MOST FRAUD CASES INVOLVE SENIOR MANAGEMENT. HOW TO PREVENT THEM FROM MISUSING THEIR POWER?

Based on Gartner

"Worldwide spending on information security will reach $71.1 billion in 2014, an increase of 7.9 percent over 2013, with the data loss prevention segment recording the fastest growth at 18.9 percent, according to the latest forecast from Gartner, Inc. Total information security spending will grow a further 8.2 percent in 2015 to reach $76.9 billion"

Unfortunately spending huge sums of money have not resulted in the reduction of Fraud cases as can be seen from a 2012 report on fraud cases in US financial services, such systems have largely been a failure.

- **IT systems detected only 6% of fraud cases, with the majority found via audit processes.**
- **Over 70% of fraud cases involve insiders.**
- **Over 50% of those involved in fraud were VPs, managers or held supervisory roles.**
- **Stealing Personal Identification Information was the most common means of fraud.**

(Cummings, Lewellen, McIntire, Moore, Trzeciak (2012), 'Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector', Software Engineering Institute, Carnegie Mellon University)

The key reason for this failure is that protecting against insider threats is not an IT problem but a business problem. Existing security solutions like firewalls, Data Leakage Prevention (DLP) systems, which try to prevent unauthorized access to sensitive information, do not tackle the issue of fraud. What is required is an approach where the auditing of users with authorized access to sensitive information is central to the implementation of the system.

1 WHY EXISTING SECURITY SYSTEMS LIKE DLPS FAIL

The biggest challenge in information security is detecting the theft of sensitive information by users with legitimate access to that information. For example, a procurement manager sending an email out to a 3rd party containing upcoming tender details. Another common example of this is copying and destruction of information by users who have resigned or are about to resign. Existing solutions, like DLP systems, are unable to meet this challenge due to the following reasons:

- **Information Owners (Heads of Department) are unable to directly control the information for which they are responsible.** Sensitive information is created daily in a decentralized manner at the departmental level. The only people who can actually decide the appropriate use of this information are the department level staff themselves. Unfortunately traditional

security approaches rely on central tagging and monitoring of sensitive information and there is no automated way of tagging new information being created on a daily basis. Further, as they rely on central monitors rather than department level monitors they have no idea what qualifies as inappropriate usage of sensitive information. **As such sensitive information which can actually hurt the organization never gets tagged and monitored.**

- **Focused on Unauthorised users rather than Authorised users.** The standard industry security solutions, such as DLP systems, are built to catch and flag illegitimate access. They do this by restricting access to sensitive information. This works fine as long as the person is not authorized to have access to the information. In the case they do have authorised access these systems don't raise any alarms. As such authorised users and their interaction remain largely unmonitored.

- **Real sensitive information is not shared with, or monitored by IT staff.**
  Real Sensitive information like board papers, new acquisition documents etc are often considered to be too sensitive and are not shared with the IT staff maintaining the security system. When the information cannot be shared with the IT staff the information never gets protected.

- **IT staff cannot identify actual leakage of sensitive information.**
  Where potential leakages of sensitive information are captured, the IT staff need to review the incidents to determine whether the leakage is genuine or a false positive. As the IT staff do not know much about the people using the information, the operational circumstances and what constitutes misuse of the information, they are unable to make this decision accurately. As a result serious leakages go unreported or else a lot of false positives get reported to the management

- **No education or involvement of users and so no modification of user behaviour.**
  DLP systems do not visually indicate whether documents contain sensitive information or not. This means that users are unaware of the importance of some documents and unwittingly violate DLP rules regarding their usage. Further, DLP systems do not allow users to provide feedback directly to the information owners as to their changing business needs regarding the sensitive information. The lack of education means the users are unable to modify their behaviour in handling sensitive information. The lack of involvement means they are unable to modify the behaviour of the DLP system to match their business needs. This quickly leads to user dissatisfaction with the DLP system.

2 THE SOLUTION → A STAFF BEHAVIOUR IMPROVEMENT SYSTEM → A SMART DLP

e-Safe Compliance is a staff behaviour improvement System. It is built on the philosophy of "**Educate**, **Trust And Verify**". e-Safe Compliance enables information owners and users to **educate** each other on what information is sensitive and the changing business needs regarding its use. e-Safe Compliance avoids operational overheads through **trust,** by making information owners responsible for protecting sensitive information through specification of document rights, and allowing users to override document rights when necessary. e-Safe Compliance enables information owners and auditors to **verify** that sensitive information is protected and not misused by monitoring its usage and highlighting potential issues.

e-Safe Compliance is the only system to protect against both insider and outsider threats:

2.1 BEHAVIOURAL ANALYTICS TO DETECT POTENTIAL THREAT POINTS

e-Safe Compliance using user behaviour analytics automatically builds a profile of each user's normal activity, and alerts security teams to anomalies. e-Safe picks up indicators of compromise like unusual use of admin / hacking tools, unusual transfers or consolidation of data, and unusual after-hours activity. When used in combination with threat intel feeds and/or perimeter security tools, e-safe can also be used to identify compromised machines and the source of an attack.

2.2 SECURING INFORMATION AT ITS SOURCE, ELIMINATING THE NEED TO BLOCK

e-Safe Compliance was designed in a way that assumes that you cannot stop information from getting out as there as just too many media (handphones, chat, websites etc) involved. Further if the insider is involved he can simply access the information from his house PC. e-Safe Compliance solves this problem by securing the information at its source by encrypting sensitive documents using **universal encryption**. The document encrypted using universal encryption can only be opened on devices having the e-Safe agent installed and with the relevant user credentials, and is tracked throughout its lifecycle from creation to deletion using e-Safe. This ensures that admin doesn't need to worry if the sensitive document gets out as it is encrypted.

2.3 EMPOWERING END USERS TO CLASSIFY AND MONITOR SENSITIVE INFORMATION THEMSELVES

e-Safe Compliance ensures that all transactions done by authorized users are analysed and monitored by users who understand them. This is made possible via e-Safe Compliance decentralized management components which are as follows:

- Using e-safe Compliance information tagging utility authorized information owners can classify large amounts of information into rules which are applied within their department.
- Information owners can classify sensitive documents as secret, confidential or internal use using document rights management. They can also specify who can access this information by defining document rights without involving the central Admin.

- Potential data leak incidents which are produced by these decentralized definitions are reviewed by the information owners themselves. In some cases without involving the IT admin completely. As the information owners have a good understanding of the people using the information, the operational circumstances and what constitutes misuse of the information they are able to identify serious misuse of information accurately.

The decentralized security facilities ensure that end-users are engaged in maintaining the security of the information as they can clearly see the results of any mishandling, thus making security part of everyday operations.

2.4 REALTIME FORENSIC MONITORING

e-Safe monitors complete usage of documents and information throughout their lifecycle from creation to deletion using e-Safe's real-time forensic monitoring technology. The technology provides an unequalled audit trail for the monitoring of information by administrators. For example they can know at any time where the particular information resides, who had this information, the movement of that information and a complete history of different versions of the information even if it gets modified.

2.5 SECURITY MANAGEMENT WORKFLOW

e-Safe Compliance security management workflow ensures that any dubious transaction done by the user is reported to the user's boss (the information owner) along with the security personnel. This mechanism of reporting to the users who actually understand the information ensures that staff don't misuse the information. Further, to ensure that the information owners are not stealing sensitive information, the usage reports are centrally audited by the Security department (or similar). This dual reporting is a central requirement for compliance to ISO27001 standards.

A high level diagram of the checks and balances within e-Safe Compliance is shown in figure 1 below.

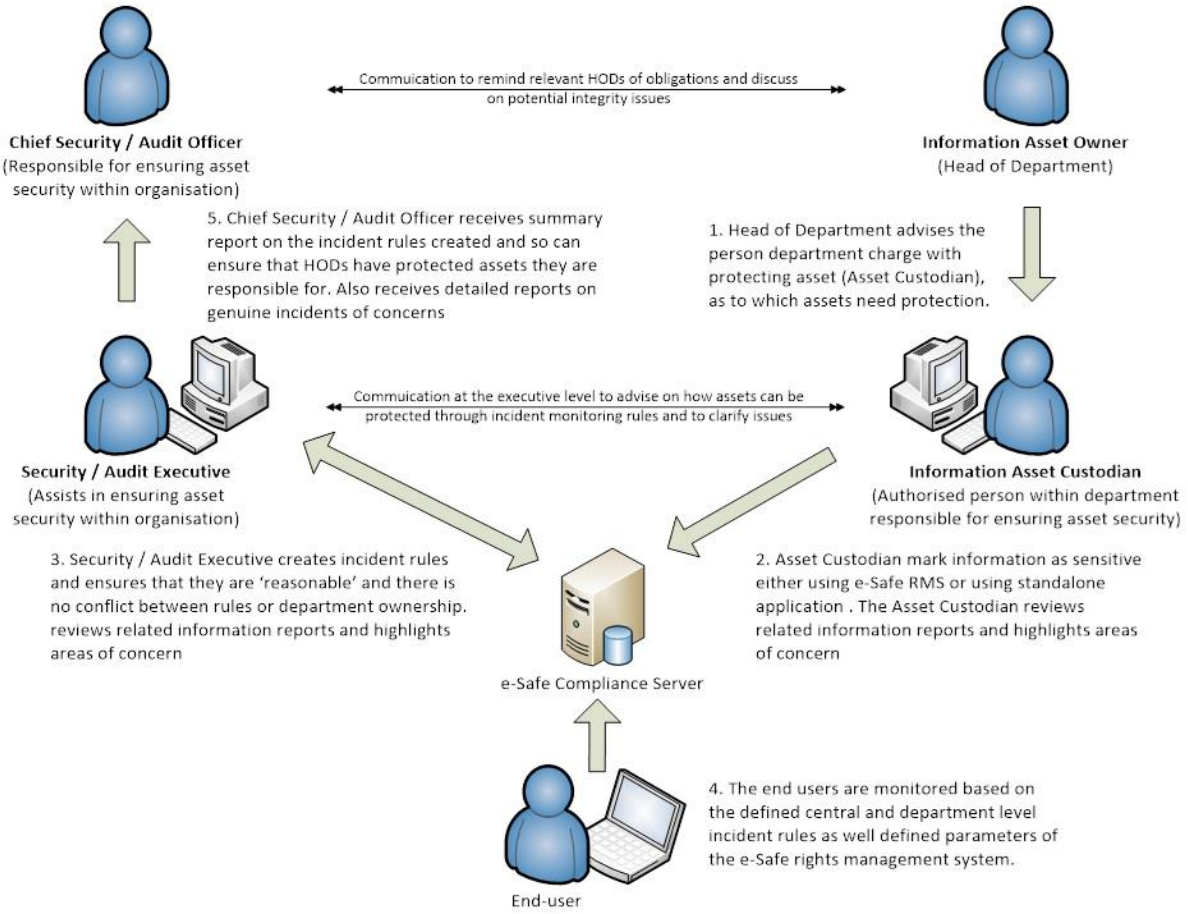

Figure 1 - Decentralized Information Monitoring System (Security is everyone's responsibility)

2.6 VISIBLE SIGNALS ENSURE ONGOING EDUCATION AND ENSURE COMPLIANCE

e-Safe Compliance assists in improving the behaviour of users by educating them on acceptable usage. e-Safe Compliance monitors user behaviour and, when misuse of **sensitive information** or **inappropriate behaviour** is found, it displays warning messages to the user for guidance. For example sensitive information is clearly marked with triangles based on their sensitivity levels (displayed below). The visual representation ensures users are aware they are dealing with sensitive information with appropriate warning messages displayed when they mishandle the information.

Highly Sensitve | Sensitive | Office Use | No Access

In addition to this, users are warned of any misuse of the company property by displaying a clear policy screen when logging into the company's PC**. This visible screen (displayed below) sends a clear customisable message to members of staff that this machine is monitored and thus acts as a perfect deterrent to prevent infringement of the company's IT policy.**