knowledge powering results

February 2008

Security Framework and Best Practices in Offshore Outsourcing

By Indy Banerjee, Director
Bindu Sudhir, Senior Research Analyst
Prabhash Thakur, Senior Advisor

CONTENTS

INTRODUCTION

The continuous evolution and growth of outsourcing has caused service providers to increasingly offer their clients services from multiple locations across the world. Because of this upsurge, client operations have been extended into the service providers' various offshore sites. While this development has generally led to client cost savings and added capability, it has also raised client concerns about data security at those sites.

Both client and service provider organizations have understood these offshore security issues in varying ways. This paper analyzes and clarifies issues surrounding offshore security; discusses how clients and service providers can both adopt a systematic security framework to reduce security risks, and outlines observed best practices.

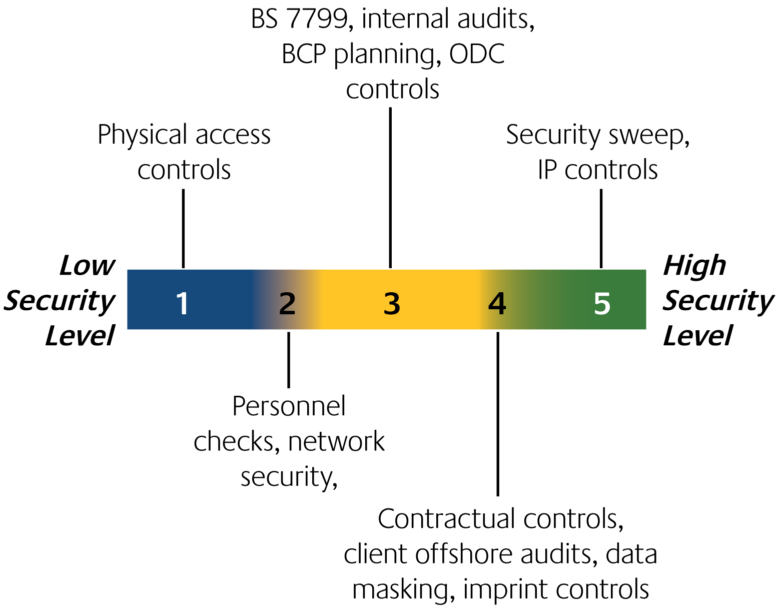
OFFSHORE DATA SECURITY CONCERNS

Common security-related concerns include:

- **Access to confidential data**: Clients are concerned about potential security breaches when external service providers have access to confidential and private data.
- **Compliance with regulations**: Regulatory and legal frameworks vary across geographies. For example, European Union (EU) law requires data protection encryption and mandates that access to certain sensitive data must occur within EU boundaries. The United States similarly has export control laws for select industries, and the Gramm-Leach-Bliley Act requires United States financial corporations to protect customer data. Additionally, the legal and regulatory frameworks of different offshore countries offer protection that varies considerably.
- **Constant churn of service provider staff**: In recent years, many service providers have been rapidly hiring new employees to accommodate growth and counter attrition. Providers must develop a continuous education program that addresses corporate security policies to a young workforce with diverse cultural backgrounds.
- **Lack of a comprehensive security program**: While clients increasingly outsource functions and geographies to offshore locations, they lack a comprehensive program to sensitize all stakeholders to security issues.

SERVICE PROVIDERS: SECURITY CAPABILITIES

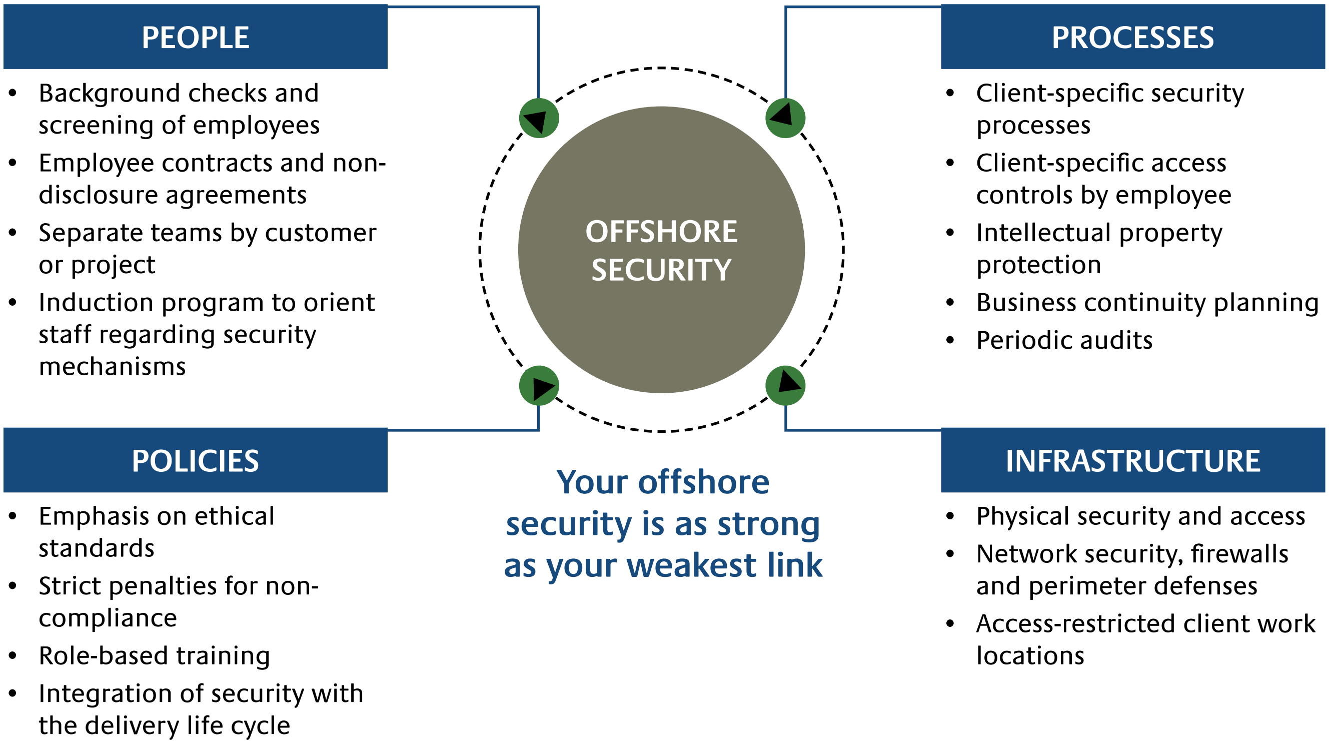
The service provider community has generally recognized keen client concern about privacy and security issues and has, accordingly, invested in security infrastructure, compliance and training. Despite many service provider measures to improve and meet client expectations, service provider offshore security capability varies widely because its evolution has been inconsistent — reflecting fluctuating client security needs, regulatory requirements and cost implications. The following diagram represents the spectrum of security controls in place for different offshore service providers:


BS 7799, internal audits, BCP planning, ODC controls
Physical access controls
Security sweep, IP controls
Low Security Level
1
2
3
4
5
High Security Level
Personnel checks, network security,
Contractual controls, client offshore audits, data masking, imprint controls

To achieve a best-in-class offshore security program, both client and service provider must be willing to participate and to be held accountable for its success.

OFFSHORE SECURITY PROGRAM

Designing and implementing a structured approach to offshoring and outsourcing is essential for mitigating offshore data security concerns. The key factors that must be considered to help identify, assess and address client concerns are illustrated in the following diagram.



OFFSHORE SECURITY

PEOPLE

- Background checks and screening of employees
- Employee contracts and non-disclosure agreements
- Separate teams by customer or project
- Induction program to orient staff regarding security mechanisms

PROCESSES

- Client-specific security processes
- Client-specific access controls by employee
- Intellectual property protection
- Business continuity planning
- Periodic audits

POLICIES

- Emphasis on ethical standards
- Strict penalties for non-compliance
- Role-based training
- Integration of security with the delivery life cycle

INFRASTRUCTURE

- Physical security and access
- Network security, firewalls and perimeter defenses
- Access-restricted client work locations

Your offshore security is as strong as your weakest link

A well-defined framework encompassing people, policies, processes and infrastructure can help both client and service providers realize benefits.

OBSERVED BEST PRACTICES

TPI has deep experience with offshore programs and has observed the following best practices that can benefit clients who must address common offshore data security issues.

1. Refine the enterprise IT architecture to improve security: To make their enterprise architecture security compliant, client companies may need to tweak it, as significantly overhauling should be unnecessary. They must first understand the information technology (IT) systems that control sensitive data and then take some specific initiatives to secure the data and the systems:

- **Data classification and masking**: Data is classified according to its criticality; therefore, critical data fields should be masked before they are sent offshore. This is usually completed as a major one-time project followed by progressively smaller efforts. Properly understanding the principle of criticality is important.

  By effectively classifying data, clients help service providers put successful controls on only the important data without wasting effort trying to control all data.

  Follow this example to classify an application according to the criticality of its intellectual property:

  - Critical — possesses *significant* business/competitive advantage
  - Manageable — possesses *some* business/competitive advantage
  - Commodity — possesses *little* or no business/competitive advantage

Financial, pricing, personal customer data and client strategy data are key types of critical information that usually reside in client data warehouses

- **Role classification**: A subsequent step in data classification is identifying critical data, which can be accessed only by certain roles that clients must define — roles that sometimes must be kept onsite at client premises. Clients may need to change their IT systems to permit role-based data access. To ensure that proper system changes are made, clients must first define the roles. Then they must find those gaps in the system that enable role-based data access that does not comply with security policy.
- **Define enterprise security standards**: Clients should write network, desktop and server standards that incorporate security policies. For example, network standards can include policies for network segregation, firewalls and data encryptions. All service providers must adhere to these standards, which reduce the risk of breaches and provide audit trails for future analysis.

2. Carry out a detailed pre-assessment of each provider and its delivery site: Before signing a “go-live” authorization, clients should complete a pre-assessment that includes these steps:

- Review service provider security policies for corporate information and for physical and facility security to ensure that all key risks are covered.
- Ensure that network security controls exist and the delivery site is certified, per industry-standard security policies, which satisfy internationally recognized security compliance standards, including ISO 27001, BS17799 and others as applicable.
- Check that an SAS 70 (or equivalent third-party audit) Type I and II assessment has been done for the delivery location.

- Carry out or review a detailed risk assessment for individual delivery locations followed by an onsite audit of each delivery site before "signoff."

3. Set up a regular audit and assessment program.

This program should include:

- A review and audit of the remote service provider's security policies, which must occur at least once a year
- An on-site review of the specific site and area used to conduct client business, which should be conducted biannually or as project requirements and risks dictate

4. Build security obligations into the outsourcing contract.

Clients should include all security-related controls in the contract.

- The contract should provide for:
  - Non-disclosure agreements (NDA)
  - Personal background checks
  - The understanding that service provider staff cannot work for a direct competitor until a specified amount of time elapses
  - Security assessments
  - Definitions of security breach and related liabilities
- If required, the contract should insist that the service provider take insurance to cover liabilities arising from a security breach.
- Contract termination provisions, which a client can invoke as a last resort if a material security breach arises

5. Build a culture of security in the organization.

Above all, a culture of security is paramount. It must be supported by the right set of people, who are willing to take some specific actions to sustain a secure culture and to constantly reinforce the importance of the message:

- **Strengthening the client security team**: Clients must create IT security teams or, if these teams already exist, increase the number of people in them. The security team is aware of issues that may arise and can thus publish the security policies that apply to service providers and assist in ensuring the controls. The team makes sure that client and service provider stakeholders are continuously educated, and it also interacts with the service provider security team to understand the latest procedures for ensuring corporate security.
- **Customer visits**: Clients should regularly visit service provider facilities to help service provider teams appreciate client business and concerns. To make these visits structured and more effective, clients should prepare a list of items about security policy and go over them in their discussion with service provider staff.
- **Formal assessments and scorecard**: Formal assessments should occur annually and result in a scorecard that is circulated to key stakeholders. Such assessments keep the focus on key open items during security-related discussions and help improve accountability. Additionally, service providers should perform a voluntary assessment annually and submit the findings to the clients.

- **Adopt an industry-standard security framework**: Organizations are increasingly concerned about the complexity and cost of managing various processes dealing with IT compliance and risk. Sometimes, teams laboring on compliance and regulation issues operate in silos. This practice tends to conceal redundant work taking place, which increases governance burden. A standard security framework across the organization facilitates communication and provides all the stakeholders with a common frame of reference.

  For example, the financial services industry has been experimenting with an Information Technology Governance, Risk and Compliance framework (IT GRC) to improve the consistency of risk-related data and to enable for common interpretation companywide.
- **Training and policies**: TPI's experience with past assessments has indicated that more than 70 percent of the team on a long-term sourcing contract consisted of personnel with less than two years' experience. Therefore, the client should have an explicit security policy. To avoid any risk due to omission on the part of an inexperienced employee, the client should provide a well-developed training program around security policy.

CONCLUSION

As organizations embrace offshoring, their IT systems and data will become more and more dispersed. A well-thought-out security program that balances control and flexibility can be an effective tool for securing business and increasing the confidence of clients and other stakeholders. To summarize, best-in-class offshore security programs require the client to:

- Classify applications and data, and classify roles according to their ability to access sensitive applications and data
- Carry out an exhaustive risk assessment program for offshore operations
- Create an in-house security team that regulates the policies of offshore providers
- Consistently communicate the policies and procedures to both onshore and offshore teams
- Enforce the standards at the applications, network, desktop and server levels
- Set up a structured assessment program
- Embed security in routine service management and governance activities
- Structure the contractual language and NDA to cover identified risks

LOOKING FOR A STRATEGIC PARTNER?

TPI's Global India experts can help you achieve your organizational goals through objective advice, knowledge of your industry and experience with sourcing arrangements from simple to complex.

Looking for a strategic partner? Contact **Indy Banerjee**, Director, Global India, TPI, at **+ 91 80 51518538** or **indy.banerjee@tpi.net**.

ABOUT THE AUTHORS:

Indy Banerjee

Indy Banerjee offers TPI clients significant experience in the IT and BPO industries and brings both an extensive client and supplier perspective to engagements. Based in Bangalore, India, Indy advises TPI clients on aspects of their Global Service Delivery. He has extensive experience advising clients on their sourcing strategy globally to low-cost locations. Indy provides strong strategic, operational, transitional and quality experience and an extensive network of relationships for Indian IT outsourcing and business process outsourcing (BPO). His practical experience includes a broad spectrum of exposure in various functions and businesses in the BPO, IT services, Public Sector & Infrastructure Consulting and Fast-Moving Consumer Goods industries.

Prior to joining TPI, Indy worked in the outsourcing industry in leadership roles spanning global offshore strategy development, opportunity identification and transition, enterprise program management, offshore service delivery and Six Sigma in Fortune 10 companies.

Bindu Sudhir

As part of TPI's research group, Ms. Sudhir provides analyses and insights about outsourcing market trends that have an impact on sourcing decisions. She has expertise about the importance of offshore security, as well as market intelligence knowledge about the service provider marketplace and offshore destination.

Prior to joining TPI, Bindu worked as an Associate Manager in the Strategic Global Sourcing group at Infosys Technologies, where she provided business development support, market and segment analysis, and opportunity identification and assessment for large transactions. At Xansa, a United Kingdom-based service provider, she was responsible for creating and disseminating market intelligence and business updates, and liaising with third parties to perform primary research.

Bindu holds an undergraduate degree in mechanical engineering from Jawaharal Nehru Technogical University and a master's degree in human resource and information systems from the Institute of Public Enterprise. Both institutions are in Hyderabad, India.

Prabhash Thakur

Prabhash is a part of TPIs Global Service Delivery Practice and is a seasoned advisor in the Offshore Application Development and Maintenance (ADM) and Information Technology Operations (ITO) space. He has extensive experience in designing and implementing sourcing strategies and has worked for some of the worlds largest businesses helping them with their offshore needs, both as an employee and as an Advisor. He brings in strong operational experience, a deep understanding of technology and a valuable network of relationships for IT and business process outsourcing. At TPI, Prabhash has advised clients in the Financial Services, Telecom and Hi-Tech sectors on their ADM activities. Prabhash is a certified six sigma black belt, and has led many projects aimed at process and productivity improvement in ADM. He has extensive practical experience on the course correction of IT projects by using techniques such as re-assessing project plans and team skills, engaging key stakeholders, improving the productivity of project teams by decoupling unrelated tasks and co-locating them, and publishing realistic project status reports. Prabhash is delivery-focused, with exceptional communication and collaboration skills and has extensive experience in the Information Technology Infrastructure Library (ITIL) processes and frameworks.

Prior to joining TPI, Prabhash worked in the outsourcing industry with a special focus on ADM portfolios. At GE Capital International Services, Prabhash worked with different GE businesses including Consumer Finance, Commercial Finance, Energy and Mortgage. He worked to transition ADM work from GE Capital IT solutions in US and Canada to India. In this role, he managed the process of baselining effort, metrics development and knowledge transfer. He worked with the global delivery program management team of GE Corporate to ensure standardization of service levels, knowledge management and contract adherence. Prabhash graduated from Global Leadership Development program of GE Capital.

Prabhash holds a Bachelor of Technology (Engineering Physics) from Indian Institute of Technology, Mumbai and a masters in Business Administration from XLRI, Jamshedpur — both premier institutes in India.

ABOUT TPI: TPI, a unit of Information Services Group, Inc. (ISG) (NASDAQ:III) is the founder and innovator of the sourcing advisory industry, and the largest sourcing advisory firm in the world. We are expert at a broad range of business support functions and related research methodologies. Utilizing deep functional domain expertise and extensive practical experience, TPI’s accomplished industry experts collaborate with organizations to help them advance their business operations through the best combination of business process improvement, shared services, outsourcing and offshoring. For additional information, visit www.tpi.net.

Americas
Nigel Jones
Manager, Business Development
+1 650 384 5405 or
nigel.jones@tpi.net

EMEA
Denise Colgan
Marketing Manager
+44 (0)1737 371523 or
denise.colgan@tpi.net

Asia Pacific
Arno Franz
Partner & Managing Director, Asia Pacific
+61 (0)2 9006 1610 or
arno.franz@tpi.net

tpi SM

knowledge powering results