CASE STUDY: COMPUTER EQUIPMENT MANUFACTURER

1 KEY ISSUES:

- Combating industrial sabotage
- Ensuring the productive use of internet and computer facilities
- Monitoring mobile users with laptops
- Securing sensitive corporate information
- Using company machines for storing personal images and videos
- Time spent by R&D members playing games
- Measuring the effectiveness of their central blocking system to prevent access to unproductive sites

With 25,000 employees the company faced various challenges in monitoring and securing their desktop and network environment, ranging from productive use of facilities to securing corporate information. To secure their networks the company deployed **Websense security** to monitor and block unwanted material at a global level and **Trend Micro Anti-virus** on the endpoints. However, this approach was proving insufficient in solving the issues. With respect to information security, the company had installed **Symantec DLP** for certain departments but its complexity and price was a major inhibitor in a mass rollout. Further Symantec DLP had no ability to control the information being sent over social media sites such as Facebook or online chats such as Gtalk. Consequently, the majority of their endpoints were mostly unguarded and the company constantly received reports of people are using 3G modems and proxy's etc to bypass Websense. The issues were further multiplied when the company implemented a 'bring your own device' policy with more and more staff bringing laptops and the company with no means of identifying what employees did with the company's data once they left the office.

As a leading equipment manufacturer the company has a substantial R&D department whose staff members needed to be given admin rights. These rights meant they could install whatever applications they like. In many instances the company discovered employees had installed games and other non-productive activities but faced an uphill battle in locating these software applications and in the absence of an audit trail to suggest who installed them, employees simply denied they were responsible.

More importantly the company had recently become a victim of industrial sabotage, the source of which it was unable to trace. The company produced HDDs at its factory, with the resulting products rigorously tested against a range of parameters to ensure their quality prior to their release. The test results of random batches of HDDs were being manually altered so that faulty HDDs were released onto the market, damaging the company's reputation.

2 E-SAFE COMPLIANCE SOLUTION

The company evaluated *e*-safe Compliance and found it increased visibility of employee IT activity and provided a solution to their issues in the following ways:

1. Setting DLP rules to monitor documents containing test results, the company was able to track who was changing the test results and most importantly what those changes were, allowing it to find the insiders responsible for the industrial sabotage.

2. *e*-safe Compliance gave the company the ability to monitor communication and documents not only in desktop machines but on laptops. If the laptops were removed from the office premises (network), *e*-safe Compliance was still able to monitor and report on any infringements.

3. *e*-safe Compliance provided a complete audit trail of sensitive information being discussed over online source and sensitive documents being copied onto USB drives.

4. The application usage reports from *e*-safe Compliance gave the auditors clear evidence of which staff were playing games and spending time on unproductive applications. All employees were informed that they were to be monitored and as a result the time wasted on non-work related and unproductive activities has ceased.

5. Using from *e*-safe Compliance's Software Audit and Application Monitoring facilities, the company was able to block unauthorised applications.

6. With *e*-safe Compliance's advanced porn detection technology the company was able to identify staff who were responsible for storing and accessing pornographic material, both in their machines and on the server shared drives

7. The company no longer has to worry about employees connecting to the internet using non-corporate network sources such as 3G modems or external Wifi networks, as they are now constantly monitored by *e*-safe Compliance.

8. *e*-safe Compliance has assisted the company in analysing their internet utilization. The majority of internet activity was found to be unproductive. Using Websense, the company only received visibility of the number of hits on URL's but had no idea how much time was spent on these websites. Furthermore it was difficult to identify who was responsible for the activity. Using *e*-safe Compliance they are now able to obtain reports on time spent on unproductive internet websites at various levels such as overall organisation, department or by particular user. This has enabled the company to manage employees more effectively and raise productivity