Master Thesis

“Dealing with information loss”

“Information as a valuable asset and extrusion detection for protecting e-mail usage. An insight out oriented approach”

Author: Arjen Constantijn Berends

Programme: Informatics & Economics

Erasmus University Rotterdam

Supervisor at Erasmus University Rotterdam: Dr. Ir. Jan van den Berg
Supervisor at Deloitte Netherlands BV: Drs D.M. Wieringa, H. Bootsma

Preface

This Master's thesis results from a six-month internship at Deloitte Enterprise Risk Services.

This thesis is about information loss and primary about loss by e-mail. Besides describing the problem, current practises are analyses, to see if the problem is covered. Last additional controls are introduced to close the remaining gap.

Supervisors H. Bootsma and D.M. Wieringa gave me the chance to write this thesis about information loss. By providing an insight in the auditing world, I got a better understanding of the matter. I want to thank both for this insight. I also want to thank J. van den Berg for the outstanding guidance in methodology and direction of the thesis.

I could not have finished this thesis without the unending understanding and patience of my supervisor J. van den Berg at Erasmus University, grandmother and my Mother. Joy of ending a great study and the good job opportunities carried me to the end. The years at Erasmus University are never to forget. I've met great people, participated in many projects and Erasmus even brought me to Africa.

Finally I want to thank my grandfather, who is not longer among us, but always has been an inspiration to fulfil my journey to the Master's degree.

Stakeholders

Deloitte Nederland BV

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 140 countries. With access to the deep intellectual capital of approximately 135,000 people worldwide, Deloitte delivers services in four professional areas—audit, tax, consulting and financial advisory services—and serves more than 80 percent of the world’s largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

Source: www.deloitte.nl

Erasmus University

Erasmus University is a university that provides education and research on three domains.

- Economics and Management
- Medicine and Health
- Law, Culture and Society

This thesis was written to complete the Information & Economics course of the Erasmus School of Economics. This school is a faculty in the Ecomoics and Management domain.

Erasmus University Rotterdam has been in existence in its present form since 1973. Its history, however, dates back to 1913, the year in which the Netherlands School of Commerce was founded through private initiative with broad support from the Rotterdam business community.

Source: www.eur.nl

Management Summary

Information is a valuable asset for organizations. Protecting sensitive information has top priority especially now legislation like SOX and Privacy Protection are enforced.

Information loss is a problem and current security practices are not closing al the gabs by witch information can be lost. Although the Security Frameworks mention, the threat of information loss, some even advice consideration for controls, there is no referential found to outbound content scanning.

In this thesis the relevance of extrusion detection is described and how it could contribute to implement current frameworks like CobiT and BS7799 more completely.

Extrusion detection is not an illusion. There are products on the marked providing extrusion detection functionality and they are maturing.

Table of Content

1 Introduction

The motivation to do this research is described. The research objective is explained, and the research methodology to answer the research questions formulated in the research objective. The thesis outline is described in the last part of this chapter to guide the reader.

1.1 Motivation

1.1.1 Introduction

In recent decades the fraction of our economical output that is not physical but information has been rising. [Greenspan,1] Given this shift, the protection of information gains importance.

Information security has been on the agenda of management for a long time. In the networked economy, security has become even more important. Securing the networks linking organizations to the internet has gotten top priority.

Information Security has three properties to which the safeguards contribute. Availability, Integrity and Confidentiality ‘CIA’. Confidentiality is defined as ensuring that information is accessible only to those authorized. Integrity is defined as safeguarding the accuracy and completeness of information and processing methods. Availability has to do with the ability of accessing the IS when needed.

Confidentiality plays an important role. For example, you don’t want users that have access to information that provides a competitive advantage, to forward that information to competitors. Also you don’t want the use of information is violating regulation. Especially privacy regulation is enforcing information security, because more and more personal information is stored digital. Confidentiality is undermined when information is lost. As mentioned before Confidentiality is one aspect of IS and confidentiality can be compromised by authorized users in cases of theft and loss.

This thesis focuses on a different aspect of information security namely the protection of information after authorized access has occurred. Often forgotten, but even the authorised user can cause great damage. In chapter two I’ve listed a few recent incidents involving information loss. These recent incidents show that information loss happens frequently. This loss can be intentional but for a great part also unintentional. For organisations to maintain trustworthy this loss has to be controlled [Gonzalez and Sawicka, 1].

Figure 1.1.1 depicts the situation where a firewall protects the organizations against the outside world but the question arises whether the risk of information loss is also covered? Most implemented controls are oriented on inbound flows. The outbound flow is often forgotten. At most the outbound flow is logged but rarely scanned to see if it is authorised.

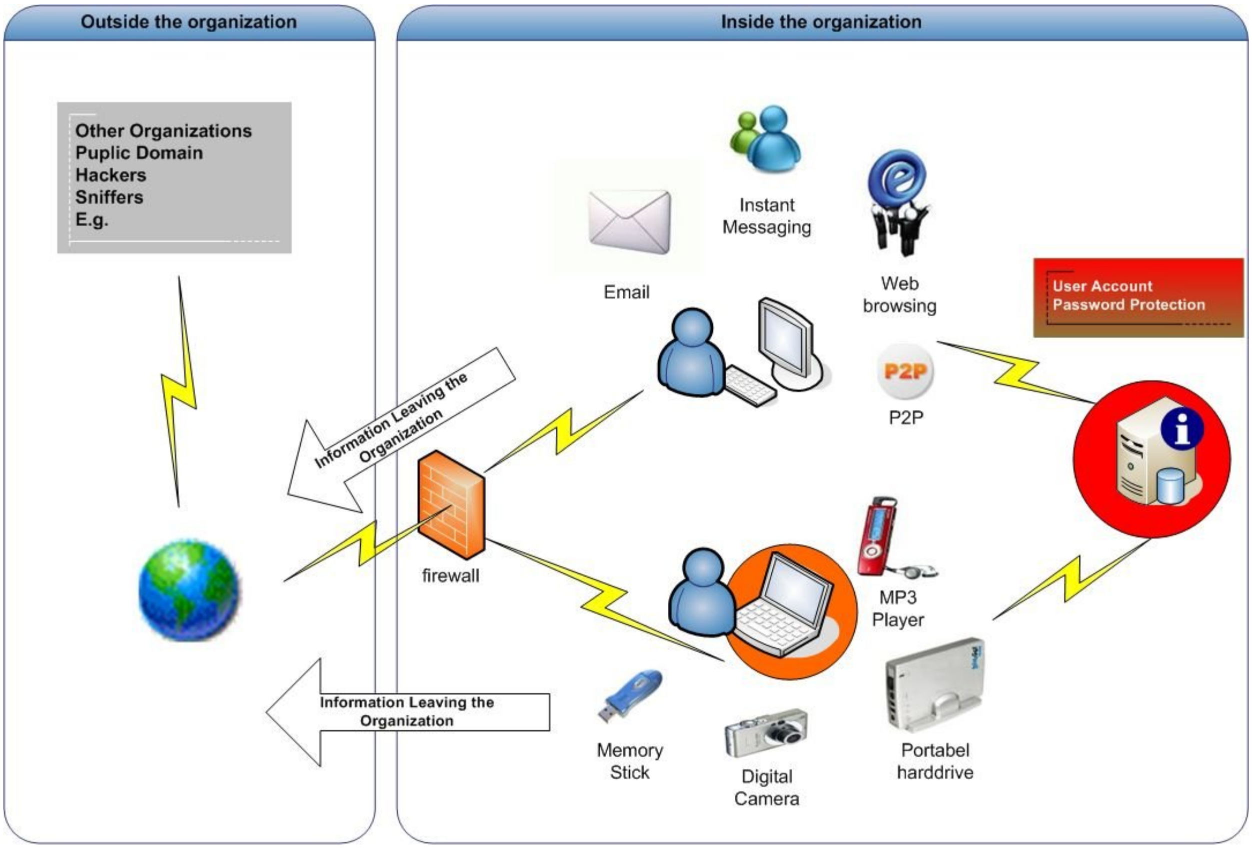


Figure 1.1.1 “Ways how information can leave an organisation"

Beside intrusion detection, a system that detects outgoing information could be useful in protecting information. Such a system is called an Extrusion Detection System (EDS).

1.1.2 Business Drivers

Information is of great value for organizations. Losing information can destroy their competitive advantage. Not only does this information need to be protected against outsiders. Insiders are a threat as well. [Carroll,1]

Intellectual Property

If you look at R&D departments, the information produced is of incredible value for the organisation. A lot of time and budget are located to R&D but information loss can shorten the time competitors need to follow and thereby reducing the return on investment of R&D.

Insider Threat

External threats like viruses and other malware are top security concern but growing awareness of information loss and the damage it can cause sets the spotlight on the insider threat [A,Spee A.Nuijten,1]. This insider threat not only consists of malicious intentions but for a large part of operation errors.

1.1.3 Law and Regulation

Organizations have to comply with regulatory policies. These policies are in place to protect customers and ensure business is done fairly. In chapter Two, I will describe some regulatory drivers that have a direct link with the security of the content of information.

The drivers chosen are:

- Sarbanes-Oxly
- Privacy Regulation
- Health Care Regulation
- Trade Secrets
- Export Regulation

Sarbanes-Oxley

The corporate scandals of 2001 and 2002 involving Enron and WorldCom made that the Sarbanes-Oxly act ‘SOX’ was passed in 2002 in the response to fraudulent management and lack of supervision by Board of Directors. The main goal of SOX is to re-establish the confidence of the shareholders in the financial reporting. CEO’s can be held personally responsible, if there is lack of sufficient internal control’s, for unauthorized acquisition , use or disposition of assets that has a material effect on the financial statement.[NetSec, 1] Assets here has a broad description including digital assets like source code, trade secrets and other sensitive information.

Privacy Regulation

Privacy regulation is another legal driver for protecting information. The security of personal data needs to secure CIA with extra attention to confidentiality. [WBP, 2] Artikel 13 in WBP mentions: security against loss and security against unauthorized distribution which have a direct relation with the need for protecting information. European legislation also requires appropriate technical and organisational measures to ensure security of personal data stated in regulation (EC) NO 45/2001 section 7 article 21.

Health care Regulation

Health care legislation is a third legal driver. In health care a lot of privacy information is present. This information can harm individuals if it gets in the public domain. Insurance agencies for example could reject applications based on this information. It can also have social implications if medical information is loosed.

Trade Secrets

To rely on protection of trade secrets by legislation, you have to comply, in the U.S., with the Trade Secret Act. This act has a six factor test. One of the six factors is the extend of measures taken by the organization to guard the secrecy of information.[Halligan and Weyand,1]

Export Regulation

Export regulation, as a last driver. Governments restrict export of certain assets and products especially when it is military. Two dimensions appear to exist namely the end user/end use and the technology or product. Technology can be defined as ‘specific information necessary for the development, production or use of a product’.[NASA,1] This broad definition of technology and the combination of a networked environment makes information security in relation with export regulation a necessity. This necessity to protect information becomes even more stringent at joint military development projects. Before participating for example in the ‘Joint Strike Fighter Project’ the U.S. will check the level of security including information security before participation is granted.

1.2 Research Objective

Information security is of great importance not only to maintain competitive advantage but also for compliancy and protection of privacy information. A lot of effort is made to secure information against unauthorized access. As soon people have access, my feeling is that little effort is made to secure the way people use the information. This feeling arose while reading literature and during my internship at Deloitte. Three depth interviews were conducted to test this feeling.

I want to research how great the information loss problem is, how current information security practices deal with information loss and if there are ways to reduce the information loss problem with a focus on e-mail. Four sub-questions are formulated to meet the thesis objective. The chapters in which these questions will be addressed are mentioned at the end of each question.

1. To what extent is information loss a problem? *(ch2)*

2. Are the current security practises enough to protect against information loss *(ch3)*

3. Is e-mail usage protected against information loss? *(ch4)(ch5)*

4. To what extent can the risk of information loss, by e-mail, with products offered on the market be reduced? *(ch6)*

Figure 1.2.1 provides a graphical view of how the four sub-question fit, in the big picture, information leaving the organization and the risk of loss. The red arrows are ways how information can leave an organization unprotected. In yellow an EDS attempt to diminish the risk created by e-mail usage.

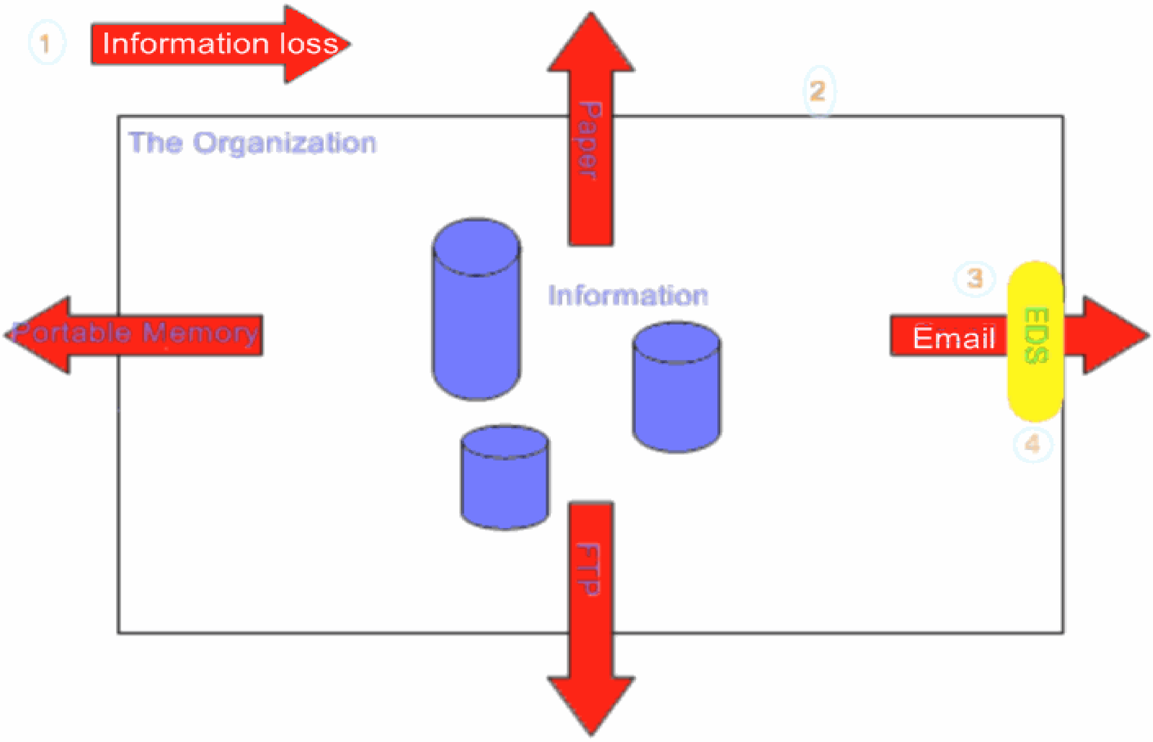


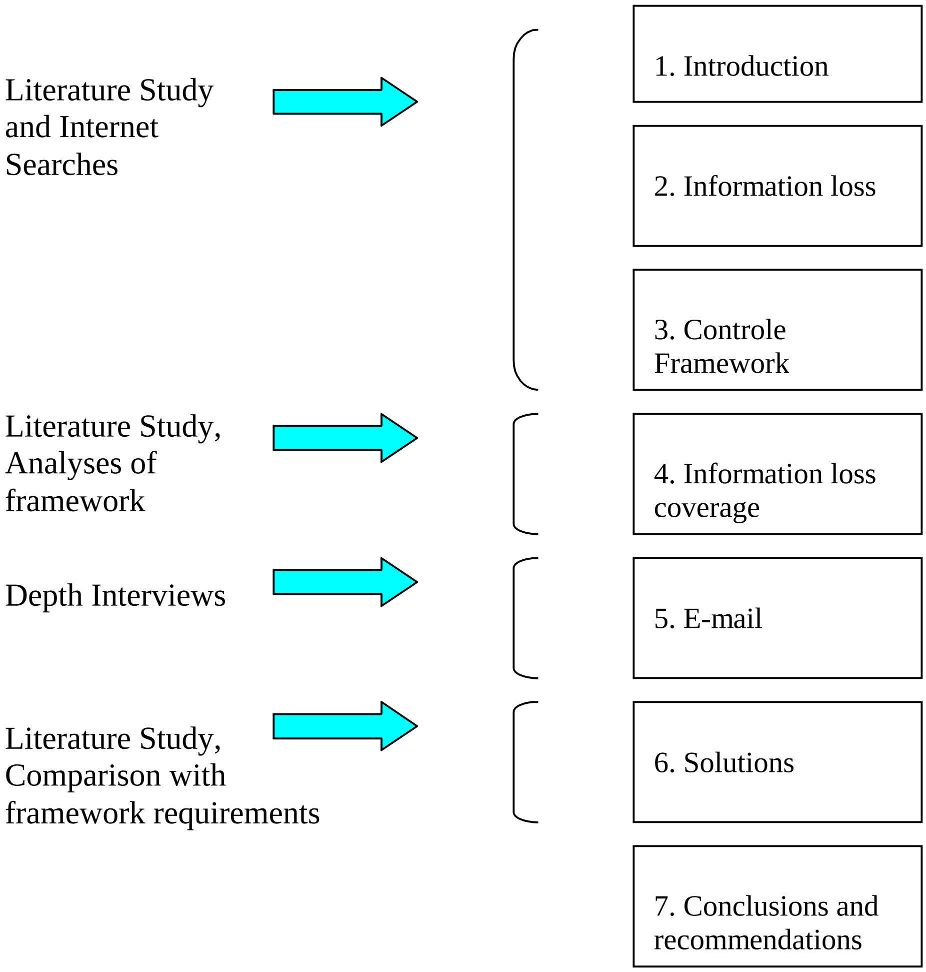
Figure 1.2.1 "Graphical representation of the thesis. The numbers link to the research questions."

1.3 Research Design

This thesis is an explorative research (Wikipedia,1), to see if there is an information loss problem and if an EDS contributes to the reduction of information loss risk. Two control frameworks are also explored on how they cover information loss.

To answer the research questions stated in paragraph 1.2 available literature was studied and three depth interviews were conducted to verify the findings. A short overview of the methodologies used of answering the research questions can be found in picture 1.3.1

The scope of this thesis limits to the problem of information loss, with the focus on e-mail usage.


Literature Study and Internet Searches
Literature Study, Analyses of framework
Depth Interviews
Literature Study, Comparison with framework requirements
1. Introduction
2. Information loss
3. Controle Framework
4. Information loss coverage
5. E-mail
6. Solutions
7. Conclusions and recommendations

1.4 Reading Guide

In this paragraph an outline of the thesis is given. The content of each chapter will be described brief.

Chapter 2: Information Loss

Information loss problem is described and an exploration is made on the impact of loss and how loss occurs. Also the question why organizations should protect against loss is addressed. This need comes not only from the organization itself but is also enforced from the outside.

Chapter 3: Current Control Framework

Current practises on information security are studied. A focus will lie on information leaving the organization and how current practises protect it. BS7799 and CobiT are given a closer look. This chapter is an introduction to chapter four where for outbound information the security gap will be analysed.

Chapter 4: Coverage of information loss by Control Frameworks

In this chapter the information loss problem is compared to the control frameworks to see if there is a mismatch in security practises.

Chapter 5: E-mail

Depth interviews about how people use information, with a focus on e-mail and how well the information is protected, conducted at three companies are worked out in this chapter. These interviews must validate if there is really an information loss problem and maybe a gab in the security practises.

Chapter 6: Solutions for closing the e-mail security gab

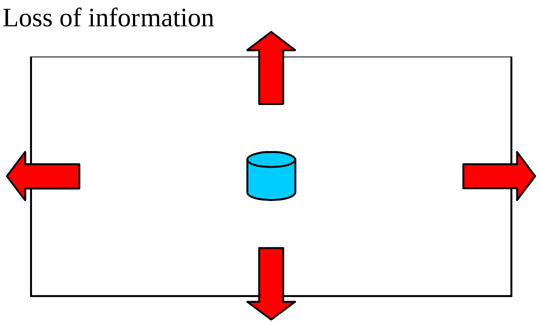
Literature study and analysis of product functionality must provide an overview how some products on the marked can close the security gab found at e-mail usage. Although real life test results where not present, a study of functionality of the products and control requirements provided by security standards should give a overall view how the security gab can be closed or at least be partly closed. Last the limitations of the products described are mentioned.

Chapter 7: Conclusions and recommendations

In this last chapter, the conclusions of the research are presented and proposals for further research given.

2.0 Information loss

In this chapter the information loss problem will be addressed. The different risks loss can have and how loss occurs.



2.1 Introduction

The definition of information loss used in this thesis is; "Information that falls into the hands of unauthorized persons". This definition implies that not only loss occurs when outsiders like hackers provide themselves unauthorized access but also when information is lost by insiders to unauthorized people.

Loss of information may have regulatory consequences. Fines can be imposed and thereby loss has financial consequences. In paragraph 2.3 I will broaden on that.

2.2 Intellectual Property

Everything made in the West can be made cheaper in less developed countries. What gives the West a competitive advantage is information technology. This advantage can only be maintained if the West can maintain the credibility of the information technology. This means assuring Protection of intellectual property [Carroll,1]. Computer insecurity creates a credibility gap. Caroll also mentions the risk of widespread theft of corporate assets by persons with proper access to them, already in 1990.

Ownership of physical assets is easy to be determined. A car, for example, has ownership documentation. A car is linked by a number plate to a person. Information however is not touchable and can easily be reproduced and distributed especially in a digital environment. Who owns information!

Innovation improves existing products and creates competitive advantage but it also leads to considerable investments. Technological assets represent intangible assets because the real added value for an organization is not immediately clear. It represents the qualities of public goods in general. Non-rival possession, low marginal cost of reproduction and distribution, makes it difficult to exclude others from access. If you add the high fixed cost of production, we see to generating returns on these assets is difficult, when the goods are not well protected. To ensure returns higher or at least equals the marginal cost of production technological development would come to a stop if organizations are not able to protect their immaterial assets. [Jemewein, 1]

For protecting immaterial assets like intellectual property, organizations can use several instruments. One is the law with patents, copyrights and trade secrets. Patents allow a market of exchanges of exploitation rights which creates incentives for organizations to share and exploit there knowledge. Protected against imitation organizations can use information in commercially viable activities. [Maskus and Rechman, 1]

Not al information can be protected by law because it is too expensive to patent it or patent information makes imitation relative easy. [Moulton and Bigelow,1].

Information that can not be protected by law needs other instruments for protection. If the likelihood of information loss is reduced, it becomes less likely to resort to the legal system. Instruments for reducing this loss can be found in existing control frameworks.

2.3 Regulatory Drivers

2.3.1 Sarbanes-Oxley

Legislators have an enormous influence on Information Systems these days. Companies are responsible to protect client information and credit card information. But it goes further, the U.S. Public Company Accounting Reform and Investor Protection (Sarbanes-Oxley) Act of 2002 is an act influencing companies world wide. The main goal of SOX is to increase the shareholders confidence in the financial report of organizations. I will describe the impact of SOX on information security briefly.

Background

The introduction of SOX has a close relation to the Enron scandal at the end of 2001. Enron’s complex accounting practises made it possible to mislead shareholders. By reporting fake profits and parking losses at subsidiary companies Enron’s increased its value by 1,2 billion dollars. The decrease in confidence of financial accounting by shareholders diminished even further when it turned out that Enron was not an isolated incident. WorldCom also got bankrupt. Adelphia, HealthSouth, McKesson, Tyco and Qwest were all under investigation after 2001. [Brickey,1]

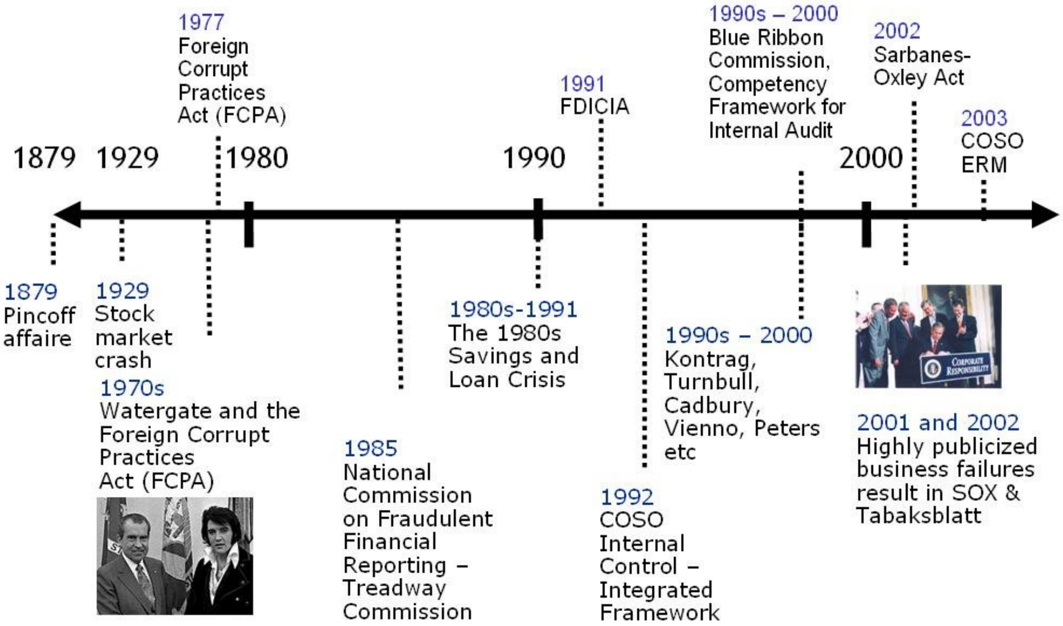


Figure 2.3.1

In figure 2.3.1 we see several scandals and the emerging of the control framework COSO and in 2002 the birth of the SOX act.

To re-establish shareholder confidence, the integrity of corporate managers and accountants had to be safeguarded. SOX is an attempt to safeguard this integrity by making CEOs personally responsible and oblige companies to implement controls to guarantee transparency and correctness of information systems By establishing an oversight board (PCAOB) auditors are inspected and separation of audit tasks from non-audit tasks is closely watched.

Although SOX not explicitly mentions IT controls, it does demand corporate governance. Because IT plays an important role in governance, organizations rely on IT to enhance corporate governance. Direct influence can be found in sections 302, 404 and 409. These sections encompass responsibility for financial reporting, assessment of internal controls and real time issuer disclosures. Section 802 “Criminal penalties for altering documents” makes audit of file use and access a necessity.

404 has the biggest impact where there is a statement required that adequate internal control over financial reporting is present.

(ITGI, 2004)

- *“A statement of management’s responsibility for establishing and maintaining adequate internal control over financial reporting for the company.*
- *A statement identifying the framework used by management to conduct the required assessment of the effectiveness of the company’s internal control over financial reporting.*
- *An assessment of the effectiveness of the company’s internal control over financial reporting as of the end of the company’s most recent fiscal year, including an explicit statement as to whether that internal control over financial reporting is effective.*
- *A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management’s assessment of the company’s internal control over financial reporting.*

COSO a framework describing control objectives is frequent used to meet compliancy with SOX.

2.3.2 Privacy Information Regulation

People buy more products on the internet each year. A lot of online businesses provide an option to save privacy information like credit card data, address and phone number to speed up the ordering process when a customer returns for a second purchase. People, unaware of the security risk leave their privacy information. But how careful is this information handled by online businesses? Not only hackers are a risk for loosing this information but internal handling of this information can also cause loss. Do employees have access to this information? Is it common to mail this information? If so, human mistakes can lead to disclosure of the privacy information. In the Netherlands the law ‘wet bescherming persoonsgegevens’ WBP is enforcing organizations to protect privacy information even against loss.[cbp, 1] Legislation to which all organizations within Europe needs to comply concerning privacy information is regulation (EC) NO 45/2001.

Article 13 of WPB mentions that appropriate measures should be taken to protect privacy information. Paragraph 2.6 says that the taken protection measures should meet three criteria 1) technological possibilities 2) cost of measure 3) risks brought along by processing the protected data and the nature of it. I can imagine that when outbound scanning is becoming common and easy to implement, Dutch law is going to enforce outbound scanning because it is technical possible.

In the US, 21 states now have final or proposed Breach Notification Laws similar to California SB1386. SB1386 states “Any agency that owns or licences computerized data that include personal information shall disclose any breach of the security of the system following discovery or notification of the breach in security of the data” Beside fines that can be opposed this notification can harm an organization’s reputation witch is expensive to restore. SB 1386 also specific mention that the confidentiality and integrity of personal data must be safeguarded.

The health care institutes also posses a lot of privacy information of their patients. In the U.S. the HIPAA act (The Health Insurance Portability and Accountability Act of 1996) defines administrative, physical and technical safeguards, which include standards for keeping the privacy of electronic protected health information (EPHI). It also addresses keeping track of EPHI moving in, out and within the institutes.

See table 2.3.3 for an overview of what is considered privacy information.

PERSONAL INFORMATION	• Name • Gender • Date of birth • Home address • Personal telephone number	• Personal email address • Biometric identifier • Photograph or video identifiable to an individual • Behavioral information (e.g., in a CRM system)
HEALTH INFORMATION	• Medical records • Health plan beneficiary information	• Physical or mental health information • Provided health services or any information collected during the health service
FINANCIAL INFORMATION/ SPECIAL HANDLING PII	• Government identifiers (Social Security Numbers)	• Account numbers (bank accounts, credit cards, etc.) • Personal Identification Numbers (PINs) and passwords to financial accounts
SENSITIVE INFORMATION	• Racial or ethnic origin • Religious or philosophical beliefs • Trade-union membership	• Health or sexual orientation • Offenses, criminal convictions or security measures • Combinations of certain information (e.g., name and ssn)

Table 2.3.3

2.3.3 Export Regulation

Doing business abroad is not always as simple as mailing the product to a foreign buyer. You have to be aware of custom duties but also export rules. You must be allowed to export the product to the country you intent to.

Also in joint projects with foreign organizations you have to be compliant with export rules. Good examples are found in defence projects. If an organization in the US needs subcontractor for a defence project it needs a Global Project Authorization GPA. A GPA consists of a list of allowed subcontractors, regulatory requirements, scope and compliance. The US organization is also responsible for the compliance of subcontractors. To ensure this compliance subcontractors have to sign contracts. In the case of technical assistance a Technical Assistance Agreement ‘TAA’ has to be signed. A TAA is very precise and detailed. In a TAA are for example sales and export limits described and there is an obligation to secure information from unauthorized users.

International Traffic in Arms Regulations ‘ITAR’ are also to be considered within military projects. ITAR applies to the transfer of specific physical items and information and the provision of specific services to persons and entities outside the United States.

It is for a subcontractor very important to show compliancy with these agreements will he be allowed to participate.

Looking at the Joint Strike Fighter ‘JSF’, if you want to participate compliance with U.S. Policies is needed.[JSF,1] This compliance begins with the Arms Export Control Act of 1976 ‘AECA’. AECA requires that the recipient meet de following three conditions prior to the delivery of the relevant equipment, data, and services:

- The recipient must agree not to transfer the equipment, data or services to a third party without prior U.S. government consent.

- The recipient must agree not to use the equipment, data or services or permit their use for other than the purpose for which they were provided without prior U.S. government consent.

- The recipient must agree to provide the same degree of security as the U.S. government for the equipment, data or services provided.

The last condition shows that for subcontractors security is very important. Controls that can contribute to the security of information and authorized use are helpful in getting compliant. This is not trivial and gets even more complicated if employees have multi nationalities and the security incentive of a TAA.

Non military exports are also controlled. The Departments of Commerce regulates the exports of items and information that have civil applications. Items subject to the jurisdiction of The Bureau of Industry and Security ‘BIS’ who is enforcing the export controls, are listed on the Commerce Control List. BIS also maintains the Denied Persons List to witch exports are not permitted.

Penalties for violations of the U.S. export laws can include [Harvard,1]:

Criminal:

“Wilful violations:

- Corporation – a fine of up to the greater of $1,000,000 or five times the value of the exports for each violation;
- Individual – a fine of up to $250,000 or imprisonment for up to ten years, or both, for each violations;

“Knowing violations:”

- Corporation – a fine of up to the greater of $50,000 or five times the value of the exports for each violation;
- Individual – a fine of up to the greater of $50,000 or five times the value of the exports or imprisonment for up to five years, or both for each violation.
-

Administrative:

For each violation, any or all of the following may be imposed:

- the denial of export privileges;
- the exclusion from practice, and/or
- the imposition of a fine of up to $12,000 for each violation, except that the fine for violations involving items controlled for national security reasons is up to $120,000 for each violation.

2.4 Information losses in practice

It is relatively easy to lose information. Who has never left something when leaving after a visit? Who has never sent an e-mail to the wrong person? Just search the internet and you will find that information loss occurs more than you think. In this paragraph some cases of information loss are provided. These cases are found in newspapers and during internet searches by Google.

Information loss by e-mail

PalmBeachPost.com reported on 22 February 2005, that an employee of a health department, conducting research on HIV infected people in Palm Beach, managed to send a list of names to 800 county health department employees. This mistake was made by sending the list to the wrong group in the e-mail program. [Palm Beach Post,1] This was an error in a secured technical environment.

Bbc.co.uk reported on Tuesday 26 October 2004 that two e-mails prepared for the executive director of the bush campaign containing a so called “caging list”, a list of addresses and names of voters mainly in the black and democrat areas of Jacksonville Florida. (BBC,1) these e-mails where send to an unauthorized person and the existence became public.

Recent cases of information loss involving memory devices.

A national Dutch newspaper reported on 2 February 2006, that a USB memory stick has been left in a rental car by a Dutch defence employee. On this stick classified information about activities in Afghanistan and the security of Dutch representatives visiting Afghanistan was stored. This is embarrassment is even greater if you know it is not the first time a Dutch defence employee loses information in public. Resent 23 February 2007, again loss of a USB stick with sensitive information was mentioned in the newspaper (AD,1)

business.timesonline.co.uk reported on 30 May 2005, that the investment banking giant UBS has launched an internal inquiry into the disappearance of a computer disk thought to contain sensitive client information. The article also mentioned a case of information loss where an employee of Brunswick left a sensitive document in a Covent Garden restaurant.

In general information can be lost by transmission over a network. E-mail, p2p programmes and Instant Messaging makes forwarding sharing and misaddressing possible. Second, information can be lost if stored on portable storage devices like USB keys, memory in digital camera’s and portable hard drives. Last, printed information can be lost as we have read in the article of TimesOnline. Sure there are more way’s information can be lost but this thesis will focus further on information leaked by transmission over a network and especially by email.

2.5 Insider Threats

A lot of effort is made to prohibit access to information by unauthorized users. But what about information, going out of the organization, initiated by authorized users. The insider can be a danger to security when he makes mistakes or has malicious intend. So in the attempt to be compliant with regulation organizations shouldn’t forget the insider. [S. Pramanik, 1]

The following statement will illustrate the insider thread. “We have a firewall so we are protected from the Internet” But what if an employee uses a dial in internet connection bypassing the firewall? This line is not protected by the firewall and thereby a security risk. Another example could be “Our private information is encrypted so loss isn’t a risk”. If an employee doesn’t encrypt, to make working at home possible the risk of loss is still present. If an employees chooses to act differently or collaborate the security measures are bypassed.

Some threats that can be exploited by insiders are listed in table 2.1 [S.Pramanik,1]:

1 An insider can read, copy, print and send a document he has access to unless fine grained access control is in place.

2 An insider can become owner of a document by copying it

3 An insider can forward a document to a person either inside or outside the organization

4 An insider can work after business hours when maybe detection systems are not running

5 An insider can copy content of a document into another document

6 An insider can remember content and retype it in a lower classified document

7 An insider can get a dump of memory (such as the video buffer) and then print the document

8 A malicious insider can tamper with the existing rights on the document

9 An insider can misaddress an e-mail. To a wrong email group or person

10 An insider can make a typo in an e-mail address addressing it wrongly. Instead of J.doe P.doe gets the e-mail or by spelling mistakes a e-mail is send to a domain owned by the competitor for example you own .com and the competitor .net

11 An insider can become victim of phising

Table 2.1

Threats 9, 10 and 11 in table 2.1 are added because employees can also make mistakes.

The insider is mentioned but who is this insider. In an article of A.Spee different definitions are mentioned.[A,Spee A.Nuijten,1]. The one used in this paper is;

“Employees, board members and other internal team members, who have legitimate access to information and or information technology. Insiders typically have special knowledge of internal controls that are unavailable to outsiders and they have some amount of access. In some cases, they perform only authorized actions as far as the information systems have been told. They are typically trusted and those in control often trust them to the point where placing internal controls against their attacks are considered offensive.”

If an insider has malicious intent he will always find a way to get information out of the controlled environment. Information security can only delay theft or limit the exploits that can be used.

2.6 Security Survey

During my Internship at Deloitte, a security survey [Survey,1]was held among technology, media and telecommunications companies around the world. Among them where companies like Google, Yahoo, Shell and ING. In total around 300 companies filled in the survey.

The results of that survey relevant for this thesis are listed in table 2.6.1. These results show that the need for protecting information is largely enforced by legislation.

Question	**Result**	**Relevance**
Question 24: What are your organization ‘s top five security initiatives to focus on in 2006	With 34,8% Security regulation and compliance was number one, followed by governance with 23,6 % on two.	Regulation is a big driver for information security
Question 25: What major information challenges does your organization face in today’s operating environment	Budget constraints came one with 20,8% second Increase sophistication of threats and third Emerging technologies like p2p and instant messaging with 11.2 %	With p2p and Instant messaging it is shown that outbound flows are seen as a threat
Question 49: What aspects of security are getting the most investment	The most investment where getting: Logical access controls, Physical access controls and Infrastructure protection.	Focus on access controls not how people use information there is an insight oriented approach
Question 52: What are the biggest regulatory initiatives impacting your organization last year	Privacy and SOX both outscored the rest by 20% Privacy at 28% and SOX at 32%	Regulation is a big driver for information security, already seen by question 24
Question 57: Using scale 0-5 rate the intensity of the following threats you envision the next 12 months	Theft of intellectual property and loss of customer data scored high in comparison to the other threats like viruses and financial fraud.	Information is valuable and needs to be protected

Table 2.6.1

2.7 Conclusion

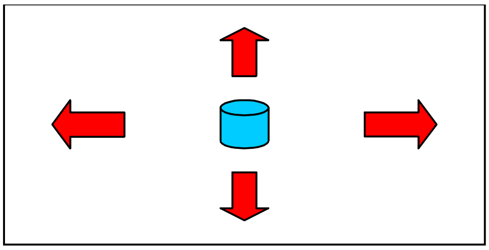
If you combine the insider threat with the information loss cases in chapter 2.4 you can conclude that loss of information is a problem. The problem is big because, it not only consists of intentional attempts, but for the most part of unintentional mistakes. Both from within organizations as from outside, a need to protect against loss is present. Laws like Sarbanes-Oxley and privacy regulation impose an even greater need to protect information against loss. Information loss can have financial consequences in the form of fines. In cases of export rights being not enough secured against loss, can mean losing export rights or rejection of application.

The information loss problem is real and must be addressed. In chapter three current security frameworks will be studied to see if the problem is sufficient addressed.

3.0 Current Control Framework

In this chapter current control frameworks as CobiT and BS9999 and common practices will be studied and their relation to information loss analyzed.

Organization boundary protected by Frameworks



3.1 Introduction

The purpose of information security is to protect organization’s valuable resources supporting the attempt to meet their business objectives. Protecting these resources, such as hardware, software and information require the selection and application of appropriate safeguards. Frameworks like CobiT and BS7799 help with the selection of appropriate safeguards.

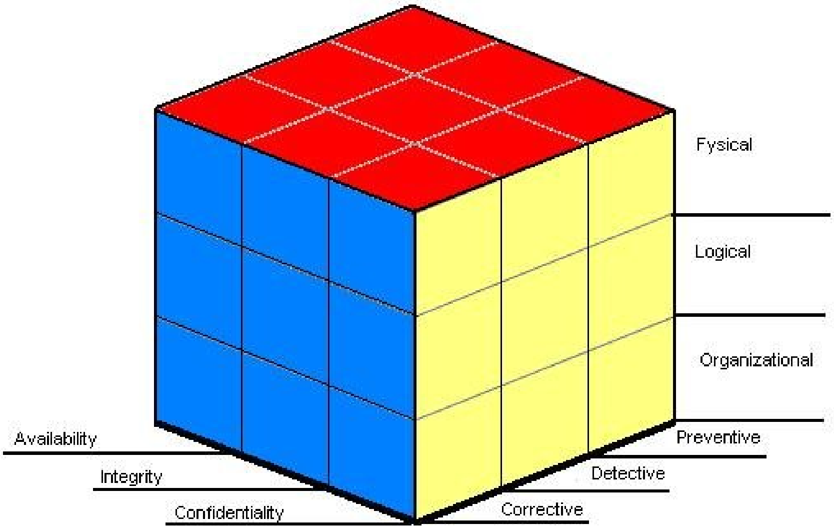
The safeguards protecting the IS differ in nature.[Overbeek,2] We can distinguish physical, logical and organizational safeguards. In this thesis the logical nature is of most importance. This is because the thesis has a focus on information loss by e-mail.

The safeguards have also three different requirements to which they contribute. Availability, Integrity and Confidentiality ‘CIA’. Confidentiality is defined as ensuring that information is accessible only those authorized to have access. Integrity is defined as safeguarding the accuracy and completeness of information and processing methods. Availability has to do with the ability of accessing the IS when needed. Confidentiality is of most importance when we look at information loss because loss is a confidentiality breach.

Last safeguards can fulfil different functions. A safeguard can have a preventive, detective and a restoring function. A detective and restoring function combined is known as a repressive function.

Picture 3.1.1 below shows the universe of safeguard properties.

Picture 3.1.1Universe of safeguard properties



Three safeguards, one from each nature, that protect against information loss, are listed along with their shortcoming on their protection against information loss, in table 3.1.1.

Safeguard	Firewall	Conduct Policies	Security Guard
Relation to information loss	Protecting the IS against outsiders and Limiting outbound connections for example to web mail services. Limiting the way information can leave the organization	Formal writing on how employees should handle sensitive information. On non-compliance legal actions can be taken.	Examine employees leaving the organization (for example control if employees leave with a memory stick)
Nature of safeguard	Technical	Organizational	Physical
Shortcoming	Not able to make decisions based on content	Not able to monitor real-time, needs technical implementation	Not able to make decisions based on content and not able to control digital information leaving the network

Table 3.1.1

3.2 Security Standards

In this paragraph two information security standards, BS7799 and CobiT will be described. These standards are tools for organizations to meet the control level stakeholders desire and sometimes is enforced, as could be read in the paragraph about regulatory drivers.

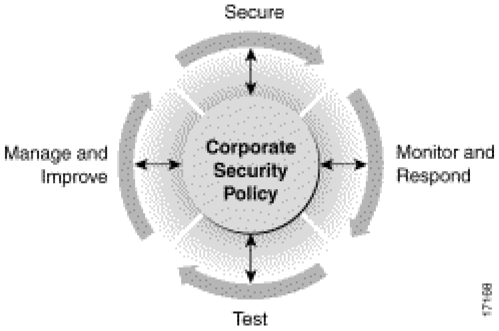
BS7799 The British Standard for information security management was first issued in 1995 to provide a comprehensive set of controls comprising best practices in information security [BS7799,1]. BS7799 has the following definition of information security ‘Preservation of confidentiality, integrity and availability of information’. This standard is chosen because it is widely accepted as a security standard. BS7799 is also known as ISO17799 and after the last updates as ISO27001.

CobiT is an IT-Governance Framework that aims to bridge the gap that exists between the business control models like the Internal Control Integrated Framework ‘COSO’ and the more focused control models for IT. It positioned itself as being more comprehensive for management and operates at a higher level than technology standards for information systems management.

3.3 Security Policy

Establishing policies is an important activity. Policies and procedures help management to ensure risk responses are carried out. Standards like BS7799 and CobiT describe policies that have to be formulated in order to be in control. In this paragraph policies relating to information security will be described and the necessity to monitor compliance.

A security policy is a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide.[RFC,1] The security policy can be seen as the centre of security (figure 3.4.1) All activities affect the corporate security policy. Security has to be monitored and on incidents must be responded. If the responses are not effective the security has to be improved.



“Figure 3.4.1: Security Wheel “

For an organization information is an asset and management is expected to ensure that appropriate levels of controls are implemented to protect this resource. Security officers often see protecting the integrity, confidentiality and availability as the overall objective of an information security program. Information security should be included in all organization’s policies to guarantee appropriate level of control. T. R. Peltier et el mention eleven organizational wide policies which should have a reference to information security.[T.R. Peltier et el,1] In table 3.4.1 the policies covering information security are listed.

Policy	**Description**	**Link to information security**
Employee standards of conduct	In this policy the conduct and expectations of an employee are addressed.	It should also address confidential information “Employees shall also maintain the confidentiality of corporate information”
Information Security	This policy established the concept that information is an asset and the property of the organization, and that all employees are required to protect this asset.	The cornerstone of information security program.
Asset Classification	This policy establishes the need to classify information, the classification categories, and who is responsible for doing so.	If you want to protect, you should at least know what.

Table 3.4.1

Policies can be translated into Standards, Procedures and Guidelines to meet the policy’s objectives [T.R. Peltier et el,1]. The policy is a high level statement of organizational beliefs, goals and objectives and because of the formal nature provides a basis for all standards and procedures.

- Standards are mandatory. They can range from hard and software to use, to the remote access protocol that has to be used. An example is that an Intrusion Detection System (IDS) has to be implemented. An IDS is a monitoring standard.

- Procedures are also mandatory and provide detailed actions required to successfully complete a task. A procedure example would be “if a phising email is detected immediately notify the security officer”.

- Guidelines are more general statements. They are recommendations. Guidelines provide a framework within to implement procedures. The difference between a procedure and a guideline is that a guideline provides a direction and a procedure is enforced.

I will deepen on three policies about information handling monitoring and classification. These three are chosen to illustrate the relation of information loss with policies. See the appendix for the examples. Included as examples, are an automatic forwarded email policy [policy 1], email usage policy [policy 2] and an information sensitivity policy [policy 3].

In the first example we read that the purpose of the policy is to prevent disclosure of sensitive company information. That this policy has to be taken seriously is made clear by the enforcement, which mention up to and including termination of employment and the fact that the CEO has signed the Security Policy. Monitoring of email usage is necessary to control if employees comply with the policy. This monitoring is made possible because in policy 2 section 3.3 states that employee shall have no expectations of privacy in anything they store send or receive on the company’s email system. The usability of this statement differs. In the U.S. this statement is enough. In Europe employees have more right on privacy. Scanning of email even of employees is not always allowed [M. Rustad, 2005]. Policy 3 gives insight in what is meant by sensitive information. Policy 3 describes the categories used and states that who has access and how electronic distribution should be done. If an organization wants to write an Information Sensitivity Policy, it at least should be able to identify its information assets.

3.4 Conclusion

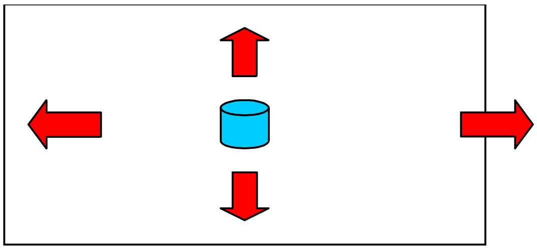
A lot is done in an effort to secure information but as shown in table 3.1.1 there are shortcomings when we look at information loss. The biggest problem is that current security relies on correct labelling of information, by the creator.

In chapter four the security frameworks will be further analysed to see if there is a security gab when it comes to information loss with a focus on e-mail.

4.0 Coverage of information loss by Control Frameworks

In this chapter two frameworks CobiT and BS7799 are analysed to see if information loss is covered.

Total control?



4.1 CobiT

CobiT provides good practises for bridging the gaps between business risks, technical issues, control needs and performance measurement requirements.

Looking at high level control objectives of Control & Delivery, you will see that the main effort lies in protecting information against access. The following text comes right out of CobiT page 100.

System Security is enabled by

> logical access controls which ensure that access to systems, data and programmes is restricted to authorised users
>
> **and takes into consideration**
>
> 1. • confidentiality and privacy requirements
> 2. • authorisation, authentication and access control
> 3. • user identification and authorisation profiles
> 4. • need-to-have and need-to-know
> 5. • cryptographic key management
> 6. • incident handling, reporting and follow-up
> 7. • virus prevention and detection
> 8. • firewalls
> 9. • centralised security administration
> 10. • user training
> 11. • tools for monitoring compliance,
> 12. intrusion testing and reporting

Consideration 2, 4 and 8 are good examples that the main focus of CobiT lies on access control. Keep unauthorised users away and you are safe. In chapter two we concluded that it are those authorised users who lose information.

It goes too far to think CobiT ignores the information loss problem it does mention it at section Planning & Organization. Contole 6.8 *Security and Internal Control Framework* policy, state the following “The policy should comply with overall business objectives and be aimed at minimisation of risks through preventive measures, timely identification of irregularities, limitation of losses and timely restoration.” CobiT only lacks good practises to limit loss by authorised users.

In chapter two it became apparent that compliance with external requirements like SOX, export regulation and privacy regulation is important. In section Planning & Organisation page 55 of CobiT controle 8.2 and 8.4 refer to that. CobiT state ‘Appropriate corrective actions are taken on timely a basis to guarantee compliance’ and ‘management should ensure compliance with privacy, intellectual property, transborder data flow and cryptographic regulations’. CobiT only doesn’t mention anywhere controls to do so. It mentions firewalls, access controls but never mentions detection of unauthorized outbound flows.

In section Delivery & Support section manage data of CobiT, the importance of protection against loss is presence. The objectives of control 11.16 and 11.17 include security of output reports and for those awaiting distribution. These objectives also recognize the danger of output already distributed to users. Unfortunately CobiT relies on procedures for protection. Unless these procedures have a technical support, detection of loss will be limited.

4.2 BS7799

Britisch standard 7799, information security management [BS7799,1], is issued in to parts. Part 1 provides a code of practise and part 2 gives a specification for information security management systems.

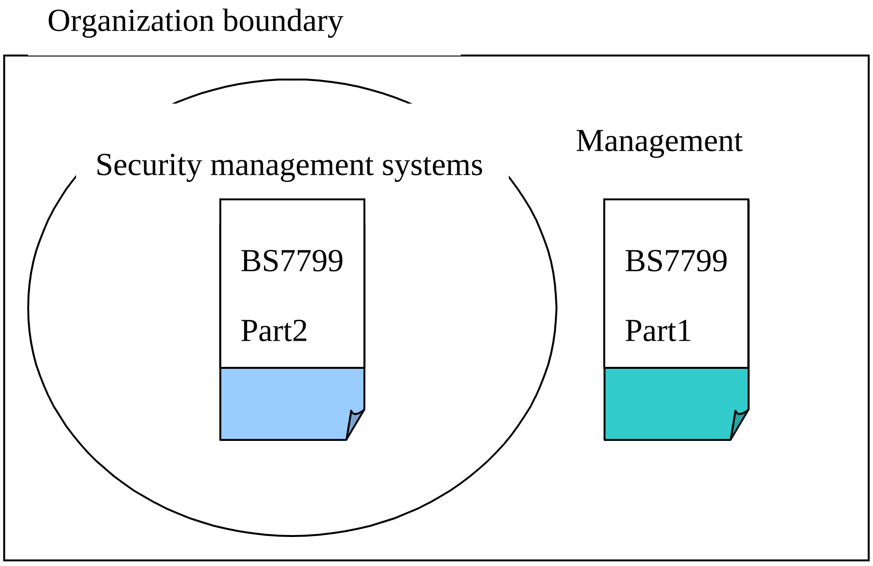


Figure 4.2

Figure 4.2 shows how the two parts of BS7799 relate. Security management systems 'SMI's', support management in an effort to secure the organization.

First a look at part1 will be given, the code of practice for information security management. Section 5 is about asset classification and control. Objective of this section is 'To maintain appropriate protection of organizational assets'. 5.2 even has as objective 'ensure that information assets receive an appropriate level of protection'. Looking further at section 6 'Reduce the risks of human error, theft, fraud or misuse of facilities', is an objective to protect personnel security. Reading these objectives it can be concluded that protection of information also against loss by mistakes is important.

The most important section, section 8 communications and operations management, asks for a control an EDS could fulfil. 8.7.1 Information and software exchange agreements, lists conditions that should be considered.

The list of conditions mentioned in section 8.7.1:

A. Management responsibility for controlling and notifying transmissions, despatch and receipt.

B. Producers for notifying sender, transmission, despatch and receipt

C. Minimum technical standards for packaging and transmission

D. Courier identification standards

E. Responsibilities and liabilities in the event of loss of data

F. Use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected

G. Information and software ownership and responsibilities for data protection, software copyright, compliance and similar conditions

H. Technical standards for recording and reading information and software

I. Any special controls that may be required to protect sensitive items, such as cryptographic keys

Condition F is exactly what should be implemented to protect against information loss. Although such a system should be automatic, to diminish errors.

Section 8.7.3 securing of electronic e-mail, is surprising. It is yelling for an EDS. In brief it says ‘its speed, message structure, degree of informality and vulnerability to unauthorized actions differs e-mail form traditional forms of communications. Considerations should be given to the need for controls to reduce security risks created by electronic mail’ it even lists the risks where the first two are; ‘vulnerability of messages to unauthorized access or modification or denial of service’ and ‘vulnerability to error, e.g. incorrect addressing or misdirection, and the general reliability and availability of the service’. This covers information loss by e-mail.

On a high level BS7799 covers the information loss problem but it lacks controls. Reading part2, specifications for information security management systems, security of electronic email states; ‘A policy for the use of electronic mail shall be developed and controls put in place to reduce risks created by electronic mail.’ During my internship at Deloitte I found out that implementing encryption and implementing an e-mail usage policy covers this section in practise. BS7799 recognizes human mistakes and misaddressing as risks. Encryption isn’t a control against that.

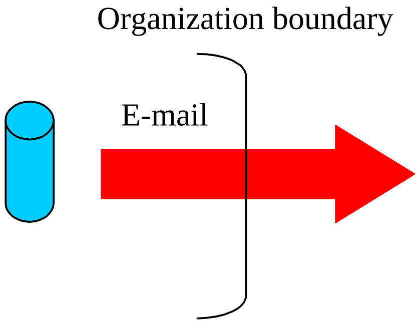
4.3 Conclusion

Both frameworks, CobiT and BS7799, mention loss and human mistakes as a risk. BS7799 asks consideration for controls protecting e-mail against incorrect addressing. CobiT only mentions the problem very brief. My opinion is that both frameworks cover the information loss problem. CobiT should only point out more that technical controls should be considered to protect against loss.

The biggest problem, I noticed in practice during my internship at Deloitte, is that EDS is not yet a standard for protection against loss. Professionals in the field are not all aware of such products. I also have to say that most products are fairly new and pilot programs are being enrolled on a small scale. In chapter 5 information loss by email is analysed, to see if in practise, loss is covered.

5.0 Information loss by E-mail

In this chapter I will research the information loss problem caused by e-mail usage. A focus on e-mail is chosen because it has become a common communication tool. E-mails in majority also contain a lot of information especially if they include attachments. Several cases will illustrate how email is used and how this communication tool is secured. Problems with the security of email will be addressed.



5.1 Security problems with e-mail

E-mail has become a common communication tool for almost every organization over the years. Email has made it possible that digital information can be distributed at the speed of light and to numerous recipients at ones. The ease of use and the fact that after the send button has been hit, the transmission can not be undone, that in combination with misaddressing and multicasting makes email an information security threat.

If we only look at e-mail usage we can distinguish intention and unintentional misaddressing as a security risk. Unintentional misaddressing occurs when employees make mistakes and intentional misaddressing occurs when people try to leak information or even steal. Intentional misaddressing can also occurs when processes are not enough secured. An example of the last, are employees who work also at home and find it convenient to email their work in progress to their private email address.

Other security risks for email are fishing and 419 scams [419SCAM]. Fishing is sending emails and pretending for example you are a bank and need a reconfirmation of the users account information. Credit card information or login information for online banking can be acquired this way. Recipients trust the email and don’s check if the reply address or website to which is redirected is genuine.

The 419 scam letter is an email with the intention to rob the recipient [419SCAM]. The sender claims to be a bureaucrat, banker, royal toadie or relative of a powerful personality who wants to cut you, and only you, in on the financial deal of a lifetime. He claims to be in a position to skim

public accounts, siphon off an unclaimed inheritance, or in some other way make off with a lot of money. He only needs help to move the funds abroad. The 419 scam latter offers the recipient a generous commission if he is to provide a bank account and help moving the funds abroad.
All the claims are fake and at some point the sender will ask the recipient to pay some amount in advance. If you pay you will never see the money again and are scammed.

Of course sensitive information can be encrypted and email usage is often logged but logging doesn’t protect against loss and encryption only helps if it is applied consisted and according policy. Anti virus and anti spam software will protect against attacks but only to the known ones. Employee awareness and commitment to email and encryption policies will also reduce the risk but the human factor is still present.

5.2 E-mail cases

Three cases will illustrate how is dealt with email security in practice. In every case a relation is made between the importance of information security and the current security measures. The cases are built from the interviews conducted.

5.2.2 Interview’s outline

Two depth interviews [E. Babbie,1] were conducted one at a financial organization and one at an organization dealing with a lot of privacy information. Last an informal conversation was held with an employee working at one of the biggest oil concerns. This employee works with a lot of intellectual property which has high value for the competition.

The respondents where chosen by judgmental sampling [E.Babbie,2]. They had to be in a position to know, how information leaves the organization and which security measures are taken to protect the information. An attempt was also made to interview people form different types of organizations. These types are based on possessing a lot of financial, privacy or intellectual property information. These are also the three types where information loss can have a big impact.

The intention of the depth interviews was to get a feeling how secure the organizations feel towards email usage, what information is send by email and which security controls are implemented. (*See appendix for the Interview outline*) In the second part of the interview questions about EDS were asked to see if EDS principles where know and if they would think, such a security measure would be helpful. The first two interviews were held with high placed security mangers and took about an hour.

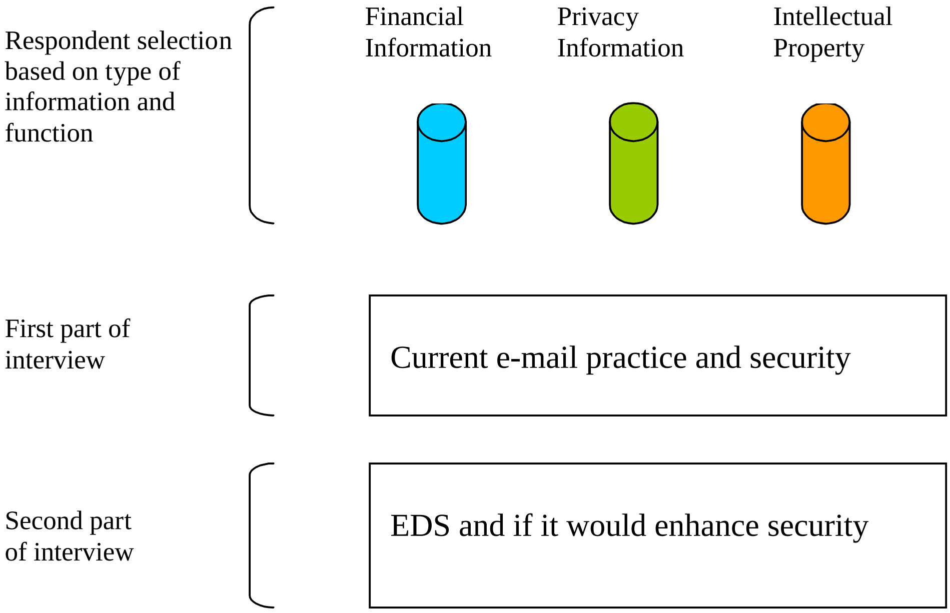

Respondent selection based on type of information and function
Financial Information
Privacy Information
Intellectual Property
First part of interview
Current e-mail practice and security
Second part of interview
EDS and if it would enhance security

Figure 5.2.1 “Interview layout”

5.2.3 Interview’s outcome

Financial Org

Financial org is a multinational active in banking and insurance with around 115.300 employees worldwide. Financial Org is active in over fifty countries. Privacy is of high concern for protecting their reputation. The last five years legislation is more and more enforcing adequate information security practices. Employees work on fixed workstations and notebooks provided by the organization. The respondent being interviewed is information security policy manager at the organization.

Current practice

Financial org uses chip cards employees must use to identify themselves if they want to use encrypted email. The use of a token is an extra security measure used in combination with username and password. Financial org relies on a Public Key Infrastructure for their encryption. If email is encrypted financial org checks if the recipient is known and listed. Instant messaging is not allowed.

Risk Perception

Financial org thinks it has its security in order but recognizes that it can always be improved. Continuous awareness programs for which grades are given to employees are an example of this mind set. If confident information is lost, it will have a negative impact on their reputation. Privacy, stock and market information are considered confidential information. If secure information is lost fines may be imposed and can have a huge impact on their reputation. Financial reporting and information about merges are considered secure information. Now only five percent of the employees work with confident or secure information says the respondent. Five percent of 115.300 are still a lot of employees working with this information.

Information Loss by Email

Although financial org uses an public key infrastructure for securing their information send by email it still relies on the judgment of employees to encrypt emails. If emails are encrypted a check is performed to see if the recipient is trusted but if no encryption is used emails can be freely send. Employees are monitored on their internet usage so in case of a leakage forensic searches can be done. Only finding the perpetrator after information is lost, is not diminishing the impact. Now the offices in the United States are looking at outbound content scanning but in Europe it is unknown. The respondent saw the benefits of outbound content scanning for the five percent working with confident and secure information. He also mentioned some criteria for such product. It should be used on a closed user group and on a limited amount of documents. Further should it posses logging and monitoring functionality.

EDS

Surprisingly the respondent thought that their headquarter in the USA was looking into EDS systems. He wasn't sure but remembered reading about EDS. In the Netherlands they are not looking into it. The respondent liked the functionality an EDS can offer but to him it only looked manageable if applied to a small group, say only top management. If an EDS would be implemented it should prevent loss real time, be easy manageable. After implementation the loss of information by e-mail would be coffered but the respondent said if people want to steal they will always find a way.

Privacy Org

Privacy Org is an organization that helps children and parents of children till the age of eighteen, with problems. These problems can have to do with school, the home situation, personal problems and more. Information is shared among co workers but also with entities outside the organization like social workers working on schools, law enforcement and heath care. Privacy law in the Netherlands enforces Privacy Org to implement appropriate security measures to reduce the risk of information loss.

Current practice

Privacy Org is pretty secure. Beside firewall, anti virus and an active account management, Privacy Org limits access to internet only to personnel that really needs it although everyone can use e-mail. Further remote access is provided through a terminal so downloading and uploading is limited to the terminal and only authorized personnel has access to documents on the terminal. By the use of this terminal it is not possible that home workers download information to their home computer. RSA keys are used for further access security. Last Privacy Org has a continuous security awareness program.

Sensitive information is always transmitted over a secure channel. If it is not possible to deliver sensitive information over a secure channel the information is delivered personally.

Risk Perception

Privacy Org thinks it has its security in order and on a high level. The risks Privacy Org faces, if you look at the financial impact, are limited. Information loss can cause big reputation damage though, where the loss can damage clients severe. Imagine that information about child abuse is loosed and the neighborhood gets access to it.

Information Loss by Email

Although Privacy Org has a high level of information security, a hole can be found in email usage within the organization. All email is logged by sender, receiver and subject in a database. On this database periodically searches are done to find inappropriate behavior. Sender receiver relation in combination with dictionary searches on subject of send emails is checked. This sounds like Privacy Org controls the email usage but that is not entirely true. If the subjects of sensitive emails don't reflect the information of the email or can't be found in the dictionary used for finding sensitive emails the security measure can be bypassed. Also if there is no security restriction between sender and recipient the security measure can be bypassed. For example misaddressed emails that are also lacking encryption won't be detected. This hole in information security should not be taken lightly, because every employee has access to email.

EDS

The respondent was skeptic about EDS. He thought about the cost-benefit and said it mustn't cost much. At first he thought his own made monitoring system was good enough. After some examples how information could be lost and bypass his system he liked the real time scanning capability a little more. Still price would be decisive for him. For Privacy Org, price and preventive properties would be the main criteria for implementation.

Intellectual Org

Intellectual Org is an organization in the oil business and is one of the biggest in the marked. Although the respondent was not an high security officer, the employee interviewed was able to provide a picture of daily practice. The employee works with blueprints of factories and is responsible that people requesting them are authorized to do so.

Current practice

Besides standard security measures like firewalls, logging and anti virus employees have to confirm that attachments are allowed to be send to the recipient. This confirmation is logged and has to be repeated for every attachment and every recipient.

Risk perception

The employee interviewed is aware of the security risk that loss of information can have. A nice anecdote was a story that part of a blueprint, of a new factory, was lost and the competition got their hands on it. On purpose the organization leaked the rest of the blueprint but with intentional mistakes in it. The competition decided to build the factory according the blueprints but after completion had to conclude that the factory wasn’t able to work correctly. Now this anecdote has no direct link with information loss by email but illustrates the risk of information loss.

EDS

The respondent didn’t had enough knowledge about information security to answer the questions about EDS. He did say that his organization is always looking into ways to secure their intellectual property.

5.3 Conclusion

After conducting the three interviews we can conclude that information loss by email will not be prevented at the three organizations. Privacy org periodically tests emails on subject, sender and receiver. This control indicate that information send by email is seen as a risk. Although this will monitor misaddressing and will increase user awareness but will still not doesn’t prevent loss. It seems that the organizations trust their employees not to make mistakes. In chapter two we have seen that this is a dangerous trust.

At financial org a PKI infrastructure is used to secure e-mails. If emails are encrypted recipient and sender are checked against an authorization list. Misaddressing is prevented by this check but only if e-mails are encrypted. If emails aren’t encrypted no checks are performed. So misaddressing is only prevented if information is encrypted. This is funny because encrypted email can’t be read by persons not having the decryption key. You can say misaddressing of encrypted mail is not a security risk but misaddressing unencrypted information is. Now financial org lacks controls that protect against misaddressing of unencrypted e-mail. Current security practices are not covering information loss by email.

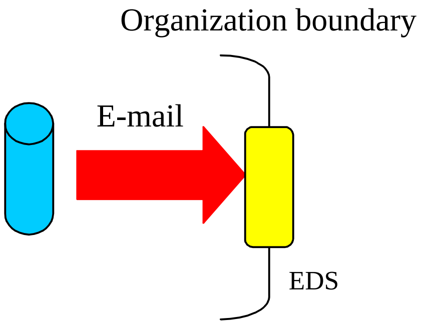
Financial Org and Privacy Org both saw an EDS as an improvement on information security. Privacy org was only concerned about the costs of such a system. They would need a good cost-benefit analysis. This cost aspect is of importance to them because they don’t have a big budget. Financial org saw problems with the maintainability because of the many employees it has and documents that would needed to be scanned.

All organizations are capable to classify their information. This is of importance for an EDS because without proper training, such systems are useless.

We now see that information loss by email is not well protected. The organizations are interested in the functionality of an EDS. In chapter six a closer look at EDS products should make clear if these products can close the security gab found at e-mail usage.

6.0 Solutions for closing the e-mail security gab

In this chapter, solutions for closing the security gab we found in chapter four and five are explored. These solutions will also be linked to security practises described in chapter three. Not the entire universe of solutions against information loss is used. This thesis only focuses on those solutions protecting against information loss based on automatic outbound content scanning. Extrusion Detection Systems 'EDS' will be used to refer to systems that have the ability to scan outbound information and block when desired.



6.1 product offering

If we look at the market place we find several players already offering outbound scanning products. To the contrary of inbound scanners against spam, of which many products are available, the offering of outbound scanning is limited.

In this paragraph I will highlight three players. These players are chosen on their product offering, outbound scanning of information and their world wide presence. On the next page a brief overview is given of the three players in table 6.1. Also a list of common functionality is given.

Table 6.1 shows the companies with their products.

Company	Product	Type of data that can be scanned
Entrust	Entrust Entelligence™ Content Control Server	Any standard format like Word, Excel, PowerPoint, etc
Proofpoint	Proofpoint Digital Asset Security	• Plain text and email • Microsoft Word and other word processing formats • Microsoft Excel and other spreadsheet formats • Adobe PDF documents • Microsoft PowerPoint and other presentation formats • Documents included in archives including ZIP, GZIP, TAR and TNEF (Windows email archive) archive formats.
Stork	Beeble classifier engine and Sealed Media	Standard documents including office files and plain text.

Table 6.1

The functionality the products have in common are;

- Providing customised policies.
- Providing lists of authorized users.
- Providing documents to train the classification engines.
- Interfaces for easy integration within existing IT-infrastructure.
- Generating reports on classification results and performance.

Entrust

Entrust provides software solutions that [Entrust,1]

- protect your digital identity through authentication
- enforce policy via advanced content scanning
- protect your information assets through encryption

Entrust has a history of more than 10 years. In 1994, Entrust built and sold the first commercially available public-key infrastructure (PKI).

Entrust use concept based filtering for their compliance and anti spam. The analysis combines partial natural language processing (NLP) and statistical linguistic analysis. The analysis includes stemming, fuzzy matching and index capabilities. NLP is used to break down sentences into their basic grammatical components. The knowledge of human experts is then used in combination with statistics to generate accurate matches. Entrust patented Structure Extraction Engine provides using the above mentioned techniques to return categories, summaries and meta tags.

Proofpoint

Proofpoint was founded in June 2002 by Eric Hahn former CTO of Netscape. Proofpoint, Inc. is a provider of enterprise-class messaging security solutions [Proofpoint,1]. Their solutions are to protect organizations from the threats and risks of both inbound and outbound email and other messaging streams.

The products of proofpoint use different methods to classify information. It looks at message origin, destination but also attributes like attachments in emails. Further proofpoint uses keywords and their patented MLX technology with advanced machine-learning technologies to classify.

Stork

Sork Information Sciences specializes in high-end software applications for Enterprise Information Intelligence and Secure Information Lifecycle Management [Stork,1]. The solutions of Stork are based upon high speed detection, analysis, classification and processing of both structured and unstructured information.

The beeble classifier engine uses semantic classification. To train the engine a reference set of documents is needed and a taxonomy for the classes in use made by experts. After the enginge is trained to an adequate level of coverage new input for example an email can be analyses and the enginge provides a ranking of classification results. This ranking shows the probability the input has to belong to the classes defined.

6.1.2 Implementation

The products offered work like a proxy. All information leaving the organization has to go through it. Figure 6.1 shows where in a network the products should be placed. IProxy indicates the location of the scanning engine. All traffic has to go through this Proxy.

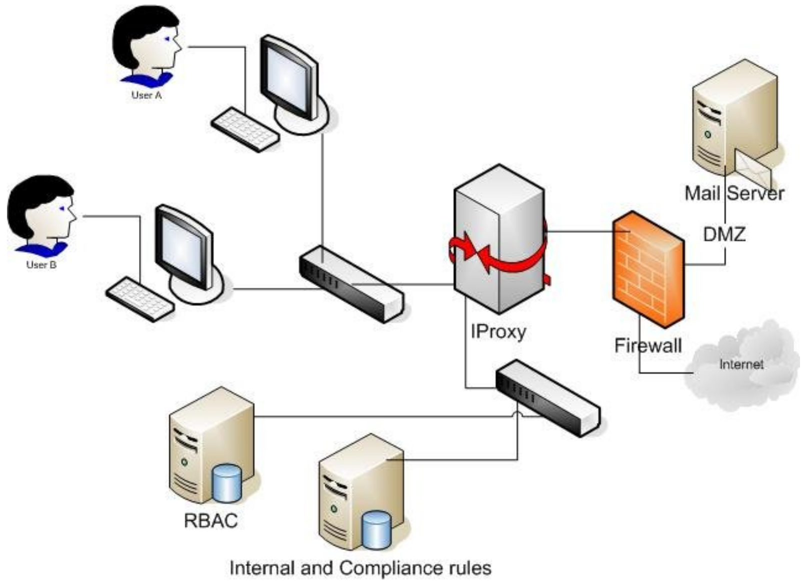


Figure 6.1

How an EDS works is shown in figure 6.2. The UML diagram (Wikipedia,2), shows the application diagram. Most is trivial but after a visit at a Dutch company, that offers EDS functionality, it became clear that classification is the most difficult part. Their classification engine works by comparing pieces of text or binary data. Changing one piece by, for example alter capitals or add extra spaces lowered the rate of detection.

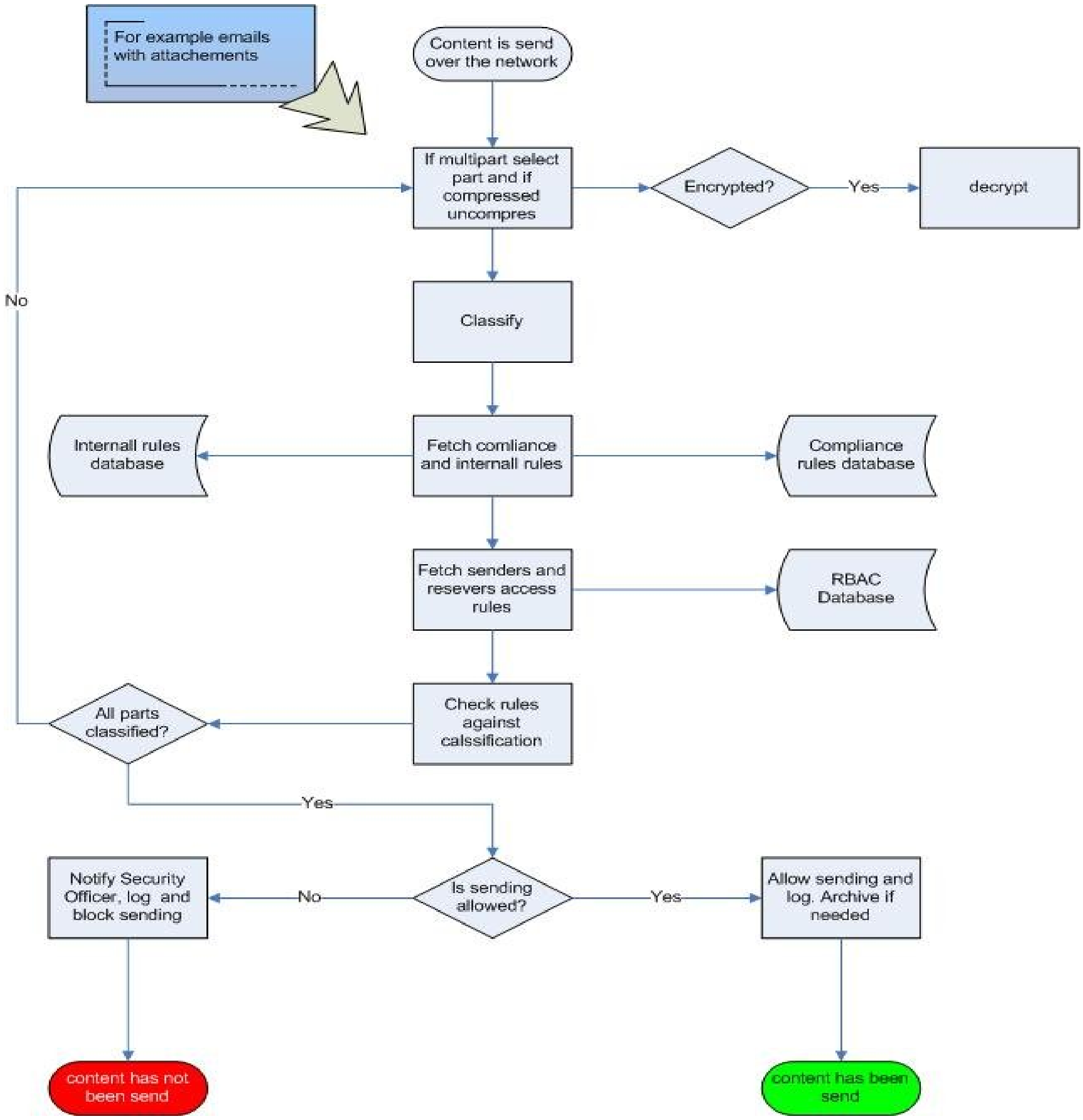

For example emails with attachements
Content is send over the network
If multipart select part and if compressed uncompres
Encrypted?
Yes
decrypt
No
Classify
Internall rules database
Fetch comliance and internall rules
Compliance rules database
Fetch senders and resevers access rules
RBAC Database
All parts classified?
Check rules against calssification
Yes
Notify Security Officer, log and block sending
No
Is sending allowed?
Yes
Allow sending and log. Archive if needed
content has not been send
content has been send

Figure 6.2

6.2 Place within information security

Outbound scanning products are technical implementations that support information security policies. These product can also be used to implement security objectives stated in CobiT and BS7799. In chapter three and four these standards are already mentioned in general the objectives for unauthorized access and disclosure of sensitive information can be further med by these outbound scanning products. The products have a preventive function.

The general contribution of an EDS to the two standards would be the accuracy of the digital transmitting process and prevention of non-authorized access.

In table 6.2.1 you can find a summary of the relevant elements of the standards in relation with content security. Relevant elements are those elements of which the objective can be met by implementing an EDS.

Table 6.2.1

EDS Function	BS7799	CobiT
Preventive function	Part2 4.6.6.3 Information handling procedures “procedures to protect information from unauthorized disclosure or misuse”	Planning and Organization 8 Ensuring Compliance with external requirements “Appropriate corrective actions are taken to guarantee compliance”
	Part2 4.6.7.4 Security of electronic mail “Policy and controls must be in place to reduce security risks created by electronic mail”	Delivery & Support 11.17 Protection of sensitive information during transmission and transport “adequate protection of sensitive information during transmission and transport against unauthorised access, modification and misaddressing.”
	Part1 6.1 Security and job definition and resourcing “Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.”	Manage Human Resources 7.3 Roles and Responsibilities “Management should clearly define roles and responsibilities… employee’s responsibility for information security and internal control.”
Monitoring function	Part1 5.2.2 Information labelling and handling “Procedures are defined for information labelling and handling in accordance with the classification scheme… these procedures need to cover information assets in physical and electronic format”	Planning and Organization 6.6 Compliance with policies, Procedures and standards. “Appropriate procedures to determine whether personnel understand the implemented policies and procedures… and are being followed.”

An EDS should have the functionality to monitor employee’s commitment to policies. For example if an email usage policy is in place an EDS could monitor if employee’s really use their email as described in the policy. A policy is useless if it is not followed. Figure 3.4.1 illustrates the relation between the policies and an EDS.

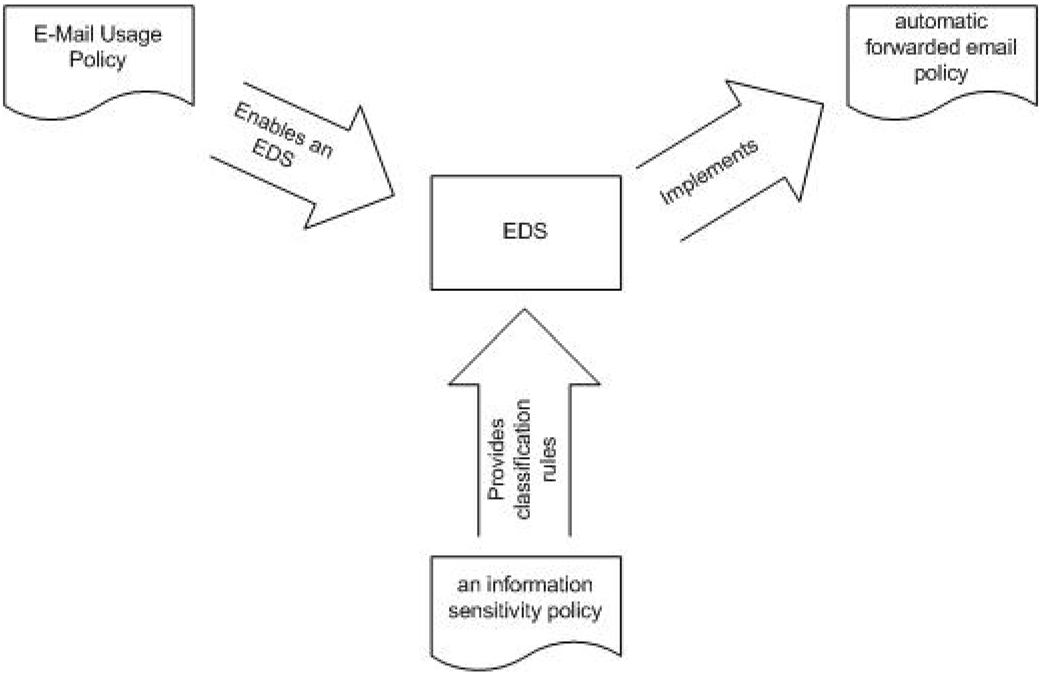

E-Mail Usage Policy
Enables an EDS
EDS
Implements
automatic forwarded email policy
Provides classification rules
an information sensitivity policy

Figure 6.4.1

6.3 Limitations

The classification engines used are not 100% secure. There will always be misclassifications. In a single case of information leakage the threat remains but is limited. Frequent information loss will be detected it will only be a matter of time.

Although information lost bye mail is mitigated the information loss problem itself hasn’t. It is still a people problem and they will always find way’s to bypass security measures. Storage on portable devices should also be monitored and never forget hard copies. Hard copies of documents containing sensitive information can be lost or deliberate leaked.

If the focus is limited to digital file transfer by e-mail, ftp and http the products on the market mitigate the risk of information loss.

6.4 Conclusion

Extrusion detection is possible. EDS can meet control objectives, in two frequent uses security frameworks, CobiT and BS7799. As a protective measure against information loss by e-mail EDS makes the security gab found in chapter four and five smaller. So why is EDS not widely used? EDS is new and expensive. Only a few players on the marked are able to provide a functional EDS. If the hart of an EDS, the classifier doesn’t function well, EDS will not work. Organizations are capable to classify their information, the interviews in chapter four made that clear. Current technologies provide classifiers that can correct classify up to 80% [Nigam,1]. The only reason I can think of why EDS is not widely used, is that the insider threat and especially the employee making mistakes is not taken serious enough and that the cost benefit analyses are qualitative. The cost off loss will only be known exactly when loss occurs. The interviews in chapter four made clear that the risk e-mail usage has is not always clear.

7.0 Conclusions and recommendations

When the depth interviews were conducted it became clear that a security problem with e-mail is present. Combining the information loss examples and the fact that organizations have limited control over e-mail, you can say that the information loss by e-mail is problem that has to be recognised and controled. The interviews also show that the organizations rely heavenly on their employees, when it comes to e-mail behaviour and information handling. For a part this is because current security controls can’t protect based on information content. Current security controls rely on correct classification and right settings by employees. Mistakes and deliberate misclassification bypass these security controls. Current controls are therefore not protective enough.

Legislation is maybe the biggest driver for organisations to invest in more e-mail security. Not because of the fear of fines or reputation damage but because they are enforcing more security.

The product described in chapter five will provide better e-mail security. E-mail can be controlled by a technical solution. Mistakes and misclassification will be noticed and corrective actions can be taken by these solutions. These products also contribute to a more complete implementation of two security standards, widely used.

There is a gab in information security. Loss of information is not enough controlled but new extrusion detection systems can close this gab for a big part. If delibered intent exists to steal information, there will always be found a way. This means that the gab will never be closed completely but can be made as small as possible.

If you ask me if educating employees on the security risks of e-mail is enough, I have to say no. In most cases employees don’t deliberate loss information. Mistakes happen and now there are products to prevent these mistakes. It would be foolish to believe you are secure when no security measures are implemented.

Deffinitions

Recipient: A person, program or country to which the information is to be send.

Information loss: Information that unwanted comes in into the hands of the competition or public domain.

Insider: “Employees, board members and other internal team members, who have legitimate access to information and or information technology. Insiders typically have special knowledge of internal controls that are unavailable to outsiders and they have some amount of access. In some cases, they perform only authorized actions as far as the information systems have been told. They are typically trusted and those in control often trust them to the point where placing internal controls against their attacks are considered offensive.”

Abbreviations

Deloitte	Deloitte Netherlands BV
CIA	Confidentiality, Intergrity, Availability
WBP	Wet Bescherming Persoonsgegevens
HIPAA	The Health Insurance Portability and Accountability Act of 1996
RBAC	Role Based Access Control
OS	Operating System
EDS	Extrusion Detection System; Detecting information leaving the organization unauthorized. a control that blocks and logs unauthorised digital information flows

COSO	Internal Control Integrated Framework
IS	Information System

Literature

[419SCAM] 'Eve Edelson', 'The 419 scam', Lawrence Berkeley National Laboratory, 1 Cyclotron Road MS 90-1060, Berkeley CA, 94720 USA,

[Brickey,1] 'Brickey, K.F. 'From Enron to Worldcom and beyond: life and crime after Sarbanes-Oxley', washington University in St Louis, School of law, 1 juni 2003

[BS7799,1] 'British Standard Information Security Management BS7799', BSI/DISC Committee BDD/2, 05-1999, www.bsi.net

[Carroll,1] 'Security and Credibility in an information intensive Society', John M. Carroll, Computer & Security, 9 (1990) 489-498

[cbp, 1] 'College Bescherming Persoonsgegevens', www.cbpweb.nl

[CobiT,1] 'CobiT 3rd Edition Control Objectives', IT Governance Institute tm, 2000 , www.itgovernance.org

[Cynthia R. Cook et al,1] 'Assembling and Supporting the Joint Strike Fighter in the UK', Rand Europe 2003, "MR-1771.", ISBN 0-8330-3463-4 (pbk.)

[E.Babbie,1],'The practice of social research 10th edition', Earl Babbie, 2004 Wadsworth, page 263.

[E.Babbie,2]. 'The practice of social research 10th edition', Earl Babbie, 2004 Wadsworth, page 183

[Entrust,1] 'Securing your Digital Life, Email compliance through advanced policy based content scanning', Entrust September 2004. www.entrust.com

[Gonzalez and Sawicka, 1] 'A framework for human factors in information security', Presented at the 2002 WSEAS Int Conf on Information Security, Rio de Janeiro, 2002

[Greenspan, 1] 'Remarks by chairman Alan Greenspan','Intellectual Property Rights', California, February 27, 2004

[E.J. Stofbergen,1] 'Informatiebeveiligin op een hoger niveau', E.J. Stofbergen, doctoraalscriptie Erasmus University 15-11-2004

[Halligan and Weyand,1] 'the Sorry State of Trade Secret Protection', Corporate Counselor magazine, August 2001

[H.F.Tipton,1,768] ‘Information Security Management Handbook Fifth Editon’, H.F. Tipton, M. Krause,Auerbach Publications, ISBN 0-8493-1997-8, 2004

[Jemewein, 1] De. Klaus Jennewein: ‘Intellectual Property Management: the role of technologie-brands in the appropriation of thechnological innovation’, Physica-Verlag Heidelberg 2005

[Maskus and Rechman, 1] ‘International public goods and transfer of technology under a globalized intellectual property regime’, Cambridge Univsersity Press 2005 isbn 12 978-0-521-84196-2, blz 89

[Moulton and Bigelow,1] ‘Protecting Ownership of Proprietary Information’, Computer & Security, 8 (1989) 15-21

[NetSec, 1] ‘Security Brief Sox and Security’, november 2004

[Nigam,1] ‘Text Classification from labeled and Unlabeled Documents using EM’, K Nigam, A.K. Mccallum, S Thrun. T Mitchell. Machine Learning, 1-34, Kluwer Academic Publications Boston 1998.

[Palm Beach Post,1] ‘E-mail graffe reveals HIV, AIDS names’, Palm Beach Post Stafff Writer’, Jane Dougherty, february 22 2005

[Proofpoint,1] ‘Best Practices in Messaging Security’, Ziff davis media November 2004, www.proofpoint.com [Survey,1] ‘TMT Security Survey – 2006’, Deloitte Netherlands BV 2006.

[Stork,1]’Stork information sciences SIS-DOC-0123 WP Management v1.4’, Stork information sciences BV 2005.

[Swartz, 1] ‘the lock down on data has begun’, information management journal, sep/oct 2003 page 6

[T.R. Peltier et el,1] ‘Information Security Fundamentals’, T.R. Peltier,J. Peltier, J. Blackley, Auerbach Publications, 2005, isbn 0-8493-1957-9 page 1

Internet

(AD,1) http://www.ad.nl/binnenland/article1015866.ece accessed on: 15-03-2007

(BBC,1) http://news.bbc.co.uk/go/pr/fr/-/1/hi/programmes/newsnight/3956129.stm accessed on: 12-04-2006

(Wikipedia,1) http://en.wikipedia.org/wiki/Exploratory_research accessed on: 17-05-2007

(Wikipedia,2) http://nl.wikipedia.org/wiki/UML accessed on : 12-09-2007

(Eur) www.eur.nl

(Deloitte) www.deloitte.nl

(Etrust) www.etrust.com

(Proofpoint) www.proofpoint.com

Appendix

Automatically Forwarded Email Policy

1.0 Purpose
To prevent the unauthorized or inadvertent disclosure of sensitive company information.

2.0 Scope
This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of <Company Name>.

3.0 Policy
Employees must exercise utmost caution when sending any email from inside <Company Name> to an outside network. Unless approved by an employee's manager InfoSec, <Company Name> email will not be
automatically forwarded to an external destination. Sensitive information, as defined in the *Information Sensitivity Policy*, will not be forwarded via any means, unless that email is critical to business and is encrypted in accordance with the *Acceptable Encryption Policy*.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
Terms Definitions
Email The electronic transmission of information through a mail protocol such as
SMTP. Programs such as Eudora and Microsoft Outlook use SMTP.

Forwarded email Email resent from internal networking to an outside point.

Sensitive information Information is considered sensitive if it can be damaging to <Company Name>
or its customers' dollar value, reputation, or market standing.

Unauthorized Disclosure The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

6.0 Revision History

Email Use Policy

1.0 Purpose
To prevent tarnishing the public image of <COMPANY NAME> When email goes out from <COMPANY NAME> the general public will tend to view that message as an official policy statement from the <COMPANY NAME>.

2.0 Scope
This policy covers appropriate use of any email sent from a <COMPANY NAME> email address and applies to all employees, vendors, and agents operating on behalf of <COMPANY NAME>.

3.0 Policy
3.1 Prohibited Use. The <COMPANY NAME> email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any <COMPANY NAME> employee should report the matter to their supervisor immediately.
3.2 Personal Use.
Using a reasonable amount of <COMPANY NAME> resources for personal emails is acceptable, but nonwork related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a <COMPANY NAME> email account is prohibited. Virus or other malware warnings and mass mailings from <COMPANY NAME> shall be approved by <COMPANY NAME> VP Operations before sending. These restrictions also apply to the forwarding of mail received by a <COMPANY NAME> employee.

3.3 Monitoring
<COMPANY NAME> employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. <COMPANY NAME> may monitor messages without prior notice. <COMPANY NAME> is not obliged to monitor email messages.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
Term Definition
Email The electronic transmission of information through a mail protocol such as
SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Forwarded email Email resent from an internal network to an outside point.
Chain email or letter Email sent to successive people. Typically the body of the note has direction to
send out multiple copies of the note and promises good luck or money if the
direction is followed.
Sensitive information Information is considered sensitive if it can be damaging to <COMPANY
NAME> or its customers' reputation or market standing.
Virus warning. Email containing warnings about virus or malware. The overwhelming majority
of these emails turn out to be a hoax and contain bogus information usually
intent only on frightening or misleading users.
Unauthorized Disclosure The intentional or unintentional revealing of restricted information to people,
both inside and outside <COMPANY NAME>, who do not have a need to know
that information.

6.0 Revision History

Information Sensitivity Policy

1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of <Company Name> without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect <Company Name> Confidential information (e.g., <Company Name> Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Infosec.

2.0 Scope

All <Company Name> information is categorized into two main classifications:

<Company Name> Public

<Company Name> Confidential

<Company Name> Public information is information that has been declared public knowledge by someone
with the authority to do so, and can freely be given to anyone without any possible damage to <Company Name> Systems, Inc.

<Company Name> Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, evelopment programs, potential acquisition targets, and other information integral to the success of our company. Also included in <Company Name> Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of <Company Name> Confidential information is "<Company Name> Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to <Company Name> by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we’ve connected a supplier / vendor into <Company Name>’s network to support our operations.

<Company Name> personnel are encouraged to use common sense judgment in securing <Company Name> Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

3.0 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as <Company Name> Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances
and the nature of the <Company Name> Confidential information in question.

3.1 Minimal Sensitivity: General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.
Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".
Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "<Company Name> Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "<Company Name> Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, <Company Name> information is presumed to be "<Company Name> Confidential" unless expressly determined to be <Company Name> Public information by a <Company Name> employee with authority to do so.
Access: <Company Name> employees, contractors, people with a business need to know.
Distribution within <Company Name>: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of <Company Name> internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
Electronic distribution: No restrictions except that it be sent to only approved recipients.
Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.2 More Sensitive: Business, financial, technical, and most personnel information
Marking guidelines for information in hardcopy or electronic form.
Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "<Company Name> Confidential" or "<Company Name> Proprietary", wish to label the information "<Company Name> Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.
Access: <Company Name> employees and non-employees with signed non-disclosure agreements who have a business need to know.
Distribution within <Company Name>: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of <Company Name> internal mail: Sent via U.S. mail or approved private carriers.
Electronic distribution: No restrictions to approved recipients within <Company Name>, but should be encrypted or sent via a private link to approved recipients outside of <Company Name> premises.
Storage: Individual access controls are highly recommended for electronic information.
Disposal/Destruction: In specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.3 Most Sensitive: Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company
Marking guidelines for information in hardcopy or electronic form.
Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that <Company Name> Confidential information is very sensitive, you

may should label the information "<Company Name> Internal: Registered and Restricted", "<Company Name> Eyes Only", "<Company Name> Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of <Company Name> Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.
Access: Only those individuals (<Company Name> employees and non-employees) designated with approved access and signed non-disclosure agreements.
Distribution within <Company Name>: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution outside of <Company Name> internal mail: Delivered direct; signature required; approved private carriers.
Electronic distribution: No restrictions to approved recipients within <Company Name>, but it is highly recommended that all information be strongly encrypted.
Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
Terms and Definitions
Appropriate measures
To minimize risk to <Company Name> from an outside business connection. <Company Name> computer
use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access <Company Name> corporate information, the amount of information at risk is minimized.
Configuration of <Company Name>-to-other business connections
Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.
Delivered Direct; Signature Required
Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.
Approved Electronic File Transmission Methods
Includes supported FTP clients and Web browsers.
Envelopes Stamped Confidential
You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.
Approved Electronic Mail
Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited
to, [insert corporate supported mailers here.]. If you have a business need to use other mailers contact the
appropriate support organization.
Approved Encrypted email and files
Techniques include the use of DES and PGP. DES encryption is available via many different public domain
packages on all platforms. PGP use within <Company Name> is done via a license. Please contact the

appropriate support organization if you require a license.

Company Information System Resources

Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge

To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac.s and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of <Company Name>.

Encryption

Secure <Company Name> Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication

One Time Password Authentication on Internet connections is accomplished by using a one time password
token to connect to <Company Name>'s internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer
in an unusable state to an object that is immovable. Methods of accomplishing this include having a special
key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted
to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference
room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it
with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop
and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that <Company Name> has control over it's entire distance. For example, all <Company Name> networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private
link. ISDN lines to employee's homes is a private link. <Company Name> also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies
which <Company Name> has established private links include all announced acquisitions and some shortterm
temporary links

6.0 Revision History

Interview outline outbound content scanning

Part1

1) General background information

Branch

Organization size

Job level respondent

2) Is e-mail used as a common communication tool?

3) Are there information security measures implemented? (ids,virus scanners, firewall etc)

4) Does the organization feel their information is appropriate protected?

5) What are the drivers to implement information security measures?

6) What kind of sensitive information does the organization posses?

7) What are the risks for the organization if sensitive information is lost?

8) Is the organization aware of the insider threat?

9) What is done against the insider threat?

Part2

1) Is the organization familiar with outbound content scanning systems?

2) Would an outbound content scanning security measure have an added value to information security?

3) Are there plans to implement such a measure or does it already exist, maybe?

4) On which criteria is or would the implemented outbound content scanning system be chosen?

5) Are you satisfied with the current implementation?

6) Are there still risks not covered after an implementation?