CASE STUDY: MNC SHIPPING AND LOGISTICS

1 BUSINESS CHALLENGE

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

The company is one of the largest shipping and Logistics Company. Being in the logistics business they employed an extensive admin work force. The number of orders and the speed with which they can be processed is extremely important to their delivery business. As such monitoring the productivity of these staff is crucial to the profitability of the company. In order to tackle the issue of unproductive use they have established extensive desktop and internet usage policies which had to be signed by any employee joining their work force. In order to enforce these policies they and block unproductive sites and secure their information they deployed **Trend Micro Antivirus.** However they didn't see any considerable increase in productivity.

The company's sales staff used Skype and Facebook as a means of communicating with their customers however had no way of monitoring their usage as Trend Micro could not monitor activities over social media sites, chats etc or being copied on thumb drives. It only served to protect the company from outside threats such as hacking and sniffing but failed to detect what people were actually doing in the office.

Due to the global nature of their business majority of their internal application were run on the internet; however they faced bandwidth bottle necks during peak hours. They had in the past consistently upgraded their bandwidth to solve this problem but didn't have any satisfactory results.

The company decided to try e-Safe Compliance to evaluate their desktop utilization.

2 E-SAFE COMPLIANCE FINDINGS

e-Safe Compliance proof of concept implementation displayed shocking results. e-Safe Compliance was installed in silent mode in this phase.

1. Nearly 60% of internet usage was of personal nature and had nothing to do with the company. These accounted for mostly the admin staff members who were not required to use Facebook to connect with their customers.
2. For the sales staff members who were required to use Facebook, e-Safe Compliance helped to identify numerous instances of staff spending time playing Facebook games or just using it for personal purposes.

3. e-Safe Compliance detected various instances of inappropriate chat conversation with the customers which could directly hurt the reputation of the company
4. Some admin staff members were detected having watched movies or playing games for more than 50% of their PC usage time. This directly related to underutilization of some staff members.
5. e-Safe Compliance detected foul language interactions between staff and their customers using company emails.
6. e-Safe Compliance detected some staff copying emails containing customer's information over thumb drives. Considering majority of the business of the company is run over the email, this was an unusual activity which required investigation.
7. e-Safe Compliance detected high access of unauthorized documents being accessed by staff members from file servers.
8. e-Safe Compliance detected some staff accessing pornographic websites, images and videos. Trend Micro as mostly a URL lists based blocking system was unable to block the various different kinds of pornographic websites and it has no way to detect offline pornographic images and videos. As staff knew they will not be caught they continued in these activities. This was considered as a serious breach as the company had zero tolerance on pornography
9. 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 500GB of video files in his 750 GB hard drive.

2.1 BUSINESS BENEFITS

The company decided to proceed with e-Safe Compliance. 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 during specified hours or unless specifically authorized by their managers.

1. e-Safe Compliance provided the top management a view of those people who were under-utilized by overall organization, by department and by individual user. As such in the event department heads asked for more resources the top management now had means to verify their claim. Further to solve the problem completely, they employed a process of sending the desktop and internet usage of each department with details of their staff to the department heads. The department heads now had clear idea about their staff utilization and could take appropriate actions against those who were not performing. This process dramatically helped in improving the productivity of the entire organization and helped in reducing the use of internet bandwidth for unproductive reasons.
2. The process of letting the department heads know using e-Safe Compliance's department level reports about what their staff are doing was also done for the potential information leaks for example via thumb drive etc. This was done as the department heads were the best people to know and question the transfer of that information. This greatly helped in eliminating the information leaks within the organization. Further this process also helped in eliminating foul language transaction between staff members and company's customers.

3. The use of Facebook and Skype by sales staff for personal use was drastically reduced as they knew they are being monitored.
4. The issue of pornography was completely solved. As people knew they can be get caught while accessing this kind of material whether from online or offline sources they stopped doing it.
5. The company had an existing policy where staff members were only allowed to store the personal files in a specific folder on the PCs desktop. Using e-Safe Compliance drive audit the IT personnel could now verify this and also manage the amount of personal content allowed per staff. Further staff members were informed that based on company's existing IT Policy they are not supposed to download these media using the company internet connect and that they will be personally held liable in the case any of the stored information is found to break any piracy laws. By implementing a policy of alerting the top violators they managed to drastically reduce the amount of personal media file and completely eliminated the use of company's internet for personal downloads and uploads.