based buyers for a large number of websites. A web designing company started an ecommerce transaction page for those who wanted to avail of their website designing services online, and availed the services of this credit card data transaction processing organisation. The services to the website designing firm were started soon after and the company made multiple transactions in subsequent months, amounting to approximately ₹ 300,000. The transactions suddenly stopped and no more transactions were recorded after almost six months.

After six months, the credit card companies started receiving charge-backs from card-holders, denying using the web designing services for which they were being charged. Upon investigation, it was found that the web design company's owner's son detected an anomaly in the transaction processing company's systems, and was able to extract the credit card and identification details of customers of the credit card companies. The owner's son defrauded the customers by assuming their identities charged their cards to their website designing services and absconded with the money. After much activity, he was apprehended by the Mumbai Police nearly a year after the incident was reported. He's been booked for cheating under Section 420 of the Indian Penal Code.

[4] Source: www.indiaforensic.com

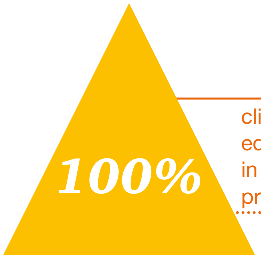
[5] C2002-2003

The roadblocks

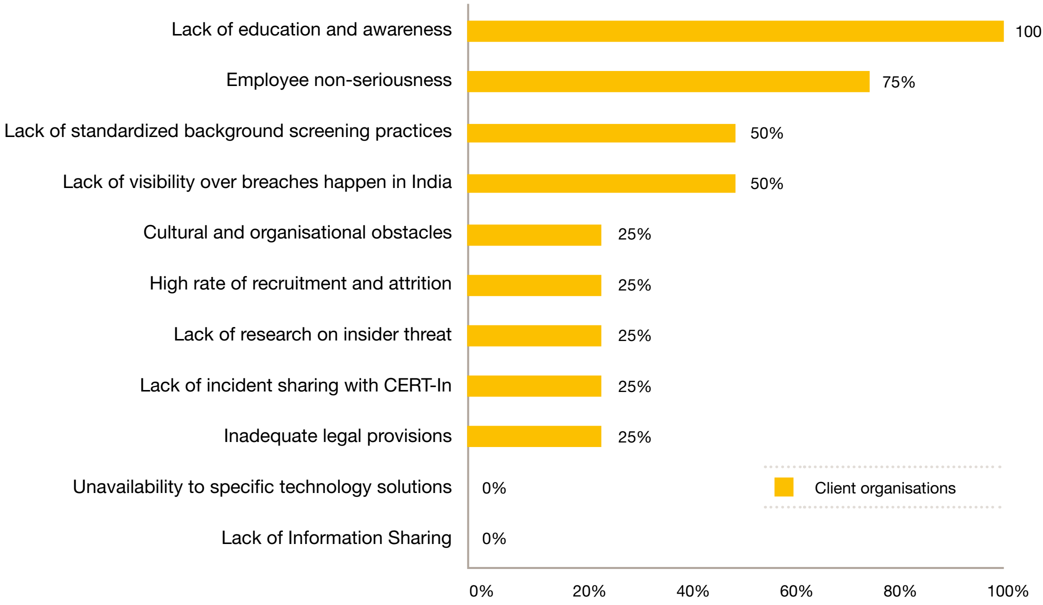
Obstacles in prevention

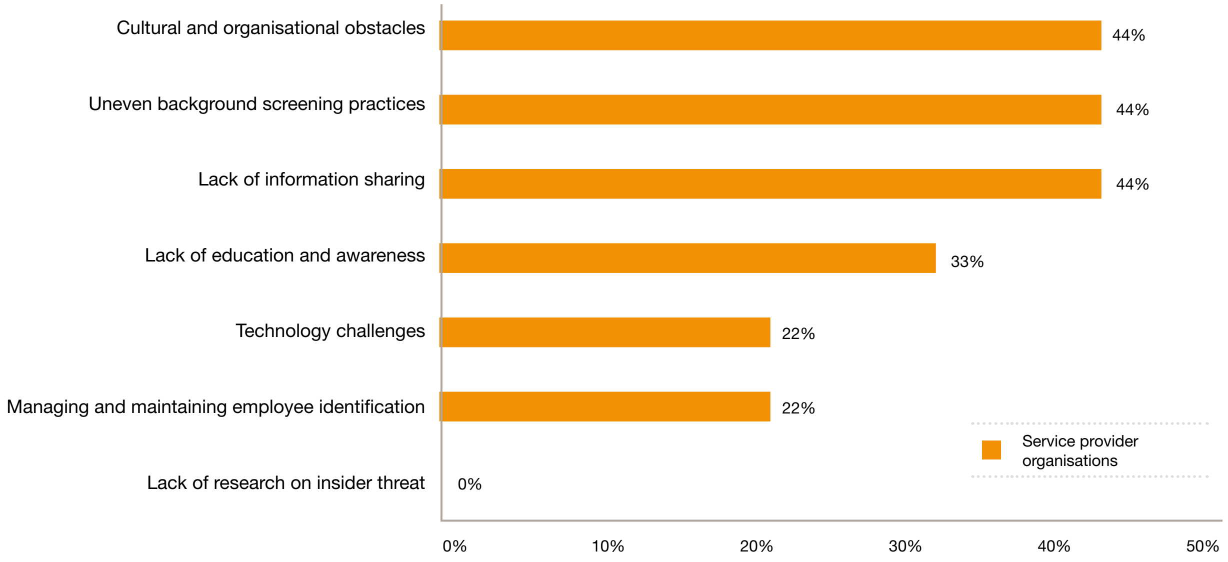
Any security breach in IT/BPO companies in India results in damage to India's image as a secure global sourcing partner of companies around the world. Therefore, service provider organisations, in many cases, have implemented controls that are even more stringent than what have been deployed by their client organisations. For example, BPO employees (agents) in India are required to deposit everything that could lead to data theft, like mobile phones, PDAs, pens and notebooks, while entering the premises.

All client organisations believe that lack of education and awareness is a major obstacle in addressing insider threat in service provider organisations. However, only 33% of all service provider organisations have highlighted lack of education and awareness as obstacle.



client organisations believe that lack of education & awareness is a major barrier in addressing insider threats at service provider organisations





Both, the service providers as well as client organisations agree that lack of standardisation of the employee screening process is one of the obstacles in addressing insider threat at service provider organisations.

Lack of insider threat-related information-sharing is also one of the major obstacles faced by service provider organisations (44%). This may be due to the fear of negative publicity, sensitivity of the incidents and lack of collaboration within the industry vis-à-vis insider threats.

We have seen a paradigm shift in the management focus towards information security in the IT/BPO industry. Today, information security frequently finds place in the boardroom agenda. This is also reflected in the survey findings, wherein none of the service provider organisations identified limited or no support from their executive management as a barrier to good security measures.

However, the techniques that can be used to address insider threats are not the same that can effectively repel an external threat. Addressing the roadblocks for effective insider threat management demands a comprehensive approach that must include awareness, education, policy, culture and technology. In addition, companies need to proactively address perceived shortcomings of their individual corporate cultures and communicate with employees on an ongoing basis so as to enforce sustainability in the overall process.

The modus operandi
Mechanisms used by insiders

More than 55% of the service provider organisations believe that social engineering is used by insiders to commit a breach. This has been supported by client organisations, with 50% of the respondents agreeing that social engineering can be used to commit a breach at service provider organisations.

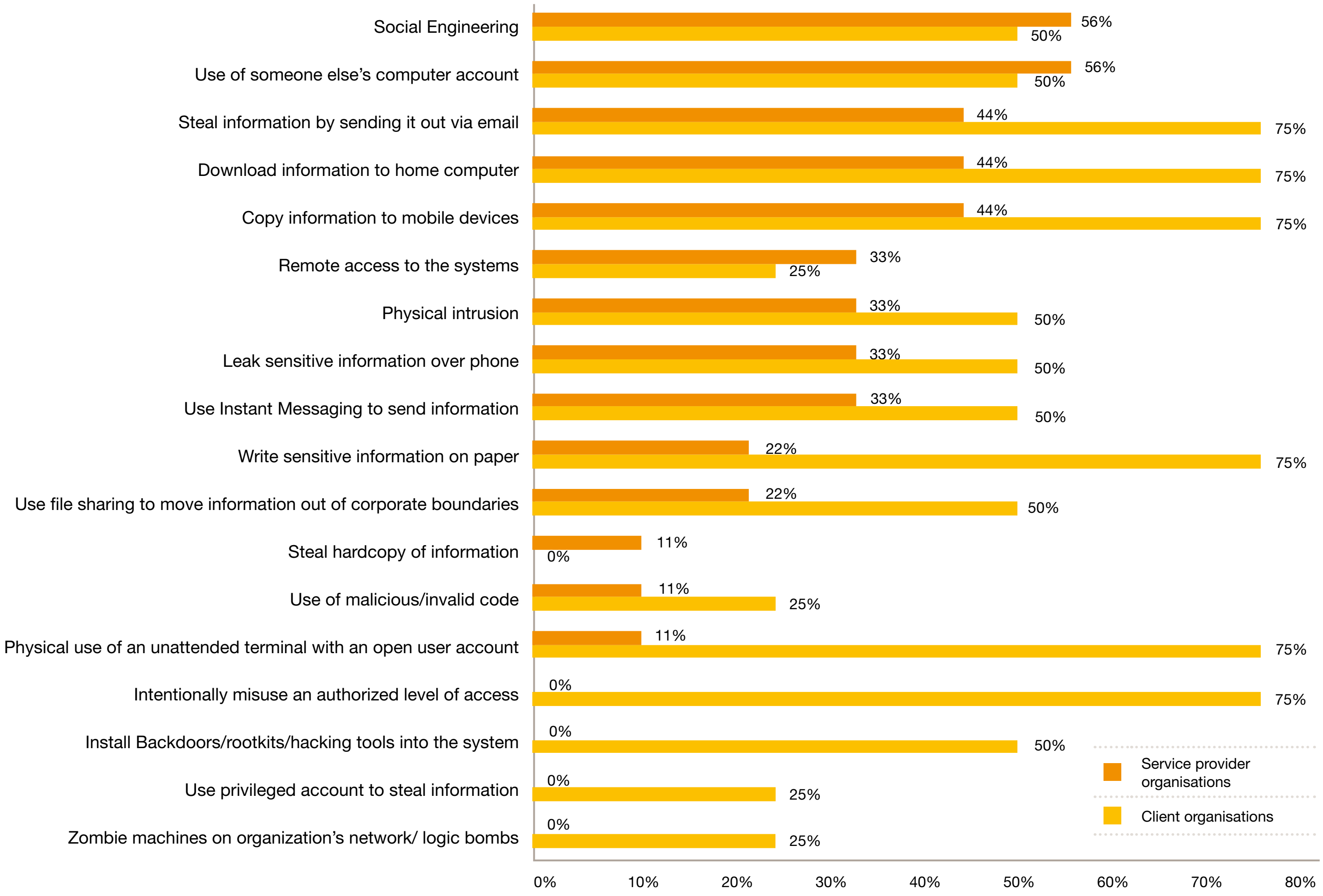
Almost 75%, of the client organisations believe that insiders at service provider organisations used mechanisms such as copying of sensitive information on mobile devices like USB drives, PDA, mobile or portable handheld devices, sending information out via email and writing sensitive information on paper. It is interesting to note that such perceptions exist among client organisations even though most of the BPO service providers are supposed to have strong technical controls in place such as, restrictions on the use of paper/pen in the production area, blockages of all external interfaces including restriction on the usage of portable devices such as USB and mobile devices. All the service provider organisations surveyed have physical security controls for mobile media.

Around 50% client organisations believe that insiders at service provider organisations commit breach using someone else's computer account. This has been supported by 56% of the respondents from service provider organisations. This clearly highlights the need for information security awareness and training.

More than ***55%*** of the service provider organisations believe that social engineering is used by insiders to commit a breach

More than ***50%*** client and service provider organisations believe that insiders use someone else's computer account to commit a breach at service providers

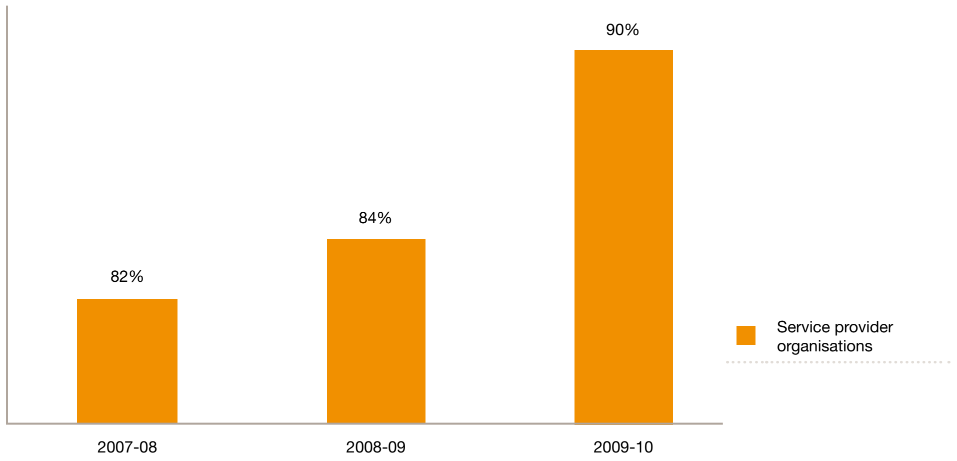
It is interesting to note that none of the service provider organisations believe that technical mechanisms such as logic bombs, installing backdoors, rootkits, etc. are used to execute breaches.



Patterns and trends

Incidents and actions

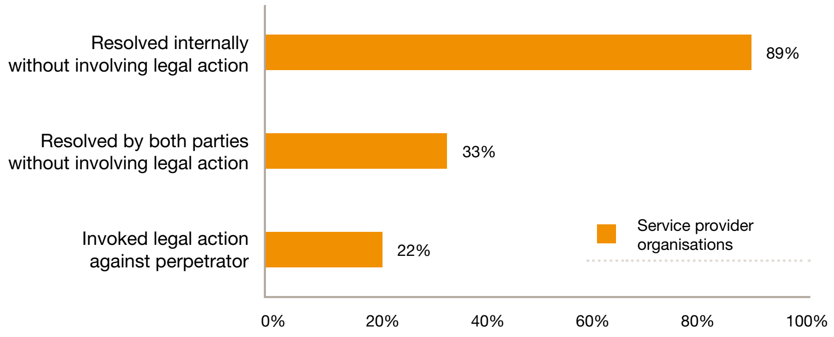
Insider incidents as a percentage of total security incidents



As per the survey, 89% of service provider organisations resolved the cases of insider incidents internally, without involving a legal agency. Only 22% service providers initiated legal action against perpetrators. The main factor for unwillingness of service provider organisations, as revealed by the survey, to report incidents to Law Enforcement Agencies is insufficient level of damage to warrant criminal charges, highlighted by 44% of the service provider organisations.

As per 75% of the client organisations, service provider organisations should inform the Law Enforcement Agencies about the insider incidents, in addition to reporting it to business partners (75%) and customers whose information is compromised (50%).

89% service provider organisations resolved the insider incidents internally without taking legal action



The attack vectors

Security threats from Insiders

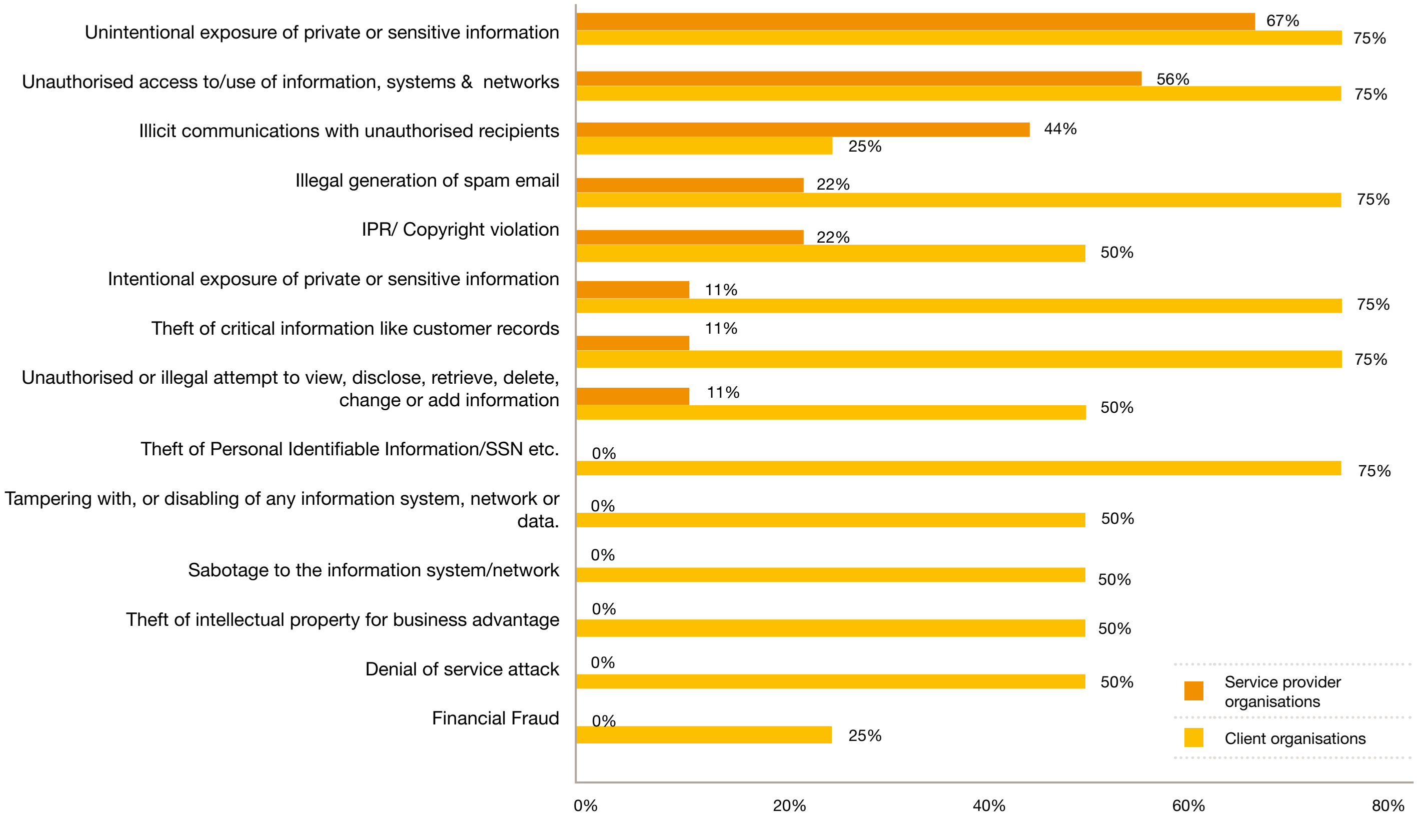
It is critical to understand the type of insider security threats in order to define the mitigation strategies. Almost 67% service provider organisations have experienced that the insider incidents carried out in their organisations were due to unintentional exposure of private and sensitive information. This has been strongly supported by the client organisations with 75% of the respondents agreeing that unintentional exposure of private and sensitive information is a security threat at their service providers.

In **67%** service provider organisations insider incidents occurred due to unintentional exposure of private and sensitive information

Around 75% of the respondents from client organisations believe that theft of critical information like customer records is a possible security threat from the insiders at service provider organisations. However, only 11% of the service provider organisations have faced such a threat from insiders.

It is interesting to note that only 25% of the client organisations believe that financial fraud can be conducted by the insider at service provider organisations and supporting this belief is the finding that not even a single respondent in the service provider organisations so far has witnessed financial fraud because of insiders.

In only ***11%*** service provider organisations insider incidents occurred due to intentional exposure of private and sensitive information



The revelation

Detection and corrective action

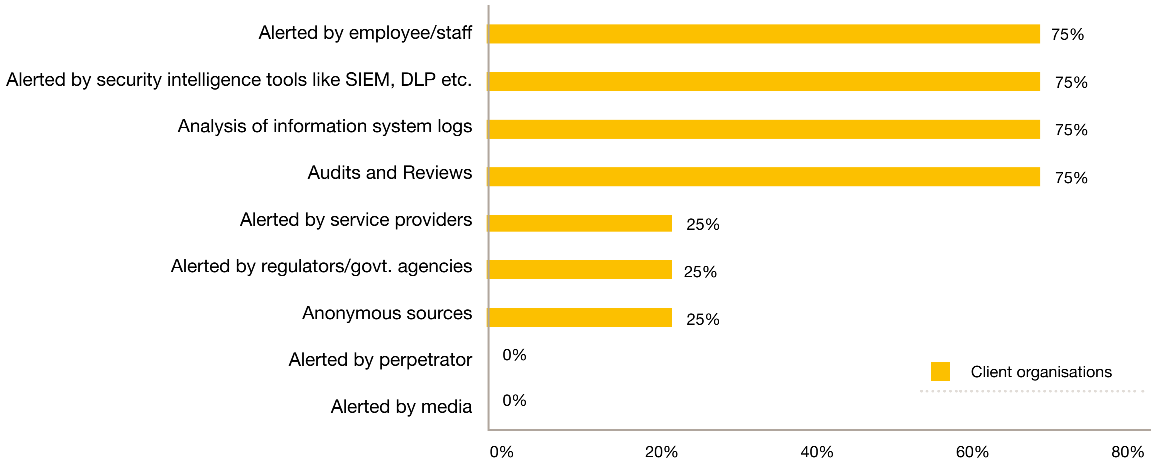
Interestingly, audit and review is still the primary source of identification and learning about insider incidents with around 89% service provider organisations and 75% client organisations being alerted about insider incidents at service provider organisations through this method.

Alongside, analysis of system logs and alerts from employees/staff are other prominent sources of threat detection highlighted by 78% of service provider organisations and 75% of client organisations, respectively.

Seventy-five per cent client organisations also get alerted about insider incidents at their service providers through security intelligence tools like Security Incident & Event Management (SIEM) and Data Loss Prevention (DLP) . In contrast, 33% service provider organisations are alerted by such tools.

89%

service provider organisations are alerted about insider incidents through audit & reviews

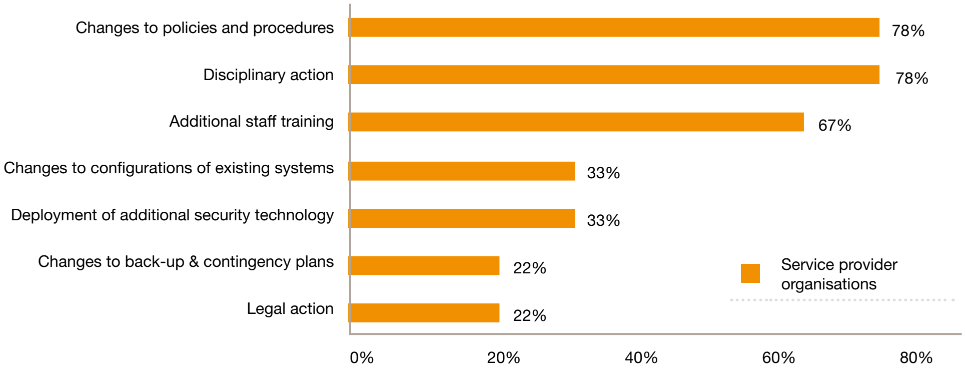


Corrective Action

Service provider organisations take several corrective actions after an insider incident. These include changes in existing policy and procedures, changes to configurations of existing systems, legal action and training.

More than 75% of the service provider organisations have made changes to their existing policies and procedures and around 67% of the service providers have carried out additional training for their employees.

It is interesting to note that 78% of the service provider organisations have taken disciplinary action after insider incidents. Moreover, around 22% of the service providers have also taken stringent steps by taking legal action against such insiders.



Case | Intellectual Property Right Violation and theft[6]

The Vice President (VP) in charge of marketing in an e-learning firm was asked to resign on account of reported misbehavior. As was customary to any resignation, the VP was asked to handover all internal confidential and not-so-confidential data that he was given as per his role and rank. This included the source code of e-learning solutions developed. However, the VP was angered on being fired and decided to do just the opposite. Instead of returning all intellectual property of the company, one of which was a source code of a very important soon-to-be-released e-product, the VP copied the source code and other important product related material and quietly took it along with him once he left the premises. The VP then used this source code to start a venture of his own and published stolen information on his venture's website. This included software designs, solutions, products and information which were only privy to the e-learning firm.

The fraud came to light when an employee of the e-learning Company noticed information and products confidential to his company on the VP's new company's website. Exactly similar features of an e-product were being advertised on the VP's company's website. The product that was planned to be release by the e-learning company was already out as someone else's product. Due to this theft of Intellectual property the e-learning company had to book losses to the tune of ₹ 47 crore!

[6] http://www.expressindia.com, http://www.indianexpress.com

The safeguards

Best practices deployed

With the occurrence of the insider incidents being on the rise, most companies are initiating steps to safeguard against a possible insider attack.

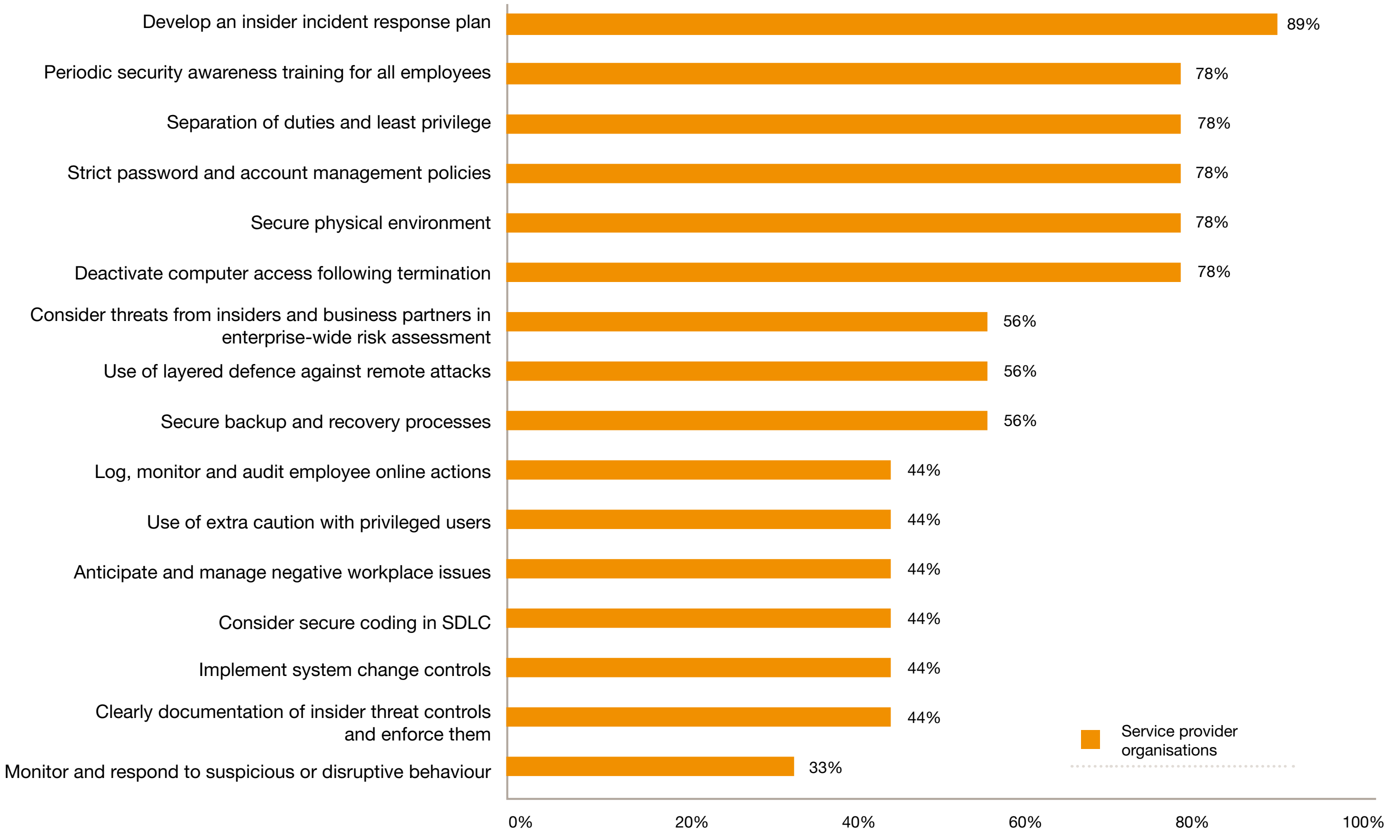
More than 50% of the respondents in service provider organisations have considered threat from insiders in their enterprise risk assessment. This clearly reflects the importance and management focus towards risks associated with the insider threat.

It is encouraging to note that more than 88% of the service providers have defined the insider incident response plan to manage such incidents in their organisations.

As highlighted earlier, employee awareness plays a very vital role in the prevention of insider threat. It is encouraging to note that more than 75% of the service provider organisations provide security awareness training to all the employees.

Around 45% of the service provider organisations have documented controls related to insider threat and also implemented these controls.

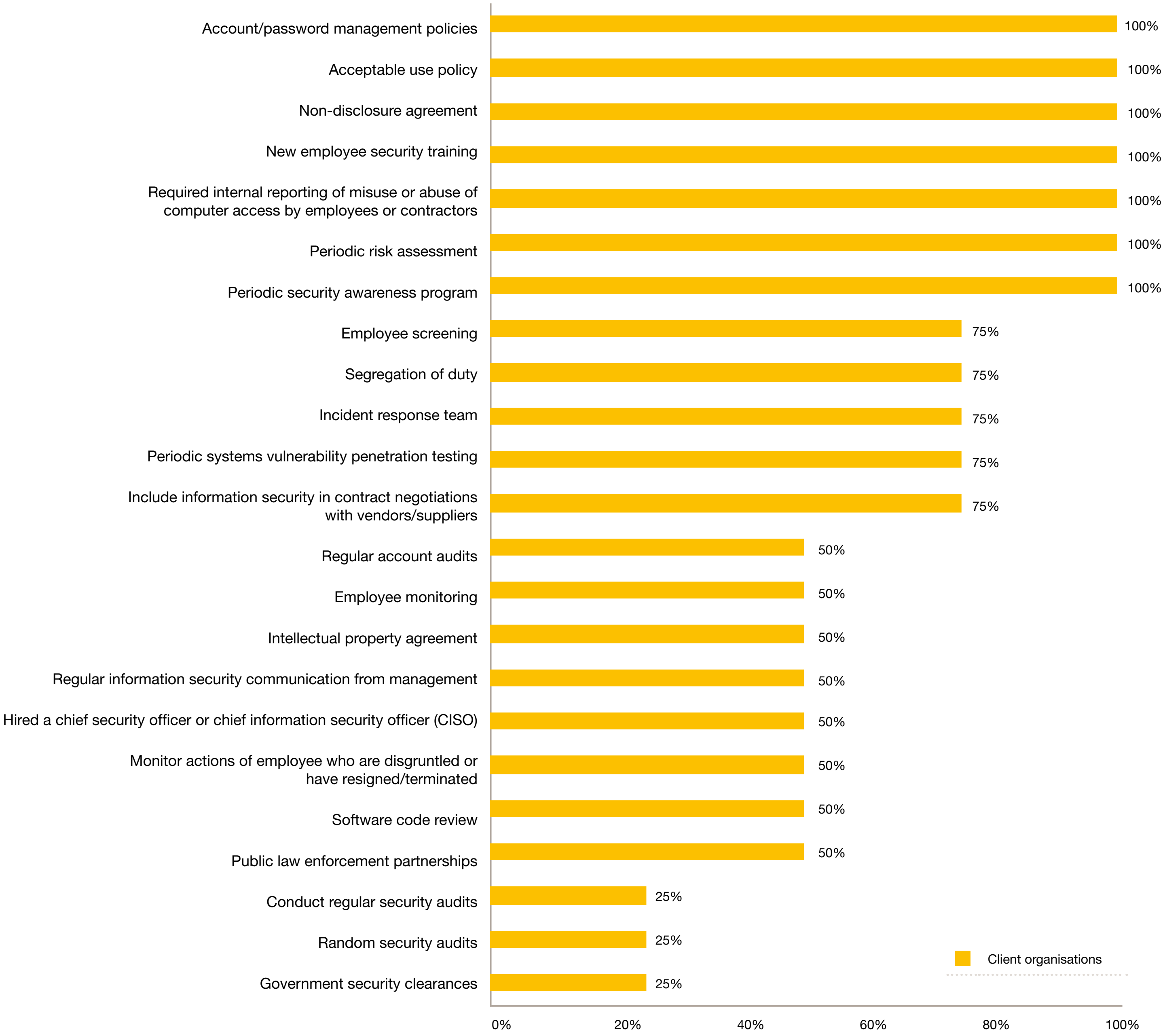
More than **50%** service provider organisations consider threat from insiders as part of Enterprise Risk Assessment



Safeguards mandated by Client organisations

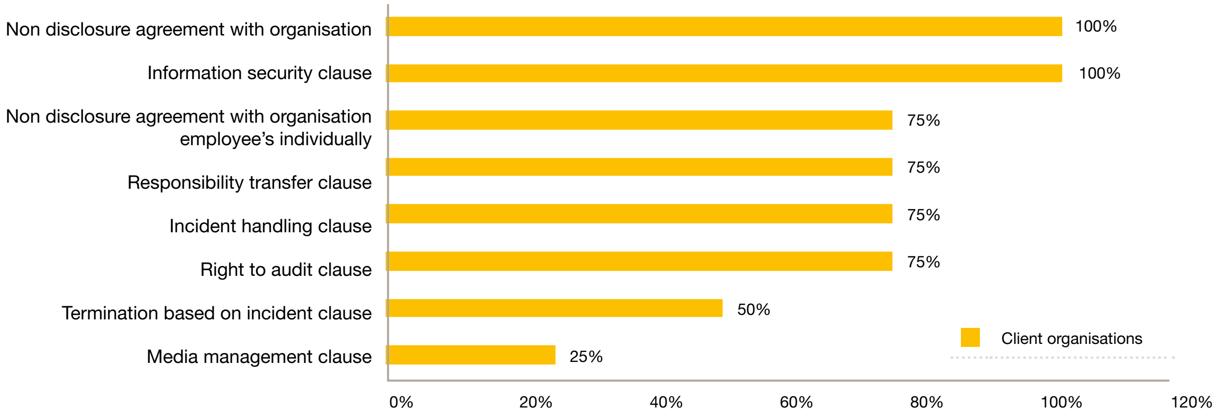
Amongst other safeguards, a lot of emphasis is given on security awareness and risk assessment by client organisations. All the client organisations mandate periodic security awareness and risk assessment on their service providers.

1. *Develop an insider incident response plan.*
2. *Consider threats from insiders and business partners in enterprise wide risk assessment.*
3. *Periodic securiy awareness training for all employees.*
4. *Clearly documentation of insider threat controls and enforce them.*
5. *Deactivate computer access following termination.*



Contractual controls enforced by Client organisation

Survey highlights that all the client organisations have signed non-disclosure agreement with their service providers as part of the contract. Moreover, 75% of the client organisations have also signed individual non-disclosure agreement with the service provider employees.



Recommendations

- *Recommendations to Government*

  - ***Improvement in data breach notification***

    A data breach notification system should be mandated by the Government of India.

    - In the event of an insider incident occurring in an organisation/industry, a central organisation should be made responsible to register and to assist the organisation/industry in investigating the insider threat or attack.
    - The Government and regulatory bodies must aim at implementing strict measures to ensure the confidentiality of the reported incidents.

  - ***Simplification of insider case registering process***

    - The process, for registering an insider case with the Law Enforcement Agencies/ regulatory bodies should be simplified for enabling better reporting and tracking.

  - ***Insider threat awareness***

    Awareness should be given significance in the overall information security plans:

    - Intensifying awareness and education campaigns to restrict and stop unintentional insider cases.
    - Conducting focused research on insider threats to improve overall knowledge of such incidents.

- *Recommendation to Industry*

  - ***Comprehensive insurance from data theft***

    Data theft insurance policy can be initiated under the direction of the regulator/ Government and industry bodies to protect the service provider from litigation which might arise due to insider incidents.

  - ***Knowledge sharing***

    Industry bodies must provide a platform for organisations to collaborate and share best practices and procedures. Industry bodies should compile best practices and encourage their member organisations to adopt the same.

  - ***Database of security and data breaches***

    The industry should collaborate to build a database of security and data breaches. This way the industry will be able to create repository of types of breaches, profile of the executors, methods deployed for execution, etc. This can immensely help in providing valuable inputs and direction to the organisations (by providing a platform for sharing learning and experiences) and can enable them to proactively mitigate insider risks.

  - ***Increase awareness and culture towards National Skill Register(NSR)***

    Industry should leverage the National Skills Registry when recruiting new employees. NSR is a quick and credible reference to profile of professionals. It is a security best practice for the industry and assures identity security, industry acceptance to honest professionals. It provides comfort to the clients as the industry uses a standard background verification practice and builds up an information infrastructure which is transparent.

- *Recommendation to individual organisations*
  - ***Internal awareness programs***

    There should be sustained internal information security awareness programs running within the organisation from time to time, so that insider incidents attacks alike could be curbed. The consequences related to an insider threat or attack might be highlighted for both intentional and unintentional attacks.
  - Insider threat should be considered an important element of the security initiative of an organisation.
  - An organisation should conduct scenario-based risk assessment.
  - An organisation should establish insider threat investigative capabilities.
  - An organisation should align protection strategies to manage insider threat:
    - Adopt data protection policies and processes
    - Use technology to prevent and manage insider incidents
    - Prioritize investments towards threat management
  - Service providers should demonstrate granular understanding of possible insider situations for clientele as per processes, relationships and functions.
  - Client organisations must undertake the following
    - Understand local legal policies and implications
    - Have a vendor risk management system aligned to the services availed from the service providers
    - Collaborate with industry bodies/initiatives to spread awareness and take corrective actions in the event of a breach
    - Possibility of data leakage within the client organisation should be documented

The study team

We would like to take this opportunity to thank all the team members for their contribution to the creation and finalisation of this report

DSCI

Vinayak Godse
Director – Data Protection

Vikram Asnani
Senior Consultant – Security Practices

Rahul Jain
Senior Consultant – Security Practices

Shweta Suri
Security Analyst – Security Practices

PwC

Rahul Aggarwal
Managing Consultant

Manish Tembhurkar
Principal Consultant

Ankur Ahuja
Senior Consultant

Nidhi Jain
Designer

DSCI Project Advisory Group

Prof. N. Balakrishnan, Chairman, DSCI and
Associate Director, IISc

Mr. B.J. Srinath, Senior Director, CERT-In

Prof. Anjali Kaushik, MDI Gurgaon

Mr. Akhilesh Tuteja, Executive Director, KPMG

Mr. Kartik Shahani, Country Manager, RSA

Mr. Satish Das, CSO, Cognizant

Mr. Baljinder Singh, Global Head of Technology,
Information Security & Business Continuity, EXL Service

Mr. Vishal Salvi, CISO, HDFC Bank

Mr. Ashwani Tikoo, CIO, CSC

Mr. PVS Murthy, Global Head – Information Risk Management Advisory, TCS

Mr. Deepak Rout, CISO, Uninor

Ms. Seema Bangera, GM – Information Security, Intelenet Global

About PwC

PwC firms provide industry-focused assurance, tax and advisory services to enhance value for their clients. More than 161,000 people in 154 countries in firms across the PwC network share their thinking, experience and solutions to develop fresh perspectives and practical advice. See pwc.com for more information.

In India, PwC (www.pwc.com/India) offers a comprehensive portfolio of Advisory and Tax & Regulatory services; each, in turn, presents a basket of finely defined deliverables. Network firms of PwC in India also provide services in Assurance as per the relevant rules and regulations in India.

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

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

Sivarama Krishnan
Executive Director
+91-9650788787
sivarama.krishnan@in.pwc.com

Siddharth Vishwanath
Executive Director
+91-9873434609
siddharth.vishwanath@in.pwc.com

DSCI and PwC have taken reasonable steps to ensure that the information contained in this report has been obtained from reliable sources. However, this report 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 report 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. DSCI and PwC, their members, employees and agents accept no liability, and disclaim all responsibility, for the consequences of a reader acting, or refraining to act, in reliance on the information contained in this report or for any decision based on it.

In this report, “PwC” refers to PricewaterhouseCoopers Private Limited (a limited liability company in India), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

NJ 178-June 2011 Insider-Threats.indd
Designed by: PwC Brand & Communications, India