HORIZON contact centers
Innovation & Excellence

White Paper

Information and Data Security Case Study

Author: Nicholas Nganga, Director of Information Technology, Analytics and Business Process Management, Horizon Contact Centers

2010

Adherence of Privacy Laws by Offshore Partners

For companies in developed economies where data privacy laws exist, the impact of their clients' data loss overseas does not stop at their home countries border.

Kenya BPO companies targeting markets where such laws are entrenched and becoming more stringent must implement strategies that give credence on their internal information and data security measures.

These measures must be up-to par with the requirements that their clients have to meet in their home countries.

Emerging BPO Destinations Challenge

Business Process Outsourcing and Contact Center companies in emerging economies, looking for outsourced high end services work from developed economies, have to contend with misconceptions like their capability to deliver world class quality services or their ability to securely manage private information and data.

These organizations have to mitigate their IT security capabilities against ever increasing stringent privacy law legislations that have been adopted in the developed economies and against the potential risk to their client's business due to possible IT security breaches. The risk negatively impacts clients that have outsourced their processes, financially and legally, as well as the nascent BPO sectors of emerging economies, like Kenya, affecting their bottom line and the country's credibility as a BPO destination.

Horizon understands the challenges potential client's face while trying to take advantages of the cost arbitrage as demanded by their stakeholders and at the same time ensuring privacy of their clients' information in outsourcing destinations like India, Philippines, South Africa or Kenya. These clients must comply with all relevant privacy laws in their own countries and ensure similar level of adherence by their offshore partners, especially where there is lack of legal remedy in the BPO destination.

Clients raise concerns on the threat to IT data sent offshore in three main areas. Firstly the multimedia contact center platform services that capture client interaction information and the vendor's end to end IT infrastructure. Secondly the BPO back-office operations and processing centers that are linked to their network directly or indirectly and finally the HR, Operations and IT administrative policies and practices of their outsourcing partners.

Privacy Law Case Study

Horizon Contact Centers offers inbound customer services and outbound telemarketing services to clients in the U.S and U.K market within the Internet Service Provision and Finance Industries. This case study looks into our experiences and solutions to one such client, a Public Limited Company based in Manchester City, for whom we conducted 'warm-calling' and outbound sales on a business to consumer and business to business which involved collecting bank and credit card details of their customers

Challenge: Client Confidence

Our initial challenge was to instill confidence in our client that their customer's information and data would be secure while transiting or residing in Horizon's IT infrastructure.

White Paper

The necessary IT skillsets and procedures needed to be in place from an information and data security perspective at the same level as at the client, especially given the strict UK privacy laws and the potential damaging effect to their business if there was a security breach of their customer's personal information.

In addition to a secure infrastructure, it was critical that Horizon did not capture this information outside of the client's systems either electronically or on hard copy.

As a vendor, Horizon was required to employ the appropriate technical, administrative and physical controls that protect the client's corporate customer information from unauthorized disclosure, use and loss.

Our Approach

Horizon worked together with the client, based on its own capabilities, to create a very high level of confidence around all aspects of information and data security at Horizon and between Horizon and the client's data center.

This meant Horizon extended its own best practices in Information and Data security in design and implementation that were adopted for the client's outsourced processes.

Technical Controls

- Secure and dedicated connectivity links to our client's data center through tier 1 telecommunications providers, running data and voice. Other Horizon services that were not client related were run on other disparate links.
- Secure and dedicated internal networks and workstations running the client's outsourced processes.
- A secure hosted call center platform compliant with UK and France Ministries of Defense requirements.
- PCI compliant internal call center operations management technology platform.
- A secure client/server application services design for all clients' systems accessed at Horizon servicing the client's outsourced process.

Administrative Controls

- Automated access control processes, policies and procedures for all systems involved in the outsource process workflow. This included dedicated roles from network engineering to access control execution that ensured adherence to established administrative controls.
- Strict HR policies on recruitment requirements to ensure a right fit with client's agent and operational support staff profiles.
- Strict HR policies on operational requirements on the outsourced process on the Horizon floor.
- Strict Horizon IT Information and Data security policies and for all our employees, vendors and suppliers servicing the client's outsourced process.

Physical Controls

Our ability to control the physical flow of employees, vendors, suppliers, visitors and any other third party partners within the facility, which included the following measures:

- Secure location in an ultra modern business park with restricted access.
- Controlled physical security and biometric access to office facilities
- Physical Facilities and Environmental Security for the Data Centre
- Integrated access control system to monitor the facility all year round.

Benefits

Horizon was able to create confidence in its capability to manage sensitive third party information by leveraging and extending its highly secure IT infrastructure to the outsourced process. The clients benefited as follows are:

Keep all data and information at the client's data center

- Zero security breaches for the duration of the project internally at Horizon or externally at the clients end.
- Raised the clients confidence in of Horizon's overall capability to handle other sensitive outsourced processes.
- Cemented a long term business relationship through exception services provided.

Horizon Contact Centers is East and Central Africa's first state-of-the-art and fully on demand International Contact Center and Business Process Outsourcing (BPO) Company, offering a broad portfolio of voice and non-voice services to the global market. With a world class facility in Nairobi,Kenya and a scalability to house over 1,200 agents, Horizon is the largest Outsourcing Contact Center in the region.

For more information, visit: www.horizoncontactcenters.com.

FOR MORE INFORMATION:

Horizon Contact Centers Ltd
Gateway Park, Mombasa Road,
P.O. Box 3027-00506
Nairobi, Kenya

Tel: +254 (0) 20 698 7000

Email: info@horizoncontactcenters.com