Global Information Assurance Certification Paper

E-mail Content Scanning: the Pro's, the Cons and the Legal Issues
Barry Darnton
December 31, 2000

Overview

Even if we don't like it, e-mail is now part of our life and while the Internet has brought a major change in the way that we do things from shopping to system support, it has also introduced legal problems and issues that can effect productivity. A desktop Virus scanner can help to reduce lost productivity and user inconvenience due to system downtime from an e-mail borne worm but constantly deploying updates to a thousand plus desktop's is always going to be a slow and costly process.

Anything that makes an organisations computer system inoperable can cost large amounts of money in very short periods of time, in some cases even send the company broke. The first line of defence for the e-mail system should be to install a content scanning system at the point of entry into the company, this way only one or two machines need to be regularly updated for new virus identities to reduce the risk of desktop infection. This does not mean the desktops do not need their antivirus software updated, only that the timeframe for achieving this is longer. This will be a good start for the malicious threats but the next issue is the legal problems. E-mail is as good as a written letter and anything written in e-mail is admissible in court, the company can be held liable for the content of any messages that are sent by their users. Just a general comment to a friend could result in the company being sued for defamation etc.

It is a legal requirement that an employer provide a safe working environment for all employees. Most people clearly understand that a company can be held liable if an employee complains that a person is harassing them at work and the company does nothing to stop it. What is not so obvious is that harassment does not require a face to face situation, constantly sending a person unwanted abusive or offensive e-mails is harassment as well. The only way a company can attempt to comply with this legal requirement in regards to e-mail, is to install and properly configure a content scanner.

E-mail content scanning is no different to keeping a log of who and when someone other than yourself drives your car. In the event of something going wrong you can protect yourself from litigation as well as ensuring that you are not held responsible for another person's actions. It is unrealistic for any employee to expect their employer to foot the bill for their actions, if they were aware that it was not legal. The purpose of e-mail content scanning is to help protect corporate systems from malicious software and legal liability for both the employee and the company.

How Internet e-mail works (The basics)

For an e-mail to get from point A to point B across the Internet the sending system needs to do a DNS lookup for a Mail Exchanger (MX) on the receiving domain. If the domain resolves OK the sending systems Message Transfer Agent (MTA) will connect to the MX IP address, usually on the standard SMTP port 25 and tell the system who they are, the sending persons e-mail address (FROM) and the receivers e-mail address (TO). If the receiving system accepts this without error, the message will then be sent on this connection.

The loss of e-mail services can be attributed to a number of things that are beyond the control of the system managers such as system failures, power blackouts, floods etc. These should be addressed as part of your Disaster Recovery Procedures (DRP) and are beyond the scope of this document. The other reason for loss of e-mail services can be due to malicious behaviour by person or persons unknown to the organisation targeted. The threats will usually fall into one of the following categories.

The Threats that your MTA can control

Denial of service

The most common denial of service attacks in regards to e-mail can be attributed mail exchangers that are not configured to prevent open relay. Basically what this means is that a person who does not originate from your domain wants to send a message to someone

who is also not in your domain and the MTA permits this. You can imagine what would happen if this person decided to send an e-mail to 100,000 people with a 5meg attachment using your system as the relay. A simple test for an open relay would be to telnet to your MX on port 25 and issue the following commands (in Bold).

Telnet mail.here.com 25

220 mail.here.com ready for mail

ready at Sat, 17 Mar 2001 12:27:42 +1100

helo santa

250 mail.here.com Hello [192.168.15.1]

mail from:<president@whitehouse.gov>

250 2.1.0 president@whitehouse.gov....Sender OK

rcpt to:<anyonelwant@anywhere.com>

550 5.7.1 Unable to relay for anyonelwant@anywhere.com

If the message sent back from the mail exchanger after the

rcpt to:<anyonelwant@anywhere.com**>** says OK then your system is configured as an open relay and you really need to fix this.

Spoofed Mail

Spoofing an e-mail address is forging the sender's ID and fooling the person who receives the e-mail into believing it is from someone they know (and possibly trust). This can lead to the user clicking on a link in the e-mail and accessing an undesirable site or perhaps executing a Trojan attachment believing it to be from a trusted person. You can limit but not prevent spoofing by configuring your MTA to do a DNS lookup on the connecting IP address to see if it matches the sender's domain.

Terri Kring has written a paper on open relay and this can be found at http://www.sans.org/infosecFAQ/email/mail_relay.htm.

If the MTA you are using is Sendmail then you can find out how to prevent open relay at http://www.sendmail.org/tips/relaying.html.

The Threats that your MTA can't control

Spam Mail

Spam mail is usually from a person that is trying to sell you something or get you to visit a web site to make a million dollars. I don't really need to say much on this as I am sure that anyone that uses e-mail on a regular basis has seen this before. Most companies with Internet connections usually have their E-mail addresses advertised on the corporate website, but even if they don't these people have numerous resources such as mailing lists etc that they can get addresses from. A spam mail will usually be addressed to many people within your organisation and if there are enough recipients or large enough attachments this can slow your e-mail system down for a considerable amount of time. If your MTA is Sendmail then this can be controlled to a point, however functionality is limited but the standard version of Sendmail is free. Information on configuring Antispam in Sendmail can be found at http://www.sendmail.org/antispam.html.

Additional ways of preventing spam from entering your site is to configure the MTA or scanner to use publicly available lists of known spamming sites or open relays. Information on this can be found at

MAPS RBL (Mail Abuse Protection System Realtime Blackhole List)
http://maps.vix.com/rbl

MAPS RSS (Mail Abuse Protection System Relay Spam Stopper)
http://maps.vix.com/rss

MAPS DUL (Mail Abuse Protection System Dial Up User List)
http://maps.vix.com/dul

ORBS (Open Relay Behaviour Modification System)
http://www.orbs.org

Viruses

The number, types and variations of viruses available today could fill a seven thousand-page book. What make matters worse is that there are tools freely available on the Internet where the only skills required to make up a new virus is to be able to click OK with a mouse. If that isn't scary enough, do you think any large corporation will successfully be able to prosecute a seven-year-old for killing their network with a virus. Anyway, enough of the melodrama, in order to protect your network from viruses all you need is a good virus scanner right??, Wrong. Viruses are not just executable files anymore and while reputable antivirus vendors cater for a much wider range of variants now you still need another level of checking as a backup. If a new virus comes out that can slip past the virus checker the scanner can quickly be configured to block this based on a known variable, the additional level of checking equates to defence in depth. One note about virus scanners, some of them only check the first 5 bytes of a file to check for a virus, you should check with your vendor about this before deciding on a supplier.

Another form of virus are what are known as macro viruses, these use the built in functions of applications such as word, excel and outlook that run with the same privilege as the user. Most virus scanners will detect these when the file is opened. The user then has to call the helpdesk to get assistance in removing the virus or deleting the file and asking the sender to resend the message without the embedded virus. This has a cost in terms of lost time and productivity. A scanner can search within documents for key words (usually VBA) prior to delivery and if a suspect word is found, notify the sender advising them that the message has not been delivered and advise them what to do. Word documents that contain macro's will automatically run when the document is opened by word, this has been fixed in word 2000. There would be some occasions where you want the embedded macro with the document, but in most cases any macro should be treated with suspicion. Asking for documents to be sent in RTF format is one possible solution however you can rename a .DOC file to a .RTF file and word will open it as a document file and run the macro. A scanner should be able to detect a renamed doc file. Scanners are capable of calling external programs so perhaps a program will become available to convert word to rich text format on the fly one day.

The next type of virus comes in the form of a VBS attachment which until recently was easily spotted by an alert user (we all have alert users don't we). If you are using a mail client such as GroupWise this attachment has to be run manually so is a bit more obvious to our alert users. In exchange however you can just click on the attachment and it runs, scripts are even worse, they can run just by opening the e-mail. For the few alert users who bothered to read the filename of the attachment and got suspicious if it was a .vbs file the script kiddies came up with a new idea as was seen in the AnnaKournikova virus. Microsoft in its wisdom didn't think it was necessary by default to show the MS-DOS extensions to the user. If you send a file named AnnaKournikova.jpg.exe it only shows up in outlook as AnnaKournikova.jpg. What harm can there be in opening a Jpeg file, well anyone who got this and expected a sexy picture of the tennis player would know. Not being able to see the extension is easily fixed by going to menu options, view, and uncheck "Hide MS-DOS file extensions that are registered" but it is still left up to your alert users to even bother to look at these names.

One advantage of using a scanner is that keywords if chosen properly can detect highly suspect words such as "Hkey_local_machine" and either block the file or warn the recipient that the code may be

malicious. The decision here will be made by the security policy of your company.

Inappropriate Content

This one is subjective to say the least, what one person finds offensive another does not. Unfortunately from a legal point of view the employer must provide a safe working environment for it's employees. For example, you have an electrician working on your site and he is instructed to check the fuses in a high voltage circuit that has a manual circuit breaker switch installed. This person then electrocutes himself or herself, is the company liable?. Well if the company has proof that the person was qualified, was instructed on safety procedures and was aware of the breaker switch then it would be highly unlikely that the company would be found liable in such a case (but you know lawyers). A petroleum company in the US found out recently that permitting inappropriate e-mail into their network without making any attempt to filter content cost them $2.2 million when sued by four female employees. It would not be possible for any system to guarantee 100% that it can prevent inappropriate e-mail from entering the network, but the company only needs to prove that it took reasonable steps to prevent it in order to not be liable.

What should a scanner look for

A scanner should be capable of a number of things

Recursive disassembly - Capable of pulling apart a message no matter how many times an object or file is embedded in the message.

Compression/Decompression - Capable of decompressing the embedded messages in a number of formats such as, RAR,ZIP,LZH, the list goes on

Content recognition - The scanner should be able to recognise a file by looking at the data not the name. If a scanner only recognises an AVI file by it's name then it would be simple to circumvent and not very useful.

Text analysis - The text analysis engine should be able to find text in all parts of the message from the header through all the attachments. It should also support weighting of keywords to reduce false positives as well as BOOLEAN expressions such as "near", "and", "from" etc.

Binary pattern detection - Sometimes it may be necessary to search for a pattern in a message at a particular offset, this may be in the case of a new virus that the vendor has no update for yet.

Multi language support - Most companies have multicultural employees these days so replicating your keywords into multiple languages help protect the company from problems with non-English employees.

Text attachment - It is common now for companies to append a disclaimer to e-mail saying that the opinions are not necessarily that of the companies. This is done to protect the company not the employee.

Event and user notification - When an e-mail is outside of the policy a mechanism to notify either the sender or the recipient of the problem and stating what action needs to be taken to process the message correctly.

Queuing and holding areas - Messages that are outside of the policy need to be held pending a decision from the sender as to what action to take. This holding area should be capable of releasing the message and bypassing policy if required. A queuing area would be used for messages with large attachments that can be automatically sent after normal business hours.

Automatic userlist maintenance - The system should integrate with your user database system such as your NT domain users,NDS or Ldap. This will reduce the number of e-mails bounced to the administrator for unknown

users as well as instant notification to mailing lists etc for users that have left but have not unsubscribed from lists.

Audit trail - Depending on your business needs you may need to keep track of message data for a period of time. For example we are required to keep the sender, recipient, subject, bytes transferred, Date and time of each message for a period of five years. Depending on the number of e-mails you transfer a day and the amount of information you need to keep, it may be necessary to keep the data in a separate database server.

Reporting - Mail scanning software is not cheap and there may be some requirement from the internal auditors to generate reports for audit purposes. You may want to generate HTML reports for the top 10 users each week and embarrass them on the Intranet (great for building employee moral). The real benefit of good reports is to provide information to the executives that shows the benefit of the scanner for everyone by showing statistics on blocked viruses and spam messages etc.

Encryption support - Support for encryption that conforms to the Public Key Infrastructure(PKI)

Encryption

E-mail that is not specifically encrypted is transmitted across the Internet as clear text. This is inherently insecure as it is trivial to capture and read an e-mail message if you can get in its path. This is becoming a major problem for companies that send confidential information or for health professionals that need to talk to each other about patients. It would be unacceptable for a user to install an encryption package on their desktop and send encrypted e-mail as the scanner would be prevented from doing it's job. To overcome this problem you can install a key server. When you install a key server and register your domain certificate (either yourself or from a vendor such as verisign) your users can then send and receive encrypted e-mail. While this sounds easy in theory getting it going in practice is difficult and training your users is even harder.

You need to generate a pair of keys for encryption to work, a Private key and a Public key. A message encrypted with a public key can only be decrypted with the matching private key. To start the encryption process your users need to give their public key to every person that they want to receive encrypted mail from. In addition to this your users must receive the public key from anyone that they want to send encrypted mail to. The key server will store all the public keys for external users and the private keys for internal users.

When an internal user sends a message to an external user it will not be encrypted. The scanner will first scan the unencrypted e-mail and ask the key server if the recipient has a public key. If the recipient has a key listed and the message has passed the rules it will then encrypt the message with the recipient's public key. The recipient will then decrypt the message using their private key.

If the e-mail is coming into the network and it is encrypted the scanner will ask the key server for the private key. If the key is found the message will be decrypted, scanned and passed to the recipient if it passes the rules, if no key is found for that recipient it will block the message. Centrally storing the keys on a key server has security issues in regards to the administrator of that server, this issue will need to be addressed by each organisation.

There is a lot of information on encryption and VPN at
http://www.sans.org/infosecFAQ/encryption/encryption_list.htm.

PGP Documentation can be found at
http://www.pgpi.org/doc

OK we understand that we need a key server to generate the users keys, and we understand how each party in an encrypted e-mail can read the message. If this is all done correctly the process is transparent to the user. When they send a message it will automatically be scanned and encrypted without the user

doing anything. If the recipient does not have a public key and the message is outbound then the message will be sent without any encryption.

The Legal and Moral perspective

I don't profess to be a lawyer or know anything about the law other than what is generally regarded as common sense, for issues regarding e-mail you would need to seek advice from your company's legal representatives for your country before applying any rules to your scanner. A good scanner can do a lot of different things including modifying the contents of the original message. It is even possible to automatically forward copies of e-mail destined to a particular user to someone else in the organisation without the sender or recipient even knowing. What is legal and what is not will depend on what country you are in.

Some content scanning engines even allow you to write applications that can be called from the scanner on certain events. This opens up a huge number of possibilities as well as a potential security problem. Imagine if a hacker was to compromise your mail scanner and insert there own rules or application, The number of things that they could do to your e-mail is enormous. Some of the possibilities would be

Bypass the virus scanner and insert Trojans

Change the outgoing Legal disclaimer

Change certain words to obscene words or change the intent of the message

Copy confidential Information to a competitor

Setup a mail relay for spamming

If an encryption key server is used it would also be possible to read encrypted messages.

The possibilities are endless for the devious mind and your company could be held liable for anything that is sent out. If your scanner runs on NT which almost has a new exploit found in something every day it would be a good idea not to run it directly on the Internet connection unless all it is doing is scanning. If this is the case, disable every service that you can, don't run DNS on it, point it to your DNS server and put it in the DMZ filtered by the choke router and firewall. This should be a reasonably secure setup unless an exploit in the software itself is found.

The Sendmail program is the most common MTA used on the Internet today and has similar problems to the scanner. If you can compromise the MTA, then you can get Sendmail to run external programs on events, but it does take a little more effort than most script kiddies can muster to hack a well configured Unix system and not be noticed than it does with NT.

It is possible to run a dumb mail receiver such as Trusted Information Systems Smap program. This is essentially a tiny version of Sendmail with no features, it simply accepts correctly formatted SMTP messages and stores them for the Smapd program. The reason that this is more secure is due to the size of the code, around 1300 lines compared to the latest version of Sendmail that has a total of over 100,000 lines of code. The logic being that a small program is less likely to have an exploitable error than a large program. This logic seems to hold true. I was unable to find any security advisories on the Smap program but there are around 150 for Sendmail(for various O/S and versions).

So why doesn't everyone use the Smap program, it's free from the toolkit and it seems to be secure, well once again it's a security versus functionality issue. Smap is secure but dumb, it blindly accepts e-mail from anyone without question. If you want mail rejected from certain sites such as known spammers or bounce e-mail to non-existent users then Smap won't do this for you. Smap only supports the basic SMTP commands, it does not support any of the Extended commands such as message size. Without this feature a person could send you a file of any size and cause a denial of service by filling your hard disk or waste bandwidth by sending a large file that gets rejected by the scanner. There is no support for the Smap package in the toolkit so any bugs that arise will have to be fixed by the individual, this in itself may compromise the security of the code. Smap is simple to configure and run. The commercial version of Gauntlet Firewall includes SMAP but is much more configurable through the netperm table.

Sendmail supports Extended SMTP and has lot of features that can help keep the mail system running efficiently. Sendmail on the other hand can be a beast to configure properly for the inexperienced, but plenty of help is at hand from the Sendmail site www.sendmail.org. and the bible on Sendmail published by O'Reilly.

When e-mail arrives at the destination MTA it is no longer on the public network and not covered under the telecommunications act. In other words you cannot scan the e-mail as it is transmitted from source MTA to destination MTA, but once the destination MTA has received the entire message and the connection is closed it is then the property of the company, not the user.

So legally, the company can read anyone's e-mail and do whatever they like with it and they are under no "legal" obligation to tell the user that they have done this. It would be morally unethical as well as complete and utter stupidity for any company to expect to get away with this type of behaviour with no repercussions from the employees.

How do you get a good balance between the two. First of all you need your HR people and key users on side and involved in the security policy, then you need to make all the users aware of what is being scanned, why and who has access to this information. A large proportion of employees would like to see a good joke or two but how can you permit jokes without running the risk of winding up in court. If e-mail arrives that has a video or image attached you can't determine if the contents will be offensive to the recipient. If however you pre-pend the message with a warning that it has an attachment that could be offensive, and offer a screening mechanism if required then you have achieved protection for the employer as well as the employee without reduced functionality. This will of course be dependent on the executives to make the decision if any inappropriate material is permitted, they may be flexible but I would be surprised if most companies would permit e-mails if they contain a certain four letter word more than ten times in a single message.

Each company will also need to weigh the cost of personal e-mail verses an intensive regime of e-mail monitoring that will cause bad will amongst employees and probably require a full time position to enforce it.

All monitoring and filtering should be Overt,

> employees should be aware of the guidelines and policies that apply. Monitoring should not be used unless a problem has been identified.
>
> The employee should at all times be made aware of the level and type of electronic monitoring.

One possible method for user awareness is to display the policy each morning on boot. If the user does not agree with the policy then Internet access and e-mail is disabled for the duration of that connection. If the policy changes the users must be made aware of the changes prior to them being enforced.

Scanners can look in a message in a variety of ways as well as within any embedded attachments. What follows is a small sample of things that scanners could look for. The examples are by no means complete and need to be constantly updated from sources such as your scanner supplier, Bugtraq ,SANS, CERT etc. You will also need to add things when something gets through and the user gets clobbered, it's a never-ending task.

Sample detection entries

Inappropriate words (Should be weighted)

> Not listed for obvious reasons

VBS or HTML script entries

Whenever a new script attack comes out you only need to get access to the source code and see if your keywords are listed, if they are then the message will be stopped, if not then you need to find a word that

is unique to filter it on.

- ActiveXObject
- CreateObject
- DriveType
- End Function
- End Sub
- FileSystemObject
- GetNameSpace
- GetObject
- hkey_local_machine
- new ActiveXObject
- On Error Resume Next
- Outlook.Application

Spam entries (can be in subject or message body)

- a great opportunity to make
- amazing business
- be rich
- Create residual income
- cyberspace communications
- e-mail is the sales tool of the future
- e-mail messages every hour
- e-mail promotions
- fantastic savings
- financial freedom
- financial independence
- free submission to
- guaranteed lowest prices and largest selection
- here is how it works
- if you wish to be removed from future mailings
- mail order marketing business

proven ability to generate

quick cash

You are virtually guaranteed

(The list goes on and on)

Worm Entries

Be careful what you open. It could be a virus

Bill Gates is guilty of monopoly. Here is the proof.

Bill Gates joke

choose your poison

click attachment to see some stunningly HOT stuff

Disregard Macro Warning

Have fun with these links. Bye.

Here's a digital video for you

Here's some pictures for you!

Hi! Check out this neat doc I found on the Internet!

Mad Cow Joke

Meltingscreen

newest and funniest screensaver

paramount pictures website

startrek screen saver

take a look at the attached zipped docs

The Bubbleboy incident

This document is very Important and you've GOT to read this

what's up ?

(and the list goes on)

Testing your mail scanner

You have installed your scanner and are ready to go, but if you don't test it with as many variations as you can think of then how do you know if it's working. The MIMEsweeper eval CD has a good collection of threats in the test directory that is a good starting point. Obviously if you are using the Baltimore MAILsweeper product it is certain to detect everything on the CD if it is setup correctly so you may need to modify some of them to test it thoroughly. All of these tests come from the MAILsweeper CD and are a reasonably thorough set of checks, you can modify the order of compression and embedded files if you

feel it to be necessary. An EICAR file is a file that has a virus signature it is not actually a real virus, when your testing is complete it would be a good idea to run multiple real viruses through the system. You should test each file and verify the behaviour is what was expected. Tests should be carried out from both inside and outside the network.

A zipped EICAR file which has been embedded in a Word document.

A zipped EICAR file, which has been embedded in a Word document, and then embedded in an Excel file.

A renamed AVI file that has been zipped and embedded in a Microsoft Word document.

A BinHex-encoded EICAR file in a Unix format.

An EICAR file in a password-protected self-extracting RAR file.

An EICAR in a self-extracting ARJ file, in a self-extracting Zip file, in self-extracting RAR file.

A UUE-encoded AVI file that has been renamed as a .txt file.

An EICAR file embedded in an Excel spreadsheet, which has been MIME encoded.

An AVI in a self-extracting ARJ file, within a self-extracting Zip.exe file.

A BinHex-encoded AVI file.

An AVI file renamed as a UUencoded self-extracting executable file.

A zipped and renamed AVI file within a Word document, which has been embedded in an Excel file.

A password-protected and zipped EICAR file.

A zipped AVI file within an ARJ file.

A zipped text document containing phrases in your Spam and Inappropriate lists

Notifications for e-mail that contravene policy

The purpose of sending notifications to users is to inform users that a computer scans e-mail not a person, and that any messages sent or received that contravene policy will not be opened unless the sender gives permission. This is to assure the user that only the sender of the e-mail has the authority to allow anyone other than the intended recipient to open the message. The intent here is to give the users their right to privacy while still maintaining a reasonable level of security.

Outbound Virus Notification message

Notification to Sender

Your message to user@domain.xxx.yyy was not delivered because a Virus was detected

If you feel this message is an error please reply to this e-mail and the message will be re-checked.

Please note by asking for the message to be re-checked it will be necessary for a person from IT services to open the above E-mail and extract the suspect file to determine if it can be cleaned. If this is not acceptable please call the help desk and ask for your desktop to be scanned for virus.

This message has been quarantined in a secure area and will be automatically deleted in 30 days.

Notification to Receiver

None

Inbound Virus Notification message

Notification to Sender

Your message to user@domain.xxx.yyy was not delivered because a Virus was detected

Please check your system for any viruses before resending this E-mail.

If you feel this message is in error please reply to this e-mail and ask for the message to be re scanned.

Please note by asking for the message to be re-scanned it will be necessary for a person from IT services to open the above E-mail and extract the suspect file to determine if it can be cleaned.

This message has been quarantined in a secure area and will be automatically deleted in 30 days

Notification to Receiver

A message from user@domain.xxx.yyy to you is believed to contain a virus. This message has been quarantined and will be automatically deleted in 30 days.

The sender has been notified of this problem and will either resend the message after cleaning or request the IT department here to try and clean the message on their behalf and forward it on to you. We will not attempt to open this message without the permission of the sender.

In bound Video/Audio/Movie File

Pre-pended to receivers message

A message from user@domain.xxx.yyy to you has a "TYPE" file attached. It is not possible to determine if the contents of this attachment contain material that may offend. If you have any concerns as to the type of material that this message may contain please forward the message to the helpdesk so that it's contents can be checked. Please note that forwarding this message automatically gives permission for an authorised person from IT services to open the message and read it's contents.

NB TYPE will say video, Audio, Movie or Image

Notification to sender

None

Inbound Inappropriate messages

Notification to Receiver

A message from user@domain.xxx.yyy to you contains offensive words. If you have any concerns as to the type of material that this message may contain please forward the message to the helpdesk so that it's contents can be checked. Please note that forwarding

this message automatically gives permission, for an authorised person from IT services to open the message and read it's contents.

Notification to sender

While I would love to send them something it would probably be classified as flaming, so I will leave that one alone and send nothing.

Conclusion

Access controls and security features of a network (passwords etc) give the user an illusion of privacy and they may not be aware that their e-mail content can be scrutinised. The purpose of access controls is to prevent unauthorised access and despite the fact that they are using government or corporate equipment, staff may consider that their e-mails are as private as phone calls. Without instructions the proper use of e-mail may not be clear, it is essential that management spell out clearly their expectations and permitted practices to employees. Users must be made aware the risks of litigation from Internet communications is far greater than from the telephone because e-mail leaves a mark whereas a telephone conversation does not. It is necessary for companies to collect personal information if it is only being collected for a lawful purpose and only by a person that is directly related to that function. Any personal data collection must be done by lawful means. If staff are not made aware of the logging procedures within the company, then this could be considered to be unfair and possibly unlawful. All users need to be made aware of the logging practices of the organisation, the purpose of the logging, who will do the logging, who has access to the information and for what purpose. In dollar terms we have already seen many companies reporting large losses due to Internet borne e-mail viruses such as the Melissa virus. If users can be convinced that these systems protect both the company and the employee then harmony in the workplace can be achieved. Unfortunately there will always be the hard liners in the privacy movement that believe that everything that is done is a big brother and in violation of their constitutional rights. I will concede as with any type of record keeping system that this information can be used for good or for evil but if we always took that approach we would still be using horse and carts. Most modern inventions have come from military research, research initially into weapons of mass destruction.

References

RFC-821
Postel Jonathan B "Simple Message Transfer Protocol" August 1982
ftp://ftp.isi.edu/in-notes/rfc821.txt

RFC-2920
Freed N "SMTP Service Extension for Command Pipelining" September 2000
ftp://ftp.isi.edu/in-notes/rfc2920.txt

RFC-1869
Klensin J, Chair WG "SMTP Service Extensions" November 95
ftp://ftp.isi.edu/in-notes/rfc1869.txt

RFC-1870 Klensin J, Chair WG
"SMTP Service Extensions for Message Size Declaration"
ftp://ftp.isi.edu/in-notes/rfc1870.txt

General Information on privacy in Australia
www.privacy.gov.au

Costales Bryan. "Sendmail Second Edition" November 1997

Internet content security
www.mailmarshal.com

Content Security Issues
www.mimesweeper.com

Virus and worm Information
www.spohos.com.au
http://astalavista.com/archive/index.asp?dir=virus/mailworms

E-mail threats
http://enterprisesecurity.symantec.com/article.cfm?articleid=613&PID=3326377#email

The Melissa Virus
http://www.zdnet.co.uk/news/specials/1999/03/virus/002.html

Information on Spam
http://spam.abuse.net/