TELEGENISYS
Service Excellence

ELECTRONIC RISK MANAGEMENT IN BPOS – AN OVERVIEW

Table Of Contents

Positioning Statement

It's been almost two decades since Business Process Outsourcing (BPO) firms started offering optimized and cost-effective outsourcing services to clients worldwide and although they have been hugely successful, they have had their own share of problems and bottlenecks. As of now, one of the main concerns of BPO firms is the rising incidence of electronic data theft cases, some of which were perpetrated by inside sources whereas most others were a result of hacker attacks. Who actually was responsible is however irrelevant because in almost all cases, both BPOs and clients have incurred significant losses. This white paper intends to identify the main risk factors and provide an overview of electronic risk management solutions and strategies that BPO firms can deploy for securing confidential data.

Introduction

With rapid advancements in Information Technology (IT), almost every business now uses electronic systems for business transactions. BPO firms are not an exception since most of them handle the confidential data of their clients for providing a wide variety of outsourcing services such as telemarketing, customer support, technical support, data entry services and many others. Sharing and distribution of confidential data such as credit card details, medical records, customer profiles and others cannot be eliminated since they are crucial for the targeted service delivery process. Options, as such, are fairly limited, something that makes it even more important to deploy effective security systems for protecting confidential data and information. With rising aspirations for a better living and increasing cases of cyber crimes, it is has become vitally important for businesses, especially BPO firms to take proactive steps towards providing a more secure environment for both clients and customers.

Enterprise Risk Assessment – An Overview

Enterprise risk assessment is the first step towards securing confidential data and information being shared between clients, BPO firms and end-users. In this step, all the various risk variables are identified as may be rightly applicable to the processes in use by a BPO firm. Risk variables are different for each BPO firm and since it is often not feasible to exercise control over all the potential risk factors, it becomes necessary that time, effort and monetary resources be allocated only for the most critical of identified risks. Described below are some of the most common risk factors that BPO firms can use as a guide to assess whether or not they apply to the ongoing processes.

I. Data Theft

Data theft is currently the worst problem being faced by BPO firms. The main reason is probably the basic nature of electronic data, although lack of advanced security systems is also responsible for this growing menace. Here are some potential reasons that explain the increase in the number of cases related to data theft.

- In the absence of security systems, stealing electronic data is the easiest thing to do. Moreover, since it can be carried out in just a few seconds and also because there is often a high-value attached to it, more and more people are getting lured by the greed of making a quick buck.
- Transferring stolen data from the source to third-party buyers operating in the virtual dark alleyways of the World Wide Web is possible with just a click and can be achieved through a variety of means such as emails, free upload sites, etc.
- Data storage devices such as Pen Drives and technologies such as "Bluetooth" are now being produced for mass consumption, something that is making it easier for potential perpetrators to put their plans to action.
- In the absence of security systems, potential perpetrators know very well that tracing their activities will be virtually impossible. Moreover, since options such as "proxy" servers that hide the real IP address have now become readily available, it is adding to the confidence of potential perpetrators.
- Cyber crime laws vary depending on the country and unscrupulous sellers and buyers use this to their advantage to ensure that even if they are caught in the act, they can walk away free, with minimal punishment.

- Aspirations for a better living are rising the world over and people, especially the younger generations, have started to believe that they have every right to manipulate the system for their own personal gains, even when it might involve indulging in illegal activities.

II. Hacker Attacks

Defacing a website to prove personal or nationalistic superiority is no longer the sole objective of hackers and their communities. Now, it is being fueled more by the lure of monetary gains than anything else. The usual targets are businesses such as BPOs that have plenty of confidential data and information – precious booty that always has eager buyers in large numbers. Here are some potential reasons that explain the increase in the number of cases related to hacker attacks.

- Tracing the source of an online hacking event is quite difficult and can take weeks, especially when the target and the perpetrator(s) are thousands of miles apart. Hackers or their communities can work from the remotest parts of the world and if the right means are available, virtually any online resource can be targeted.
- Uncanny as it may appear, sometimes it is business competitors that hire hacking services, either to gain inside information about the target or to carry out disguised operations such as "Denial Of Service" attacks that severely restrict the ability of a business to service its clients or customers.
- Hacking has now become the favorite hobby for many teenagers and although not all are involved with hacking attacks, it indicates a growing trend that convicted criminals are not the only ones involved with online cyber crimes. This has made policing a lot more difficult for enforcement agencies.

III. Physical Data Loss or Corruption

Data stored in electronic form may be less susceptible to the forces of nature, but it has its own set of problems that can easily result in irretrievable loss of critical data and information. This can adversely affect customer services, something that needs to be avoided at all costs. Here are some factors that can lead to data loss or corruption.

- Human error may be the most unlikely factor, but in the absence of proper backup systems, it is always a possibility and needs to be guarded against. It can be anything from an unintentional error to a fabricated attempt by a disgruntled employee, but that is irrelevant because in both cases, it is necessary to safeguard confidential data and information.
- Using sub-standard storage equipment may save a few pennies, but it can also lead to data loss and corruption. In these cases, no insider or hacker is required; sub-standard storage equipment is prone to data loss from day one and it’s only a matter of time.

- Sometimes employees dealing with data storage and retrieval may not have been provided the right training or inputs as might be necessary for securing critical data and information stored on local and online web servers.

Eliminating Risks – Enterprise Solutions And Strategies

Now that the potential risks have been identified, it's time to devise effective solutions and strategies that can tilt the balance in favor of BPO firms and empower them to eliminate identified risk factors. Here's some time tested solutions and strategies that virtually all businesses including BPOs can deploy for securing their confidential data and information.

I. Policing The World Wide Web

This may be impossible to do manually, but can be made a lot easier by using advanced systems such as "Web sense". These fully automated systems can be configured to suit the specific needs of a business, even while they limit the options available to insiders, having potential to turn into full-time professional cyber criminals.

II. Deploying Fail-safe Automatic Log Systems

It would help if BPO firms use the same technology, as used by some hackers, for preventing unauthorized use of confidential data and information. Cost-effective automatic log software systems are readily available, which can be used for keeping a detailed record of activities as carried out on each computer terminal connected to the LAN network. Using these advanced systems, BPO firms can easily keep a record of all incoming and outgoing emails, chats, attachments, uploads, downloads and virtually everything else that can be considered a threat.

III. Active Advertising

Automatic log systems may have their benefits, but since prevention is always better than a cure, it would help if BPO firms highlight the presence of advanced security systems, irrespective of whether they might be fully functional or still in the testing phase. Just like advertising motivates a buyer to choose a particular product or service, highlighting the presence of security systems has the same affect with only one major difference in that as compared to the former, the latter acts as an effective deterrent. For optimal results, the presence of security systems must be communicated to all involved parties such as employees, vendors, suppliers and other third party service providers.

IV. Security Audits

Since hackers and potential saboteurs are becoming increasingly skillful and resourceful with each passing hour, it has become necessary that security audits be carried out to assess the efficacy of deployed security systems and processes. The main objective of such audits should be to identify any loopholes in the existing security system and consequently find effective solutions that can fix those loopholes. Security audits can be carried out by an internal team, but since the stakes are often high, it would be better if professional services are hired for this purpose. Depending on the type of business processes, security audits can be carried out quarterly, semi-annually or annually.

V. Holistic Approach

It may not always provide the desired results, but since there is no harm in making a sincere effort, following a holistic approach is always worth a try. In this approach, the root cause i.e. the distorted mindset of a potential perpetrator is targeted through a variety of methods such as community programs, incentive schemes, reward & recognition programs, psychological counseling etc. Crime, in most cases, originates from a repressed mind and since a holistic approach provides the right medium for release of suppressed energy, it does help in minimizing security risks although it can never guarantee 100% security.

Conclusion

Potentially crippling risk factors such as data theft and data loss have become quite evident and BPO firms, especially those that have aspirations to make it big, will have to work harder on ensuring the safety of confidential data and information. As for the clients, it would be recommended that they assess the level of security provided by a BPO firm before actually signing a service contract. Options are fairly limited once critical data or information has been compromised, and it always helps to take proactive measures. As for end-users, i.e. the customers, it would be recommended that they do not reveal their personal information until and unless they are sure that the information is being requested from a reliable source. All these measures will help restrict potential risks associated with data theft and will allow BPO firms to continue delivering the best quality and the most efficient services to both clients and customers.