Email security policy implementation in multinational organisations with special reference to privacy laws

By

Henry George Dixon

Submitted for the partial fulfilment of the degree

Magister Technologiae : Business Information Systems

in the

Faculty of Computer Studies

of the

Port Elizabeth Technikon

Promoter: Prof. Rossouw von Solms

December 2003
Dedication

This paper is dedicated to the memory of my father, George, who passed away on 22 July 2002, and to my mother, Rose, who has always believed in me.
Acknowledgements

Professor Rossouw von Solms for his guidance and thoroughness as promoter for this paper.

Elsa Strydom for her encouragement and positive attitude throughout the course.

Stuart Lehy for endless patience and an unfailing belief that I could complete this.

Piet Boonzaier, for meticulous proofreading.
# Table of Contents

1. **CHAPTER 1: INTRODUCTION** ................................................................. 1
   1.1 INTRODUCTION .................................................................................... 1
   1.2 DESCRIPTION OF PROBLEM AREA .................................................... 2
      1.2.1 Conceptual framework of study ...................................................... 2
      1.2.2 Identification of problem area ......................................................... 3
      1.2.3 Rationale ....................................................................................... 4
      1.2.4 Problem statement ....................................................................... 5
   1.3 RESEARCH OBJECTIVES ..................................................................... 5
      1.3.1 Primary research objectives ........................................................... 5
      1.3.2 Secondary research objectives ..................................................... 5
   1.4 LAYOUT OF THE PAPER ..................................................................... 6
   1.5 CONCLUSION ...................................................................................... 7

2. **CHAPTER 2: EMAIL IN THE CORPORATE ENVIRONMENT** ................ 8
   2.1 INTRODUCTION .................................................................................... 8
   2.2 A BRIEF HISTORY OF EMAIL ............................................................. 8
      2.2.1 How email works ......................................................................... 10
   2.3 EMAIL USAGE IN GENERAL ................................................................. 11
   2.4 EMAIL IN CORPORATE ENVIRONMENTS .......................................... 12
   2.5 THREATS INTRODUCED BY EMAIL .................................................. 15
      2.5.1 Breach of confidentiality ................................................................. 15
      2.5.2 Malicious software and Viruses ....................................................... 15
      2.5.3 Legal liability ................................................................................ 17
      2.5.4 Productivity loss ........................................................................... 18
      2.5.5 Resource abuses ........................................................................... 18
   2.6 LEGAL POSITION OF EMAIL ............................................................... 21
      2.6.1 ECT Act of 2002 .......................................................................... 21
      2.6.2 Legal document ........................................................................... 22
      2.6.3 Retention ...................................................................................... 22
      2.6.4 Disclaimers .................................................................................. 24
      2.6.5 Encryption and Digital Signatures ............................................... 27
      2.6.6 Invasion of privacy ..................................................................... 29
### 3 CHAPTER 3: INFORMATION SECURITY POLICIES ........................................32

3.1 INTRODUCTION .................................................................................................32
3.2 WHY SECURITY POLICIES ARE NEEDED.........................................................32
3.3 HOW INFORMATION SECURITY POLICIES ARE CREATED............................34
3.4 DEVELOPING AN INFORMATION SECURITY POLICY FRAMEWORK ..............38
   3.4.1 The Information Security Policy Framework ............................................38
   3.4.2 Framework components ...........................................................................39
3.5 OTHER POLICY FRAMEWORKS .....................................................................42
   3.5.1 ISO17799 .................................................................................................42
   3.5.2 BSI ..........................................................................................................43
   3.5.3 ITIL ..........................................................................................................43
   3.5.4 NIST .........................................................................................................43
   3.5.5 SABS .......................................................................................................44
   3.5.6 SANS Institute ..........................................................................................44
   3.5.7 HIPAA ......................................................................................................44
3.6 CHARACTERISTICS OF A GOOD SECURITY POLICY ......................................45
3.7 HOW INFORMATION SECURITY POLICIES ARE IMPLEMENTED AND ENFORCED ..47
   3.7.1 Methods of policy implementation ..............................................................48
   3.7.2 Enforcers of policy ...................................................................................50
3.8 CONCLUSION ....................................................................................................53

### 4 CHAPTER 4: PRIVACY LEGISLATION & EMAIL MONITORING ............55

4.1 INTRODUCTION .................................................................................................55
4.2 PRIVACY ...........................................................................................................55
4.3 WORKPLACE PRIVACY ....................................................................................58
4.4 MULTINATIONAL ISSUES ................................................................................61
   4.4.1 United States of America ..........................................................................62
   4.4.2 European Union ..........................................................................................64
   4.4.3 South Africa ...............................................................................................65
   4.4.4 Asia and Latin America ..............................................................................68
   4.4.5 Cross-border transactions ..........................................................................69
4.5 PRIVACY ISSUES SURROUNDING EMAIL .........................................................71
  4.5.1 Monitoring..........................................................................................71
  4.5.2 Arguments against workplace monitoring .........................................72
  4.5.3 Arguments in favour of workplace monitoring .....................................74
4.6 CONCLUSION .............................................................................................75

5 CHAPTER 5: DRAFTING AN EMAIL SECURITY POLICY .........................77
  5.1 INTRODUCTION .......................................................................................77
  5.2 FRAMEWORK DEFINITION .................................................................77
  5.3 ADDRESSING THREATS AND LEGAL ISSUES IN EMAIL POLICY ........78
    5.3.1 Productivity .....................................................................................79
    5.3.2 Threats ............................................................................................79
    5.3.3 Offensive material ..........................................................................79
    5.3.4 Retention & mail quotas ...................................................................81
    5.3.5 Disclaimers ......................................................................................81
    5.3.6 Encryption .......................................................................................82
    5.3.7 Privacy and monitoring .................................................................82
    5.3.8 Other issues .....................................................................................84
  5.4 STRUCTURING AN EMAIL SECURITY POLICY ......................................84
    5.4.1 Language ..........................................................................................85
    5.4.2 Objectives .......................................................................................85
    5.4.3 Scope ...............................................................................................85
    5.4.4 Definitions .......................................................................................86
    5.4.5 Monitoring .......................................................................................86
    5.4.6 Usage guidelines ..............................................................................87
    5.4.7 Passwords & encryption keys ..........................................................88
    5.4.8 Communications ..............................................................................89
    5.4.9 Software ...........................................................................................89
    5.4.10 Copyright .......................................................................................89
    5.4.11 Violations .......................................................................................90
  5.5 CONCLUSION ..........................................................................................90

6 CHAPTER 6: IMPLEMENTING AN EMAIL SECURITY POLICY ...............92
  6.1 INTRODUCTION ......................................................................................92
List of illustrations

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Classification of email messages in a corporate environment</td>
<td>14</td>
</tr>
<tr>
<td>3.1</td>
<td>Steps in creating security policies</td>
<td>35</td>
</tr>
<tr>
<td>3.2</td>
<td>The Moses Model</td>
<td>37</td>
</tr>
<tr>
<td>3.1</td>
<td>The Hierarchical Policy Structure</td>
<td>39</td>
</tr>
<tr>
<td>3.2</td>
<td>Components of Framework</td>
<td>40</td>
</tr>
<tr>
<td>4.1</td>
<td>Gartner’s privacy scenarios</td>
<td>58</td>
</tr>
<tr>
<td>6.1</td>
<td>Email policy implementation cycle</td>
<td>92</td>
</tr>
<tr>
<td>6.2</td>
<td>Security Policy Lifecycle</td>
<td>93</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

1.1 Introduction

In 1971, scientist Ray Tomlinson sent what is now considered the first email message. It was considered as “nothing short of revolutionary … deserv[ing] a spot in the list of great communication inventions such as the printing press, telegraph and telephone” (Festa, 2001). Whereas email was first used exclusively in the military (Arpanet) and in academic circles, it has now become almost ubiquitous, used widely for private, as well as for business correspondence. According to a Berkeley study (Berkeley, 2000), there were approximately 440 million corporate and personal [e-] mailboxes worldwide in 2001, of which more than a third was corporate mailboxes.

As a result of the extensive use of email in the corporate environment, Information Officers have to ensure that the use of email adds business value. In an “always on” market place, the efficiency, immediacy and cost effectiveness of email communication are immediately evident. A study by Ferris Research, quoted by Nchor (2001), shows that there is “an overall productivity gain of US$9000 per employee as they send and receive emails to get projects done.” However, the use of email in the corporate environment also poses business risks that need to be uniquely addressed. Among these “key business risks” (Surfcontrol, 2001) are security risks, viruses, legal liability, productivity loss and bandwidth abuse.

To address the risks mentioned above and to protect the business value of email, specific policies have to be implemented that address email usage. Information Security Policies are defined in most corporate environments. In a study done by Elron Software (2001), 83% of respondents who have abused email have company policies regulating email usage. There appears to be a gap between policy conception and policy implementation. Various factors inhibit effective policy implementation – ethical, legal and cultural. The implementation of corporate policy becomes especially complex in multinational environments where differing information laws may supersede company policy.
Email usage is ubiquitous in the modern business environment, but few companies adequately manage the risks associated with email.

1.2 Description of Problem Area

Email is generally accepted as a business tool and the user does not have to have an understanding of the inner working of an email message. Management, however, should understand the nature of email in order to identify and manage the associated risks. Once the risks are understood, policies to mitigate this risk can be formulated and implemented. Policy implementation is often problematic, as various legal and other factors have to be taken into consideration.

1.2.1 Conceptual framework of study

In a loose definition of email as “messages transmitted electronically”, telegraph messages and Morse code could be considered forerunners of email. Mainframe systems used in the sixties and seventies allowed the exchange of messages on those systems, but it was only with the growth of personal computers in the late 1970s and 1980s that a “new genre of email technologies” (Vicom, 2003) was developed.

With the evolution of company networks from small terminal based environments to PC based workgroups; the use of email grew quickly into a useful business tool. The development of a graphical user interface for email management in 1988, called Eudora, and the introduction of Lotus Notes in 1989, (Left, 2002), accelerated the acceptance of email by the normal user to make its use pervasive in most corporate environments. Email “has fostered a dependence on instant communication that has transformed the pace of business life” (Festa, 2001). Email has a relatively low cost and is instantaneous, thus increasing productivity during collaborative projects – up to 15-20% per employee in a study by Ferris Research (Nchor, 2001). Nchor (2001) also refers to a Gallop poll that reveals that 9 out of 10 people use email at work.

Despite the fact that 97% of the respondents to the same Gallop poll said that email usage has improved their lives, it is also the field where employees can do
the most potential harm to a company, either through ignorance or with malicious intent. In many countries email has attained the status of a legal document (Andrews, 2002), which also gives it contractual validity (ECT Act, 2002). This opens the door for litigation for false representation through employee opinion expressed in company email and for offensive material being sent via email. The business value of email is often subverted by, among other things, “unauthorised transmission of intellectual property … email-borne viruses … productivity loss through unmanaged email usage … bandwidth congestion with non-essential messages” (SurfControl, 2001) and of course, viral marketing or “spam”.

The formulation of policies to prevent the abuse of email has become essential to ensure that business value is retained in email usage. However, formulating policies, and specifically email policies, is often problematic in itself.

1.2.2 Identification of problem area

Email is a resource that should add value to a company. Misuse and mismanagement of email can detract from the potential value it can contribute.

Email is so pervasive and has so much potential to be abused; therefore, clear policies need to be established to guide the use of email as a resource in a company. Several standards have been set for Information Security Policies, among them ISO 17799. According to ISO 17799 (2001), a security policy exists “to provide management direction and support for information security.” The King Report on Corporate Governance for South Africa states that the board is ultimately held accountable for risk management, which includes security policies (Dekker, 2002).

To ensure email adds business value and to protect the corporation against litigation, appropriate policies have to be defined and enforced. "The goal of information security professionals … has been to not just get policies written, but to also get compliance” (Wylder, 2003). There appears to be a gap between the formulation of policies and the effective implementation of such policies. “It is important to draw the distinction between policies, standards, guidelines and
procedures” (Zegiorgis, 2002) in order to implement policies effectively. It is important to understand the process of policy creation – its structure and hierarchy – in order to determine how best to implement them. A policy has no purpose unless it is understood and accepted by those persons whose behaviour the policy attempts to regulate.

Various alternatives for enforcement are highlighted by Wylder (2003): technology-based enforcement, executive enforcement, audit as enforcement and traditional managerial enforcement. Wylder proposes a “personal security plan” that becomes part of performance appraisals as an enforcer (2003, p.34). This would mean that, as part of an employee’s annual performance appraisal, an item relating to compliance to company security policy would form a metric.

There are several further approaches to ensure that policy is adhered to: Bureaucratic (through dictate); Incentive (through reward); and Cultural (through ethnic practices and corporate culture). By creating a model of the ideal policy framework with reference to the work of Palmer (2001), an attempt will be made to analyse the factors that hinder effective policy implementation, and specifically, email security policy implementation.

1.2.3 Rationale

Despite the pervasive nature of email usage and the inherent risks the technology carries, there appears to be a gap between policy formulation and the implementation and user acceptance of and adherence to such policies.

Implementation of policies is problematic in multinational corporate environments, because of legal and other issues. As an example, Germany has very strict privacy laws. Corporate policy may require monitoring of email and internet usage. It is not possible to implement such a policy in Germany, as it contradicts national laws.

This study will attempt to bridge this gap between conceptualisation and implementation of specifically email security policy, with due consideration to ethical, legal and cultural (both corporate and “ethnic”) factors.
1.2.4 Problem statement

The unmanaged use of email does not necessarily add value to the business environment. Well-defined security policies are required to ensure that value is in fact added by email usage. The creation of a policy framework and the implementation of email security policies are problematic in multinational corporations. This is mainly due to variations in privacy laws in different countries.

The essential problem that will be examined in this paper is the effective formulation and implementation of email security policy in multinational companies. An understanding of the nature and risks of email is required, as well as some knowledge of security policy frameworks. This information can then be used to create an effective email security policy. When looked at in the context of a multinational company, cognisance should be taken of governing laws in countries where the organisation may have a presence.

1.3 Research objectives

The implementation of an email security policy is a very comprehensive topic and it is important to narrow down the study to specific objectives. The primary objectives will be the focus of this paper, while the secondary objectives will be addressed in order to meet the primary objectives.

1.3.1 Primary research objectives

The primary objective of this study is to determine how corporate environments can ensure that email usage adds sufficient business value and to determine how policies should be formulated in order to regulate proper email usage. A further objective is to develop a model and a generic draft policy as to how email security policy can be implemented and enforced in multinational corporate environments.

1.3.2 Secondary research objectives

The secondary objectives of this study are as follows:
- To determine why policy is not adhered to.
- To prove that most email security policies are contrary to the way modern employees view the work environment.
- To analyse the policy frameworks in use in various organisations and how these policies are implemented in different environments. (Bureaucratic, Incentive, Culture).
- To indicate that policy implementation in multinational organisations is problematic due to various cultural, legal, and other factors.

1.4 Layout of the paper

In Chapter 1, the problem area for this study was identified and contextualised and the research objectives documented. The nature of email and the threats email impose on a company will be elaborated on in Chapter 2. The history of email will be touched on and the usage of email will be investigated. The chapter will conclude with an analysis of the legal aspects surrounding email.

Chapter 3 will pose the question why security policies are required. Various information security policy frameworks will be examined and the characteristics of a good security policy will be identified. The chapter will conclude with a section on security policy implementation and enforcement.

Privacy legislation and privacy issues around email will form the core of Chapter 4. The nature of privacy will be investigated and workplace privacy will be highlighted. Privacy legislation in various parts of the world will be compared. Finally, workplace monitoring will be scrutinised to determine whether this is a desirable practice in an organisation.

In Chapter 5, the information from the preceding chapters will be drawn together to examine what the components of an email security policy should be. The threats of email abuse will be highlighted and addressed in a proposed structure for an email security policy. The implementation and enforcement of an email security policy will be discussed in Chapter 6.

Chapter 7 will conclude and summarise this paper.
1.5 Conclusion

The result of the study conducted in this paper should be a clear guideline to companies on how to formulate and implement an email security policy. The reader of this paper will gain an understanding of the issues surrounding email usage in a corporate environment. The importance of placing an email policy within the context of an Information Security Policy framework will be stressed.

Most importantly, issues surrounding privacy and workplace monitoring will be highlighted, as well as the challenges a multinational company faces because of diverse legislation in different countries.

A well-written policy may be completely ineffective unless there is an implementation plan and adequate enforcement of the policy. The paper will conclude with some observations surrounding email security policy enforcement.

In the appendix, a draft policy for a multinational organisation will be proposed.
Chapter 2: Email in the corporate environment

2.1 Introduction

Email is accepted by most people as an integral part of daily communications, both privately as well as in the workplace. Few people, though, consider the risks and legal implications associated with email usage. This chapter will begin by looking at the history of email and briefly explain how email works. The general use of email will be explored, but emphasis shall be placed on usage of email in the corporate environment. Specific threats introduced into the work environment by email will be highlighted and the chapter will conclude with an investigation into various legal aspects surrounding email.

2.2 A brief history of email

If email has to be defined as “messages transmitted electronically”, one could classify early uses of the telegraph and Morse code in the 19th Century as forerunners of modern email usage. Vicom (2003) extends the argument by claiming that the telex network used extensively by businesses world wide from the 1920’s to the 1980’s can be considered a true Internet system. The telex system had its own network independent of the telephone network. Any telex machine could connect and communicate with any other telex machine and communications were made relatively secure through a process called handshaking. However, the telex network was expensive and relied on specialised equipment and trained operators.

The increased usage of mainframes and mini computers during the 1960s and 1970s brought about the usage of messaging on those systems. Users of terminals connected to the mainframes could send text messages to each another. As computers were connected within companies, messaging could take place on a worldwide basis.

Festa (2001) considers the first email (in the modern sense) to have been sent by a scientist called Ray Tomlinson in 1971. The US Department of Defence’s research into computer networks gave birth to ARPANET, which would eventually lead to the Internet as it is known today. Left (2002) ascribes the usage of the @-symbol to identify
addresses to Tomlinson. Another scientist working on ARPANET, Larry Roberts, developed an email management system in 1972 which enabled users to “list, select, forward and respond to messages” (Left, 2002).

The usage of email was initially limited to the military and to academic institutions. Later computer enthusiasts started using email and with the invention of the personal computer and later the World Wide Web, email usage “exploded into the mainstream” (Festa, 2001). This mainstream popularity was assisted by the development of a graphical interface for email, Eudora, developed by Steve Dorner in 1988.

Many proprietary “dial-up” systems were set up for the exchange of messages by subscribers to the same systems. No interoperability existed between different systems. Enthusiasts set up “Bulletin-Board Systems” (BBS) to send and receive messages and exchange information. These systems were used “by hundreds of thousands of personal computer users … prior to the Internet becoming available for general use” (Vicom, 2003).

In 1998 Lotus Notes was released and 35 000 copies were sold in its first year (Left, 2002). Microsoft released Internet Mail and News in 1996 with release 3 of Internet Explorer. This would later be renamed Outlook. Company networks slowly replaced host-based mainframe systems with personal computers. As Local-Area Networks became standard in most corporations, LAN based email gained popularity, specifically because of the ease of use of graphical interfaces that enabled users to send attachments with their messages. These LAN based systems were extended into Wide Area Networks and eventually connected to the Internet.

“Email is nothing short of revolutionary…it is a way to transport the goods and services of the 21st Century: ideas. What railroads were to the 19th Century and what airplanes were to the 20th Century, email is to the 21st” (Festa, 2001).

Email may be a revolutionary communication medium, but in context of modern technology, the working of email is relatively simple, as the next section will show.
2.2.1 How email works

Essentially, all that is required for email is an email client and an email server with which the client can communicate. Many commercial clients, like Eudora, Pegasus, Outlook and Lotus Notes, are available.

Generally the email client does four things (Brain, 2003):

- It shows a list of messages in one’s mailbox by displaying the message headers (sender, date, subject and size);
- It allows one to select a message header and read the associated body of the message (and any attachments);
- It lets one create new messages and send them;
- It allows one to add attachments to messages.

The email server consists of an SMTP (Simple Mail Transfer Protocol) server that handles outgoing mail and a POP3 (Post Office Protocol) server that handles incoming mail. The SMTP server listens on port 25 and the POP3 server listens on port 110.

When a message is composed on the email client and the “send” button pressed, the following happens:

- The client connects to the SMTP server using port 25;
- The client passes the address of the sender and recipient, as well as the body of the message to the SMTP server;
- The SMTP server takes the “To” address and breaks it into the recipient name and the domain name;
- The SMTP server has a conversation with a Domain Name Server (DNS) and requests the IP address for the recipient domain;
- The sender SMTP server connects with the receiver SMTP server and passes the message on. The receiver SMTP server recognises the domain name and hands the message to the POP3 server for delivery to the recipient.

When the recipient checks for email using an email client, the POP3 server requests a username and password and allows the recipient to access the text file
containing that user’s messages. The client then brings the message(s) to the local machine and (generally) deletes it off the server.

The user of email does not need to know or understand the inner workings of the email system. Software takes care of the correct routing and delivery of messages without any intervention from the user. It may be because of this ease of use that email usage has become so ubiquitous and popular with the general computer user.

2.3 Email usage in general

In 1996, web-based email was popularised by Hotmail. The rationale for this was to allow people to maintain email accounts that could be accessible from any computer connected to the Internet. People who did not have a home computer or access to the Internet at work, could now have an email address and retrieve this email from “Internet cafés”. Hotmail proved to be so popular, that Microsoft bought it for $400 million in 1998 (Festa, 2001). Web-based email is now offered by most portal sites and Internet service providers at no charge.

From the history of email, it is clear that email itself is not new. What is relatively new however “is that email is now more readily available, interoperable between systems, available world-wide, inexpensive [or free], much better known, complies with standards, much easier to use [and] fashionable” (Vicom, 2003).

“Access to an email account is the top motivation to start using the Net for 67% of European consumers … once online, consumers appreciate the power and convenience of email - making it the top online activity for 85% of consumers” (Paderni, 2001).

In many respects, email has replaced traditional uses of the telephone and the postal system—especially for long-distance communication. Email is cheaper than a phone call and more instantaneous than a letter. Much personal communication with government or businesses takes place by email rather than letters or faxes. Usage of email outside the business environment is mostly recreational. It is used for the random exchange of jokes and entertainment attachments (images, movie clips, etc.). This recreational culture of email usage tends to spill over into the business environment and the security and productivity issues raised by this will be investigated in detail later.
The marketing world has exploited this ubiquitous usage of email by private individuals to give rise to unsolicited marketing emails, better known as Spam. According to a report by MessageLabs 25% of all email messages are spam (Corporate Executive Board, 2003). There are also more sinister uses of email for fraud (e.g. the Nigerian “510 scam”) that falls beyond the scope of this study.

As mentioned before, email had its origin in the military and in academia. Despite its popularity in the private environment, it is in the work situation that email becomes inimitable.

### 2.4 Email in corporate environments

“[Email] has fostered a dependence on instant communication that has transformed the pace of business life and irrevocably blurred the walls separating home and office” (Festa, 2001). “Pervasive use of email as a means of communication is a fact of life in the new millennium” (O’Brien, 2002, p. 70).

The speed and efficiency of email has made it the communication medium of preference in the corporate environment. To a large extent, email has replaced the traditional departmental or interdepartmental memorandum. It eliminates the need to play “telephone-tag” with associates that are not immediately available, thus reducing wasted time before a decision is made. Email saves on paper and postage. (A conservative estimate for the number of email messages sent and received per year in the USA is 280 billion, compared to the 200 billion pieces of mail delivered by the US Postal Service. Email volumes therefore outstrip postal volumes (Berkeley, 2000)).

Email also allows a means to store and edit documents. An increase in productivity is the major advantage of email, as it allows workers who collaborate on projects to exchange documents through attachments. Various drafts of a document may pass back and forth for editing among workers on a project before a final draft is printed or saved. A study by Ferris Research quoted by Nchor (2001), shows “there is an overall productivity gain of $9000 per employee as they send and receive email to get projects done”. This study also shows that each employee saved 326 hours per year leading to a productivity increase of 15 to 20 percent per employee.
“Companies are beginning to realise that email messages and attachments represent business records that must be retained and managed securely to support regulatory compliance, avoid legal fines or litigation costs, and satisfy auditing requirements … email represents an increasingly large part of the corporate ‘knowledge asset’ ” (DiCenzo, 2002, P.2).

Nchor also quotes a US Gallop Poll that reveals 9 out of 10 people use email at work and 8 out of 10 people use email at home. Forrester Research shows that trends amongst European users differ slightly in that “more than 80% of consumers regularly check their email account from home, while little more than 50% take advantage of access provided by their employers” (Paderni, 2001). Email can therefore be seen as a utility much the same as fax machines and telephones are a utility for communication. Although some companies previously saw email as a “perk” for employees (Gall, 2000), it can now no longer be considered such any more than use of the corporate mailroom can be seen as a “perk”.

It is important to note that “despite the fact that they are using … corporate equipment and networks staff may consider that their emails … are private” (Federal Privacy, 2000). This illusion is created by the fact the employees are usually told to have a personal password that they should keep secret. It should be clear, therefore, that not only business email is sent over corporate email systems, but also much private communication that was normally done from home, is now done at the workplace.

If one should analyse the type of work-related email usage in a corporate environment, messages can be classified according to their origin, whether a response is required or not and whether the message contains attachments. This classification can be seen in Table 2.1.

It may be argued that internal email that requires no response from the recipient may be better managed by corporate Intranet systems or by a Bulletin Board system to which the intended recipients of the notice are only sent a link via email, rather than the full message. Newsletters (subscribed or unsolicited) and product information may constitute a large percentage of email received. Although this information is usually work-related, it may not always be considered essential and employees should be educated on the relative importance they should place on digesting (and storing) this information.
Good time management principles and work prioritisation will assist a great deal in enhancing email productivity. If there is no general culture of time management in the company, employees cannot be expected to manage email effectively.

<table>
<thead>
<tr>
<th>Origin</th>
<th>Response from the recipient required</th>
<th>No response from the recipient required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside company email system</td>
<td>Project queries; Project discussion; Invitations to a meeting; Attachments for comment; Forms for completion</td>
<td>Departmental notifications; Local company notifications Corporate (global) notifications Departmental or Company Newsletters</td>
</tr>
<tr>
<td>Outside company email system</td>
<td>Order queries Customer enquiries Supplier information requests Project queries</td>
<td>Product information Supplier newsletters Order confirmation Subject Newsletter subscriptions</td>
</tr>
</tbody>
</table>

*Table 2.1 Classification of email messages in a corporate environment*

The inbox should be as current as possible with very little content older than a few days. Messages in the inbox should be handled as little as possible. The following possible actions may be performed on messages in the inbox:

1. Read and delete or file
2. Respond immediately and delete or file
3. Defer response (leave in Inbox)
4. File for later perusal (e.g. newsletters, product information, etc.)

This would ensure that the only messages in the inbox are those that require action. It will also make administrative management and archiving of email more efficient, as rules can be enforced based on which folders messages are in.

It is impossible to be prescriptive about the use and management of email at work, as it is such a versatile medium that each user moulds according to his or her preferred style of working. It is important that employees are aware of the dangers of email in the work environment. These threats will be investigated in detail in the next section.
2.5 Threats introduced by email

Ease of use is probably the major reason why email can compromise the security of corporate information. Employees are often not technologically sophisticated enough to understand the consequences of their actions. Sadly, few companies have concerted awareness programs on security risks. This lack of awareness of potential security issues exposes a company to various threats. These threats will be discussed in the following subsections.

2.5.1 Breach of confidentiality

Employees of a company are potentially the greatest threat to company security. Companies often spend millions to ensure that it is secure from outside threats to security. It is often forgotten that security can be breached from within the business as well. “Because email is easy to use and is unlimited in scope, it enables disgruntled employees to rapidly distribute company secrets” (Wynn, 2001, p.6). “Maintaining the confidentiality of … information is paramount to the survival of the organization” (Pipkin, 2000, 167). Sensitive documents may be emailed to rival companies for financial gain by employees. In cases of concerted industrial espionage, someone may be planted in a company in order to gain access to intellectual property.

There may be confidentiality breaches where confidential information is transmitted unintentionally. This may happen either because someone does not know the security classification of the information transmitted or because confidential information may reach an unintended recipient through erroneous addressing.

2.5.2 Malicious software and Viruses

“Email was initially a pretty safe mode of communication, since it consisted mostly of simple text…. The MIME standard allowed sophisticated ways of attaching any type of file to an email message. And this is where email based viruses, worms and all kinds of malicious code began making their appearance” (Festa, 2001).
Most malicious software enters an organization through its email system. In a Forrester study under European email users, 40% of users are unwilling to give out their email address due to “their fear of potential virus contamination or that opening links or attachments could cause their PC to crash” (Paderni, 2001). Any software that creates or exploits a vulnerability may be considered malicious. Pipkin (2000, pp. 45-49) identifies the following categories of malicious software:

- **Buffer overflow.**
  A program attempts to put more data in a storage location than it can hold. The extra data overflows the buffer.

- **Logic bomb**
  A program lies dormant until it is activated by a trigger that is either time or event based.

- **Parasite**
  A piece of code that is added to an existing program and draws information from the original program.

- **Sniffer**
  This is a program that watches data travel through the system and looks for a particular type of information.

- **Spoof**
  A spoof is a person or program that takes on the identity of another person or program.

- **Trojan Horse**
  This is an (apparently) useful program that contains hidden code that may perform unwanted functions when invoked.

- **Virus**
  A virus is a program that infects another program by replicating itself into the host program. Most viruses are destructive and carry a malicious payload (e.g. a logic bomb). Viruses have the largest impact of any of the malicious software, as great costs are incurred in virus protection and in recovery after infection. A virus infection that brings a company to a standstill negatively affects its productivity, as well as its reputation.
Worm
A worm is a program that is used as a transport mechanism for other programs. It utilizes the network (or email) to spread programs from one system to another. Most recent worms have exploited security holes in Microsoft Outlook’s address book.

Sophisticated software is available that can prevent most of these malicious software attacks from occurring. Such software, combined with user awareness, can prevent virus infiltration into a corporate system. It is important for virus scanning software to be kept up to date. Patches on client PCs should also be current, as the Blaster worm in September 2003 exploited a vulnerability in unpatched Microsoft operating systems.

2.5.3 Legal liability

Companies are often under the impression that they are not responsible for messages sent by their employees as long as there is a disclaimer appended to a message. However, just as a company may be held liable for information sent on its letterhead, it is identified by the domain of the email, i.e. that which follows the @-symbol (Garfinkel, 2002, p.29).

A company may be legally liable for offensive material sent or received by its employees and consultants. Issues related to libel action might arise from employee opinions documented in email, as email is considered legally admissible evidence. “Offensive, derogatory, inflammatory or commercially insensitive comments can reflect upon the organization more than the individual who keyed the email” (SurfControl, 2001c, p.3). Some statistics quoted by this source from the April 1999 BusinessWeek stated that:

- 70% [of survey respondents] have received adult-oriented personal emails while at work;
- 64% have received politically-incorrect or offensive emails while at work;
- 27% of Fortune 500 companies have been accused of sexual harassment stemming from inappropriate email use;
The U.S Supreme court ruled that “companies … must exercise reasonable care to prevent as well as promptly correct any sexually harassing behaviour… it is the employer’s duty to take reasonable business precautions to protect employees and provide a safe and healthy working environment” (SurfControl, 2001c, p.3).

More attention shall be paid to legal issues surrounding email later on in this chapter, as well as in Chapter 4. Filtering software may be used to check for certain clauses in email that may compromise a company legally, but employee awareness and self-regulation is a more effective deterrent. Self-regulation is also an effective means to ensure that employees remain productive during their workday.

2.5.4 Productivity loss

Companies may experience productivity loss as excessive personal email usage is left unmanaged. An Elron Software/NFO InDepth Interactive study (Elron, 2001) shows that on average 204 email messages are sent and received by any one worker in a typical day. According to Barsook (1998), “40% of all email messages sent by employees do not involve work-related topics”.

Many users are distracted by email overload – “39% of consumers feel they receive too many emails” (Paderni, 2001). Most users regulate the number of emails received by refusing to give out their email addresses to online marketers. Some users may not regulate themselves and companies may have to define clear policies on whom company email addresses may be revealed to.

2.5.5 Resource abuses

It is not just a loss in productivity in time spent on non work-related email, but a greater concern is the congestion of email server resources and Internet bandwidth with non-essential messages. Congestion or abusive email behaviour may cause a delay in business communications or even a loss of these communications. Bandwidth overload is the direct result of employee abuse of the system. Very often chain letters with large attachments are sent to multiple recipients,
who in turn send it to multiple recipients. This causes an exponential growth in data sent over the network.

Workers who send personal emails with large attachments like photographs or games can also drastically reduce bandwidth. “Servers often crash on or near Valentines Day or Christmas, when personal emailing is at its peak”. Furthermore, according to a SurfControl survey, “73% of U.S. workers who use the Internet for non business reasons are fully aware they are consuming valuable bandwidth and hampering mission-specific Internet use” (Wynn, 2001, p.5).

**Spam**

Another abuse that is often beyond the control of the recipient is spam. Spam is considered promotional or marketing material from someone not known to the recipient, i.e. unsolicited email. Some respondents to a MessageLabs survey also defined “mass-circulating email” (i.e. chain letters) within their companies, as spam (Corporate Executive Board, 2003, p.2).

Employees are usually intolerant of receiving spam, as “people have a personal relationship with their computer, much more so than they would have with their mailbox, so unsolicited messages become more of an invasion than postal mail” (Festa, 2002).

Some of the direct costs of spam include server disk space and bandwidth usage. However, the indirect costs include productivity loss and legal liability for further spread of spam. The 2002 Osterman survey found that “32% of organisations cite spam as the biggest concern in email management” and that the cost of spam is estimated at $16.8 billion a year, “with loss of productivity at around $960 per employee worldwide” (Corporate Executive Board, 2003).

Users should be educated not to subscribe to sites that may potentially deliver spam. Their business email address should not be supplied on the Internet for non work-related sites.

According to a SurfControl White Paper (2001c, p.6), the business risks associated with Internet email directly relate to financial indicators:
- The cost of leaked confidential information and therefore [the company’s] competitive edge
- The cost of staff replacement
- The financial impact of embarrassing incidents appearing in the media or arising in business partner organisations
- The financial drain of lost productivity
- The technical administration costs of rectifying IT systems that are attacked by viruses, worms or Trojans
- The potential legal costs a company may incur, being legally liable for employee’s comments in email to a business partner or customer.

The ECT Act 25 of 2002 deals extensively with spam in section 45. A recipient of spam (defined in the Act as “unsolicited commercial communications”) must be provided with the ability to cancel subscription to the mailing list of the sender and may request the source of the personal information used by the sender. Should the sender continue sending unsolicited messages or refuse to supply the source, the sender may be fined or imprisoned for a period not longer than 12 months. (ECT Act, 2002)

Many email systems have spam filters built into the software. The configuration and management of such filters is time consuming and often inaccurate. The software may often mistake legitimate documents for spam, potentially causing lost business or at worst, legal action from the sender.

This section highlighted some of the most prevalent threats introduced by email. Confidentiality breaches through the emailing of sensitive information, sending of messages with offensive material that may lead to legal action and productivity loss through abuse of the email system are aspects that cannot be effectively controlled through software implementations. These issues should rather be addressed through policy and user self-regulation. Malicious software, viruses, and spam can be controlled through the implementation of filtering software, but it should be noted that careful configuration and close management of this software is required. Besides the threats mentioned in this section, email has the status of a legal document in many countries, including South Africa. This implies an added responsibility in the management of email on the Executive Board.
2.6 Legal position of email

This study will place great emphasis on legal aspects surrounding email policy enforcement and privacy issues. It is, however, first necessary to establish the legal issues surrounding email per se. There are several laws that influence email and the management thereof, both nationally as well as internationally. In South Africa there is the Electronic Communications and Transactions Act 25 of 2002 (ECT Act), the Regulation of Interception and Provision of Communication-related Information Act 70 of 2002 (RIC Act), and the Promotion of Access to Information Act 2 of 2002 (PAI Act).

2.6.1 ECT Act of 2002

In 2000 a Green Paper on electronic commerce was published to elicit debate around a legal framework for electronic commerce. On July 31, 2002, the Electronic Communications and Transactions Act was signed into law by President Thabo Mbeki. This brought to an end speculation and uncertainty around legal implications of various ecommerce activities.

“Generally the Act is a very welcome piece of legislation having regard to the previous lack of legislative direction on many of the more important and pressing ecommerce issues including the validity of electronically concluded agreements, the validity of electronic data, the admissibility of electronic documents in courts of law and the legal status given to electronic signatures” (Dekker, 2002a).

The provisions of the Act still have to be tested in a court of law, as there are many issues that the Act remains vague on. Many of the requirements stipulated in the Act are contrary to current practice and too much unilateral power is given to the Minister and Department of Communications.

Despite the fact that many aspects of the ECT Act is still untested, companies need to ensure they begin to comply with stipulations in the Act. The following subsections will investigate some aspects of compliance with regulations relating to email.
2.6.2 Legal document

The ECT Act (Section 11) gives legal force to information that is wholly or partly in the form of a data message (ECT Act, 2002). This “bears a number of legal implications for companies … as it is no longer just paper files that are considered legal documents … A business agreement that is committed via email, SMS or even recorded voice is considered to be a legal document (Weideman, 2003).

“In the USA … Anything you write in an email message can be used in court” (Somis, 2003).

Companies will have to review their stance towards email use by its employees in light of the legal weight of email, not just from a security point of view, but also in the way mail is stored and retained.

2.6.3 Retention

“The growing size of email data stores is becoming a storage management issue for many companies as the time to backup and, more importantly, restore is exceeding operational limits” (DiCenzo, 2002, p.2). Most companies have a policy regarding document retention. Often there are legal requirements as to how long documents should be retained, but for general correspondence companies usually set up their own retention periods, depending on the type of documents. Many companies only consider the retention of paper documents, but in light of the legal status of electronic communications, email and other electronic documents should also be subject to these retention policies.

In South Africa, “an organisation is obliged to keep records of its business relationships and transactions for up to five years after the fact … the penalty for not following this procedure can be a fine of up to R10 million or 15 years in jail” (Weideman, 2003).

In the USA, The Sarbanes-Oxley Act of 2002 allows “harsher punishments and imposes fines and prison sentences of up to 20 years for anyone who knowingly alters or destroys a record or document with the intent to obstruct an investiga-
tion” (Iosub, 2003). Such was the finding during the Enron scandal when Enron auditors, Arthur Anderson, LLP, were found “guilty of obstructing the course of justice” (Middleton, 2002, p. 333) for shredding documents and purging data files.

Just as a company will not retain its business-critical paper documents in employees’ offices, but rather in a central departmental filing system, so too should the company make central electronic storage available for electronic documents that have business value. It is very important for a company to define clearly what documents are considered to have business value, as there is no sense in retaining arbitrary daily communication, even if it is business related. Iosub (2003) disagrees with a selective retention as during an investigation, discovery requests could “require access to all email communication”.

“It is for this reason that it is imperative that companies implement good document management systems, as there is no point to have [the Access to Information] right entrenched in the constitution if you cannot find the necessary documents due to poor corporate processes” (Weideman, 2003).

According to a Gartner study (DiCenzo, 2002), there are three basic approaches to email archiving:

- **Archiving for regulatory compliance.** All messages entering or leaving the company email system, and even communication between employees, are archived. Storage overhead is very large with this approach and is often only implemented in government departments.

- **Archiving email attachments.** This approach aims at removing attachments from the active email database and speeds up backup and restore times. Attachments are archived separately.

- **Selective archiving.** Various criteria are used with this approach. Messages are filtered according to keywords, date or sender/recipient. “Since it is widely estimated that only 30 percent of emails are worth retaining, if some intelligence can be implemented in the archiving process, fewer casual messages will be moved to the archive” (DiCenzo, 2002, p.4).
Mark Foley, a civil litigation attorney, advises on short backups of 7 to 30 days and the regular purge of the mail system. He also recommends “setting limits to the sizes of personal email boxes so that deletions are required” (Foley, 2002). This approach can be enforced through the introduction of email quotas.

A 2002 Osterman survey found that 14.7% of organisations found managing mailbox quotas one of the biggest concerns in email management, second only to the problem of spam (Corporate Executive Board, 2003). A Gartner study also confirms that most companies limit the size of user mailboxes for operational reasons, such as the time to back up and the amount of storage space required. (DiCenzo, 2002, p.3).

If mail quotas are not enforced, a company may face exponential growth in storage requirements – “up to 50% a year” (Iosub, 2003). Quotas will force employees to manage their own mailboxes, but the danger exists that documents with business importance may be deleted accidentally or out of frustration to comply with the quota.

Companies may have to look at their entire document retention policy to ensure their email retention policy is consistent with this. The main reason retention policies should be enforced is to facilitate the discovery phase in case of litigation. As a deterrent to litigation, the use of disclaimers has often been encouraged.

### 2.6.4 Disclaimers

It has been established that email messages bear legal weight. The same control that exists over company letterheads do not exist in the email environment. It has therefore become fashionable to insert email disclaimers at the end of an outgoing company email.

Although it cannot exonerate a company from any responsibility for email sent by its employees, it could play an important role in limiting a company’s risks, as it may act as a deterrent for most persons from seeking legal compensation from a company.
Email disclaimers are statements that are either pre-pended or appended to emails, either for legal or marketing reasons. Legally, it is important for a disclaimer to have been noticed and read. A legal company may want to place the disclaimer at the beginning of a message, whereas other companies may choose to place it at the end.

Although many companies only place disclaimers on outgoing messages (i.e. those leaving the internal email system), there is a strong case for appending disclaimers on internal email as well. Much litigation for sexual harassment or racial discrimination has its origin inside a company.

The following legal reasons for disclaimers have been cited (Email Disclaimers, 2001):

- **Breach of confidentiality**: By including a disclaimer that warns that the content of the email is confidential, a company could be protected against the exposure of confidential information. If the receiver breaches this confidentiality, they could be liable.

- **Accidental breach of confidentiality**: If an employee were to receive a confidential mail from someone and by accident forward it to the wrong person, the employee, and therefore the company, could be liable. Email can easily be intercepted. A statement at the end of an email, that the message is only intended for the addressee and that if anyone receives the e-mail by mistake they are bound to confidentiality, could protect the company.

- **Transmission of viruses**: If an employee sends or forwards an email that contains a virus, the company could be sued for this. A warning in the disclaimer that the email could possibly contain viruses and that the receiver is responsible for checking and deleting viruses, could protect the company from where the mail was sent.

- **Entering into contracts**: Written communication, including email, can be used to form binding legal contracts if the individuals have actual or apparent authority to do so. If a company does not wish to enable certain employees to form binding contracts by email, a statement could be included that any form of contract needs to be confirmed by the person’s manager.
- **Negligent misstatement**: By law, a person is obliged to take care when giving advice that a third party relies on. If an employee were to give professional advice in an email, the company will be liable for the effect of the advice that the recipient, or even third party, reasonably relies upon. A suitable disclaimer could protect the company from this kind of liability.

- **Employer’s liability**: A company is ultimately responsible for the actions of its employees, including the content of any emails sent. A disclaimer can decrease liability if a company can show that it has correctly instructed its employees not to send libellous, inappropriate or defamatory statements. The disclaimer could help in disclaiming responsibility if an employee breaches these rules. A company can demonstrate this by including an email disclaimer to that effect, and by implementing an email policy that clearly warns employees against misuse of email.

According to Buys (2003), “Email disclaimers are valid and enforceable in terms of section 11 (3) of the ECT Act 25 of 2002, if the disclaimer would have been noticed by a reasonable person and it is accessible in a form in which it may be read and saved by the reader”. Buys continues to say that rather than calling it an email disclaimer, it should be referred to as an email legal notice.

Depending on the nature of the company, Buys (2003) asserts that these email legal notices should address the following issues:

- Confidentiality
- Reservation of copyright in the message attachments
- Disclaimer
- Non-liability if employees use the message for non-company or illegal purposes
- The fact that the email message may be intercepted and used by the employer
- Governing law
- Disputes to be referred to arbitration
- The issues required in Chapter 3 of the ECT Act and
- Disclosure of the company’s registration number, address and directors (as required by section 171 of the Companies Act of 1973)
As this may become a lengthy document, many companies refer to their email legal notice (or disclaimer) as a hyperlink to a website. A company should bear in mind that many recipients of email do not have Internet access, and Buys (2003) recommends that a telephone number is included where a copy of the document can be requested, as he shows in the following example:

“Please read our Email Legal Notice by clicking here: www.companysite.com/terms.htm or phone +27-(0)41-123 45678 should you fail to get access to the Notice. By reading and/or acting upon this email message you are legally bound to the terms of the Notice.”

“There is no disclaimer that can protect against actual libelous or defamatory content. The most a disclaimer can accomplish in this respect is to reduce the responsibility of the company, since it can prove that the company has acted responsibly and done everything in its power to stop employees from committing these offenses” (Email disclaimers, 2001).

Ian Miles, CEO of UK Company, DespatchBox, states that “the use of disclaimers is nothing more than a corporate fashion statement that endangers the confidentiality of sensitive information” (Townsend & Taphouse, 2002), as it gives the company a false sense of security. A disclaimer cannot safeguard messages – encryption should be used in addition to any disclaimer in a message.

“Essentially the use of … disclaimers is a lazy way of putting off the creation of an institutional email and digital information policy which lays out what can be sent by email and whether or not it should be encrypted” (Somis, 2003). It is important to note that disclaimers carry different legal weight depending on the governing law of the country.

It is clear that disclaimers are merely a deterrent to possible litigation. It has become common practise for companies to use disclaimers, but this should not be considered to be a guarantee against legal action.

2.6.5 Encryption and Digital Signatures

According to the ECT Act 25 of 2002 certain transactions require digital signing, although email may be submitted as legal evidence without such digital
signatures. The law refers to digital signatures as “Advanced Electronic Signatures” (ECT Act, 3:13(1)).

Irrespective of legal compliance, there are valid reasons for using signatures and encryption on certain company email. An email message is like a postcard – it can be read by anyone and theoretically be altered by anyone before it is delivered, without the recipient being aware that it has been altered. Digital signatures prove whom email comes from and that it has not been altered in transit. It also allows you to encrypt email so that it can only be read by the intended recipient.

Although some commercial packages (e.g. Lotus Notes) authenticate the sender of all messages, a digital certificate can be installed on a PC using either the SMIME standard or the PGP standard. Digital certificates may be obtained from www.thawte.com, (the company Mark Shuttleworth started), or from a company called Verisign, at a small fee. Various browsers also have built-in encryption, 128-bit encryption being the norm.

“Authentication allows the receiver of a digital message to be confident of both the identity of the sender and the integrity of the message” (Thawte, 2003). Authentication works by establishing the identity of a sender through a trusted third party and this identity is then proven by a credential issued by a Certification authority, such as Thawte or Verisign.

There are governing laws in each country that determine the maximum encryption strength for private / commercial use. In South Africa, Chapter V of the ECT Act requires cryptography providers to make the encryption keys available to the government in order to maintain a register. Some companies in their Information Systems policies require users of encryption to provide their managers with their keys. This may prove to be a requirement under section 11 or 30 of the Promotion of Access to Information Act 2 of 2000.

When the identity of the sender of an email message needs to be verified, companies should use digital signatures. This will assist in cases of litigation and may even be legally required for certain electronic documents.
2.6.6 Invasion of privacy

“At exactly the same time they are training their staff to respect consumer privacy; [companies] are increasingly monitoring their employees’ physical activities on and off the jobsite, client contacts, telephone conversations, email transactions and web site visits. While this is to some extent driven by regulation, concerns about enhancing productivity and reducing the possibility of prosecution, failure to respect the personal privacy of employees may have long-term destructive effects” (DeLotto, 2002, p.8). If employers monitor their email systems without notifying employees of their right to inspect messages, they risk invading the privacy of employees.

In America, it has been established in the courts that private sector employers are free to monitor employees, so monitoring becomes “an issue of ethics, not really one of legality” (Van Slambrouck, 2000, p.1). A company should draw a distinction between privacy and confidentiality, as an employee has the right to expect certain things to remain confidential. Information that an employee may justifiably consider confidential is, among other things, medical records and salary information. Private information may relate to correspondence not intended for a third party.

“Gartner research indicates that by 2005, most US financial service providers will have experienced significant employee relations problems relating to privacy in the workplace (0.8 probability)” (DeLotto, 2002, p.9).

It is imperative that companies consider privacy issues before implementing monitoring procedures. In Chapter 4, closer attention will be given to privacy in email policies.

2.6.7 Email monitoring

When considering the risks associated with email in corporate environments, there is no doubt that companies have an obligation to safeguard itself against such risks. The obvious risks are viruses, junk email and libellous material.
Unless such messages are filtered out, a company may waste bandwidth, storage, as well as employee time.

“As an employer [in the U.K.] … you would be very unwise to start monitoring without your employees’ knowledge … You must make clear to your employees what you are monitoring for, why and how” (Infant, 2002).

It may be an easy task to motivate why email is monitored – to protect the company from litigation and to protect business systems. The method of monitoring (how) may be prescribed by the particular software the company chooses to use. The difficult issue is to determine what is being monitored.

According to a Surfcontrol White paper (Surfcontrol, 2001c, p.5), mail should be monitored for material that contains information that is

- Confidential
- Breaches privacy
- Offensive, libellous or otherwise commercially inappropriate
- Pornographic
- Virus infected

Content-filtering software will allow for the automated monitoring of the above categories with various degrees of success. However, filtering alone will not ensure that a company is protected against all email threats. Policies that allow for the monitoring of email may have to be implemented. As the implementation of such monitoring policies is a potential minefield, Chapter 4 will explore the legal implications of email monitoring in depth.

This section discussed the legal implications of email. The Electronic Communications and Transactions Act of 2002 has a major impact on how companies should view their email communications. Issues like retention and disclaimers become important, as electronic documents now have legal status. In its quest to ensure that employees comply with legal issues, companies run the risk of running foul of the law through possible illegal monitoring of email, which may be considered an invasion of privacy.
## 2.7 Conclusion

Usage of email has been one of the fastest growing technological tools over the past two decades. Once the domain of the military and education, email usage has become ubiquitous – both in private use as well as in the business environment.

Despite its usefulness and key role in business, it has introduced abuse and several threats into the business environment. Some of the threats are technological (e.g. viruses), but many threats stem from abuse of email systems by employees. Companies need to protect themselves against litigation. “Apart from legal disclaimers … companies can use other tools to protect themselves against the legal implications of email. Among them are implementing an email policy, and using email filtering and anti-virus software” (Email disclaimers, 2001).

The nature of threats and abuses introduced by the use of email at work requires a multi-pronged approach. Some of these precautions have been touched upon in this chapter. Unless a company has a clear and concerted strategy to counter potential email threats and abuses, it will either alienate its workforce or be unsuccessful in stemming abuse. The creation of security policies is an essential ingredient of this multi-pronged approach.

In Chapter 3, the nature of security policies will be investigated. Creating a policy is not enough in itself – the policy has to be implemented and enforced in order to be effective. Chapter 3 will investigate why security policies are needed and look at various approaches to create an Information Security Policy framework.

Once a framework has been identified, the position of an email policy in such a framework will be highlighted. In a later chapter, the content of an email policy will be discussed in detail.
Chapter 3: Information Security Policies

3.1 Introduction

In Chapter 2 it was shown that managing email in an organization is not a simple task. Although software can be used to make this management task easier, many aspects of email requires self-management. A company cannot accept in good faith that all employees will practise self-management. Policies need to be put in place to give the company leverage in enforcing certain principles of email usage.

In order to understand how best to create and enforce email policies, it is necessary to understand what policies are and in what context they are created. Various frameworks for Information Security Policies will be examined. Barriers to effective implementation and enforcement will be evaluated. This general study of Information Security Policies will be used later in this paper and applied to email policies in particular.

3.2 Why security policies are needed

Although Information Security has always been considered an integral part of an IT department’s functions, nothing has catapulted the need for good disaster recovery procedures into the corporate mind than the events of September 11, 2001. Several companies were crippled (and even closed down completely) by the destruction of the World Trade Centre in New York. (Nair, 2002, p.37).

Not long after this disaster, the Enron scandal placed corporate governance under a microscope (Wessels, 2002, p. 102) when Enron auditors, Arthur Anderson, LLP, were found to have shred documents and purged data files.

The King Report on Corporate Governance in South Africa 2002 places a direct responsibility for Risk management on the board: “The board is responsible for ensuring that the company has implemented an effective ongoing process to identify risk, measure its potential impact against a set of assumptions, and then activate what it believes is necessary to proactively manage these risks” (Dekker, 2002b).
According to Alberts (2001) “many organisations form protection strategies for their information systems by focussing solely on infrastructure weakness”. Strategies to secure the infrastructure are necessary in an era where viruses, hacking and denial of service attacks are daily occurrences in most large companies. Companies spend large amounts of capital to build redundancy into their network and hardware infrastructure and on IT Recovery (DRP) sites. This capital intensive strategies often lull companies into a false sense of security, where perceived threats are considered as being external only, albeit human or natural.

A security infrastructure requires six key elements to ensure it is comprehensive and implementable: “security policy, user authentication, encryption, access control, audit and administration” (Edmead, 2002). Edmead continues to state that “the foundation of the security infrastructure starts with the development and adoption of a security policy.” This emphasis on policy is supported by Pipkin (2000), who asserts that “[human] error is by far the most common threat against an organization’s resources” (p. 36) and that policy is the primary means buy which to control the human aspect of security.

Although there is an awareness of these internal threats, many companies do not have adequate policies in place to manage these threats. Even if there are policies in place, these policies are seldom adequately enforced. “For a policy to show any return on investment, it must become integrated into the processes and procedures of business, along with the support of the people who are meant to follow it” (Peikari, 2003).

It is necessary to define exactly what is meant by a policy, as there is often confusion about the distinction between policies, procedures, standards and practices. The SANS (SysAdmin, Audit, Network, Security) Institute security policy project draws distinctions between the various levels of security and policy and procedure documents. “A policy is typically a document that outlines specific requirements or rules that must be met … A standard is typically [a] collection of system-specific or procedural-specific requirements that must be met by everyone … A guideline is typically a collection of system-specific or procedural-specific ‘suggestions’ for best practice. They are not requirements to be met, but are strongly recommended” (SANS, 2001).
The Mirriam Webster Online Dictionary has the following among its entries under *policy*:

**Etymology:** Middle English *policie* government, policy, from Middle French, government, regulation, from Late Latin *politia*

**Date:** 15th century

1. *a:* prudence or wisdom in the management of affairs  
   *b:* management or procedure based primarily on material interest

2. *a:* a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions  
   *b:* a high-level overall plan embracing the general goals and acceptable procedures especially of a governmental body

For the purposes of this paper, the entry under 2.b. is especially relevant.

A more complete description, which highlights both the purpose of a security policy, as well as the method of meeting this goal, is proposed in Peikari (2003): “A security policy can be defined as a set of documents that describes the security goals as required for the sole purpose of protecting the physical and information assets of a business.”

This chapter will investigate the various approaches to security policy creation, implementation and enforcement. This information will be used later in this paper to create an email policy.

### 3.3 How information security policies are created

In the general risk management methodology, it is standard practice to perform a risk assessment exercise where resources are defined, threats are assessed and assigned (monetary) values, and safeguards are defined and implemented. (Pipkin, 2000).

These approaches have been refined by various writers in the Information Security field, but there is a measure of consistence in their approach. Edmead (2002) identifies six steps in developing a security policy. For him, security policy is the foundation of an information security plan in any organisation.
### Table 3.1. Steps in creating security policies

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Classify the systems:</strong> Do an inventory of all systems and determine how they are used in the organisation.</td>
<td><strong>Resource inventory:</strong> Identify resources, assign ownership, determine their value and give a security classification.</td>
<td><strong>Phase 1: Build asset based threat profiles:</strong> Identify assets, examine threats to and security requirements of those assets. Determine what will happen if those assets are unavailable or lost to the organisation.</td>
</tr>
<tr>
<td><strong>Determine security policies:</strong> Each system must have its own security policy.</td>
<td><strong>Threat assessment:</strong> Determine what possible threats there are to each system and define through policy how to mitigate those threats.</td>
<td></td>
</tr>
<tr>
<td><strong>Assign risk factors:</strong> Understand the risks if the policy is NOT followed.</td>
<td><strong>Loss analysis:</strong> Determine the cost of a loss through breach of security.</td>
<td></td>
</tr>
<tr>
<td><strong>Define acceptable activities:</strong> Address what is acceptable, as well as what is NOT acceptable.</td>
<td><strong>Identify vulnerabilities:</strong> Any activity that can be exploited to an advantage is considered a vulnerability, i.e. direct actions or neglecting to perform certain actions.</td>
<td><strong>Phase 2: Identify Infrastructure Vulnerabilities:</strong> Evaluate the information infrastructure and examine weaknesses that may lead to unauthorised action.</td>
</tr>
<tr>
<td><strong>Provide security awareness training:</strong> Train employees on the policies.</td>
<td><strong>Assigning safeguards:</strong> Safeguards can be implemented with hardware or software or with policies and procedures.</td>
<td><strong>Phase 3: Develop Security Strategy and Plans:</strong> A protection strategy and mitigation plans addressing the highest priority risks are developed and enforced.</td>
</tr>
<tr>
<td><strong>Determine the administrator of the policy:</strong> This entity will revise, update and enforce the policies.</td>
<td><strong>Evaluation of current status:</strong> Asses current policies and procedures and evaluate the quality of implementation.</td>
<td></td>
</tr>
</tbody>
</table>
Pipkin (2000) also identifies a six-step plan during the inspection phase for building an information security plan. Another approach to information security risk evaluation is the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) methodology (Alberts, 2001). This methodology reflects a similar approach to Pipkin and Edmead, but through a three-phase plan.

These approaches are summarised in Table 3.1 and show that, although the emphasis differs, there is a direct correlation between the approaches to creating a security policy and creating a comprehensive security plan for an organisation.

In an unpublished article, Von Solms (2002) identifies three levels of policy analogous to what he calls “The Moses Model”. The Ten Commandments, which were delivered to Moses, form the basis of this model. From these commandments, hundreds of laws were derived to assist with the interpretation of the commandments. Finally, the laws were developed into directives to address various groups and situations.

This analogy can be translated into the corporate environment as executive level policies, secondary level or systems-specific level policies and finally, procedures. Just as the original commandments were handed down by God, executive level policies should originate and be signed by the most senior official in the company to ensure credibility. This view is supported by Cobb (1996): “Policy not only has to start at the top, it has to come from the top”. Von Solms continues that “executive level policies should be fairly static over time, not [be] too cumbersome and should address conceptual issues rather than specifics.

Just as various laws supported the Ten Commandments, executive level policies “should be augmented by secondary level policies that are more dynamic, specific and quite detailed, taking the current economic, business and technological situations into consideration” (Von Solms, 2002).

Finally, analogous to the directives that supported the laws, is a series of procedures that are “logically ordered, prepared in a non technical way and specifically spells out the actions and behaviour” of the employees.

“The Moses Model” of Von Solms can be represented as in Table 3.2.
Table 3.2. The Moses Model analogy

Using this categorisation, one can conclude that policies are usually defined at corporate (head-office) level. Standards are essentially the documents that are enforced on regional or branch level and may differ in various countries, subject to legislation and differing local standards. Guidelines (or procedures) may then be used to clarify the procedures at user level to simplify the understanding and implementation of policies.

“It is important to draw the distinction between policies, standards, guidelines and procedures. While policies are a high-level overview of security directives, standards are adopted national or international levels of performance to reach or maintain if already attained. Guidelines are modes of operation to be followed voluntarily at the discretion of a person or organisation, while procedures are mandatory how-to steps to follow in performing a task” (Barman, 2002).
3.4 Developing an Information security policy framework

The bulk of this section is based on the work of Palmer (2001), outlining the development of the METASeS Information Security Policy Framework.

“An information security policy framework provides an organisation with a concise yet high-level and comprehensive strategy to shape its tactical security solutions in relation to business objectives … it clearly defines the value of information assets, represent organisation wide priorities, and definitively states the underlying business requirements and assumptions that drive security activities” (Palmer, 2002, p.13).

Many organisations lack a reference to a framework against which they can measure existing policies or base the development of new policies. Organisations find that their existing policies are either outdated or have been developed piecemeal over time. It becomes difficult to review policies over time, as policies are often incomplete, cross-threaded and not traceable back to the business objectives and needs.

3.4.1 The Information Security Policy Framework

Palmer and his associates assessed numerous information security policies and performed a gap analysis to highlight possible improvements, and then developed a baseline reference model that organisations could use and customise to address their specific needs. This framework model incorporates five comprehensive concepts:

1. **Risk management basis** – Risk is a function of threat, vulnerability and asset value. Risk cannot be eliminated, but can be managed by applying security measures.

2. **Hierarchical Policy Structure** – The policy structure is directly linked to the risk management strategy and with other framework elements such as standards, guidelines and procedures. This hierarchy is illustrated in figure 3.1 below.
The Information Security Charter at the top of the hierarchy empowers all the activities within the information security programme.

- Policies further define the information security objectives in a number of topical areas.
- Standards provide more measurable guidance in each policy area.
- Procedures describe how the standards must be implemented.

This hierarchy ensures that elements lower down are traceable back to the business objectives.

3. **Guideline definition** – Guidelines enable policy guidance prior to the formulation of fully developed standards and procedures on a specific topic.

4. **Threat and vulnerability policies** – Explicitly address vulnerabilities and threats at the policy level.

5. **Policy Interpretation** – The framework is comprehensive in its coverage and requires minimal changes to top-level policy areas. Other frameworks apply a new top-level policy area for each new application of technology, which leads to a complex, ad-hoc and cross-threaded policy framework. By using policy interpretation documents for a specific audience or a specific technology, this complexity is eliminated.

### 3.4.2 Framework components

Figure 3.2 below illustrates the content of the Information Security Policy Framework, consisting of an Information Security Charter and seven policies.
Information security program Charter

“The charter summarises the organisation’s attitude and philosophy regarding security.” (p.21). It also addresses management issues like scope of coverage, executive ownership, management responsibility, accountability, policy enforcement and communication.

Under policy enforcement, the consequences for non-compliance and methods for handling exceptions are outlined.

As stated before, and corresponding with the Moses Model, the Charter should be approved and signed by the CEO to ensure security related initiatives are not challenged and do not require individual justification and approval.

Policies, standards and procedures

“A policy defines an organisation’s high-level information security philosophy in a topical area. Policies are brief technology- and solution-independent documents.” (p.22). Standards provide more measurable guidance in each policy area, whereas procedures describe how to implement the standards.

Each of the Framework policies is briefly discussed below and is taken from Palmer (2001, pp.23-24).
1. **Asset Identification and Classification Policy** – An organisation must properly classify the information assets relative to its criticality, sensitivity and value to the organisation, e.g. restricted, confidential, internal use only, public.

2. **Asset Protection Policy** – The organisation's specific standards for providing an appropriate degree of confidentiality, integrity and availability for information assets is defined by this policy.

3. **Asset Management Policy** – This policy defines the objectives for properly managing a company’s information technology infrastructure, including its servers, networks and systems in order to support the objectives of the Asset Protection Policy.

4. **Acceptable Use Policy** – It defines an organisation’s objectives for ensuring the appropriate business use of information assets, including Internet, email, telephones, etc. It also states an organisation’s position on the right to monitor, record, and audit the use of such systems and equipment and addresses the reporting of potential misuse.

5. **Vulnerability Assessment and Management Policy** – A vulnerability assessment is an activity in which an organisation identifies and prioritises technical, organisational, procedural, administrative, or physical security weaknesses.

6. **Threat Assessment and Management Policy** – Defines an organisation’s objectives for threat assessment activities and ongoing threat monitoring efforts. It defines how it will detect, respond to and recover from any threat activity.

7. **Security Awareness Policy** – This policy defines how the formal Security Awareness Program is implemented and ensures that appropriate education and training is provided.

Specific key standards will provide more measurable criteria for supporting the high-level objectives of the policies. Standards may be more technologically specific and state what needs to be done. Procedures give detail in easy to understand language on how a standard should be implemented and may go as far as giving systematic instructions.
3.5 Other policy frameworks

Several bodies have endeavoured to create standards for information security policies. Often these are generalised guidelines applicable to all industries, e.g. ISO17799, BSI, ITIL, NIST, SABS, and the SANS Institute. In some instances, the guidelines are specific to an industry, e.g. HIPAA.

Often national bodies adopt the standards of an international body, like the International Organisation for Standardisation (ISO). In other cases, a national standard is so thorough, that it becomes an ISO standard. Each of these security standards will be discussed briefly in the following subsections.

3.5.1 ISO17799

The International Organisation for Standardisation (ISO) consists of a network of national standards institutes from 147 countries working in partnership with international organisations, governments, industry, business and consumer representatives. It forms a bridge between public and private sectors.

For many companies an effective starting point to define a security policy strategy is the ISO 17799, which is an international information security standard. This standard is organised into ten major sections. Each section contains detailed statements that comprise the security standard.

- Security policy
- Organisational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications & operations management
- Access Control
- System development and maintenance
- Business continuity management
- Compliance
ISO17799 is essentially an internationally recognised generic information security standard that is intended to serve as a single reference point for identifying a range of controls needed for most situations where information systems are needed in commerce or industry. This standard had its origins in a British Standards Institution code of practice. (ISO17799, 2003).

3.5.2 BSI

The British Standards Institution (BSI) was founded in 1901 and is a leading global provider of professional services to organisations worldwide. Among its functions is the development of private, national and international standards.

The BSI developed a Data Technology Code of Practice, which it published as Version 1 of the BS7799 in February 1995. This standard was not widely embraced at the time, as Y2K issues were taking precedence. It was revised and published as Version 2 of BS7799, before it was accepted as an ISO standard. (BSI, 2003).

3.5.3 ITIL

ITIL (IT Infrastructure Library) is a widely accepted approach to IT Service Management. ITIL provides a cohesive set of best practice, drawn from the public and private sectors internationally. It is supported by a comprehensive qualification scheme, accredited training organisations, and implementation and assessment tools. The best-practice processes promoted in ITIL both support and are supported by the British Standards Institution’s Standard for IT Service Management. (ITIL, 2003).

3.5.4 NIST

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. (NIST, 2003).
3.5.5 SABS


3.5.6 SANS Institute

The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. The SANS Institute enables more than 156,000 security professionals, auditors, system administrators, and network administrators to share the lessons they are learning and find solutions to the challenges they face.

At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community. The SANS Institute is a collaborative organisation and makes available much of its research free of charge. (SANS, 2001).

3.5.7 HIPAA

A further standard that is being enforced in the USA is the standards for information security determined by Health Insurance Portability and Accountability Act of 1996 (HIPAA).

“HIPAA is designed to protect confidential healthcare information through improved security standards and federal privacy legislation. It defines requirements for storing … information before, during and after electronic transmission” (SANS, 2001). There are more than sixty-eight information security conditions in three areas that must be met to ensure compliance with HIPAA. (Federal Register, 2003). These areas are:

- **Technical Security Services**: user authorisation and authentication, access control and encryption;
- **Administrative procedures**: formal security planning, record maintenance and audits; and
- **Physical Safeguards**: security to building, privacy for office and workstations that handle patient information.

It is clear that much work has been done towards the creation of security policy standards. These standards overlap, but they still have to be adapted into a framework that suits a specific organisation. Rather than being selective about which aspects of a policy standard to implement, a company should try to be comprehensive in its security coverage. The next section will look at the features of a good security policy.

### 3.6 Characteristics of a Good Security Policy

Many companies inherit security policies that have been created in an era where the threats on a technological security level were not as severe. The ownership of the Information Security Policy often lay with a local IT manager, rather than with the Executive. Organisations must re-evaluate their policies.

This section will highlight 15 characteristics that a good security policy will comply as identified by Palmer (2001, p. 22).

- Both senior management and users must accept the policy as the official reference document on security
- The policy should firmly integrate security within the overall business and technical strategies, and within risk management practices
- The business should drive the policy and policy enforcement – not the other way around
- The policy must be consistent with existing corporate directives and guidelines, and with applicable government legislation and regulations
- The scope of the policy should define what resources are affected and to whom the policy applies
- The policy should be limited to stating the organisation’s security objectives, priorities, and high level strategies, thus serving as a framework for the various business areas
- The policy should be concise and written in clear, unambiguous language that speaks directly to a broad audience. It should be carefully structured to allow easy reference to particular sections
As a living document, the policy should be reviewed at regular intervals, or as significant events, such as a merger or acquisition, require

The policy should focus exclusively on broad principles and objectives

The policy document should be carefully worded and ensure that all terms are accurately and precisely defined, and used exactly as intended

The policy should clearly delineate responsibility, accountability, and lines of authority across the organisation

The policy must be technically and organisationally feasible

The various constituents governed by the policy should have access to the relevant policy material, rather than being required to read and understand all of the policy information

Each policy should clearly describe how exceptions to the policy are to be considered and adjudicated

The initial policy document, and subsequent updates, should have a version number and a date

Peikari (2003), quoting an InformIT (2003) article, summarises the characteristics of good security policies as follows:

They must be implementable through system administration procedures, publishing or acceptable use guidelines, or other appropriate methods;

They must be enforceable with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible;

They must clearly define the areas of responsibility for the users, administrators, and management.

They must be documented, distributed, and communicated.

The article continues with what content security policies should cover:

Prevent waste or inappropriate use of organisation resources;

Limit or eliminate potential legal liability, be it from employees or third parties;

Preserve and protect valuable, confidential, or proprietary information from unauthorised access or disclosure.
A company can evaluate the content of its security policies against the criteria mentioned in this section. It may comply with the criteria, but if the policies are not implemented and enforced, they have no effect on the organisation. The implementation and enforcement of policy is integral to the security policy strategy, and a concerted implementation plan is required to make policies part of an employee’s daily work life.

The next section will investigate how security policies can be implemented and enforced, and also look at barriers to the enforcement of policy.

3.7 How Information Security Policies are implemented and enforced

Protecting the infrastructure from external threats has become de rigueur in Information Technology best practice. “Perhaps the most overlooked threat in a security program is the threat posed by employee behaviour” (Hook, 2002). Furthermore, “it is the human element that is the weakest link in the security chain” (Otter, 2002).

The Working Council for Chief Executive Officers has identified that, “in addition to the growing number of widely publicized external information security threats to corporate networks … serious threats also lie within the corporations themselves, in the form of insider negligence, misuse and abuse of corporate information systems…Two of the three most prevalent types of security breaches reported by large organisations in the latest CSI/FBI survey are internal” (Corp, 2000, p.8).

Mark Danton, in charge of e-security at Ernst & Young, stated that “good security is 20% technology and 80% people and process” (Otter, 2002). Otter also quotes Trent Rossini, head of security at Discovery Health, who puts “people and processes at the top of [his] security checklist, followed by performance management and access control.”

Although there is always a risk of employees or contractors within the company having a destructive agenda, most risks are accidental through human error. Users should be educated in both the content and the motivation for Information Security Policies that exist in a company. It is not enough to have employees sign a user agreement form and assume that they understand the conditions contained therein.
“Procedural threats originate from the lack of training on system procedures or lack of adequate procedures” (Xiao, 2000, p. 36). Many employees in a company have a vague awareness of the existence of security policies in the company, but most are ignorant of the content of these policies.

### 3.7.1 Methods of policy implementation

Various attempts to ensure compliance with Information Security Policies have attained, at best, limited success. Traditionally, internal or external audits are used to measure compliance, but have had limited success in changing the behaviour of individuals. “Senior management pep talks, executive management memoranda, and security awareness campaigns” were all felt to be unsuccessful (Wylder, 2003, p. 29).

Section 6 of the ISO17799 security standard has as its objectives “to reduce risk of human error, theft, fraud or misuse of facilities; to ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work; to minimise the damage from security incidents and malfunctions and learn from such incidents”. There is an emphasis on making users aware of policies – the existence of a policy does not eliminate the threat. “The human side of security policy is an essential ingredient for its most successful implementation” (Tittel, 2002).

It is important that “the implementation of security should never hinder ongoing business processes” (Otter, 2002). As soon as policies become too intrusive, users develop a resistance to implementing them, especially if they do not understand their importance. A combination of physical, technological and social techniques can be used to ensure effective policy implementation.

**Physical**

Physical security is an essential part of policy implementation. Fire protection, access control systems, air-conditioning standards, as well as the physical handling and storage of backup media all form part of the physical implementation of a security policy.
Technology

Very often technical security is the main emphasis of an information security policy, as these policies are very often written by technical staff. There is a perception that all policies can be implemented by using technology only. Although many aspects of policy can be technologically implemented, this is often not cost-effective. The user base may also not take kindly to a “Big Brother” approach to policy implementation. Areas where technology is often used to implement policy, is with user IDs and passwords, firewalls and intrusion detection systems. The use of email filtering software and the ethical and legal issues surrounding its use will be discussed in detail in the next chapter.

Social

Social or non-technical implementation of policy relies mainly on user education. Some of the approaches with this type of implementation include the requirement of users to take a self-study course on the company’s security policies, annual testing of security awareness, inclusion of policies in employee handbooks and public relations campaigns using the intranet, email or posters. A Pentasafe survey quoted by Wilder (2003, p.30) found that “nine out of ten employees were likely to open and execute an email attachment without questioning its source or authenticity”.

Another example of the importance of user education is in implementing a password policy. “A comprehensive password policy is the first line of defence in a well-rounded IT security plan,” (TechRepublic, 2002a). Users should be educated in the need to keep their passwords confidential and sufficiently complex. They should be made aware of strategies like social engineering and brute force efforts by malicious insiders to obtain passwords.

An understanding of the consequences of unauthorised access will encourage users to accept and adhere to password policies. To assist users in adhering to password policies, the IT department can introduce a single logon structure that obviates the necessity for users to remember numerous different passwords, thus implementing the password policy on a technological level.
Rather than blaming a lack of awareness of the policy or a lack of understanding of the consequences, employees blame the pressure to be productive as the main reason for not complying with certain policies.

Tittel (2002) makes recommendations on how to ensure buy-in from employees on information security policies. Employees need to understand why security is important. Training on the content of policies is important for both new and current employees. The security policies should be broken down into small, digestible pieces of no more than a page in length. In order to ensure buy-in, employees should sign off that they have read and understood the security policy documents and if there is a violation of a policy, the consequences must be clearly spelled out and imposed. To ensure that policies do not hamper productivity, user input should be solicited in the creation and revision of policies. Finally, Tittel suggests creating a “neighbourhood watch” mentality amongst users to ensure they regulate themselves.

3.7.2 **Enforcers of policy**

The creation and implementation of policy is often only the first steps in an information security programme. The goal of such a programme is to get compliance. Ultimately, “the one thing that really matters when it comes to information security: change behaviour [of employees]” (Verton, 2000).

Several approaches to the enforcement of policies have been proposed and practised. This section will look at bureaucratic, incentive and cultural methods of enforcement of policies.

**Bureaucratic**

Just as some policies can be implemented using technology, so too can such policies be enforced by using technology. Executive management decisions can be forced onto users by strong password control, through email filtering and blocking, as well as by monitoring usage. Employees can be held accountable by signing forms that they have read and understood policies, and occasionally an example can be made of an employee who broke policy through disciplinary
action. Such an approach will alienate employees and security staff will constantly have to police system usage for any contravention of policy.

Traditionally, various levels of a bureaucratic approach are favoured by many companies to enforce policy, whether it is through executive decree, security audits or traditional management enforcement. The main reason for this approach is a lack of understanding of the changing nature of the workplace and an inadequate implementation strategy.

**Incentive**

There is a need to make employees personally accountable for their role in compliance with information security policies. Wylder (2003, pp.36-38) proposes that compliance with policy becomes part of the employee’s annual performance assessment. Compliance becomes a job performance criterion and a Personal Information Security Plan is included in every employee evaluation.

Part of this document would be any specific security issues relating to the particular employee’s job, as well as a record of password resets and infringements of the company’s web and email policy. During the performance appraisal, an employee will sign this Personal Information Security Plan to indicate that s/he is familiar with the policy documents relating to his or her position.

By making an employee accountable for policy compliance by incorporating such a security plan in an annual appraisal, incentives like bonuses or an increase is directly linked to how well an employee complies with policy.

Although there is much merit in such a system, there is still a need to monitor and measure actual compliance, adding to the administrative burden of direct managers or Information Security staff.

**Culture (Ethnic & Corporate)**

One of the strongest enforcers of policy is employee self-regulation. In order to ensure consistent self-regulation by all employees, an organisation should ensure that security policies become part of the culture of the organisation.
“The challenge of many [security] awareness programs is the corporate culture … determine your culture’s boundaries and figure out what you can do within those boundaries … A business will have good security if its corporate culture is correct. That depends on one thing: tone at the top. There will be no grassroots effort to overwhelm corporate neglect. Organisations don’t change … people change. And then people change organisations.” (Verton, 2000). If there is a culture of compliance with policy, enforcing policy becomes a relatively simple matter, as people tend to know the boundaries of what they are allowed to do. In some countries, ethnic culture sets the trend as to what happens within the business environment and the reliance on corporate culture is less important. However, in multicultural, and increasingly, multinational environments, corporate culture has to be developed and nurtured to ensure common business values are shared.

When new policies are introduced or policies are changed, they should have a “low cultural impact” (Surfcontrol, 2001a) on the organisation. Changes should be incremental and should slowly modify the employees’ behaviour.

Cahir (2002) gives a broad definition of culture as “the values the members of a given group hold, the norms they follow, and the material goods they create”. The culture of a group is more closely defined as “a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think and feel in relation to those problems” (Schein, 1992,). This above implies that “education plays an important part in cultivating a culture” (Von Solms, 2002).

Company culture is influenced by (a) what you see done; (b) what policies are enforced; and (c) habits and beliefs. “Information laws can be seen to play an important role in the formation and content of cultural artefacts” (Cahir, 2002).

Policies must be acceptable to the employees of an organisation. “Everybody must agree that these are for the benefit of the organisation, as well as that it is
not infringing on any of the individual’s personal assumptions and beliefs” (Von Solms, 2002).

It can be concluded that organisational culture informs the creation and enforcement of policies, but at the same time, policies play a strong role in creating the cultural environment of an organisation.

This section highlighted some of the methods of security policy implementation and enforcement. The creation of good security policies is often the simplest part in an information security strategy. Ensuring compliance with these policies is crucial to the success of the strategy. The content and wording of a policy will often assist in the implementation, especially if associates can see that a policy is sensible and fair.

3.8 Conclusion

Many companies are internally vulnerable to loss of data confidentiality, integrity and accessibility, because “security policies and procedures are often far behind technological advances, and adequate staff education is rare and infrequent” (Hook, 2002). Having advanced hardware and software systems in place is not necessarily sufficient to eliminate these risks, as “good IT security is 20% technology and 80% people and process” (Otter, 2002).

Technology should be implemented to make security as unobtrusive to the user as possible, but a company should not rely solely on technology. An overview of information security policies should form part of a Human Resources induction programme for new employees. Every training program on new company systems should include a general security refresher module. If users are aware of the consequences of the loss of data integrity or compromised security, they will readily be more conscientious. Policies should not be conveyed with an attitude of mistrust in the employee, but employees should be aware that there are consequences if they deliberately ignore policies.

Well-written policies and user education on these policies will eliminate many of the internal security risks a company faces. However, instilling a culture of compliance with policy is the ideal way to enforce information security policies.
In the next chapter legal issues relating specifically to email policy will be investigated. It is much easier to ensure compliance if employees deem a policy to be fair. Emphasis will be placed on privacy issues, as a perception from employees that their civil liberties are compromised, may damage a company more than what certain policies set out to protect.
Chapter 4: Privacy legislation & email monitoring

4.1 Introduction

Brief reference to the legal aspects of email was made Chapter 2. It was shown that an electronic document, like email, is considered a legal document in South African law. For this reason, it has become necessary for organisations to manage email more closely. Chapter 3 showed the necessity of email security policies. Policies assist organisations in managing security aspects around use of company electronic resources. When it comes to email, these policies need to be written in such a way that they do not contradict the laws of the country.

This chapter will look at the legal aspects surrounding email policy and place special emphasis on privacy. Firstly, a general overview of privacy laws in various parts of the world will be highlighted. Secondly, various approaches to workplace privacy will be investigated and finally, the problem of email monitoring in the workplace will be explored.

4.2 Privacy

“Privacy is a fundamental right. It underpins human dignity and other values such as freedom of association and freedom of speech. It has become one of the most important human rights of the modern age” (Andrews, 2002, p.1). She continues that nearly every country in the world includes a right of privacy in its constitution. “At minimum, these provisions include rights of inviolability of the home and secrecy of communications.”

Privacy is a difficult concept to define. In its simplest form, it is seen as a way of drawing the line at how far society can intrude into a person’s affairs. Andrews (2002, p.3) divides privacy into the following separate but related concepts:

- Information privacy;
- Bodily privacy;
Privacy of communications – which covers the security and privacy of mail, telephones, email and other forms of communication; and

Territorial privacy

There are four major models for privacy protection identified by Andrews (2002, p.4).

- **Comprehensive laws** established by government to regulate privacy in both the public and private sectors;
- **Sectoral laws** govern privacy issues in particular industry sectors (e.g. HIPAA for the health industry in the USA);
- **Self-regulation**, through which companies and industry bodies establish codes of practice and engage in self-policing;
- **Technologies of privacy.** These include encryption, anonymous re-mailers, proxy servers and digital cash.

The above privacy models are used by governments in various combinations. Governments that protect privacy most effectively, usually use all these models together.

The recognition of privacy is deeply rooted in most cultures and has historical references to classical times. Various references to privacy laws in Western history can be found as far back as 1361. (Andrews, 2002, p.5). The modern privacy benchmark at international level can be found in the 1948 Universal Declaration of Human Rights. Article 12 states:

> No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour and reputation. Everyone has the right to the protection of the law against such interferences or attacks.

With the advent of information technology in the 1960s and 1970s, the interest in the rights of privacy increased. The first data protection law in the world was enacted in a region of Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977) and France (1978). (Andrews, 2002, p.8). From these laws, two international standards evolved which affect all legislation on data protection around the world. The first was The Council of Europe’s 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal
Data. The other was the Organization for Economic Cooperation and Development’s (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.

The major reasons for countries to adopt comprehensive privacy and data protection laws are

- **To remedy past injustices** where privacy violations took place under previous authoritarian regimes. (Andrews (2002, p.9) sites South Africa, together with central Europe and South America as examples of such countries.)
- **To promote electronic commerce.** Electronic commerce knows no (national) boundaries and customers would like to know that their personal information is protected by uniform rules no matter where it is sent.
- **To ensure laws are consistent with Pan-European laws.** Countries wish to ensure that trade will not be affected by the requirements of the European Union Directives.

A further reason why countries adopt privacy laws is to allow for the interception of information of possible terrorist origin. One of the major events of this century, the 11 September 2001 terrorist attack on the World Trade Centre in New York, has had a significant impact on privacy laws across the world. The growth of electronic commerce has increased the amount of data that is collected on individuals in the course of a transaction. Many new “anti-terrorist” laws enable the authorities to access such data without the individual being aware of it.

A Gartner study by de Lotto (2002) proposes four possible scenarios for information privacy. These scenarios, which look at the possible extremes of privacy legislation, are illustrated in figure 4.1 below.

The article concludes by making some recommendations for companies to ensure that they are prepared to answer questions on privacy issues from a hostile media. Companies should track privacy concerns in popular fiction and other entertainment media. A movie on hacking may elicit more enquiries about identity theft from the public than the passing of a major privacy law. Companies must also remain alert to proposed local (privacy) legislation to ensure that such legislation does not harm the industry.
Finally, risks may be reduced by being alert to the forerunners of change. (De Lotto, 2002, p.14).

![Figure 4.1 Gartner’s privacy scenarios](image)

It is important that organisations take cognisance of existing privacy laws in the countries where they are represented. Policies created within the organisation may not contradict national laws. Very often, the “right” of a company to monitor its employees conflicts with the basic human right to privacy. It is therefore necessary to look more closely at workplace monitoring.

### 4.3 Workplace privacy

The monitoring of workers is nothing new. There have always been supervisors looking over the worker’s shoulders to ensure that s/he performs adequately and produces goods of acceptable quality. This monitoring has always required physical intervention by an individual and the employee being monitored was at least aware of the monitoring taking place, even if consent was given grudgingly.

The nature of the workplace has changed, however, as did the nature of work. This has led to changes in the way that employees are being monitored. Technology has allowed
more covert and invasive monitoring practices to be implemented, which calls into question the employee’s most basic right to privacy and dignity within the workplace.

“Privacy advocates have long maintained that providing notice of a monitoring or surveillance policy should, as a bare minimum, be required before employers can engage in such invasive activities” (Andrews, 2002, p. 87). Such a monitoring policy should not be vague, but spell out exactly what the boundaries and nature of monitoring will be. For example; will email activity only be monitored electronically by mail filtering software; will monitoring be random or continuous; can keystroke-logging software be installed without the knowledge of the employee; etc.

The 1997 International Labour Office’s *Code of Practice on the Protection of Workers’ Personal Data* has as its general principles the following (Andrews, 2002, p.87):

- Personal data should be used lawfully and fairly; only for reasons directly relevant to the employment of the worker and only for the purposes for which they were originally collected;
- Employers should not collect sensitive personal data (e.g. concerning a worker’s sex life, political, religious or beliefs, trade union membership or criminal convictions) unless that information is directly relevant to an employment decision and in conformity with national legislation;
- Polygraphs, truth-verification equipment or any other similar testing procedure should not be used;
- Medical data should only be collected in conformity with national legislation and principles of medical confidentiality; genetic screening should be prohibited or limited to cases explicitly authorised by national legislation; and drug testing should only be undertaken in conformity with national law and practice or international standards;
- Employers should ensure the security of personal data against loss, unauthorised access, use, alteration or disclosure;
- Employees should be informed regularly of any data held about them and be given access to that data; and.
- *Workers should be informed in advance of any monitoring and any data collected by such monitoring should not be the only factors in evaluating performance.*
This code of practice is not law and is not of binding effect. It may be used as a guideline to the development of legislation, but unfortunately, laws on workplace privacy differ from country to country and few countries have laws relating to workplace surveillance.

It is not clear whether the last bullet point above implies that an employee should be warned before every instance of specific monitoring, or whether a once-off waiver of privacy signed by the employee (e.g. at the time of employment) is sufficient.

“Many believe that since employers have ownership or control over the working premises, its contents and facilities, that employees give up all rights and expectations of privacy and freedom from invasion” (Andrews, 2002, p.88). It is important for organisations to endorse the fact that the privacy of users will be protected. However, this must be “in balance” with the assertion that corporate email boxes and IT infrastructure are corporate assets (Surfcontrol, 2001c, p.5). Some companies make employees sign a consent form as a condition of employment that allows the company to monitor all the employees’ activities in the workplace. “Nearly 80 percent of employers engage in electronic monitoring of employees work-related communications and activities … Most monitoring is done on a spot-check, rather than on a continuous basis” (Towns, 2002)

Many companies have put policies in place where staff members have to respect consumer privacy. However, the same companies that expect their staff to respect the privacy of customers monitor the activities of their employees. Much of this monitoring is driven by genuine concerns about productivity and avoidance of prosecution, but long term destructive effects may result from the failure to respect employee privacy.

“Gartner research indicates that by 2005, most US FSPs [Financial Service Providers] will have experienced significant employee relations problems relating to privacy in the workplace (0.8 probability). These events will be quite heated, and may result in negative publicity, decreased staff retention or unscheduled job actions. National security will not prove to be an acceptable excuse for managements prying into employee’s personal affairs” (De Lotto, 2002, p.9).

In the USA, courts have been slow to recognise employee’s rights to privacy. Employers have broad ability to monitor employee’s communication for “business purposes.”
About 14 million employees in the United States are subject to this kind of surveillance on a continuous basis. In Austria, Germany, Norway and Sweden there are strong labour codes and privacy laws that directly or indirectly prohibit workplace surveillance. In the UK, a working paper preceding legislation requires monitoring of employees to be transparent, necessary and the only means by which employers can get the same results. In Australia, limited restrictions are placed on an employer allowing monitoring of email communications, provided there is a policy on this that had been made clear to all employees. (Andrews, 2002, pp. 88-92).

Although there is often the attitude that corporate rules supersede country laws, the reality is that it applies the other way round. Corporate policy is subject to the legislation of the country where the business or branch of that business resides – not the country where the head-office is situated.

It is clear from the examples that there is no consistent standard for workplace monitoring or for the interception of communications in various countries. This becomes problematic in multination corporations, as the corporate policies are usually generated at head-office level and regional offices are expected to implement these policies locally. Often there is no local expertise to determine whether the policies comply with the legislation in the local country.

In the context of this paper, it will be important to determine methods of email policy formulation that will respect the privacy laws of a country, that will retain the employee’s sense of dignity and right to privacy, but will still give an organisation the control necessary to ensure that resources are not abused.

4.4 Multinational issues

It is important to determine how policies for a multinational company should be worded and what provisions should be made for adaptation to the local country laws. A Gartner article by Meera Singh illustrates the complexity of this issue. Singh asserts that if corporations do not adequately formulate privacy policies, “governments worldwide [will] jump in to address the Internet privacy crisis” (Singh, 2002, p.2). Government intervention in privacy law formulation is not always desirable, as priorities for Government often differ from the priorities of the citizen or business.
Government may place a greater emphasis on intrusive monitoring policies, e.g. the USA Patriot Act mentioned later in this section. Citizens may place a greater emphasis on the guarantee of privacy as a right through civil liberties groups. Business may want to find a middle way where employees are monitored, but customers are guaranteed privacy of information.

In the following subsections a single question will be asked in order to highlight the varying approaches to legislation in different countries.

### 4.4.1 United States of America

In the United States users do not own their data. Companies are allowed to create consumer databases of Internet usage in order to do targeted advertising. Data collection is done through “cookies” or registration on certain websites. The question arises:

*Does a consumer have the legal right to privacy at work, at home, while shopping or while visiting Internet Web sites?*

“In the United States, the answer to all the above is no. An individual’s habits and behaviour may be examined by an employer, a supermarket and by companies performing operations on the Internet.” (Singh, 2002, p.2).

“The courts in the United States tend to favour the employer in workplace surveillance cases … the US Constitution contains no express right to privacy” (Bonsor, 2002). This view is supported by Ken Dayton, law professor at the University of Kansas who is quoted as saying that “private sector employers are free to monitor employees, whether or not they’ve told employees they are doing so… this is an issue of ethics, not really one of legality” (Van Slambrouck, 2000, p.1). He is contradicted by University of Illinois professor of law, Matthew Finkin, who states that “employers risk invading employee’s privacy if they monitor email systems without notifying employees of their right to inspect messages” (Barsook, 1998, p.10).
The events of September 11, 2001, as well as the Enron scandal, may have spurred lawmakers in the USA on to revise their stance of self-regulation, as “more than 255 bills dealing with information privacy alone are pending in Congress” (Kidd, 2003).

The following are typical laws that IT professionals in the USA now have to work with:

- **Gramm-Leach-Billey Act** – This limits financial institutions’ ability to disclose non-public personal customer information to third parties;
- **Health Insurance Portability and Accountability Act (HIPAA)** – This contains measures to protect the security and integrity of patients’ private information;
- **USA Patriot Act** – Extends law enforcement’s surveillance and investigative powers and makes business responsible for seeking, detecting, and reporting computer trespasses;
- **Sarbanes-Oxley Act** – Requires that companies are more fiscally accountable and prescribes data retention practices. This Act is applicable to all American owned companies, even if situated outside the USA.

From the above it is clear that some measures are taken to protect the privacy of data on some levels, but that individual privacy is compromised by others, e.g. the USA Patriot Act, in the guise of security. Unfortunately there is no all-embracing law on privacy and legislation remains fragmented among several bodies, e.g. the North American Electric Reliability Council, the Federal Energy Regulatory Commission, and the Supervisory Control and Data Acquisition body. (Kidd, 2003). There are also several law enforcement agencies; from military – CID, OSI, NCIS, DISA; US Federal law enforcement – FBI, US Secret Service, US Customs Service, US Postal Inspection Service, Bureau of Alcohol, Tobacco and Firearms; State and Local law enforcement; and finally, the Royal Canadian Mounted Police. (Pipkin, 2002).

It is clear that there is no comprehensive standard for the formulation or implementation of privacy laws. Different agencies may have different laws which
may be enforced federally. Each US State also has different laws, drafted in language that is often open to interpretation. One example follows:

The Texas Computer Crimes Act, defines that “a person commits an offence if the person knowingly accesses a computer system without the effective consent of the owner” and derives a benefit from the action. A computer system is defined by statute as “a data processing device that functions by manipulation of electronic or magnetic impulses” and access is defined as “make use of”. By definition, looking at someone’s digital watch without permission could be a felony. (Pipkin, 2002).

There is an effort in the United States to legislate around privacy issues, but often laws are passed for political expedience rather than for a real concern around privacy. The USA Patriot Act, in name alone, implies that if an individual opposes this law, it is a sign of not being patriotic. This act compromises many civil liberties. In contrast, HIPAA strictly enforces the protection of privacy of medical records.

In the examples in section 4.4.5, it will be indicated that compliance with privacy concerns is often implemented in individual companies in the USA in order to comply with EU standards.

4.4.2 European Union

Once again, the question is asked:

*Does a consumer have the legal right to privacy at work, at home, while shopping or while visiting Internet Web sites?*

“In Europe, the answer is yes. In most European countries, it is illegal to monitor an individual under any of these circumstances and use the information to target the customer. Enforcement of these policies becomes the issue, however.” (Singh, 2002, p.2).
In Europe, the right to privacy is defined as a human right under Article 8 of the 1950 Convention of European Human Rights. The protection of personal data of EU citizens is expressed in Directive 95/46/EC. (Kenny, 2003, p. 20). EU citizens may choose whether they want to make personal information available. A Privacy Commissioner ensures that policies are enforced and there is sufficient recourse to the law if an individual feels their privacy has been violated. “EU citizens have the specific right to judicial redress if they feel their information is misused” (De Lotto, 2002, p.16).

A Reuters report posted on 12 March 2003 stated that the government amended laws after it was slammed as a “snooper’s charter” by civil liberties groups. Home Office minister Bob Ainsworth said that “in a democratic society there is always a difficult balance to strike between respect for privacy and ensuring crime is tackled effectively … the new proposals defend the privacy of the citizen while ensuring crimes are investigated.” (IT-Web, 2003)

It is immediately apparent that EU laws are more coordinated, as the position of an EU Privacy Commissioner has been established. Governments also appear more sensitive to public opinion expressed through civil liberties groups.

4.4.3 South Africa

Again, the question is asked:

*Does a consumer have the legal right to privacy at work, at home, while shopping or while visiting Internet Web sites?*

In South Africa, the answer to all the above is yes. The Electronic Communications and Transactions (ECT) Act and the Regulation of Interception of Communications (RIC) Act ensure the privacy of the individual is protected by law.

In South Africa the laws regulating electronic media usage had been lagging behind the rest of the world. In 2002, however, the Electronic Communications
Email security policy implementation in multinational organisations with special reference to privacy laws

and Transactions (ECT) Act (Act 25 of 2002) was passed. ‘As well as making
digital signatures legal, the law enables contracts to be concluded online [and] 
email communications to be submitted as evidence in court … of note are the 
provisions for end users and consumers, which protect their rights and privacy”
(Wecke, 2003, p.16).

Both the ECT Act, as well as the King II report on corporate governance, im-
plies that companies must ensure that they protect themselves by keeping track 
of their transactions and communications. “While companies don’t have to pre-
serve documents, the failure to do so in most cases infers the worst – a cover up. 
Good practice in terms of a policy of storage and protection of email and other 
electronic documentation ensures that the integrity of a company is preserved”
(Castleman, 2003, p.44).

The legislation most relevant to the privacy of employers is The Regulation of 
Interception of Communications and Provision of Communication-related In-
formation Act 70 of 2002 (The RIC Act). Sections 2 and 6 of this Act regulate 
the extent to which individuals and corporations may legally intercept and 
monitor the communications of their employees. Unlawful interception may 
carry a fine of up to R2m or up to ten years’ imprisonment.

The basic principle is, therefore, that employers or any individual may not inter-
cept any communication and to do so, other than in terms of the exceptions 
stated in the Act, amounts to the commission of an offence. (Bortz, 2003, p.30).
According to the Act, an entity may lawfully intercept a communication in three 
instances. They are as follows:

Any person, including an employer,

- may intercept any communication if s/he is party to the communication;
- may intercept any communication if one of the parties to the communi-
cation has given their prior consent in writing to such interception;
- may intercept any indirect communication in the course of the carrying 
on of any business, provided that certain requirements are met (“the 
business exception”)
This business exception allows an employer to monitor communication without consent of the employees, provided interception occurs in the course of transmission. This means that once a message arrives at its destination (i.e. the employee’s mailbox) it may not be monitored without the express consent of the employee. The implication is that mail-filtering software may be used, as this is used during the transmission of messages, but that an administrator may not browse through employee mailboxes to search for incriminating messages.

Commentators agree: “the total impact of the [ECT] Act will only become clear as it is applied” (Wecke, 2003, p.17). In addition, concerning the RIC Act, there is “uncertainty as to how the courts will apply the business exception” (Bortz, 2003, p.38). Only during a test case will it become clear whether the use of private communications over company systems may be intercepted, in light of the clause “in the course of the carrying on of business” in the third bullet above. Reinhardt Buys from Buys Attorneys Inc. states that the clause seems to indicate that only business-related communications may be intercepted in the course of its transmission over a telecommunications system; and that by definition, a server operated by a private business is not part of this definition. Furthermore, email blockers may also present a problem, as they are only blocked once they enter the IT system of the recipient’s business and therefore appear to the sender as having been delivered. This may pose a legal problem if it was blocked and the content contained time-sensitive information (Guedes, 2003).

It is also not clear whether an employee should be informed that his or her mailbox would be browsed for compliance with policy prior to each monitoring activity, or whether a once off consent will apply to all subsequent monitoring.

One argument is that the ECT Act recognises email as legal documents, therefore “company email remains the property of the company” (Paslovsky, 2003), even if the policy allows personal use as long as it does not interfere with business. IT Law Attorney Lance Michaelson believes that “click-wrap agreements, which require a user to click on an ‘I accept’ button when logging onto a company network, will be acceptable” (de Wet, 2003) to gain monitoring consent from users. Buys advises employers not to only rely on interception agreements, but also to ensure that policies are correctly worded. “Simply using the
term ‘pornography’ or ‘racism’ in a policy without adequate definition could cause problems in the case of legal action” (de Wet, 2003).

“According to labour law, an employee can only be held responsible for an offence if there was a rule in place to begin with and if that rule was communicated to them and then broken” (Parak, 2003, p.1).

Although many aspects of the newly implemented ECT Act and RIC Act still have to be tested in a court of law, South Africa has embarked on a legal journey in line with international privacy standards. Privacy of consumer information, as well as access to private information pertaining to an individual is guaranteed by law.

South Africa may have lagged behind the EU in the formulation of laws relating to electronic privacy. Legislators may have learnt from what has been implemented in other countries to ensure local South African legislation is comprehensive and in line with best practices internationally. There is some criticism that the ECT Act is vague and open to interpretation. Many aspects of the law may have to be tested in a court.

What is clear, however, and pertinent to this paper, is that there is definite legislation regulating what is considered an invasion of privacy in the corporate world. Any policies regarding email security will have to take cognisance of the South African laws, which explicitly protect the privacy rights of an individual. Room has been left, however, for a fair implementation of monitoring of resources within an organisation.

4.4.4 Asia and Latin America

For a final time, the question is asked:

*Does a consumer have the legal right to privacy at work, at home, while shopping or while visiting Internet Web sites?*

“In Asia and Latin America, the attitude in most of the developing countries is one of ambivalence. While security issues are of key
concern, privacy is a non-issue for most consumers.” (Singh, 2002, p.3).

Many of the countries in Asia and Latin America have fledgling Internet communities as most citizens do not have access to the Internet. Often the judicial systems are inefficient and struggle to deal with basic issues of crime. Privacy rights issues fall low on their priority lists.

4.4.5 Cross-border transactions

It becomes clear that consumers in different parts of the world have different expectations of privacy. What is also clear is that policy makers in different countries have different approaches to the level of privacy consumers and individuals can expect. The following extract from Singh (2002, p3) addresses the complexities of cross-border commerce:

“Different cultures and policies adopted by governments have produced various ideologies as to what defines consumer privacy and thus present dissimilar policies with regard to what privacy rights its citizens may enjoy. As a result, a company (such as a multinational) must set up different marketing strategies for different parts of the world.

The Internet destroys boundaries, so most businesses will have to be aware of the privacy laws of other nations they deal with or even may deal with in the future. International businesses will have to begin to live with the concept of meeting the highest common denominator when it comes to privacy.”

De Lotto asserts that “the underlying divergence between national privacy models remains and will intensify over time, regardless of any exogenous events. Conflicts will also exist, regardless of the country, between the agendas of local and central policy makers. Homeland security issues, starting in the United States, will significantly affect the evolution of the privacy situation in ways that are impossible to predict” (2002, p.8).
The fact that there is currently no clear model for organisations to embrace in dealing with cross-border privacy issues is highlighted in a study done by Deloitte & Touche. “Organisations doing business in multiple jurisdictions are subject to regulatory and cultural variances on what data are protected, how the data must be protected, and what rights are afforded to the enterprise, the regulators and the individual” (Karol, 2001, p.4). Karol recommends that companies conduct a “Privacy Impact Assessment” in order to provide documented assurance that privacy issues have been identified and either adequately addressed or referred senior management for direction. As compliance with national and regional privacy regulations are complex and constantly evolving, it is suggested that each organisation has a designated authority (a “privacy officer”) to review the business process for privacy implications.

“The 1995 European Union Data Protection Directive (EUDPD) … essentially prohibits the export of any personal data from the EU to countries that do not meet the EU’s minimum standards for consumer privacy protection, regardless of cost or inconvenience to businesses” (De Lotto, 2002, p.16). In essence it boils down to “no privacy, no trade” (Davies, 1998). Two examples of the application of this principle are sited below.

**Example 1**

In November 1994, the US Citibank proposed a project in conjunction with the German National Railway to launch what would be the biggest credit card project in German history. When it emerged that personal data of German citizens would be processed in the US, a huge public outcry followed. The German privacy authority insisted that privacy standards at least equal to those under German law (stricter than the EU directive) had to be adhered to by Citibank.

**Example 2**

Sweden’s privacy watchdog instructed American Airlines to delete all health and medical details on Swedish passengers after each flight unless “explicit consent” was obtained. The airline appealed to Stockholm’s
District Administrative Court, claiming that obtaining consent was impractical and that passengers would be inconvenienced by having to supply the information every time they flew. The court concluded, “Inconvenience does not constitute an exemption from legal rules for the protection of data.” (Davies, 1998).

Davies (1998) concludes his article by stating that the “view from Brussels is that no current US self-regulating system would be acceptable to a European privacy commissioner.” EU data protection legislation is inherently extraterritorial, and it is a non-negotiable condition for societies wishing to do business with EU countries to comply with accepted privacy policies. (Kenny, 2003, p. 23).

This section highlighted the fact that there are many different approaches and attitudes to privacy legislation in different countries. This adds to the complexity in creating email security policies in multinational organisations, as it has to be considered whether a particular policy can be implemented in every country where an organisation has a presence. The next section will look at the specific issues surrounding email monitoring.

4.5 Privacy issues surrounding email

In the previous section, attention was given to the status of privacy legislation in different countries. Many of the laws are open to interpretation, as it is often not clearly spelled out what the rights of an employer are. This section will analyse the interpretation of the legislation and the attitude to email monitoring in the workplace.

4.5.1 Monitoring

A variety of reasons is given for monitoring employee email. “Some say it is to protect trade secrets or preventing sexual harassment incidents. Others want to prevent oversized mails clogging networks and using too much bandwidth. Others simply don’t want employees ‘wasting’ company time by using systems for personal activities” (Andrews, 2002, p.92).
Nearly two thirds of all companies discipline employees for abuse of email or Internet connections and 27% dismiss employees for those reasons. (Andrews, 2002, p.93).

“The more the employer monitors, or reserves the right to monitor email content, the more responsibility may be inferred by persons seeking to hold the employer liable for the employee’s statements” (Aftab, 2003).

In the UK, the interception of an employee’s email is illegal, unless it is done with “lawful authority” (Infant Technology, 2002).

In an article about workplace surveillance in the United States, Kevin Bonsor states that “employers are not required to notify you that you are being observed” (Bonsor, 2002). He continues to name five basic methods by which employee activities can be tracked:

- Packet sniffer
- Log files
- Desktop monitoring programmes
- Phones
- Closed-circuit cameras

In United States law, electronic communication in transit may not be intercepted, just as telephone conversations are protected by law. However, when email is stored on a server, it is not in transit and may therefore be accessed. If the analogy is extended to conventional mail (which is protected by the law), post would be protected while it is being transported to your letterbox, but as soon as it has been placed in your letterbox, anyone would be free to open your mail. (Bonsor, 2002).

4.5.2 Arguments against workplace monitoring

Although companies have a right to ensure their employees are productive and not engaging in illegal activity on the Internet or through emails, “an unintended consequence of spying on employees as they work is that the vast majority of productive workers could become demoralised” (Seglin, 2000). Monitoring
email traffic or web usage leads to the dehumanisation of the work environment. “Companies that assume the worst of people and monitor their every move will never have a culture characterised by integrity, empowerment, quality and spontaneous fun. At best, [they] will have a culture of compliance” (Seglin, 2000). Companies should ensure that the correct people are attracted to the business, rather than try to force compliance using technology.

Most employers recognise that using the Internet for errands or short personal breaks and sending an odd personal email in the course of the day “has become part of the fabric of normal human behaviour” (Oldman & Underwood, 2000). Often managers prefer that workers send emails rather than make phone calls, as it is less distracting for other workers. Just as some employees take half-hour long smoke breaks on a regular basis, so too some employees will abuse technology. Oldman concludes that, rather than invading the privacy of employees through monitoring emails and Internet usage, employers should rather concentrate on the productivity of workers and deal with under performers accordingly.

Lori Fena does not totally oppose monitoring at work, but insists that such monitoring is done subject to clear policies and reflects monitoring based on real needs, not just for policing. (Bennett & Fena, 1997). In a policy, it should be spelled out exactly what is not allowed in email and what types of sites may not be visited on the Internet. She argues that constant monitoring is most likely overkill – the output of employees should be measured and based on that monitoring can take place if necessary. Employees will regulate themselves when presented with statistics of top sites visited and the periods spent on the Internet.

Christine O’Brien, professor of Law at Boston College, questions whether a “business-use-only email policy does in fact avoid legal problems and whether such a policy is practical in the light of pervasive use of email as general communication. (O’Brien, 2002). She contextualises this argument within the framework of unionised employees, who are protected by specific laws (e.g. in the USA by the National Labour Relations Act). Her argument is based on the fact that, where an employee’s primary task is limited to a computer, email becomes the equivalent of conversation or oral solicitation (p. 71). Labour laws allow oral solicitation on union matters; therefore, company email policies can—
not forbid the use of email for union matters – especially if they do not strictly enforce the policy relating to the use of email for other non-business related matters. “The bottom line appears to be that where employee use of workplace email is significant enough to constitute a “work area,” employers may not totally restrict employee email that is equivalent to oral solicitation … a total ban on non-business use of the email system is not the answer to potential labour law violations in all cases” (O,Brien, 2002, p.75). Email monitoring may be problematic when it includes the surveillance of union activities.

4.5.3 Arguments in favour of workplace monitoring

The main arguments for workplace monitoring include the abuse of bandwidth, problems with productivity and concerns about legal issues. Companies justify their monitoring of employees based on statistics of other companies that have fired or disciplined staff for abuse of company resources. Underwood recognises the need for usage policies, and monitoring is justified as an enforcer of those policies. (Oldman & Underwood, 2000).

From an employer perspective, Wayne Bennett argues that there is nothing new to monitoring principles, and these principles should simply be expanded to include new media like email and Internet usage. (Bennett & Fena, 1997) His main reason for opposing what he calls “employee empowerment,” is employer liability in cases where the company is accused of harbouring a hostile work environment through unacceptable communications between employees via email. He concludes by stating that employees should not be consulted on the creation of employee policies. However, the company should inform all employees on the reasons for those policies, which should lead to greater acceptance.

Employee monitoring may be new for most people, so management should make sure an employee monitoring policy is formulated and communicated to all employees. “Employees are not hired to tend to personal Internet and email matters … anyone who holds privacy dear to their heart should consider separating business from pleasure” (Beaver, 2002).
As long as the monitoring policy is documented and employees made aware of the policy, an organisation can implement the technology to monitor and enforce the policy. A manager that leads by example will help maintain the morale of employees and thus help to influence the culture of the organisation.

Proponents of workplace (and email) monitoring have valid arguments regarding the protection of a company’s resources and insuring worker productivity. Opponents to workplace monitoring argue that happy workers who feel that they are trusted will be more productive and will voluntarily ensure that abuse does not occur. The approach of an organisation will usually be determined by the corporate culture in that organisation. Where employees are not valued as individuals, a Big Brother-type punitive approach may be implemented. The modern trend in management recognises individuals and a more cooperative approach to compliance may be encouraged, rather than resorting to punitive monitoring.

4.6 Conclusion

This chapter highlighted the differing approaches to privacy legislation in the USA, the EU, South Africa, Asia and Latin America. It was shown that in order for cross-border transactions to take place, many companies have to comply with legislative expectations from countries other than their own.

One area that evokes much controversy is the privacy laws of each country. These privacy laws should influence the way in which a company formulates its email security policies, as the monitoring of communications is often regulated by country legislation.

In South Africa, the effect of the new legislation in the employment context is that an employer can no longer monitor emails and Internet usage at will, or discipline employees without first ensuring that the monitoring complies with the provisions of the Interception (RIC) Act. (Maserumule, 2003, p.39).

In Chapter 5, the issues pertinent to email security policy creation and implementation will be integrated. The security aspects and threats introduced into a company by email, as discussed in Chapter 2, will be considered. In context of the policy frame-
works discussed in Chapter 3, a framework will be suggested for an email policy. The framework will be measured against the privacy issues raised in Chapter 4 to ensure that such an email policy can be implemented in a multinational organisation.
Chapter 5: Drafting an email security policy

5.1 Introduction

In Chapter 2 it was indicated that the Electronic Communications and Transaction (ECT) Act 25 of 2002, passed in South Africa in July 2002, gives email messages the same legal status as traditionally printed or written documents (ECT Act, section 11(1)). Irresponsible use of email by employees could expose a company to harassment suits. The indiscriminate use of company email for personal purposes (e.g. chain letters, hoaxes and attachment forwarding) can also have an impact upon infrastructure resources and severely degrade employee productivity.

This chapter will integrate the material from the preceding chapters. The position of an email policy in a security policy framework, as examined in Chapter 3, will be highlighted first. It has been established that email usage is pervasive in organisations and that this usage introduces various threats into the organisation. Threats identified in Chapter 2 will be addressed next by suggesting appropriate inclusion in an email security policy. Attention will then be given to legal issues that may influence the drafting of a policy and multinational issues will be addressed. Finally, the creation of a draft policy will be proposed.

5.2 Framework definition

The purpose of this paper is not to define an information security framework. It is important, however, to emphasise that for a concerted information security plan to succeed, a well-defined framework is necessary.

In Chapter 3, it was shown that there is reasonable consensus on what an information security framework should consist of. Most frameworks are hierarchical in nature and start with a Charter or Executive Statement on security policy. This aspect of a policy framework is very important, as this indicates commitment to security policy implementation from the top of the organisational hierarchy. It is usually signed by the CEO, but it can be proposed that every functional manager also signs a copy as an indication
of his or her commitment to information security in his or her department. This Information Security Plan Charter should also address how policies will be enforced and what the consequences for deliberate or accidental non-compliance will be.

Such a security Charter should be readily available to all employees to ensure they are familiar with the organisation’s stance towards information security. More will be said about implementation of policies in Chapter 6.

Revisiting the “Moses Model” (von Solms, 2002) and the hierarchical model of Palmer (2002) that was discussed in Chapter 3, different levels of policy are apparent. We have a security policy, followed in the hierarchy by standards and finally by procedures. Palmer refers to guidelines as that which precedes the formulation of a comprehensive standard or procedure (see Figure 3.1 in Chapter 3.)

For the purposes of this paper, it will be accepted that a Security Policy Charter exists and that a framework has been decided upon within which Email Policy is covered. In Palmer’s schema illustrated in Figure 3.2, an Email Policy, for example, will most likely fall under an acceptable use policy, which may also include Internet usage (Palmer, 2002, p.24).

The following sections will address the components of email policy that should form part of such an acceptable use policy.

5.3 Addressing threats and legal issues in email policy

Email is a tool that should add value to a business. Experience has shown that this tool is often abused. Chapter 2 covered many of these threats and abuses. Email has also been used to exploit weaknesses within a company, both internally and externally.

This section will address the threats posed by email usage in an organisation and place it in the context of a security policy. It will also identify criteria to which a multinational policy must conform, as discussed in Chapter 4. Finally, aspects of policy that are complicated by legislation will be highlighted and addressed.
5.3.1 Productivity

One of the criticisms of email in corporate environments is the potential productivity loss that could be experienced through personal email, spam and the volume of email that is sent in a typical day. Controlling how employees manage their email probably falls outside the scope of a policy, but may be included in a guidelines document.

One aspect that should be addressed by policy is the forwarding of chain letters. This activity places great pressure on the infrastructure resources and leads to tremendous productivity loss. The forwarding of large non-work related attachments must also be severely discouraged.

5.3.2 Threats

Several threats were identified in Chapter 2. One of the threats most difficult to regulate is a breach of confidentiality. Confidential information may be sent by email deliberately or inadvertently. An email policy should include a statement on what documents may or may not be sent by email according to its security classification.

With the prevalence of viruses, it is very important to educate users on how to guard against infiltration by such malicious software. An email policy should state that virus protection should be employed on server level, but it should also address the responsibility of the user to ensure virus definitions on the client machine is up to date. Despite these precautions, stealth viruses can still slip through the system. It should be a matter of policy that suspicious email containing attachments and with senders unknown to the recipient, should be treated with circumspection.

5.3.3 Offensive material

A characteristic of much non work-related email that is sent between employees is that it contains material of a sexual nature – often under the guise of humour. What may be humorous to some may be offensive to others. It has been shown in Chapter 2 that a company can be held legally responsible for email sent under
its domain (i.e. what follows the @-symbol). A company therefore has a right
to determine what messages are considered acceptable and what are not.

Realistically, a company should acknowledge that a certain amount of private
email would be generated on its systems, just as some personal phone calls will
be made on company telephones. An organisation has to consider that email is
a de facto modern tool of communication. Rather allow an employee the five
minutes to generate a personal email to the bank than to lose an hour of produc-
tivity by the employee taking time off to visit the bank.

It may not be advisable to state explicitly that private use is allowed. This could
lead to abuse that may be justified by an employee through a distorted interpre-
tation of the policy. Limited personal email usage should be considered as fair.
What should be stated explicitly, however, is what is NOT allowed on company
email systems.

A vague or generalised statement that offensive material is forbidden is not suf-
ficient. An organisation should identify issues that may lead to litigation in con-
text of local laws and name these issues explicitly. An obvious category of for-
bidden material should be anything of a sexual, political or religious nature.
Any mail which could be considered harassment or libellous in nature should
also be forbidden.

Most companies have codes of conduct that regulate employee behaviour. In
drafting an email policy, it should be ensured that statements in the policy sup-
port the company code of conduct.

Throughout this paper, it was emphasised that email is considered a legal docu-
ment in most countries and could be used as evidence in court. Employees
should be educated to ask the question, “Can I (or the company) be sued if I
send this email?”

The legal status of email implies that care should be taken on what is retained
and for what period information communicated in email is retained. The next
subsection will address this.
5.3.4 Retention & mail quotas

The pure volume of email communications makes retention of all messages impractical and expensive. However, an email policy should define what should be retained and suggest the method of retention. In an email policy, it may be sufficient to state that retention will take place. The mechanics of this retention can be handled in procedure documents, as it may not be ideal to leave the responsibility for retention to the employee or user.

The policy should make it clear that users are allocated a certain quota for email and that it is the responsibility of the user of the email system to manage his or her email. By allowing unlimited size email boxes, strain will be placed on storage media.

A company should determine whether it would allow mail archiving by the user. Archiving may contradict corporate document retention policies. If, for example, email records are requested during the discovery phase of litigation, the company’s data retention policy may state that only 18 months’ worth of email is retained. This would simplify the collection of these records. However, if archiving is allowed, users may be contravening the policy and the litigant may insist on further document discovery.

It may be good practise to align email data retention policies with physical (paper) document retention policies. Just as there are departmental filing cabinets for company critical documents, so should there be a repository for email documents to be saved in a centralised database. As mentioned before, the mechanics of retention need not be stated in the policy, but the practise of retention should at least be referred to in the policy.

5.3.5 Disclaimers

An email policy should state that disclaimers will be appended to all email messages, but the mechanics of this need not be addressed in the policy. It may be helpful to publish the wording of the disclaimer in the policy, if only to raise awareness among the users.
In a multinational company, it should be investigated whether a standard disclaimer will stand up to the legislation of each country where the organisation is represented. To overcome language differences, it may be useful for the disclaimer to reside on the corporate website, where the recipients can choose the wording in the language of their choice.

It is advisable to ensure that disclaimers may be appended by the email system and that it is not reliant on an action from the user. The issues around disclaimers have been dealt with exhaustively in Chapter 2, subsection 2.5.4.

5.3.6 Encryption

An email policy may require documents with a certain security classification to be sent using encryption. When drafting an email security policy, a company should determine whether encryption keys should be made available to the manager of the sender. If this is not done, it may not be possible for the company to view encrypted messages in case of litigation or during a disciplinary investigation.

5.3.7 Privacy and monitoring

This paper has placed a great emphasis on privacy issues that may constrain the monitoring of employee activity on email systems. It is generally accepted that some level of monitoring of company resources will take place. In an email policy, the company’s approach to monitoring should be clearly defined. It is not sufficient to simply state that the company reserves the right to monitor all activities on company resources.

The method of monitoring, as well as the procedures around monitoring, should be clearly expressed in the policy. The policy should state what would be monitored, so there can be no confusion in the mind of the employee. Although an employee may not necessarily expect workplace privacy, he or she should always be assured of confidentiality.

When considering multinational issues, email monitoring may prove to be one of the most contentious items in an email policy. It is advisable to restrict moni-
toring rights within clearly defined boundaries, where monitoring can only be authorised by a member of the executive, preferably the Human Resources director.

In light of the issues around privacy that were identified in Chapter 4, the recommendation of this paper is that the following procedure is followed in email monitoring:

Should a manager suspect an employee of misuse of email systems, a request to monitor the employee’s email should be lodged with the HR Director, together with a thorough motivation why this is requested. Should the HR director agree to the monitoring activity, the employee should be informed that access rights to email will be temporarily removed. At the same time, the email administrator should block access to this employee’s mail file. Access should then be given to the appropriate level of authority, possibly the departmental manager, to investigate and corroborate the suspicions. At the end of such an investigation, the employee may be given access to the mail file again.

Inevitably, this procedure can only be executed if the employee has agreed in writing at some point that he or she acknowledges the company’s right to monitor the use of its systems. It may be unwise to access a mail file without the employee’s knowledge, as this may constitute an invasive act. (For the same reason, for example, the use of keystroke logging software may be illegal or against fair labour practice.)

The monitoring described above is quite invasive and would most likely be exercised in extreme cases only. However, monitoring of a more general nature may take place as a matter of procedure. General monitoring may include the use of mail filtering software to check for viruses, pornographic material, breaches of privacy and abuse of company infrastructure resources by, for example, emailing large file attachments. This routine monitoring will most likely be automated and work based on filters employed during transmission of the email. As the interception of messages during transmission is forbidden by the
Regulation of Interception of Communications Act 70 of 2002 in South Africa, the company should ensure that email-filtering software is allowed under the provisions of this act.

The email policy should define what will be monitored and what the consequences will be if the policy is ignored. The company has to be able to prove that policy is consistently enforced, as disciplinary action “to make an example of someone” could be challenged in a labour court.

5.3.8 Other issues

In a multinational organisation where employees may travel between countries for brief or extended periods, it is desirable to have a consistent email policy. Where there are any significant differences in specific laws in different countries, these should be highlighted in the policy. (An example of this is the level of encryption allowed in different countries. Until a few years ago, a special international version of Lotus Notes had to be used by travellers to France, as French law did not allow for encryption levels higher than 128 bit.)

This section highlighted issues that should be addressed in an email policy. Ideally, the issues mentioned above should form the background to the formulation of the email security policy. In the next section, a format for an email policy will be proposed.

5.4 Structuring an email security policy

This section will define a typical structure for an email security policy. As a policy document needs to be quite thorough, but not too long, the structure is very important. As soon as a policy becomes cumbersome or overly long, resistance to read the policy will be shown by employees. The sub-sections below will address specific components that should be contained in an email policy.

South African attorney Reinhardt Buys identifies basic aspects that should be covered by an email policy. “Companies [should] obtain written consent from all employees that their email may be intercepted, establish a communications policy to govern the interception of email and Internet access, post a legal notice on all outgoing mails to
cover the possible blocking of incoming mails, and agree with third parties on at what point an email will be regarded as received” (Guedes, 2003).

A multinational organisation should decide whether all policies should be published at corporate head office level only, or whether each country should adapt it for local laws and conditions. The recommendation in this paper will be that the wording of the policy should be generally applicable, but that room is left for references to local legislation – especially in the section on monitoring and privacy.

5.4.1 Language

The email policy should not be obfuscated by complex language or technical jargon. The entire policy should be in clear non-technical language that is easy to understand. Sections should be concise and clear, which should make examples and explanations unnecessary.

5.4.2 Objectives

In a single sentence or paragraph, the objective of the policy should be summarised. By reading this sentence, anyone should understand what the policy relates to.

5.4.3 Scope

At the outset of the policy, it should be made very clear to whom the policy is addressed. It must show whether the policy is applicable to company associates only, or whether contractors and consultants are also subject to this policy. The jurisdiction of the policy should be clarified and indicate whether it applies to users of email in specific locations only, or whether all employees are subject to it.

In a multinational environment, the scope of the policy may prove to be very important. Laws as discussed in Chapter 4 may be relevant in determining the scope of the policy.
5.4.4 Definitions

It is inevitable that there will be some reference to more technical aspects within the policy. A section that defines the meaning of certain technical terms may be contained. Any terms which may be ambiguous or which carry legal weight, should also be defined.

It may not be necessary to refer to specific email products, but it has to be defined whether the term email refers to the conventional messaging format only, or whether instant messaging and SMS messages will also be covered by the policy. Some organisations still use legacy systems that had built-in communication systems. It must be clear whether such systems form part of the policy. It should also make it clear whether the company allows the use of web-based email products like Hotmail for communication by employees.

One should guard against making the definitions section too exhaustive. The intention is simply to avoid ambiguity and to define technical terminology.

5.4.5 Monitoring

A brief statement on the organisation’s approach to privacy should be included in this section. Many companies make employees sign a declaration where they acknowledge the rights of a company to monitor its systems. This declaration should be referred to in the policy.

The status of documents generated on company-owned systems should be documented. It must be clear that the organisation sees email as company property with legal status, and that it is subject to the same controls as paper documents.

Although a company may monitor email, it must be made clear that such monitoring is subject to specific documented procedures. As an example, routine monitoring done by filtering software may flag certain email as suspicious or too large and warrant action from a manager. However, reading the full text of an email should be subject to stricter controls, as this constitutes a greater level of invasion of privacy.
As monitoring and privacy are two very sensitive issues, great care must be taken in this section to balance the employee’s right to privacy with the right of the employer to protect its assets. The content of this section may be challenged during a civil court case or in a labour hearing. It may therefore be advisable to have the wording checked by the legal department of the company – both at corporate level, as well as on local level – before the policy is published.

O’Brien (2002, p. 76), summarises the ideal approach to drafting a policy statement regarding the use and monitoring of email:

“Perhaps an employer is wisest to promulgate a policy that notes the email system is primarily for business use but limited personal use of a lawful nature will be permitted where such does not overburden the system. What is unlawful should be specifically outlined in language for the layperson. Employees should be warned that the system is not private, that it will be monitored for reasonable business purposes, and that material on the system, even where the employee believes it is deleted, may generally be retrieved in the event of its evidence in a lawsuit. Employers should feel free to implement email policies that won’t inhibit employees’ legal rights and yet balance the employers’ legitimate interests”

Modern management tends towards consensus rather than dictate. If employees are convinced of the need for and the sensibility and fairness of monitoring, they would agree to it.

5.4.6 Usage guidelines

Companies may wish to separate guidelines for usage from the email policy. This separation may diminish the weight of the usage guidelines, as this may be interpreted as a lesser requirement than if it were policy. This paper would recommend that guidelines for usage be included in the email policy, and possibly repeated in a general document that clarifies the guidelines for computer usage.
Under email usage, a sentence indicating the company’s stance on private use of email should be included. However, the boundaries of such personal use should be defined.

Infrastructure management issues like the size of emails and the maintenance of mailboxes may also be addressed in this section, as well as any mail retention policies the company may have. It should be remembered that such policies should be consistently enforced in order to stand up to legal scrutiny during litigation.

It is advisable to have a separate section that expressly states what material may not be transmitted using email. It must be guarded against including generalised statements that are open to interpretation.

Essentially, a section on what is allowed should be included, as well as a section on what is not allowed. Productivity issues may also be addressed in this section.

### 5.4.7 Passwords & encryption keys

The company should state its policy on how email may be accessed during an employee’s absence. Generally, the rule should be that an employee should give explicit written permission to a specific employee to access his or her mailbox. The period during which this access is allowed, should also be stated.

This may be required while an employee is on leave or on sick leave. The company may decide whether telephonic permission is also acceptable. In cases where an employee is not in a position to give permission, the procedure stated in subsection 5.3.7 should be followed.

Some mail systems, like Lotus Notes, allow a user to delegate access to an email file to another user. This delegation, which can only be executed by the authorised user, should be the preferred method of access during an employee’s absence. If such restrictions are not stated in the policy and enforced, employees may steal the identity of another employee and thus introduce a threat into the company.
5.4.8 Communications

It is important for the identity of the sender of a message to be visible at all times. The creation of email accounts that are not clearly assigned to any individual should be against policy. Anonymous emails should not be allowed to be sent within or from a company’s email system.

If a company has an account for administrative functions, e.g. “postmaster” or “info” or “sales”, these accounts should also be associated with a specific individual or group of individuals. Shared email addresses should be avoided, as this leads to lack of traceability and accountability.

In the section that deals with communications, the use of disclaimers may be stated, together with the standard wording of such a disclaimer. Although the legal weight of disclaimers has been questioned in Chapter 2, subsection 2.5.4, it is general practice to include disclaimers on company email messages.

5.4.9 Software

Brief statements may be made in this section on the sending and receipt of software in executable format. Such files are often prone to viruses; therefore, special care should be taken by the employee. If the content or origin of an attachment is unknown or questionable, the policy should state what action the employee should take.

5.4.10 Copyright

A company should not only protect itself from breaches in confidentiality, but also guard against the contravention of copyright laws by employees. Legal action may be taken against the company for copyrighted material distributed illegally by an employee. The email policy should address this eventuality.

As with many of the statements in an email policy, a company should limit its liability in case of legal action. Where the company is liable, but not responsible, appropriate action should be taken against the responsible employee.
5.4.11 Violations

This section should deal with the actions that the company would take if an employee violated any of the conditions stipulated in the email policy. These actions should align with the company disciplinary procedures and should normally not fall under the jurisdiction of the Information Services department.

Some companies may allow for penalties for minor infractions of policy, e.g. temporary suspension of internet or email privileges. Instruction for such penalties should not be arbitrarily enforced by the Information services department, but should come from the Human Resources department.

The usefulness of “petty” punishment is questionable. It may be advisable rather to issue verbal or written warnings that are recorded on the employee’s record, in order not to trivialise the policy.

It may not be possible, nor advisable, to state what violations may lead to dismissal and what violations to internal discipline only. Each case should be treated as unique and an internal investigation and hearing will determine the action taken by the company against the employee.

This section of the policy should also state that any illegal actions in the use of email may be reported to the appropriate authorities. Such illegal activities may include, for example, the distribution of child pornography.

Section 5.4 identified the topics that should form part of an email security policy and proposed a structure for such a policy. It should be guarded against a too long policy document. Sections should be clearly identified and the policy should be easy to navigate, as employees need to be very familiar with an email policy, especially if they use this medium of communication on a daily basis.

5.5 Conclusion

This chapter suggested what the content of an email security policy should be, based on the threats and abuses of email identified in Chapter 2 and the privacy and legal issues
identified in Chapter 4. The email policy was contextualised with an Information Security Policy Framework as described in Chapter 3.

Many companies have an Employee Handbook or a central repository for Human Resources policies. It may not be desirable to have the entire Information Security Policy contained under the banner of Human Resources policies. At the very least, an extraction from the email policy in the form of an Acceptable Use of Company Resources policy should be in such a repository.

Appendix 1 contains a draft email policy based on the principles identified in Chapter 5. It attempts to address the threats and abuses introduced by email usage identified in the preceding chapters. This policy will serve as a working document for a local multinational manufacturing company. However, it is drafted to be applicable in all countries where this company is represented.

As stated before throughout this paper, the drafting and existence of a policy is not sufficient in itself. A policy has to be enforced in order to be effective. In Chapter 6, various methods of implementation and enforcement of an email policy will be identified.
Chapter 6: Implementing an email security policy

6.1 Introduction

In Chapter 5 the drafting of an email security policy was discussed. To ensure email adds business value and to protect the corporation against litigation, policies have to be implemented and enforced. In this chapter, the methods of implementation and enforcement discussed in Chapter 3, section 3.6, will be revisited. Implementation methods will be examined and compared before methods of policy enforcement will be discussed.

6.2 Implementation

The implementation of a policy is the step that takes place after the policy has been drafted. A policy is most effective if a culture change within an organisation has taken place and employees willingly comply with a policy.

A Surfcontrol White Paper (2001a) identifies several steps in implementing a culture change towards the acceptance of email security policies.

Figure 6.1 Email policy implementation cycle
These steps can be compared to the security policy lifecycle identified by Lowery (2002).

![Security Policy Lifecycle Diagram](image)

**Figure 6.2 Security Policy Lifecycle**

From the above two cycles, the following methodology can be suggested to ensure effective implementation of an email security policy.

### 6.2.1 Drafting, adoption and commitment

A policy should be drafted by a representative committee that includes a member who has access to senior management. The principles identified in Chapter 5 should be adhered to when drafting the policy.

This draft policy should then be agreed to and adopted by the administration that is responsible for other company policies, usually the Human Resources department and senior management. In a multinational organisation, input should be elicited from representatives from each country to ensure compliance with local laws.

Once the policy has been adopted, senior management should express a commitment to the implementation of the policy.
6.2.2 Implementation, education and deployment

Part of the commitment from senior management should be an implementation plan. The first step in such a plan should be the identification of a repository for the email policy. This may be in an employee handbook, a physical policy file held by each manager or a database on the intranet.

Publishing a policy is not sufficient to ensure compliance. It may be advisable to give each employee a copy of the email policy at a session where the policy and its implications can be explained. It is the responsibility of management to ensure that the policy is understood. Considering the threats that can be introduced by email and what it could cost the company, such an awareness programme will be a small price to pay.

Often too much is assumed with Information Security policies. Non-technical employees often have a mental block against such policies and may feel pressurised into signing that they understand the policy in order not to appear stupid or ignorant.

Familiarity with the content of the email policy and understanding why certain rules are made, will contribute greatly to employee compliance to an email policy. The key to successful policy implementation is education. If a company can prove that sufficient user education on email security policy has been done, it will protect itself against claims of ignorance when it wishes to discipline employees who violate the policy.

6.2.3 Monitoring

Various ways of monitoring email usage have been identified in the preceding chapters. Ideally, most monitoring should be automated and alerts should be raised with appropriate staff when an email message does not comply with policy.

One is reminded that “it is not a trivial exercise to implement privacy, nor is it a human right to be taken lightly” (Kenny, 2003, p. 23). However, what is not measured or monitored cannot be managed. Items identified in the policy, e.g.
the size of email attachments, should be monitored and filtering software can alert administrators of violations of content policies. Such monitoring may be considered non-intrusive and have a lesser impact on an employee’s privacy, but it should be remembered that some countries do not even allow such trivial monitoring.

More invasive monitoring practices, like full access to an individual’s mailbox, should only take place in exceptional circumstances and with the appropriate authorisation as described in sub-section 5.3.7, and then only if such monitoring is legal in the particular country.

### 6.2.4 Enforcement

Various methods of policy enforcement have been discussed in sub-section 3.6.2. Bureaucratic methods of forced compliance favoured in old-style management have fallen out of favour. Modern business prefers to manage by consensus, but management should guard against a lackadaisical attitude towards enforcing policies.

Placing an incentive on compliance with policy may be effective, but some may argue that an employee should not be rewarded for something that forms part of his or her responsibility towards the company.

The most effective way to enforce policy may be through a cultural change, where it is part of the corporate culture to comply with policy. In an environment where email abuse most often happens between employees, such abuse can be eradicated by peer disapproval. If an employee realises that a colleague does not appreciate, for example chain letters or jokes with a sexual flavour, they would stop sending such material.

Section 6.3 will investigate email policy enforcement in detail.

### 6.2.5 Review and refocus

Part of the Information Security Policy Plan should be regular reviews of all policies. As technology advances, an email security policy may need to be re-
visited to ensure it still addresses the available technologies. An example of this is the prevalence of instant messaging which may be addressed under an email policy.

Even if a policy does not change, employees should be periodically reminded of the content of an email policy. A poster campaign may be used to remind employees of key policy issues. If management becomes aware of violations in specific areas, e.g. chain letters, email reminders of the policy may be sent to all users of the system.

It may be good practice to have a brief talk about information security policies, including email policy, at the start of every formal employee training session or departmental communication session. This will bring the email security policy implementation plan illustrated in Figure 6.1 to its full circle, back to where commitment is required from management to implement and enforce policy.

### 6.3 Enforcement

It is generally accepted that the relationship between IT professionals and computer users is often difficult. Once it becomes known that someone in the IT department has reported a violation of policy or that someone’s email had been read, irreparable damage could be done to this already strained relationship. During the policy implementation and education phase, it should be made clear how and by whom the policy would be enforced.

Many aspects of email policy can be implemented technologically. Password control, email filtering for unacceptable content and blocking of certain attachment types can all be done with software embedded in the email system or through firewall filters. Ideally, warning messages should be automatically generated and sent directly to employees to inform them that they are in breach of policy. Such breaches in policy should be kept in a log and a manager should regularly check these logs and take action against violators.

An example of a technologically enabled enforcer is email filtering. Although the specific filtering software need not be identified in a policy, it may be advisable to
indicate whether any filtering software will be used. Users of the system will then not be surprised to find that usage trends on the email system can be monitored.

When email filtering is enabled, the following possible actions can be performed on a mail message (Surfcontrol, 2001a)

- **Allow**: Email that appears legitimate will be allowed
- **Isolate**: Certain files (e.g. Wav, Avi, and Mpg) that are seldom business related can be isolated.
- **Block**: Executable files (files with extensions like exe or bat) should be blocked to determine whether they are of business use. The content of zip files should be examined to see if it falls in one of the above categories.
- **Delay**: Files greater than, for example three megabytes, but less than the allowed maximum size, should be delayed for transmission when traffic volumes are low.
- **Discard**: Email with suspect content according to certain keywords should be discarded. Files that exceed the permitted size according to policy should also be discarded, but an appropriate message should be sent to the sender.

Whether a manager is made aware of the transgression of policy stipulations through an automated process or through someone in the IT department, the responsibility for appropriate action should not lie with the IT department. Either the HR department or the manager in the employee’s chain of command should enforce discipline – the IT management should only be responsible for supplying the evidence in support of the case.

The outcome of a contravention of policy should be defined in the policy. A company may choose to issue a verbal warning for a first offence, where an employee is given the opportunity to clear his or her mailbox. A second offence may lead to a written warning and appear on the employee’s record, possibly influencing the performance evaluation of that employee. The forwarding of a chain letter may not justify dismissal, but a deliberate breach of confidentiality may lead to dismissal.
What is important is that enforcement of policy should be consistent. If a policy is not enforced completely, it becomes unenforceable. This means that a witch-hunt to “make an example” of someone is a counter-productive approach to enforcement, as it implies an inconsistency and may be challenged in a labour hearing.

6.4 Conclusion

This chapter examined methods that may be used to implement an email security policy. One may conclude that policy implementation should be a systematic and planned exercise to ensure that all employees are exposed to the content of the policy. It may be advisable to get employees to sign a declaration of understanding, but this should only be done once employees have been given the opportunity to ask questions about the policy.

A recurring line throughout this paper was that an email security policy is ineffective unless it is enforced. This chapter concluded with various methods of enforcement. An emphasis was placed on consistency in enforcement of an email policy.

Before an email security policy can be drafted, it is necessary to have a thorough understanding of the issues surrounding email. A knowledge of security policy frameworks is also a prerequisite for drafting an email policy. In multinational organisations, knowledge of the governing laws is required – particularly privacy laws – especially if monitoring will take place. These issues were addressed in Chapters 2, 3 and 4. Chapter 5 focussed on the application of this information in drafting an email security policy. Finally, in Chapter 6, proposals were made on how to implement an email security policy.
Chapter 7: Conclusion

7.1 Introduction

In modern business, technology cannot be implemented for its own sake, but has to support the business strategy. In the same way, email systems must add business value. There is no doubt as to the advantages of email in a modern, always-on business environment. The immediacy of email communications enhances productivity and eliminates many of the delays and costs associated with older forms of communication.

The issues surrounding email usage and the need for an email security policy were addressed in this paper. The complexity of email security policy creation in context of multinational privacy laws was emphasised. Finally, implementation issues were addressed.

This chapter will summarise the content of this paper. It will revisit the problem statement and research objectives stated in Chapter 1 and discuss how these research objectives have been met. The chapter will conclude with some proposals for further research in the field of email and email security policies.

7.2 Summary

Email usage and security policy creation and implementation are very broad topics. When a legal issue, like privacy, is taken into consideration, the topic becomes even broader. This paper showed that these seemingly disparate fields of study are closely intertwined and cannot be separated, especially in context of multinational organisations.

Chapter 2 examined the history of email usage and examined how email is utilised in general and in the business environment. This chapter also highlighted the various threats introduced by email and emphasised the need to manage email effectively. Email must fulfil certain conditions to add business value.
Traditionally it was considered that email must enhance productivity and reduce costs. Considering the licensing costs of corporate email systems, it has become difficult to justify email usage in a corporate environment based on cost savings alone. Email has become a necessity, as much as the telephone has become a necessity in modern business.

To ensure that productivity is enhanced, and in fact not hampered by email, it is necessary to formulate email policies to regulate the use of email and to ensure that security standards are upheld in the use of email. Various approaches to the creation and enforcement of security policies were analysed in Chapter 3. It was shown that an information security policy framework had to exist in order to ensure effective security policy implementation. Various security policy frameworks were listed and the assumption was made that an email policy would fit into such a framework. Finally, this chapter examined how policies can be implemented and enforced.

Enforcing an email security policy often implies that a certain amount of monitoring of employees’ mail needs to take place. Not all countries have the same approach to privacy in the workplace. Chapter 4 identified the differences between legislation in various parts of the world. In a multinational organisation, policy makers have to be aware of the privacy legislation in the countries where the company is represented.

Countries in the European Union have the strictest privacy legislation, where companies in the United States of America appear to comply with privacy laws only when necessary to do business with the EU. In South Africa, the Electronic Communications and Transactions Act 25 of 2002, as well as the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002, determine what level of privacy email users have. Although this legislation has not been tested in a court of law, it is important that companies take note that corporate policy does not supersede national laws. It should therefore treat the invasion of privacy through employee monitoring with the necessary circumspection.

The principles for the creation of an email security policy were identified in Chapter 5. The threats discussed in Chapter 2 were highlighted and it was emphasised that these threats had to be addressed in an email policy. The chapter concluded with a suggested layout for an email policy.
Chapter 6 examined a methodology for implementing an email security policy and looked at principles that should be adhered to when enforcing such a policy. The IT department should not be the enforcers of an email security policy. This responsibility should lie with the Human Resources department and the direct line manager of the employee who violates the policy. Strict procedures should be adhered to, especially when an employee’s email is monitored.

Monitoring can cause a loss of morale and convey a sense of mistrust. It is possible that the advantages of monitoring could outweigh its benefits. It is therefore important that a policy should spell out how monitoring will take place and what will be monitored. If monitoring takes place, it should be sufficiently justified and not be invasive. Monitoring is needed for policy enforcement and is meant to protect the organisation from litigation, to ensure employees have a non-hostile work environment and to maintain productivity.

If an incident does occur that may lead to legal action, an email policy will demonstrate that a company has taken steps to prevent the inappropriate use of email. If it can be proven that a policy is enforced and that action is taken against employees who violate policy, a company should be able to defend itself successfully during court action.

A draft email policy was created by taking all the problems and drivers stated in the paper into account. This has been included in Appendix 1. This draft policy will be used as a working document towards revising an existing email policy in a multinational company.

### 7.3 Drafting effective email policies

In Chapter 1, the problem surrounding email security policy implementation in multinational organisations was stated, together with the research objectives for this paper.

To determine whether the objectives of this paper had been met, the complete problem statement follows:

> The unmanaged use of email does not necessarily add value to the business environment. Well-defined security policies are required to ensure that value is in fact added by email usage. The creation of a policy framework
and the implementation of email security policies are problematic in multinational corporations. This is mainly due to variations in privacy laws in different countries.

From this problem statement, a primary research objective was derived. This primary research objective was formulated as follows:

The primary objective of this study is to determine how corporate environments can ensure that email usage adds sufficient business value and to determine how policies should be formulated in order to regulate proper email usage. A further objective is to develop a model and a generic draft policy as to how email security policy can be implemented and enforced in multinational corporate environments.

In this paper, it was shown that the business value of email is often undermined by abuse and misuse of the tool by employees. The reason for such abuse is more often out of ignorance and because no well-defined email security policies exist. In multinational organisations, the corporate email security policy is often abandoned, as it contradicts local privacy laws. In such cases, managers rely on local legislation to guide email usage and often do not draft locally applicable policies – either because they do not have the knowledge to draft new security policies, or because corporate policy dictates the existence of only the single corporate security policy.

The problem areas pertaining to email usage and email security policy creation were examined in Chapters 2, 3 and 4. Chapters 5 and 6 addressed the second part of the primary research objectives, where the content of a draft email security policy was proposed and suggestions for the implementation of this policy was given.

The secondary objectives of this study are restated below, followed by a statement on how these secondary research objectives have been addressed in this paper.

- To determine why policy is not adhered to. The factors why policy is ignored were highlighted in Chapter 2. The main reason email security policies are not adhered to is ignorance. Not sufficient time is spent on implementation, of
which user education is a large component. This weakness was addressed in Chapter 6.

- To prove that most email security policies are contrary to the way modern employees view the work environment. Employees want to work in an unfettered environment. They see email as a communication tool not much different from a telephone. In the employee’s mind, security issues should be taken care of behind the scenes, without their own intervention. Where monitoring takes place, it is viewed as an invasion of privacy, rather than as a method to protect the business from potential legal action. Various views on monitoring were studied in Chapter 5.

- To analyse the policy frameworks in use in various organisations and how these policies are implemented in different environments. (Bureaucratic, Incentive, Culture). In Chapter 3, different security policy frameworks were compared. Implementation methods were compared and it was concluded that a change in organisational culture was the best method to implement security policies. Chapter 6 expanded on the implementation methods multinational organisations may use to enforce email security policies.

- To indicate that policy implementation in multinational organisations is problematic due to various cultural, legal, and other factors. Chapter 4 was dedicated to the analysis of multinational issues – especially pertaining to legal and privacy issues. It was shown that privacy legislation differs in different regions where a company may be represented. One should be aware of these differences during email security policy formulation.

### 7.4 Further research

Additional research into the enforcement of email policy in different cultural environments may contribute to this field of study. Cultural differences – both in ethnicity and in corporate culture – may have a significant impact on how email policy is received by an employee.

It is also important to research the future of email. Computing is becoming ubiquitous and soon the line between email, instant messaging and short message services (SMS) on cellular telephones will become blurred. Email as one knows it today may even
become integrated with faxing and voice messages. Soon unified messaging may replace email and other messaging technologies and combine it into a single, wearable device. This would have major implications for messaging security policies, as the line between corporate and private messages will become completely blurred.

7.5 Conclusion

It is significant that legislation in several countries attempts to address the tension between a company’s rights to ensure productivity through monitoring with the individual privacy of the employee. A company, especially a multinational company, should therefore take special care in the formulation of an email security policy to ensure that the policy does not contradict local laws or compromise an employee’s right to privacy.

This fine balance between an individual’s rights and the corporation’s objectives cannot be ignored by policy makers. In multinational organisations, the policy makers are often far removed from the experiences of the average employee. This is even more true in terms of an employee in a country foreign to the corporate head office.

When drafting an email security policy, it is important to solicit input from multiple role players who have sufficient knowledge of local law to ensure that corporate policies are globally enforceable.

It is only possible to ensure that email as a tool adds value to an organisation if that tool is managed through the effective implementation and enforcement of an email security policy.
Bibliography


Corporate Executive Board. (2000, November). Information security for the Internet era.. *Working council for chief information officers*.


DiCenzo, C. (2002). Email active archiving targets restore, regulatory and content management. Gartner Inc. HARD-WW-DP-0309


Edmead, M (2002). The security foundation begins with the security policy. Retrieved 1 July 2003 from [http://searchsecurity.techtarget.com/tip/1,289483,sid14_gei883575.00.html](http://searchsecurity.techtarget.com/tip/1,289483,sid14_gei883575.00.html)


Nchor, J. (2001). Email and Productivity: Studies show increase in productivity with email usage.


TechRepublic. (2002b). Make a password policy part of your security plan. In *Network administrator’s resource kit*. (CD Rom. CNET Networks Inc.)


Appendix 1: Draft email security policy for
The Goodyear Tire and Rubber Company

1. Objectives.

This policy describes The Goodyear Tire and Rubber Company’s guidelines with regard to the usage of electronic communications, as well as the company’s right to access and disclose the content of electronic mail messages sent or received by users of IT Resources supplied by Goodyear.

2. Scope.

This policy applies to all associates of Goodyear, including its affiliates, both permanent and contract associates, in all locations.

3. Definitions.

3.1. Email is defined as all technologies used to transfer messages, including Lotus Notes, instant messaging and peer-to-peer file exchange, which are used to send and receive information that includes items such as notes, documents, letters, reports, data files, images and graphics.

3.2. IT Resources refer to handheld mobile devices, PCs, workstations, laptops, terminals, servers, storage media, voice and data networks, systems such as Internet access, and software such as word processing.

3.3. User is any person using IT resources provided by Goodyear or one of its affiliates.


4.1. Goodyear respects the individual privacy of its associates. All email messages are considered company records and in compliance with the Goodyear Computer User Agreement\(^1\) signed by associates and contractors, Goodyear retains its rights

\[4.1.1.\] to monitor its computer systems for criminal or abusive activity and to access any information placed on, or generate through the use of, such systems; and

\(^1\) All users of computer systems complete a form in which the company’s rights are expressed in terms of ownership of resources and data, as well as its stance on privacy. The compliance of this document with local law is questionable, as it has been drafted in the USA.
4.1.2. to use or allow others to use such information as evidence of your misuse of a computer system or as information that might be, or lead to the discovery of, evidence admissible in any legal proceeding, subject to the legal restrictions imposed by local governing law\(^2\) and to the procedures determined by company policy (Bulletin no. 0023205394 of 09/25/2000)\(^3\).

4.2 Goodyear therefore reserves the right to intercept, delete or block any communication that constitutes a misuse of IT resources as defined in this policy.

5. **Usage of Email**

5.1. Goodyear provides the electronic mail system to assist you in the performance of your job. You should therefore use it for official Company business. Incidental and occasional personal use of email is permitted by Goodyear, but these messages will be treated the same as business-related messages in terms of privacy.

5.2. You should, therefore, not use email to transmit any messages you would not want read by a third party. For example, you should not use the email system for gossip, including personal information about yourself or others, for forwarding messages under circumstances likely to embarrass the sender, or for emotional responses to business correspondence or work situations.

5.3. You should not use these systems for such purposes as soliciting or proselytising for personal commercial ventures, religious or personal causes or outside organisations or other similar, non job-related solicitations.

5.4. All email generated in the course of your business must be created and transmitted from Company authorised systems and not from systems such as Outlook, or free internet-based mail systems like Hotmail, Yahoo, etc.

5.5. The maintenance of your mailbox is your responsibility and has to comply with the company standards as determined by the local IT management\(^4\):

5.5.1. The maximum attachment size that may be transmitted by email is 10 MB and any attachment larger than 3 MB will be sent after hours;

\(^2\) In South Africa, the Electronic Communications and Transactions Act 25 of 2002, as well as the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 both have a bearing on the monitoring of email. It is important that a local copy of the policy have specific reference to the relevant laws of that country.

\(^3\) This bulletin describes the procedure which has to be followed to access someone’s email.

\(^4\) The United States and Europe have far more bandwidth available at a lower cost than, for example, Turkey or South Africa. This means these size restrictions may differ from one location to the next. Enforcement of these restrictions is dependant on settings on the email system or third party mail filtering software.
5.5.2. Maximum mailbox size is 100MB;

5.5.3. Inbox content older than 6 weeks and folder content older than 18 months will automatically be deleted in compliance with Goodyear’s document retention policies.

5.5.4. Personal archiving is not allowed. Documents requiring long-term retention should be placed in departmental document repositories.

6. **Forbidden Content of Email Communications**

6.1. You may not use Goodyear's email system in any way that may be seen as insulting, disruptive, offensive by other persons, or harmful to morale. Examples of forbidden transmissions or storage include

6.1.1. sexually-explicit messages, cartoons, or jokes;

6.1.2. unwelcome propositions or love letters;

6.1.3. ethnic or racial slurs;

6.1.4. any other message that can be construed to be harassment or disparagement of others based on, inter-alia, their sex, race, sexual orientation, disability, physical attributes, age, national origin, or religious or political beliefs.

6.1.5. profane or offensive language

6.1.6. chain letters

6.2. Email may also not be used for any other purpose that is illegal, or against company policy or contrary to the company's best interest. Solicitation of non-company business or any use of the company email or Internet for personal gain is prohibited

7. **Password and Encryption Key Security and Integrity.**

7.1. Associates are prohibited from the unauthorised use of the passwords and encryption keys of other associates to gain access to the other associate's email messages.

7.2. The preferred method of assuring business continuity, especially during planned absences, is for the user of the email system to use the email facility to assign a delegate. A delegate will only be assigned by a third party (e.g. IT) with the express permission of the primary user or through the delegation procedure contained in the Corporate Policy.

8. **Communications:**

8.1. The email system is password controlled. Each associate is therefore responsible for the content of all text, audio or images that they place on or send over the company's
email system. No email or other electronic communications may be sent which hides
the identity of the sender or represents the sender as someone else or someone from
another company. All messages communicated on the company's email system
should contain the associate's name.

8.2. Any messages or information sent by an associate to another individual outside of the
company via an electronic network (e.g., bulletin board, online service or Internet) are
statements that reflect on the company, despite the use of disclaimers.

Disclaimer wording is determined by the company and is currently as follows:

"The information in this e-mail contains confidential and/or proprietary informa-
tion and is intended solely for the addressee. Access to this e-mail by anyone else
is unauthorised and may not be copied or disseminated without the express con-
sent of The Goodyear Tire & Rubber Company or one of its subsidiaries. If you
are not the intended recipient, any disclosure, copying, distribution or any action
taken or omitted in reliance on this, is prohibited and may be unlawful. Whilst all
reasonable steps are taken to ensure the accuracy and integrity of information and
data transmitted electronically and to preserve the confidentiality thereof, no li-
ability or responsibility whatsoever is accepted if information or data is, for what-
ever reason, corrupted or does not reach its intended destination."

8.3. No communications sent by associates via the company's email system may disclose
any confidential or proprietary company information.

9. Software

9.1. To prevent computer viruses from being transmitted through the company's email
system, unauthorised software received as executables or otherwise (exe, bat or zip
files) may not be loaded on company owned systems. Associates should contact the
IT department if they have any questions.

9.2. An associate should not open or execute an attachment if in doubt of the origin of such
an attachment.

10. Copyright Issues:

10.1. Associates on the company's email system may not transmit copyrighted materials
belonging to entities other than this company. All associates obtaining access to other
companies' or individuals' materials must respect all copyrights and may not copy, re-
trieve, modify or forward copyrighted materials, except with permission, or as a single
copy to reference only. Failure to observe copyright or license agreements may result
in disciplinary action up to and including termination.
11. Violations:

11.1. Any associate who abuses the privilege of company-facilitated access to email or the Internet will be subject to corrective action up to and including termination. If necessary, the company also reserves the right to advise appropriate legal officials of any illegal violations.

11.2. Human Resources management will be responsible for determining any disciplinary action resulting from violations of this policy, up to and including termination of the employee’s contract.

I, _____________________________________________________, hereby acknowledge that I have read and understood and agree to abide by the guidelines expressed in this policy and by the supporting Information Systems policies. I acknowledge that I do not have a reasonable expectation of privacy regarding anything created or stored on company equipment or systems.

By signing this agreement, I agree to the monitoring of my email, Internet usage and data stored on my computer or the server, subject to the procedures determined by the company policies.

Date:__________________________ Signature_____________________
