REAL LEAKS INVOLVE PRIVILEGED STAFF – HOW TO PREVENT SENIOR AUTHORISED STAFF FROM STEALING INFORMATION?

1 INTRODUCTION

Legislation, such as the Personal Data Protection Act (PDPA), HIPAA, SOX and the adoption of industry standards such as ISO27001, COBIT, BASIL II, has made the implementation of information security management systems mandatory within large corporations. However, as can be seen from a 2012 report on fraud cases in US financial services[1], 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% those involved in fraud were VPs, managers or held supervisory roles.
- Stealing Personal Identification Information was the most common means of fraud.

The key reason for this failure is that protecting against insider threats is not an IT problem but a business problem. Solutions like 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.

1.1 WHY DLP SYSTEMS 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. 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

[1] 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

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 on what qualifies as inappropriate usage of sensitive information. **As such sensitive information which can actually hurt the organization never gets tagged and monitored.**

- **Existing security solutions only catch illegitimate access.** The standard industry security solutions, such as DLP systems, are built to only catch 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. However when dealing with security risks such as social engineering attacks and insider threat where the target is usually authorised users who have legitimate access these solutions fail.

- **Sensitive information cannot be shared with, or monitored by IT staff.** Sensitive information is often above the pay-grade of the IT staff maintaining the security system. When the information cannot be shared with the IT staff the information never gets protected. Further, where information can be shared, IT staff do not know much about the people using it, the operational circumstances and what constitutes misuse of the information. As a result serious misuse goes unreported or else a lot of false hits get reported to the management.

2 INTEGRITY MANAGEMENT

e-Safe Compliance, developed by e-Safe Systems, is an Integrity Management 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:

- e-Safe Compliance ensures sensitive information is identified and protected by empowering the information owners themselves to classify sensitive information and create the necessary rule definitions, including document rights management. The creation of rules are audited centrally by the Integrity department (or similar) to ensure coverage and avoid the creation of badly defined rules.

- e-Safe Compliance monitors the usage and movement (file transfer, email, webpost, print etc.) of sensitive information by all users.

- e-Safe Compliance presents sensitive information usage reports, with highlighted potential misuse, to the information owners as they are the best people to verify whether there is a data leak or not. To ensure that the information owners are not stealing sensitive information, the usage reports are centrally audited by the Integrity department (or similar). This dual reporting is an essential requirement to adhere to ISO27001 standards.

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

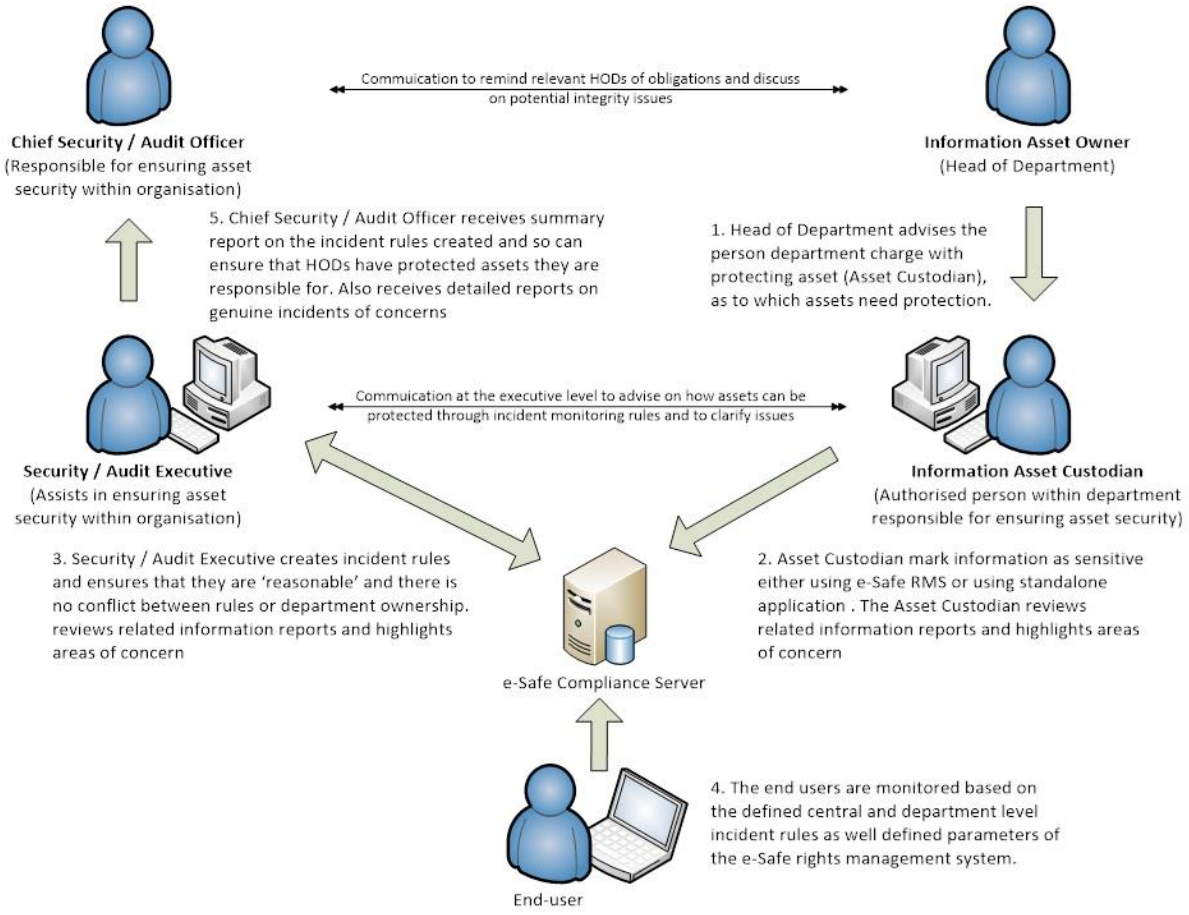

Figure 1 - Decentralized Information Monitoring System (Integrity is everyone's responsibility)

2.1 KEY FEATURES

DECENTRALISED RULE CREATION
e-Safe Compliance enables rule definition by information owners at the departmental level. The advantage of decentralising rule definition is that it makes the system more responsive to changes in business needs. It does this by ensuring that the information owners, who also audit the potential misuse of information incidents, have the tools they need to be able to create or refine rules as required in order to protect sensitive information without compromising operational efficiency.
BUILT-IN DOCUMENT RIGHTS MANAGEMENT
e-Safe Compliance's built-in document rights management i) prevents unauthorised users from opening sensitive documents, and ii) allows restrictions to be placed on the copying from, and printing of, documents by authorised users. Users can protect ad-hoc documents by simply right-clicking on the document and selecting the desired level of protection, and, if appropriate, restricting the document to a group of authorised users. e-Safe Compliance's document rights management works for **all** document formats and even when the users are **offline**.
OVERRIDING OF DOCUMENT USAGE RESTRICTIONS WHEN REQUIRED
DLP systems have two modes of operation: i) restrict document usage, and ii) allow document usage but monitor. Restricting document usage prevents users from doing their job, whilst just monitoring document usage results in the reviewing of a large number of incidents. e-Safe Compliance introduces a third way – "allow users to remove restrictions but require them to provide a reason for doing so". By allowing authorised users to override restrictions the users are no longer prevented from doing their job. By only reporting incidents where the restrictions are overridden the number of incidents to be reviewed is greatly decreased. The inclusion of a reason for overriding the restrictions makes incidents much easier to review and verify.
TRACKING OF DOCUMENT VERSIONS, USAGE AND CHANGES
In order to audit the use of sensitive information it is necessary to have all the track i) the different versions and copies of sensitive documents, ii) changes to user access profiles and content restrictions made by users, iii) the opening and modification of documents, and iv) where required the actual changes to the documents themselves.
AVOIDS CAPTURE OF USERS' PERSONAL DATA
Users often conduct personal activities within the office, such as online banking, which involve the transmission of personal data, such as credit card numbers. By differentiating between customers' personal data and users' personal data, e-Safe Compliance avoids generating false misuse of sensitive information incident reports. Further, e-Safe Compliance ensures compliance with Personal Data

Protection legislation (PDPA), which requires the protection of customer data whilst avoiding the capture of user personal data.

POTENTIAL INFORMATION LEAKAGES REVIEWED BY INFORMATION OWNERS

In e-Safe Compliance, the information owners verify potential data leakage incidents. 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 misusage of information accurately. Further, the reasons provided by users when overriding document restrictions provides feedback directly to information owners and allows them to make changes to rules as required by changing operational circumstances.