

I.T. Infrastructure – Income Tax Office, Chennai

Effective I.T. Infrastructure Management with ReSOFT Asset & Inventory Tracking



PROFILE The Indian Income Tax department is governed by the Central Board for Direct Taxes (CBDT) and is part of the Department of Revenue managed by Indian Revenue Service (IRS), under the Ministry of Finance, Govt. of India.

CHALLENGE The Income Tax Department came across challenges in the management of the I.T. Infrastructure as there were missing desktops in the premises which resulted in high hardware costs. Loss of sensitive data was a hidden cost which was of great concern as system crashes caused application damages and un-wanted softwares wasted a lot of computing time and productivity

SOLUTION The Income Tax Department utilized ReSOFT Services for constant monitoring of all system's assets and scheduling automatic Asset Survey Report and tracking login details of users. ReSOFT blocked USB ports and restricted usage of external media. Anti-Virus software was installed on all machines by using ReSOFT and there was continuous monitoring of application usage using ReSOFT.

BENEFITS By using our solution, the Income Tax Office could monitor unauthorized asset movement and generate alerts. They could track transfer of sensitive data on the network and protect the user community from relentless threats of virus infections. Problems were solved with little or no manual intervention and cost-effective system maintenance and problem management was provided. Systems were managed with limited or intermittent network connectivity

I.T. Infrastructure – Income Tax Office

Overview of Income Tax Office

The Indian Income Tax department is governed by the Central Board for Direct Taxes (CBDT) and is part of the Department of Revenue managed by Indian Revenue Service (IRS), under the Ministry of Finance, Govt. of India. The government of India imposes an income tax on taxable income of individuals, Hindu Undivided Families (HUFs), companies, firms, co-operative societies and trusts and any other artificial person. Levy of tax is separate on each of the persons. The levy is governed by the Indian Income Tax Act, 1961.

Challenge

Since recently the Commissioner of the Income Tax Office in Chennai started complaining of theft. The main concern was that equipment got stolen from the desktop machines on a regular basis. The hardware costs alone are large, and the loss of sensitive data was a hidden cost that was also of great concern. Lack of a system in place to track such incidents allowed no traceability of lost asset or data. With ReSOFT, we proposed to track these infractions and provide the necessary traceability.

The following two incidents that occurred in the Income Tax premises were typically the cases that drive the urgent need for having a system to manage, monitor and track assets.

Asset Loss from New Block

A CPU had all its essential components missing on 25th July, 2008 from Rooms in the new block.

Tampering of ReSOFT software in Devices

There were two failed attempts to uninstall ReSOFT software from a machine, by a user logged in as "TEST". Having been unsuccessful with the removal of software, the person had tampered the directory structure to make ReSOFT unusable.

Solution by ReSOFT

The HandsFree Networks team provided a comprehensive report identifying the high priority threats by ReSOFT with supporting facts regarding the same. ReSOFT's powerful Asset and Inventory Tracking and Data Leak Prevention features tracked down all the unauthorized usage of the desktops in the premises.

ReSOFT's powerful asset management feature provides a number of ways to closely monitor unauthorized asset movement. Every machine logs complete asset information to the ReSOFT server which allows us to generate asset reports and alerts.

There are very suggestive instances of data misuse and leakage at the Tax department captured by ReSOFT event logging. Data leakage can take many forms.

Although data leakage can be unintentional and result of human error, it is often the result of specific targeted actions which lead to the loss of sensitive information. The following are main causes of data leakage from Tax department network:

- Open access to USB ports on the desktops allowed users to copy data
- Access to CD-ROM drives allowed users to burn data on media
- Over 85% of the users had administrator privileges. This allowed them to freely access network resources and modify hardware settings
- Strict policies for network resource sharing was non-existent

Another major threat was out-of-date virus definitions in the Anti-Virus Programs installed on the desktops made the network sluggish and systems crashed down easily causing application damage. A huge number of events captured by ReSOFT indicated the use of various unauthorized software such as games, media players, CD burning software etc on the desktops. Users installed games, stored music files and video files that took up a lot of space on their hard drives. By not controlling the use of these softwares the Income Tax office wasted a lot of computing time and productivity. As most of the users on the LAN have administrative privileges and have access to USB ports and CD ROM drives, they are encouraged to install software and store unwarranted data on their machines.

I.T. Infrastructure – Income Tax Office

Results

ASSET & INVENTORY TRACKING

The Income Tax Office used HandsFree Networks Asset & Inventory Tracking to constantly monitor all the system's assets and received alerts regarding the same in the form of SMS or e-mail in case any changes in asset configuration took place. Scheduled automatic Asset Survey Report periodically tracked the last login and login duration on the machines. Alerts were generated when systems have not been turned on for more than 16 hours. They could clearly see the configuration of any PC on their network, diagnose problems with the PC and apply the fix. As a result of greater visibility there was better monitoring of unauthorized asset movement and track transfer of sensitive data on the network. This benefitted with cost effective system maintenance and problem management.

ANTI-VIRUS SECURITY MANAGEMENT

Anti-Virus Softwares were installed remotely on all systems through ReSOFT. Installation of updates on one machine in the network and distributing to all machines on that site enabled the anti-virus to work better and more effectively. All PCs now have 100% patch and virus definition compliance all the time without any manual effort needed from their internal employees.

DATA LEAK PREVENTION

HandsFree Networks Data Leak Prevention enabled restriction on usage of external media and blocked USB ports. Strict user access privileges were installed to block unauthorized applications from running on desktops. All external storage media usage and transfers were monitored and reported.

Next Steps

Besides using ReSOFT, HandsFree Networks also suggested the following security measures to be implemented for better I.T. security and access.

- Control network resource (files) permissions centrally. This will restrict any unauthorized use of data and asset on the network.
 - Prevent data loss due to unexpected power shutdown.
 - Tighten physical asset security by ensuring every CPU is protected using hardware locks.
 - Set up a data backup mechanism to protect critical data.
 - Every asset must be accountable for by the computer operations team. Currently there is a lack of ownership of the situation.
 - Ensure every machine must be connected to the LAN so it can be tracked. A number of machines in the "Main Block" have network cables damaged.
- Manage the user and network policies using Microsoft Active Directory.
 - Active Directory also allows administrators to assign policies, deploy software, and apply critical updates to an organization. This will add traceability at the user level and controlling user privileges.
 - Create windows username for every employee which they must use to log on to their machines.

About HandsFree Networks

HandsFree Networks is one of the leading Support Automation Platform providers to global IT services providers, MSPs, and other IT-intensive organizations. HandsFree Networks is helping IT Industry think beyond the traditional way of doing support and Infrastructure management, delivering superior user experience and effective tools to move away from traditional phone or remote control support which associates human effort through manual support tools. Our solution addresses every need, so our offerings are structured for a wide spectrum of customers.

For more information on the HandsFree Network Support Automation Platform, visit us at www.handSFreenetworks.com



HandsFree Networks Inc
1021 Main Campus Drive, Suite 300
Raleigh, NC 27606 (US)

HandsFree Networks Pvt. Ltd.,
4th Floor, Concorde Block, UB City,
Vittal Mallya Road, Bangalore-560001 (INDIA)

www.handSFreenetworks.com

HandsFree Networks and related HandsFree Networks Corporation logos are registered trademarks of HandsFree Networks Corporation. Copyright ©2009 HandsFree Networks. All rights reserved. All other company, product and brand names are trademarks of their respective owners.