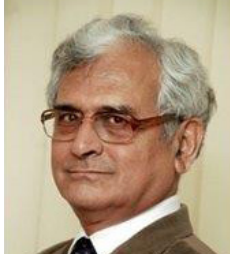


Leading industry practices in security and privacy



DSCI Excellence Awards

Foreword



Organisations today need to be increasingly secure as the environment in which they operate is more and more complex and dynamic with attackers using innovative techniques such as emerging mobile and cloud platforms. Security response to this challenge must be equally innovative - a way that helps an organisation become nimble footed to respond quickly to real threats in its environment. It should be able to assess its maturity in implementing security in different areas with a view to continually improve the same. A Security programme needs to be dynamic and vibrant such that it enables quick response to threats, vulnerabilities and actual cyber attacks. Data Security Council of India (DSCI) has been promoting such an approach through its DSCI Security Framework (DSF©) - a security discipline specific approach based on a set of security principles - visibility, vigilance, coverage & accuracy, discipline in defense; focus on strategic, tactical and operational layers, powered by a data-centric implementation methodology. It is gratifying to see that DSF© has found acceptance by the industry, and that it is being used as reference guide to improve security practices by many organisations.

DSCI decided that it was equally important to recognise, honour and reward organisations and individuals who have implemented strong, effective and resilient data protection programmes to help them address real risks, build resilience, increase trustworthiness and create an environment conducive to business. With this in mind, DSCI announced the institution of the '**DSCI Excellence Awards**' in the year 2011. In the very first year, we received 60 nominations representing 52 organisations across 10 categories in the corporate segment. In the second year, we received an even more encouraging response – 78 nominations, inspiring us to do better each year. We are very thankful to the industry for reposing its faith in DSCI.

I'm pleased to present to you '**Leading industry practices for security and privacy**' compiled based on the analysis of the actual practices implemented by organisations as revealed in the DSCI Excellence Awards nominations. This report will help the organisations benchmark themselves against the best practices, and will enable them to incorporate security and privacy best practices in their business operations.

I'm convinced organisations will be motivated to further improve their security and privacy programmes, and many more will participate in the DSCI Excellence Awards this year.

Dr. Kamlesh Bajaj
CEO - DSCI

Preface



Organisations in India are leading the pack, faring even better than their foreign counterparts, on security and privacy initiatives. In many instances, the clients, who outsource their work to India, find the security and privacy practices of India based service providers to be more robust and mature. These clients are using contractual obligations with their outsourcing partners to drive security and privacy controls more comprehensively. Having said that, given the spate of incidences that have persistently troubled our nation in the field of security and privacy, it is essential to realise that organisations in India still have a long way to go.

DSCI - a NASSCOM initiative - has been working with organisations to alleviate some of these challenges. One of the practices to achieve this is the Best-Practices symposiums conducted regularly in order to evangelise and highlight innovations. Another feature, that has become a popular part of the initiative, is the DSCI Excellence Awards. Started in 2011 to recognise and honour successful organisations and individuals in the field of security, the awards have seen an overwhelming response in the first two years of their existence. Leaders of various organisations have nominated themselves across different categories of awards. While there were over 60 nominations in various categories, the enthusiasm in 2012 topped the previous year's numbers by some margin. Organisations from the IT services, BPO, banking, telecom and eGovernance domains have participated in these awards. Year 2012 also saw the advent of a special category on privacy, highlighting the need to specifically deal with the subject. We are proud to mention that PwC has been assisting DSCI through this award process since its inception.

As a part of this process, a wealth of information has been put forward, highlighting the essential practices that these organisations have been institutionalising in their domains. An analysis of this has revealed interesting trends. For example, while business process management (BPM/BPO) organisations have worked effectively to cater to their customers using compliance-based initiatives, the banking sector has reached the stage where it finds merit in automating its GRC portfolio and incorporating security and privacy aspects as part of their control framework. Similarly, while telecom companies are striving to ensure that their infrastructure is safe from malicious intent by improving the security of the telecom infrastructure components, eGovernance projects are devising comprehensive strategies to provide reliable services despite sheer size and volume of delivery. Finally, with the user-base of social networking systems skyrocketing to never-before numbers, the risks associated with sharing information that is private to individuals is also growing in proportion. Organisations are dealing with this in surprisingly innovative ways; while ensuring due cognisance to the fundamentals of the domain.

With the intent of helping better current practices, I am proud to present this report highlighting some of the initiatives that your organisation may like to follow. We hope you find it useful for improving security posture, drive privacy and achieve compliance to regulatory requirements.

Sivarama Krishnan

Executive director - PricewaterhouseCoopers, India

Banking

With cyber-attacks becoming more unpredictable and electronic payment systems becoming susceptible to innovative attack variations, banks have started introducing certain minimum checks and balances to minimise the impact of such attacks.

Security strategy and governance

Most banks have defined and deployed a robust information security framework to mitigate risks in a proactive as well as reactive manner.

All strategic plans and decisions for security and privacy are taken by a team involving business, operations, IT and information security. As part of the structure, focussed information security forums have been formed to oversee the design, enforcement and compliance of the information security framework.

The security framework is extended and implemented through the information security policy and procedures. The policies are being framed in consultation with business owners and are approved by senior management and stakeholders. A central information security committee is being constituted to oversee and manage the security program in most banks.

As part of the strategy, most of the banks have also started using technology to have an integrated view of governance risk and compliance framework by deploying GRC tools. This helps them to have a comprehensive view of the controls framework and compliance dashboard.

Banks have started deploying automated governance risk and compliance solutions to have a comprehensive view of the control framework.

Compliance

Banks are steadily moving towards defining the compliance function as a part of the overall governance structure. Security effectiveness metrics and performance indicators help measure compliance reporting. These indicators are used to depict the compliance status and maturity of security controls.

From a compliance perspective, all applications that have an impact on the bank's financial statements, as well as critical applications are considered by banks under the purview of the regulatory framework and are audited on a periodic basis. The metrics generated from the compliance programme are populated in the security dashboard and actions are initiated for improvement.

For ensuring compliance to security, a formal audit program is in place at most of the banks. Some of them are also using independent third parties to perform audits and measure compliance effectiveness.

Awareness and culture

As part of the awareness strategy, banks have targeted both internal as well as external stakeholders i.e. employees and customers.

Small capsules of targeted training are delivered frequently so that information security stays in the mental horizon of employees. Customised audio or visual films showing various scenarios are being utilised by banks to create awareness. These short videos are thought-provoking, visually pleasing and engage the audience. Such films are shot by organisations themselves in-house in order to generate interest and better impact.

Short awareness capsules are delivered frequently instead of lengthy sessions.

Banks are leveraging on a dedicated information security portal as well as their internal staff training centres to meet security training and awareness requirements.

Security organisation

A bank's security organisation starts with the formation of apex committees with the board of directors who provide direction. The security organisation structure is formed in such a manner that it is aligned with business requirements and business goals.

Banks have a dedicated Chief Information Security Officer (CISO) who heads and governs the information security program in coordination with the functional teams.

Some banks have clearly defined the responsible, accountable, consulted and informed (RACI) matrix to provide clear roles and responsibilities with respect to security activities.

To operationalise security, we have seen a trend wherein banks are moving towards a managed security services model. In some cases, a sourcing model is followed to supplement the security organisation.

Third-party management

Banks have started developing comprehensive outsourcing policies in order to cover risks arising out of third-party engagement. These policies are aligned with the RBI guidelines and other regulatory requirements. As a process, all outsourcing contracts are endorsed by the legal division of banks. Some of the key information security aspects incorporated as part of these contracts include the right to audit, non-disclosure agreement (NDA) and specific compliance requirements against standards such as PCI-DSS, ISO 27001, etc.

Basic security controls such as right to audit, NDA, compliance to specific standards are included in the contracts.

As part of the third-party management, banks have a complete list of all third parties and have also identified single points of contact to manage these with respect to information security. Banks are using independent third-party agencies to perform periodic onsite assessment of their critical vendors based on information security controls.

Banks are also mandating third parties to provide a self-assessment compliance certificate on a periodic basis to ensure that the vendor has self-reviewed and are compliant with all security requirements as defined by the banks.

Data-centric initiatives

To meet upcoming challenges, banks are following a holistic risk management approach. They have started using process and technical controls to address data security risks. These include classification of information and using tools such as Information Right Management (IRM), Data Loss Prevention (DLP) and full disk encryption. Data exchange with third parties are protected by using technologies such as secure FTP, strong authentication mechanism and monitoring these connections on a regular basis.

Banks are also getting their critical locations such as data centre, disaster recovery site certified against information security standards such as ISO 27001, ISO 22301 and PCI-DSS. Some banks have also developed a comprehensive list of security metrics automated using methodologies such as ISO 27004.

Domain specific initiatives

Most banks have implemented a number of controls to minimise the risk of fraud due to internet or mobile banking. These controls include the following:

- Advance authentication mechanism such as SMS based one time password (OTP), challenge response questions, out of band OTP, and site-to-user authentication
- Water marking tools for mitigating phishing risks on their net banking websites
- Rule-based fraud monitoring engines for detecting real-time credit card frauds
- Real-time SMS and email alert system to customers to mitigate the risk of any fraudulent and unauthorised transactions
- One-time-use cards self created by customers with a pre-defined limit set by the customer to deter from credit card frauds
- Mobile application assessment and code signing for mobile banking

Water marking tools are used to mitigate phishing risks on net banking website.

The telecommunication network technology has evolved from the traditional public switched telephone network (PSTN) to 3G, and more recently to 4G network services. Today's telecommunication industry has to operate within a new and more accountable business environment, with a whole gamut of services such as the Internet, VAS, and IP TV apart from the traditional communication services. The networks are increasingly being targeted by motivated attackers to intercept, disrupt or deny communications. These attackers may include individual or organisational hackers or even state-sponsored agencies. Additionally, given that telecommunications constitutes a critical part of the infrastructure for any country, regulators and government bodies are looking at a comprehensive range of security solutions and are no longer simply imposing financial penalties for defaulters. Therefore, to stay ahead of the competition, operators must maintain a secure, highly available infrastructure providing resilient and reliable services to their subscribers.

Security strategy and governance

Within the telecommunications environment, we find that information security is integrated across diverse and dynamic business environments, encompassing people, processes, and technologies. Technology plays a key role today in the implementation of the information security strategy. Operators rely not only on the application of baseline security standards (for e.g. ISO 27001, PCI-DSS etc), but also focus on cyber crime analysis and investigations. The security initiatives adequately address governance and compliance issues, and ensure a risk-based security structure approach and posture.

Certification towards standards such as ISO 27001, PCI-DSS, BS 25999 / ISO 22301 is being observed.

Early detection and reducing the cost of security incidents is one of the key aspects of a well-defined security strategy. Compliance with regulatory requirements is an important consideration while creating the strategy. Last, but most importantly, the overall strategy alignment is made with the business goals.

Security organisation

In line with the goals of the security strategy of telecom companies, steering committees headed by the top management have been formed in order to govern the security strategy. The CIO, CTO, CISO are permanent members of the steering committee, while other functional heads such as the chief human resource officer (CHRO), the chief marketing officer (CMO) and the chief financial officer (CFO), are invited as and when required. Besides, cross-functional security teams have been created and business involvement and management representation is ensured in all spheres.

Given the criticality of the sector from a national security perspective, collaboration with external stakeholders is a key aspect for developing a well-framed security organisation. This also involves telecom companies actively engaging with the Department of Telecommunications (DoT), industry associations, Computer Emergency Response Team of India (CERT-In), DSCI and similar other bodies. Since some telecom companies operate in the international arena as well, they have also been aligning their central strategies to other geographies, with requisite customisation. For this purpose, international legal teams are working collaboratively in order to assist the security organisations to draft uniform policies to govern the environments.

Compliance

In the case of the telecom industry, compliance mainly revolves around factors such as, regulatory compliance, telecom network security compliance, IT security compliance, third-party security compliance, functional security compliance, compliance to various ISO standards, data protection laws, CMMI standards etc. Regular audits, risk assessments and reviews form the basis of such compliances.

Most operators have created a multi-tiered structure in order to address these compliances. The compliance process involves building in-depth security controls across all departments of the organisation, such as finance, IT, legal, HR etc. Information security teams, in consultation with other cross-functional teams provide regulatory compliance of technical and business solutions across the organisation.

Awareness and culture

Awareness usually starts from the dissemination of the information security policy to the organisation by participating in meetings, and understanding the importance of security concepts and their significance in the respective domains. The target audience is identified and the corresponding requirements understood. These trainings are delivered by means of tools, frameworks and channels. Some organisations have also taken to incentivising trainings by having properly scheduled events to train and educate employees and contractors.

Incentivising training and proper assessment is a key step towards a successful security organisation

Many organisations prefer to follow a centralised training system using computer-aided techniques, including online training modules.

Third- party management

Some of the leading telecom operators have outsourced their core network management, IT management, contact centres and retail outlets. There are several vendors and partners for sales and distribution, marketing, and HR, who handle customer and employee data. Therefore, third party security governance is a key component for these operators. For an efficient management of the third party, a risk management framework is used and risk-based audits are carried out, both directly and by using independent third-party agencies. International standards are put into contracts with such vendors and partners for de-risking operations. Operators usually prefer to have framed selection criteria for third parties and the central governance teams have standard assessment parameters for evaluation purpose. For audit observations, the vendors are time-bound to address the identified issues in order to ensure compliance.

For outsourced processes in the telecom domain, risks related to security are also being channelised to vendors and partners through contracts, where penalties are also being borne by the vendors.

Data-centric Initiatives

Most operators have a comprehensive range of data protection programmes across various functions, processes, platforms and locations. The purpose of these programmes is to evaluate, identify, design and implement various data protection initiatives in order to protect business sensitive data at various stages of its life cycle. Data leakage analysis is done for critical business functions.

Data leakage prevention tools are being deployed to de-risk business management.

Some of the telecom operators have adopted a quantitative approach towards discovering and identifying critical data elements. A layered approach for data protection is a convenient approach, and organisations usually prefer a segregated architectural treatment. Effectiveness and gaps are periodically assessed in accordance to which, required controls and initiatives are driven to mitigate the identified gaps.

Domain- specific security initiatives

Being a critical part of the infrastructure of the country, the domain security initiatives of telecom operators are tailored to the information passing through the organisations' infrastructure. To ensure the security of sensitive data, telecom operators routinely perform vulnerability assessments of their infrastructure, conduct application security assessments, maintain audit trails for all critical components of the infrastructure and carry out cyber-security drills under the aegis of CERT- In.

In addition to these, for adherence to the laws and regulations, telecom operators also certify themselves to standards such as ISO 27001, PCI DSS, and business continuity standards such as BS 25999 / ISO 22301.

As a result of regulatory changes, telecom operators have started performing a security assessment for the core telecom network.

e-Governance

Over the years, a large number of transformation and mission mode projects have been undertaken by various central ministries and state governments in order to provide quality services to the citizen in a more transparent and efficient manner. These services involve information transaction and processing, and in some cases e-payment services are being offered to the citizens. An increased usage of IT in providing these services has also exposed the government organisations to increased number of sophisticated attacks. It is therefore essential to ensure that disruptions of critical government information systems are contained and managed effectively in order to minimise their impact.

Security strategy and governance

Some of the organisations have started defining security requirements from the project initiation stage itself. Such organisations have been referring to various guidelines issued by the Department of Electronics and Information technology (DeitY) and the CERT-In to define their security strategy.

Capacity building with respect to information security is the core component of the security strategy.

Most of these departments have adopted the ISO 27001 standard in order to define the security framework and the certification requirements are clearly laid down in the tender or Request for Proposal (RFP) documents for IT projects.

Capacity building is the core component of the security strategy, and various training and certification requirements have been clearly identified for the stakeholders.

The means and mechanisms deployed in order to operationalise the security strategy include governance through an Information Security Management System (ISMS) framework and process standardisation through Standard Operating Procedures (SOPs).

Security organisation

Some organisations have a dedicated information security committee headed by the senior most member of the organisation. These committees have representation from both, internal as well as external stakeholders such as departmental heads, independent advisors and representation from service providers.

An information security committee and a security officer have been nominated in order to drive information security.

Some of the organisations have a designated chief information security officer (CISO), who is assigned to oversee the implementation and effectiveness of the implemented security framework. Further key responsibility areas (KRAs) have been defined in order to create the ownership and accountability within the organisation. These personnel who are responsible to drive the security programme have undergone trainings and also hold certifications such as CISA, CISM and CISSP.

Compliance

Organisations are appointing third-party agencies to review and report the compliance status. The scope of such reviews consists of network-level assessments, security requirements, adherence to service levels, application security audits and asset audits. Some organisations have specific service level agreements (SLAs) related to information security and penalties are levied on the third parties or vendor, in case some gaps have been identified.

Third party agencies are appointed to review and measure the compliance of the security operations.

Awareness and culture

Creating awareness within the government sector is the most challenging aspect due to the scale and stakeholder maturity.

Some organisations are using various mechanisms in order to create awareness including class room training and computer-based training programmes. Various security advisories are issued by the senior management to all project locations on a regular basis. Security newsletters are published in a bi-lingual format including English and Hindi, which have been well appreciated by stakeholders and have been able to create an impact at the ground level. Various quizzes are being organised and deserving officers are appreciated and encouraged by senior members to create a visibility within the organisation.

Third- party management

Government organisations have clearly started defining the security requirements in their tender and contract documents. These requirements include Non Disclosure Agreement (NDA) clauses, ownership of the source code, background screening and security controls to be deployed during the development, operation and independent review of these requirements as part of the contract itself.

Security requirements are defined during the initiation of the project itself.

Security requirements are created as a part of RFP and contracts and a KPI-based monitoring and assessment approach is followed.

Data- centric initiatives

Most government organisations have undertaken conscious effort to protect business critical data through the implementation of business continuity and disaster recovery (DR) plans for their datacenter. The testing of these DR plans is performed regularly in order to check the efficiency and effectiveness of the implementation.

Organisations have made clear demarcations between development and testing environments, in order to segregate duties between the development and operation teams. Various encryption mechanisms are being used to protect the confidentiality of data. Security incident and event management (SIEM) solutions are deployed in order to have a real-time view of the threat landscape. Security incidents are reported to the respective stakeholders who in turn, take corrective actions.

Domain- specific security initiatives

The applications used by organisations follow a software development lifecycle methodology and user acceptance testing is conducted before moving to production. Vulnerability assessment and penetration testing is performed by third parties appointed for networks and application infrastructure and independent code reviews help plug the vulnerabilities and thus yield performance benefits. In some of the G2B and G2C services, transactional security is ensured by SSL, secure file transfers and digital certificates. In cases where high probability of spoofing instances are likely multi-factor authentication like biometric, OTP based authentication and digital signature on public key infrastructure are used for a high degree of authentication assurance.

IT services

The IT services industry in India has come a long way since inception. With the focus shifting from pure-play development and implementation projects in the industry, effort driven towards customer satisfaction through quality, productivity and value delivery is now required. In addition to these factors, a security strategy aligned with the business strategy helps achieve a comprehensive services portfolio with a new level of confidence for customers. Security, therefore, is no more being seen as an obligatory investment but as an investment which generates returns. Service models such as cloud computing are expected to further drive integration of security in IT service delivery.

Security strategy and governance

As part of the strategy, IT companies have taken an inclusive approach rather than a standalone one in policy-framing, by setting up a management security forum chaired by the CXO and comprising senior members from various organisations. Additionally, a business-aligned security approach is enabling earlier involvement of security in new initiatives rather than having to bolt-on expensive security remedies later. Embedding risk management in daily operations, putting processes and technologies in place for information security and continuous monitoring and study of emerging threats are considered essential for the implementation of a security strategy.

Companies are making the abilities to customise and scale essential components of security policy to deal with geography and industry based risks.

For the successful implementation of the security strategy, employee awareness, physical security, compliance to statutory, audit standards and customer contracts have been defined as core components. Regular assessment of existing and new controls, comprehensive and regular risk assessment and analysis of business requirements are the basis for defining the organisation's security strategy. The information security team which has direct support and involvement from management and business is most likely to implement the security strategy effectively.

There is also focus on infrastructure optimisation, consolidation and providing flexibility to work from anywhere using mobile devices. As companies want to derive maximum benefits of technology, there is also a well-defined strategy on implementing information security measures to address new risks associated with the adoption of new technologies and the changing threat horizon.

Security organisation

In terms of creating a strategic roadmap for a responsive and competent security organisation, detailed hierarchy structures are created by most IT companies for security. The roles and responsibilities are well defined and clearly articulated. Involvement of senior management is a key aspect for proper implementation of the security strategy. To facilitate that, periodic reporting and review mechanisms are provided to senior management. Additionally, cross-functional interaction is maintained and skill up-gradation training is carried out on a periodic basis and is often incentivised.

It is critical to note that security creates value for organisations and their clients. Organisations have started creating independent teams that assist in reviewing the RFP for any business engagements and reviewing any specific security requirements. These help understand the concerns of business teams upfront and deliver the value additions.

Compliance

In most IT services companies today, the security organisation is working in tandem with the legal department to look for applicable statutes having a bearing on information security and necessary compliance requirements under those statutes. To look at compliance in a holistic manner, IT services organisations are also conducting spot audits (many times using independent third parties), reviewing security incidents, and involving all stakeholders while determining the challenges faced to comply with existing security standards. Compliance tools are being utilised to project compliance status to the management through snapshots of overall compliance of the organisation.

Organisations have a separate compliance function to adhere to regulatory and other applicable requirements.

Awareness and culture

Having policies and procedures alone does not ensure security compliance if the organisation does not create adequate awareness among its employees. Companies are integrating security and compliance awareness training into the induction programmes of their associates. These trainings are being customised as per the target audience including third-party staff. Proactive reward mechanisms for disclosure of non-compliances to policy are also being seen as a way to raise awareness and promote a culture of disclosure among employees.

Companies are resorting to various modes of communication like print media, technology, direct communication and are innovating to articulate their security and compliance policies. Customised handbooks are being designed for managers and associates. To bring in practicality to training modules, real-life scenarios, in addition to contractual and statutory requirements are being considered while designing the content.

Data-centric initiatives

Data is at the core of every business, perhaps more so in the case of IT services. Many such organisations are also seeing IPR protection as a critical area for data-centric security strategy. Organisations have built a well-defined information and asset classification policy to ensure that all information owned by the company and the client is clearly labeled and classified. Controls are being put in place to secure such data, and the strength of such controls is commensurate to the level of classification.

IPR protection is being considered as a key parameter in defining a data-centric security strategy.

Domain specific initiatives

As businesses move towards the 'cloud', clients are looking for security features in systems that enable such transitions. This has resulted in focusing a tiered approach to integrated security models. The traditional systems development life cycle (SDLC) process has been replaced with a 'secure' SDLC in IT services organisations, which enables identification of security requirements of customers and ensures customisability of information systems being implemented to handle such needs.

IT development is moving from a traditional SDLC towards a secure-SDLC, where security requirements and modules are embedded in the development process.

While segregated offshore development centres for each client have been the norm for some time, new challenges have arisen. Clients and employees have started using newer technologies such as smartphones and tablets for business purposes, demanding more comprehensive service portfolios. The security functions of IT services organisations have started enabling these transitions by introducing policies such as bring-your-own-device (BYOD).

The business process outsourcing (BPO) industry in India has witnessed phenomenal growth by providing significant cost savings, higher quality products and processes and improved operational performance. Studies have shown that security controls deployed by the BPO industry in India are much more stringent as compared to controls deployed even by their clients. Given the sensitivity of data handled by BPOs, security is an integral part of service delivery. The industry has to comply with various regulatory requirements across different geographies along with customer-specific requirements.

Security strategy and governance

While defining the security strategy, BPOs are not only considering specific security requirements of clients but also international standards and regulatory requirements.

The BPO security strategy takes into account all components of the ecosystem including employees, third parties, business partners and suppliers. Organisations are also trying to integrate their security framework with the enterprise risk management (ERM) and business continuity management (BCM) framework in order to optimise the efforts and have an integrated framework for better sustenance.

Most BPOs have ensured that their security strategy is aligned with business requirements. Organisations have taken various measures such as ensuring business representation during the formulation, review and feedback of the security strategy, which is derived from the business plan.

Integrated framework comprising information security, enterprise risk management and business continuity are deployed to optimise the effort.

Compliance

The compliance function in this sector is a dedicated and separate function in the organisation. The scope of compliance in BPOs revolves around legal and regulatory compliances, contractual compliances, policies and procedures, code of conduct, licences and ethics management.

Some organisations have a dedicated compliance manager aligned to specific functions or process to oversee and manage compliance requirements.

Compliance to ISO 27001 requirements is a basic norm followed across the BPO industry.

Knowledge management relating to compliance is done in a structured manner and compliance reports are published on a regular basis, with circulation amongst relevant stakeholders. Internal audits, metric collection and analysis, dashboard reviews and management reviews are undertaken using compliance and GRC tools to monitor the effectiveness and compliance status.

Awareness and culture

Awareness is the critical component of the security strategy. Various measures are implemented to create security awareness among stakeholders using both pull and push techniques. Such techniques include an induction programme for new joiners, e-learning modules, portal, mailers, screensavers, posters and focused discussion groups.

KPI based assessment is also done for assessing the effectiveness of awareness programmes. Deserving candidates are rewarded. Various security contests and quizzes are organised where winners are announced to the entire organisation in order to create visibility.

Security organisation

Most BPOs have drafted a layered security organisation model with clearly defined strategic, tactical and operational layers to operationalise the security strategy. Roles and responsibilities are clearly defined for all three layers and stakeholders from different functions are part of the security organisation.

In most cases, the BCP, information security and the data privacy team make sure that the security organisation is aligned to business goals. Together they form part of a holistic risk and compliance team.

Relevant information security certifications and external trainings are stressed upon and skill up-gradation programmes are carried out with proper monitoring mechanisms for the security team. Some of the organisations have gone further in setting up a centre of excellence to assist various business units for risk management.

External participation with nodal agencies such as CERT-In and industry bodies such as NASSCOM, DSCI, etc forms an integral part of the security strategy for BPOs.

Data-centric initiatives

The information security programme of BPOs mostly focuses on clearly identified and prioritised critical data in order to protect it with appropriate controls. Most organisations prefer having a data-centric security framework and methodology. Process owners are responsible for ensuring that information is classified as per the defined guidelines and deployed controls in the organisation

BPOs have started deploying comprehensive privacy policies as per the various regulatory requirements such as the IT Act, DPA and HIPAA requirements.

Conventional control mechanisms are placed such as restricted access to the workflow, physical assets, printing, internet and signing of confidentiality agreements. BPOs have also deployed advanced technical controls such as masking of confidential data, deployment of DLP and DRM tools to reduce the risk associated with the breach and exposure of sensitive data. Encryption solutions have been deployed for mobile devices, production, non-production systems, external media and archival data.

Some of these BPOs have defined comprehensive privacy principles based on the IT Act (Clause 43 A), DPA and HIPAA requirements.

Domain specific security initiatives

Most BPOs stress upon information security and data privacy across all projects. They prefer having a common approach framework for engagement executions, with a baseline of different international standards such as ISO 27001 and acts such as HIPAA.

Client-specific requirements are implemented for particular functions and processes. These include compliance to PCI-DSS, DPA or any client-specific security requirements.

Notable approaches deployed by some of these organisations include implementation of policy for mobile devices (for recording, storage and transmission), portable media declaration and encryption, aiding forensic investigation, shifting of users from role-based access to command-based access.

Privacy

Organisations are accountable for data collection and its use. Accountability is emerging as a fundamental privacy concept. The onus must lie on organisations handling and protecting personal information, rather than transferring the responsibility of data collection and usage to the individual, through complex notices, choices and consent. The revisions in privacy regulations globally, have put a lot of emphasis on accountability. In India, the framework for creating a privacy bill released by the Planning Commission also emphasises on the accountability principle. For organisations, this means having a comprehensive privacy programme in place, which is based on a well-defined privacy strategy or a policy and the programme is implemented across the organisation, with appropriate monitoring and oversight mechanisms in place in order to check non-compliances and performance. This is somewhat similar to the ways by which information security is designed and implemented in the organisations today. To build such an organisational privacy competence requires privacy standards, practices and frameworks on which such organisations can build their privacy programme.

Framework for privacy implementation

Organisations across the globe are governed by either geographic, industry vertical or function-specific privacy legislation or regulations. Absence of global standards in privacy has led to organisations developing and maintaining their privacy program in conformance to regulatory requirements. Some of them have also started using DSCI Privacy Framework (DPF) to administer and manage their privacy initiatives. Most user organisations that have global operations or are serving global clients based , have implemented a global policy and adopted best practices, guidelines and standards when it comes to the collection, use, disclosure, access, storage, retention and protection of personal information. Some of them have also started using the DSCI Privacy Framework (DPF) in order to administer and manage their privacy initiatives.

Visibility over personal information

In order achieve compliance with corporate privacy policies and privacy laws that an organisation is subjected to, it is important to have visibility over the personal information dealt by the organisation. Few

organisations have developed structured processes and perform exercises to learn which functions, processes and relationship handle personal information. Use of global privacy assessment processes and tools, helps companies to define proper methods for assessing the ways by which personal information (PI) is collected , stored, processed and transmitted, both in online and offline environment.

Organisations, after gaining visibility, classify the personal information into various sub categories such as PII (Personal Identifiable Information), SPDI (Sensitive Personal Data or Information), PFI (Personal Financial Information), PHI (Personal Health Information) etc. depending on applicable regulatory requirements. Data lifecycle management processes are instituted for managing the visibility of customer PI. Data flow maps are created for various business lines and functions which describe the flow of personal information within and outside the organisation.

Organisations are moving towards identifying Personal Information and classifying it for commensurate protection.

Organisations not only collect PI from their customers and clients, but also from their employees for the purposes of employment and the visibility scope exercise mostly covers this aspect as well.

Privacy policy and processes

Organisations have implemented the privacy policy based on the global privacy principles such as section 43A of the IT (Amendment) Act, 2008, the EU Data Protection Directive, the UK Data Protection Act, and other country-specific privacy laws. Based on the privacy policy, organisations have framed well-defined privacy processes, guidelines and standards.

The purpose of the Privacy policy is to communicate organisation's commitment for privacy protection to relevant stakeholders. It also defines organisation's role, whether of Data Controller or of Data Processor. This helps them in including the relevant privacy principles in

Note: Nominations received in the DSCI Excellence Awards under the Privacy category were mostly received from the IT and business process outsourcing (BPO) industry, and therefore the leading practices described in this section mostly reflect the industry's environment.

their policy based on the role. Some organisations have also built separate privacy policy for its employees.

The policy also mentions organisation's effort to safeguard personal information dealt with by it. Organisations are reducing the privacy risks by the combined use of privacy policy and contractual terms to create accountability in the form of transparent, enforceable commitments to responsible data handling.

Privacy organisation and relationship

A few organisations have a dedicated data privacy office headed by a chief privacy officer, who is accountable for privacy assurance to clients globally and responsible for data protection and privacy aspects across the organisation.

Each organisational unit has its responsibility for ensuring privacy. While the strategic group is primarily responsible for setting privacy goals and objectives, the tactical layer converts the finalized goals into specific roles and responsibilities and the operational team implements privacy initiatives and projects. Few companies have integrated data privacy policy and procedures as part of ISMS suite.

Organisations are slowly transitioning to having dedicated privacy resources, drifting away from conventional trend of security professionals playing dual role of security and privacy. This brings to the fore its emerging importance in the organisation.

Regulatory compliance intelligence

The regulatory landscape in today's environment demands a robust organisational structure in order to address the dynamic challenges. Organisations have addressed this by creating a dedicated structure for governance, compliance and risk. The legal services function within these companies keeps themselves abreast of all changes in regulations and compliance-related issues. The internal audit function also conducts periodic reviews in order to ensure that the compliance requirements are met.

Regulatory compliance intelligence in such firms is also strengthened by utilizing services of law firms and harping on information from open sources. Active external collaborations with organisations such as DSCI and International Association of Privacy Professionals (IAPP) also help in building RCI capabilities of organisations.

Privacy contract management

To continuously maintain trust amongst stakeholders and create accountability within an extended environment, privacy contracts are signed with clients, service providers and internal customers. These contracts are documented in line with the requirements for compliance with legislations, regulations and contractual obligations as is applicable in different geographies.

Contracts help to carry out data processing of personal and sensitive personal data strictly as per the terms and conditions stipulated by the clients and for no other purposes. Organisations are ensuring that they include privacy specific clauses in their contracts and agreements for sharing liabilities. The specific clauses are built in line with the role organisation is playing - data controller or data processor.

Self-assessments are being carried out by organisations based on the privacy principles applicable on them and their role as data controller and data processor

The data privacy office, in some organisations, maintains an inventory of the liability conditions that an organisation incorporates in the contractual terms. Formal disciplinary action is warranted when non-compliance takes place.

Monitoring and incident management

Organisations have well-defined systems to address privacy incidents. Incidents of privacy violations, security weaknesses, misuse of IT resources, violation of policies and procedures are being reported without any delay to the online security incident management systems. Employees and contractors are empowered to report incidents and prevent further attempts or damage. The learning's from such privacy incidents helps the management to take sufficient steps in order to ensure that effective privacy controls have been implemented or re-established to minimise the occurrence of such incidents.

Contractual compliances are also monitored by performing third-party assessments.

Information access and usage

Properly managed access control policies exist in most companies in order to protect sensitive personal data, along with IPR, trade secrets and software code designs, in line with the classification level. These companies employ role-based access control lists and access review processes such as quarterly employment verification and business need validation to ensure that superfluous accesses are removed. Well-defined logical and physical access controls are deployed in order to prevent breach of privacy information at various levels.

Organisations also have built capabilities to ensure that the personal information is used only for the purpose initially determined and communicated to the individuals. Periodic reviews and audits, both internal and external, are conducted to ensure that actual usage does not deviate from the purpose of usage.

Privacy awareness and training

Most businesses give utmost importance to include a mandatory privacy education programme for employees and have implemented appropriate technical and organisational measures to safeguard personal information.

Awareness sessions are designed through a collaborative approach with cross-functional work groups. Training courses and awareness programmes are designed, keeping in mind the client requirements for security and privacy, the emerging threat landscape, existing business risks statutory provisions mandated by international laws and standards.

Personal information security

Adequate controls are established to ensure the PI is secured. This includes required administrative, technical and physical safeguards. Various tools and solutions are used by the organisations to secure PI at rest, PI in Transit and PI during processing.

The lifecycle of data management is followed and requisite security controls are built to protect PI at all stages. The destruction / disposal of PI follow the information classification and handling procedure or the customer mandated requirements, as applicable.

The Security Policy and Procedures pertaining to organisational data are also applicable to PI protection.

By creating multiple layers of defense through physical security, intrusion prevention systems, firewalls, DMZ, VPNs, server hardening, logical access controls, application compliance and data encryption direct attacks on critical systems containing PI are arguably prevented to some extent.

DSCI Excellence Awards

About the Awards

In line with its objective to raise the level of security and privacy of IT and BPO service providers in order to assure their clients and other stakeholders that India is a secure destination for global sourcing and also promote data protection in domestic industry segments like Banking, Telecom, e-commerce and e- governance, DSCI instituted the 'DSCI Excellence Awards' in 2011 to annually recognize and honour organisations and individuals who have shown high level of preparedness and have excelled in the area of information security and privacy.

Objectives of the Awards

The objectives of DSCI Excellence Awards are as follows:

- **Recognition & Honour:** Recognize, honour and reward organisations and individuals who have taken strategic, proactive and innovative security and privacy efforts to help the organisation address real risks, build resilience, increase trustworthiness and create a conducive environment for doing business and thus enable the organisation to harness data protection as a lever for business growth.
- **Elevate the role of Security function:** Highlight the importance of security function and its contribution in the overall business ecosystem of an organisation.
- **Awareness and knowledge:** Bring about awareness towards the need for Information Security and privacy within organisations and society at large.

Categories for DSCI Excellence Awards

Corporate segment

Security

- Security in organisation
 - * Banking
 - * Telecom
 - * e-Governance
 - * e-commerce
 - * IT Services large and SME
 - * BPO large and SME
- Security leader of the year
- Emerging information security product company

Privacy

- Privacy in organisation
- Privacy leader of the year

Law enforcement segment

Capacity building

- State police or investigation agency

Investigation

- India cyber cop of the year

Write to awards@dsci.in or visit www.dsci.in for more details.

About PwC

PwC* helps organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with more than 180,000 people who are committed to delivering quality in assurance, tax and advisory services.

PwC India refers to the network of PwC firms in India, having offices in: Ahmedabad, Bangalore, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, please visit www.pwc.in.

*PwC refers to PwC India and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

You can connect with us on:

 facebook.com/PwCIndia

 twitter.com/PwC_IN

 linkedin.com/company/pwc-india

 youtube.com/pwc

Satyavati Berera*

Tel: +91 124 330 6011

Email: satyavati.berera@in.pwc.com

Sivarama Krishnan

Tel: +91 124 330 6018

Email: sivarama.krishnan@in.pwc.com

Siddharth Vishwanath

Tel: +91 22 6669 1559

Email: siddharth.vishwanath@in.pwc.com

Arup Sen

Tel: +91 22 6669 1078

Email: arup.sen@in.pwc.com

Harpreet Singh

Tel: +91 124 330 6012

Email: harpreet.singh@in.pwc.com

Kumar Dasgupta

Tel: +91 22 6669 1341

Email: kumar.dasgupta@in.pwc.com

Manpreet Singh Ahuja

Tel: +91 124 330 6021

Email: manpreet.singh.ahuja@in.pwc.com

Neeraj Gupta

Tel: +91 124 330 6010

Email: p.neeraj.gupta@in.pwc.com

Sanjay Dhawan

Tel: +91 80 4079 7003

Email: sanjay.dhawan@in.pwc.com

Tapan Ray

Tel: +91 22 6669 1204

Email: tapan.ray@in.pwc.com

*National Practice Leader (RAS)

About DSCI

DSCI is a focal body on data protection in India, set-up as an independent self-regulatory organisation (SRO) by the National Association of Software and Services Companies (NASSCOM), to promote data protection, develop security and privacy best practices and standards and encourage the Indian industry segments to implement the same.


DSCI is engaged with the Indian IT and BPO industry, their clients worldwide, banking and telecom sectors, industry associations, data protection authorities and other government agencies in different parts of the world. It conducts industry-wide surveys and publishes reports, organises 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 with which DSCI continues to promote and enhance trust in India as a secure global sourcing hub, and promote data protection in the country.

You can connect with us on:

 www.facebook.com/DSCI.CONNECT

 www.twitter.com/DSCI_CONNECT

 www.linkedin.com/company/data-security-council-of-india

Vinayak Godse

Tel: +91-11-26155071

Email: vinayak.godse@dsci.in

Rahul Jain

Tel: +91 11 26155070

Email: rahul.jain@dsci.in

Rahul Sharma

Tel: +91 11 26155071

Email: rahul.sharma@dsci.in

pwc.in

This publication does not constitute professional advice. The information in this publication has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this publication represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

© 2013 PricewaterhouseCoopers Private Limited. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Private Limited (a limited liability company in India), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

MS 33 - Month 2013 NameOfTheReport.indd
Designed by: PwC Brand and Communications, India