CASE STUDY: FINANCIAL SERVICES COMPANY

1 KEY ISSUES:

- Sensitive corporate information not secured
- Data leakage reports not reaching the relevant people.
- Data leakage reports not detailed enough to follow up on.
- Ensuring the productive use of internet and computer facilities
- Ineffectiveness of their existing end point productivity monitoring and DLP systems

With US$16 billion of managed assets, 3,000 employees and a reputation for propriety to maintain, Data Leakage Prevention was of paramount importance. The company had implemented **Symantec**'s end point DLP solution for protection of data and had locked down the PCs and laptops by limiting the applications / websites accessible (via **IronPort**) to those necessary for day-to-day operations. Despite this, data was being regularly leaked to the media and so the CEO requested an audit using e-safe Compliance on 500 PCs under the direction of the Chief Integrity Officer.

2 E-SAFE COMPLIANCE SOLUTION

At the beginning of the audit it quickly became apparent that, unlike e-safe Compliance, the existing DLP system did not support the decentralized specification of sensitive data and so over 50% of sensitive documents in the company were not protected. Implementation of e-safe Compliance allowed for fully coverage of sensitive data, via i) usage of the e-safe Code Generator application by department heads, and ii) by allowing the end-users themselves to protect sensitive documents through a simple mouse click.

The review of the reports at the end of the audit period demonstrated the following major advantages of e-safe Compliance over the existing system:

1. With e-safe Compliance, the department heads who had defined the rules were the ones that directly viewed the reports. In the existing system, the reports on the movement of sensitive data were centralized and reviewed by the IT department which were ineffective.

2. The reports produced by e-safe Compliance contained detailed information regarding the context in which the sensitive information appeared as well as the event context (to who the information was sent, etc). As such the reports were actionable. However, the reports provided by IronPort and Symantec were limited to statistical data in the form of pie-charts.

3. The sensitive documents were protected using Universal Encryption with user access controls and sandboxing of the viewing application. This meant that the contents of the document cannot be directly leaked by users even when that document is transferred to 3rd parties.

4. e-safe Compliance provides a larger coverage than the existing system. Users who were getting around the existing system by using portable applications over 3G modems (smart phones) to view inappropriate material and unproductive websites were caught by e-safe Compliance.

As a result of the audit, the company purchased e-safe Compliance for all its PCs.