CASE STUDY:MNC AUDIT AND ACCOUNTING FIRM

1   BUSINESS CHALLENGE

- Securing sensitive corporate information
- Monitoring of social media and online chats
- Unproductive usage of internet and the desktop machines
- Using company machines for storing personal images and videos

As an audit and accounting firm they are responsible for maintaining huge amounts of customer data. Further their main IP lies in the various audit templates and documents which are produced when Audit is done. As such the security of data is crucial for their business. Further most of our staff are highly paid individuals and as a firm whose revenue is based on chargeable man/days it is important to know if any of them are being under-utilized or are just simply wasting time.

As an Audit firm the company has strict policy on misuse of company resources and in order to ensure compliance deployed **Sophos** at the end point. They also used Windows AD configuration to block various type of chat applications and block people from installing any software on their machines. However their test showed that Sophos was not up to the task.

2   E-SAFE COMPLIANCE SOLUTION

During the initial rollout e-Safe Compliance was installed in silent mode to evaluate the level of the problem. Following is a summary of the findings:

1. They detected two of their staff members who had resigned copied large amounts of company's data on their thumb drives on their last day in office. This was a clear breach of their contracts.
2. Using E-Safe Compliance they detected their staff members opening discussing their projects with external people over Facebook, Skype and online chats such as Gtalk. This was a clear breach of the company's NDA with their customers. Although their IT guys had blocked Skype ports, they found Skype to be very resilient to any blocking.
3. E-Safe Compliance detected some unauthorized people accessing sensitive information such as client list.
4. Nearly 75% of internet time was related to time spent on unproductive websites. As most people had laptops this analysis was limited to working hours.
5. There was evidence of some people accessing pornographic images, videos and websites. Although most of these sites should have been blocked but as Sophos is a URL list based system it is unable to block the various different kinds porn sites. Further Sophos had no answer how to detect offline porn based material.

6. Nearly 10% of unproductive time spent on playing games and watching movies during working hours was detected. Although games installation was blocked people tend to play simple Macromedia Flash based games which don't require admin rights.

7. E-Safe Compliance's drive Audit detected huge number of personal video and images being stored in company machine. With the top violator having nearly 800GB of video files in his 1TB hard drive.

8. E-Safe Compliance also helped them to identify machines which had been left switched ON without much usage. This resulted in wastage of electricity and was a breach of company's IT policy.

2.1 BUSINESS BENEFITS

On analyzing the findings the company announced to their staff that their machines will be monitored and they should refrain from doing non-company related stuff on company machines as specified in their contracts and IT Policy during working hours. This resulted in the following benefits:

1. Legal notices were sent to two ex-staff to delete the copied files. This event was made public in the company which eliminated the unauthorized access of information within the company.

2. The threat of staff discussing client information over social media, chats etc was minimized. As the staff knew they will be tracked these discussions became professional in nature and these media were only used when absolutely necessary.

3. On announcing to the users that they will be monitored and the top violators will be alerted by their managers there was a 50% reduction in the amount of time spent on unproductive internet surfing.

4. Staff stopped wasting time watching movies and playing games. Using E-Safe Compliance they could now block these games from running on the machines.

5. The issue of pornography was completely solved. As people knew they can get caught while accessing this kind of material whether from online or offline sources they stopped doing it.

6. With E-Safe Compliance company implemented a policy of limiting the size of personal files per machine. Further they asked their staff to sign an indemnity stating that the staff takes full responsibility of the legality of the video and audio content stored in their machines hence protecting the company.

7. Using E-Safe Compliance company implemented shut down or hibernate settings on PCs hence helping to save electricity