Risks and Rewards of Instant Messaging in the Banking Sector

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Nicholas S. Rose BSc FCA CISA
CISSP

Location: SANS Conference Phoenix 2004

Table of Contents

Abstract/Summary

Instant Messaging (IM) was the first IP based mass communication application rolled out by users, rather than management, who saw immediate business value in this new form of communication. However IM opens up a variety of risks, especially in the Banking and Securities sector of the market and poses some serious legal and regulatory challenges. This paper seeks to explain these risks and to recommend current best practice for addressing them. This is to block all of these services at the proxy servers using a blocking product and then to selectively allow properly controlled and authorized IM and P2P services to take place through an IM enabling gateway.

Introduction

Instant Messaging (IM) is an application unlike any other, in that it was initially installed by early adopters to communicate with family and friends who happened to be online at the same time. Some of these people worked in dealing rooms and were the first to see value in the INSTANT part of the technology (rather than the MESSAGING part) as a method of quickly communicating with clients and associates in a fast moving business environment where seconds often make the difference between a profitable and an unprofitable trade. Dealing room clients quickly came to understand the competitive advantage that a direct and instant communication with their broker could give them and demanded that their brokers be available to them using this new type of communication. Saying no to such customers would mean the loss of a considerable volume of highly profitable business.

Initially[(10)], IM client software could be downloaded and installed by users without requiring local administrator access rights and so, with customers demanding this new form of communication, the client software was downloaded and installed onto a large proportion of workplace desktops, opening up many external connections to other users outside of the corporate network. This stealth rollout took place in companies all over the world, usually without management's knowledge or consent. By the time that management realized what had happened at least half of the desktops in their organization had probably subscribed to IM service providers.

In addition to the security risks of IM, which apply to all companies and will be reviewed in this paper, the Banking industry had another challenge. SEC regulations require all companies engaged in the trading of equities to log and monitor all of the electronic communications of their associates. By mid-2002 whilst some leading Banks and finance houses had applied logging and monitoring solutions to their e-mail applications, some had not and were unable to meet SEC demands to disclose "within a reasonable time" the e-mails of traders engaged in suspected illegal trading activities. This has led to some spectacular fines being imposed on those Banks. Also until recently, logging and monitoring had not been applied to Instant Messaging either, because management was unaware of the extent of the issue.

Eventually, following publicity surrounding the SEC fines, management in the Banking sector realized they had a problem. Some organizations chose to ban IM services immediately by policy but soon found out that a policy ban was easier said than done. Policy enforcement will be covered later in this paper. Others realized that with customers demanding this service, it would have to be allowed but restricted to those who had a demonstrated business requirement and logged and monitored in a way that complies with the regulations.

Finally, there has been a raft of State and Federal legislation, which places a legal duty of care upon the owners of personal information, not to disclose it to those who are not authorized.

This paper will now examine the risks that IM poses to the Banking and Securities community, the benefits that demand its use and the policy enforcement methods that may be deployed to control those risks and comply with the regulatory and legal requirements.

Section One - The Risks of Instant Messaging

For the Banking and Securities Trading sector, we will first consider the risks of IM and will then consider how they may be addressed.

1) Regulatory risks:

From the perspective of the Banking and Securities industry, the biggest risk is perceived to be the regulatory risk of failure to comply with the SEC's Books and Record keeping retention requirement contained in regulation 17a-4(b)(4) (7) and matching requirements contained in NASD rule 3010 (8). The regulations require the logging and monitoring of all "communications sent by the firm relating to its business as a broker-dealer, including inter-office memoranda and communications". This now specifically includes any electronic "communications with the public".

Compliance with the regulation usually requires the logging (or archiving) of these messages to CD-WORM drives. These must be stored for two years in easily accessible form and for the last three years in total. Monitoring means the scanning of message content for key words that may be indicative of illegal activity. This is usually accomplished by a separate content scanning engine with alerts sent into the message queues of the Compliance departments. Also customer facing associates must have these communications monitored to ensure that these communications do not contravene insider-trading rules. Additionally there is the requirement to enforce the "Chinese Walls" that prohibit communication from taking place between the Research and Investment Banking divisions of regulated entities

Following the lead taken by the New York Attorney General, the SEC has already issued some multimillion dollar fines for non-compliance of this regulation (9), so it is seen as a threat that has already crystallized and is an issue that SEC Auditors are now including in their checklists.

Some of the larger fines are as follows: In May 2002 Merrill Lynch agreed to pay a $100mm(9) penalty resulting from an action brought by the New York Attorney General for hyping stocks that internal communications revealed that they knew to be bad. As part of the settlement Merrill Lynch agreed to set up a proper system for logging and monitoring electronic communications. In December 2002 five of the largest investment banks in the world agreed to pay an SEC fine of $8mm(9) for failure to comply with the requirements of regulation 17a-4 (7). In August 2004 Fidelity Brokerage was ordered to pay a $2mm(9) fine to the SEC for breach of this requirement.

2) Legal risks:

The failure to adequately protect confidential customer information is now a violation of the Gramm-Leach-Bliley act(11) and also of CA SB1386 (12) which covers any organizations handling the data of any California based customers.

These risks are directly impacted by the lack of security, normally provided by some form of encryption, over the electronic communication services. In order to provide legal cover for these and other risks, most IM vendors used to include clauses in their End User License Agreement (EULA) specifically stating that the owner agrees not to use the service for business purposes. However, of the "Big Three" IM service providers (AIM, Yahoo and Microsoft) currently only Microsoft still includes such a clause. The others provide general liability disclaimers.

A further point that arises from this legal analysis is that because the service is provided at no charge, there is no guaranteed level of vendor support for any problems or failures that may cause business issues. This issue is common to any business relying on shareware or freeware and is a good reason for using alternatives to freeware for business critical services where at all possible.

3) Authentication & Presence Management:

Once IM buddies are set up in the IM client, they will indicate to other users of that service (using various icons or symbols) that the user is online and their availability. If available, then the external user can double click on the buddy name, open a chat dialog box and start a dialog. If the internal user has not changed their status to unavailable, then incoming messages from "known" buddies on the buddy list will immediately appear on the users screen in their own chat box.

Although a user's presence can be set to unavailable at logon, this does detract from the whole point of IM and is not something that brokerage clients like to see. If there is a business reason for using IM then this feature is usually not used. Your presence is therefore advertised to all of your clients from the moment you logon.

The important point to note from a security and control perspective is that the authentication of the incoming message is only as good as the authentication processes of the IM service provider and that these services are being provided for free. Generally speaking in technology (as in most cases) you get what you pay for and in this case you should consider that you aren't paying anything (other than paying lip service to advertisements that appear on the IM client or on any accompanying pop-ups).

The main weaknesses in IM Authentication are as follows:

1) Buddy names are displayed and transmitted unencrypted (unless the session is established over https which is an option in the AIM client).
2) Passwords are usually starred out but are transmitted in the clear (unless using AIM's HTTPS option) and also never change (unless requested by the user).
3) Passwords are not subject to stringent formatting requirements.
4) Authentication is to a server provided by the IM service provider which stores all of the ID's and passwords. Given that the service is provided for free the degree of security of this database is unknown but these centralized databases of customer information are coming under increasing attention from the hacker community.

From the above it becomes clear that you cannot always be sure that an incoming message is coming from the advertised user. In a purely social exchange identity becomes established by shared knowledge exchanges but if the exchange is business related without any corroborating authentication data then additional checks should be made before executing financial instructions contained in an Instant Message.

4) Peer to Peer Networking

This is the generic description for establishing a connection between two processors over the Internet for the purposes of sharing files or other information. Instant Messaging is a subset of Peer-to-Peer (P2P) Networking, but you are probably aware of other types of clients that can be downloaded and installed for the purposes of sharing mp3 or video files. The most commonly known of these were Napster (before it was closed down) Kazaa, and many other copycat services now appearing.

Apart from the risks to the business of breaching copyright laws resulting from any such exchange of copyrighted files, the installation of such software often expressly includes adware in the End User License Agreement to which the unwitting user ticks his or her agreement. This software is provided by other companies from whom the main P2P provider waives any legal

liability and obtains the customers agreement to that waiver in the EULA. This software periodically checks for new product and client program updates which it will download and install. If these companies decide at some point to include spyware in the update, the user will likely never even know about it unless they regularly conduct spyware scanning.
There are also legitimate uses of file sharing that have been noted within the Investment Banking world. Often during deal negotiations over complex financing arrangements financial models are prepared which must reflect the legal agreements that have been drawn up or vice versa. In this case large and complex files must be exchanged frequently between the two sides as modifications are made. If each side is connected to their home network by VPN connections then file exchange is often achieved by using external IM or P2P services. The risk is that malware (viruses, Trojans, worms etc.) may also be included in the file exchange.

5) Vulnerabilities

In January 2002 a couple of vulnerabilities were announced by AOL relating to their AIM client software versions earlier than version 2001(b)[1, 2]. These were both buffer overflow vulnerabilities in which an appropriately crafted packet, sent over an active AIM session would give the attacker the capability to run code of their choice on the compromised workstation. The remedy to this was to upgrade to version 2001(b) or 5.5.

In December 2003 a similar buffer overflow vulnerability was identified in the yauto.dll file of Yahoo's IM Client version 5.6[4]. This vulnerability was rated by Secunia as Highly Critical. Then in March 2004 Microsoft announced that vulnerability in MSN Messenger could allow an attacker to read any files on the PC hard drive to which the user has read access[5]. Updates to fix the weakness were made available at the same time.

In August 2004 another vulnerability was caused by a boundary error within the handling of 'Away' messages by the AIM client and could be exploited to cause a buffer overflow by supplying an overly long 'Away' message" of about 1,024 bytes. Once executed the hacker could redirect the client PC to a website from which more code could be downloaded and installed.

There are numerous other vulnerabilities that have been documented in all of the major IM Clients [3]. In this respect, IM clients are no different in terms of containing vulnerabilities than any other piece of mass distributed software (even the ones that don't come from Microsoft).

There has been some speculation recently in the computer press that the next big threat could be a blended threat from a worm that exploits an IM client vulnerability. This derives from the fact that unlike most application software, IM clients are up and running with connections listening continuously for traffic from previously approved "Buddies".

If both users are online simultaneously then one client can open up a dialog window on the other client at any time. These connections are usually initiated by the users, but there is no reason why they could not also be initiated by malware, which could send improperly configured packets causing a buffer overrun and loss of control at the other end. This is why it is expected that eventually a worm will be crafted to take advantage of such vulnerabilities in unpatched clients and could spread to all vulnerable clients on the Internet in less than a minute[6].

In the corporate environment these connections usually run through firewalls and browsing proxy servers over ports 80 and 443 which are usually open for internally initiated traffic. Authorized external buddies initiating a session are deemed by the firewall to be responding to a previous outbound packet which was sent out to the IM service when the client started up. The firewall will therefore let such packets straight through to the destination client.

Additionally traffic through these ports is hardly ever scanned for viruses in the way that e-mail traffic is scanned on smtp traffic by anti-virus software running on mail servers. This means that there is only a single layer of defense that will only be as good as the anti-virus software located on the recipient client workstation. It is therefore crucial that client virus definition files are maintained so that they are highly up to date. There is quite wide variability between companies in how quickly these updates and patches are rolled out.

Having identified and reviewed the risks of Instant Messaging, how then can they be controlled?

Section Two - Control of Instant Messaging

Regulatory risk:

From the perspective of the Banking and Securities industry, the biggest risk to be addressed is the regulatory risk of failing to log and monitor all IM's according to SEC 17a-4[7]. For this purpose it is necessary to set up a process that can first of all identify the SEC regulated associates who need to be logged, then identify the subset who are customer facing and need to have their message content monitored and finally identify the staff engaged in investment research, who are not allowed to communicate with their peers the trading side at all. This is often accomplished by denying this group access to any kind of e-mail or Instant Messaging communications software.

Once these groups have been identified it is necessary to block them from all forms of E-mail or Instant Messaging (sometimes referred to as I-Mail or IM) except those authorized forms which are logged and monitored as necessary. Blocking can be achieved by specifying forbidden URL's or IP addresses in a proxy server blocking list. The weakness with this method is that new web mail and IM sites keep springing up like mushrooms and a continuous effort is necessary to keep these lists up to date.

Not surprisingly, this is an area of the market that is best served by specialist vendors, who can have a team of staff continuously scanning for different types of forbidden websites and adding them to different categories of forbidden lists. These types of services are similar to anti-virus services in that updates are electronically transmitted to paying customers on a weekly or more frequent basis. Examples of such vendors are Webwasher (http://www.webwasher.com) and Websense (http://ww2.websense.com/global/en/).

Another method for preventing unauthorized electronic communications from exiting through the browsing proxy servers is to identify the offending packets through a process known as Deep Packet Inspection. In this case packets are inspected as they proceed through the browsing proxy server and their contents compared against the signatures of known IM and web mail formats. This avoids the need for the vendor to maintain a large staff dedicated to identifying new web mail and IM URL's, but it does require a small staff to keep checking for changes to web mail and IM packet structures. One example of such a vendor is Akonix (recently acquired by Webwasher) (http://www.akonix.com).

Once you have selected your blocking list and blocking tool, the next step is to identify an authorized IM Gateway product, through which all IM's will pass. This will make decisions about which IM's get logged, which ones monitored and which ones will have both. These decisions are made by reference to the user category identified in the user classification process and recorded in the blocking list. Examples of such vendors are IM Logic (http://www.imlogic.com) and Facetime (http://www.facetime.com). Hosted services are also available from vendors such as Omnipod (http://www.omnipod.com) to which an encrypted communication channel can be established over the Internet using SSL.

Finally you have to select a logging service for SEC regulated associates and a monitoring service for the subset who are customer facing. In-house installed vendor provided solutions are available (e.g. iLumin's Assentor at: http://www.ilumin.com/products/assentor_enterprise.htm) or external vendor hosted solutions such as those provided by Zantaz (which include IM logging) (See: http://www.zantaz.com/solutions/email_file_archiving/index.php)

Legal Risks:

The legal risk is basically that of the disclosure of customer confidential information to parties not entitled to that information. This would breach GLBA(11) and CA SB1386(12). To this may be added the commercial risk of disclosing confidential or proprietary corporate information which could result in the loss or damage to the company.

In assessing these risks it should be realized that there is less risk of accidental loss of confidential data through Instant Messaging than there is through e-mail. This is because e-mail uses store and forward technology, in which the e-mail data is stored on computer hard drives at various points in its journey from source to destination and may be retained on them for various periods. This leaves a data trail that is also susceptible to subsequent hacking attacks after the message reaches its destination.

IM, by contrast is more ephemeral and consists of an instant (as the name implies) non-stop transmission of the data from source to destination. To capture a complete message requires a sniffer device to be placed very close to the source or destination processor in order to capture all of the packets of a message. This is because the packets may not all take the same route due to dynamic routing. Additionally the interception can only occur at the time of transmission and cannot take place afterwards as messages are not retained anywhere in between.

However, there is a significant risk of disclosure of confidential information if two associates of the same company are discussing company secrets over AIM or any other public IM service. This risk can be reduced if not eliminated if this traffic can be contained entirely within the corporate network. This requirement is met by Enterprise Instant Messaging (EIM) Systems, such as Lotus/IBM's Sametime or Microsoft's Live Communications Server.

EIM has the advantage that as the entire IM infrastructure is contained within the internal network, including the IM servers, an enterprise can encrypt each message session from source to destination. In the days of the disappearing perimeter and the semi-permeable network, this kind of capability is an increasingly valuable control to ensure the confidentiality of corporate data.

One catch to this EIM encryption technology in the Banking and Securities industry is that it has to be configured in such a way that those messages exchanged by SEC regulated associates need to be logged and monitored unencrypted, otherwise they will present significant encryption key management issues each time the encryption key is changed. There are a number of solutions to this requirement including sending the clear text message through an IPSec or similar tunnel to the logging and monitoring servers.

Additionally, for messages which are to be exchanged within industry sub-groups, hybrid Community networks are now appearing which can be used to exchange IM's and e-mail over a semi-private network. Examples in the Banking and Securities industry are provided by Instant Bloomberg and Reuters Messaging. Other community IM networks are being developed for use by commodity traders, FX and fixed-income dealers and other sub groups within the Banking and Securities industry.

These community IM services have the advantage that additional security is provided by the fact that although encryption may not always be used, these are private networks which are only accessible to subscribing members.

Finally, if there is a genuine business requirement to communicate with customers, vendors or other external parties using an external Instant Messaging service, then all users must clearly understand that messages are normally sent in clear text and may be intercepted and read by others, particularly those providing the IM Service.

In the experience of this author, some 80% of external customers who demanded access to their brokers using IM services used AOL's AIM service and did not want to change. Another 10-15% used Yahoo and some 5% used Microsoft's MSN or Windows Messenger service.

The main IM Service Providers did experiment with offering encryption over the last couple of years in their Business Messenger products but this feature foundered over the issue of customer acceptability and support. For encryption to work you need to communicate with a client at the customer end which has the capability to perform the necessary encryption and decryption.

This poses questions relating to who bears the cost and provides the support for these customers, not to mention customer acceptability and liability issues. Eventually these challenges proved insurmountable and the options were withdrawn. AOL has now folded its Enterprise service into the IM Logic Gateway, Yahoo has withdrawn the option completely and Microsoft is folding its Enterprise IM service into Live Communication Server.

Microsoft's LCS product is the only one which will allow encrypted IM sessions between an LCS Server and Windows Messenger clients versions 5.1 or later. However, persuading customers to change their Buddy name and adopt a new service is a challenge and ultimately customer focused businesses still have to follow their customers wishes, so we are probably stuck with unencrypted Instant Message services for some time to come.

One additional legal risk that has been identified arises from the End User License Agreements (EULA) to which users are required to tick the "I Agree" box before the client software will be downloaded. Most of these EULA's specifically state that the user agrees not to use these clients for business purposes. Having discussed this at length with the vendors concerned at an RSA Conference, I was able to determine that the reason for inserting these clauses was not to be able to sue companies who chose to breach this term. The purpose was to protect the IM service providers from being sued for any losses or damage incurred by businesses due to a failure of the application or of their network services.

3) <u>Authentication & Presence Management risk:</u>

Of these two risks, the lack of adequate authentication controls is probably the most serious risk for any Bank or Securities house. If you cannot be sure that the buddy with whom you are communicating really is that person, then how confident are you in taking financial instructions?

In reality this issue has been significantly mitigated by the introduction of Enterprise IM services such as Sametime and Microsoft's LCS which restrict their audience to internal corporate users and authenticate by reference to an entity's user LDAP such as Active Directory. It also means that authentication credentials are usually sent over the internal network encrypted and do not ever go out over the Internet.

For IM communications with associates in other Banks and securities houses Community IM services will accomplish almost the same level of security. It is only when unencrypted external IM services are used (generally to communicate with customers) that the same level of security is not achieved. This is because customers have only ever authenticated themselves to their IM freeware provider (usually AOL) database. As was noted earlier, there are limits on how much security can be placed around database financed by advertising revenue.

The answer to both the security issue and the authentication issue for external clients is without doubt going to be found in web based IM solutions in which clients will be directed to a corporate website which authenticates the customer against a secure database over an SSL secured communication session. This has the advantage that additional client software can be avoided together with all the customer installation and support issues and costs. This would be no great loss to the free IM services since they were never designed to be used for business purposes as we have already seen from the EULAs.
Presence management is much less of a security issue and more of a business issue. It is related to the current ability of individuals to configure their clients to show their presence or not, as the mood takes them. Given the fact that EIM has been rolled out centrally by management as a productivity enhancing tool, it will not work very effectively if half of the users are permanently “out to lunch” or “away from their computer”. For such corporate services to be effective it makes more sense to take this ability away from the clients and centralize them at the server level or controlled by group policy objects.

With regard to external IM services announcing their users presence to established buddies as soon as they log on, to the extent that there is a business requirement for these services then users should not be allowed to configure this aspect of their clients otherwise their lack of availability eliminates the original business justification of being available to customers. However, once customers have been migrated to corporate web based IM then control over this area passes back to the business.

4) Peer to Peer Networking and file transfer risks

Although file transfer functions may be carried out with IM clients and may thus be considered a subset of IM, IM itself is really a subset of P2P networking. However, both issues can be dealt with by installing a blocking product (as discussed above) on the proxy servers which will stop all of this traffic. It is then possible to install an enabling gateway product (also discussed above) which will allow specific authorized IM services only (such as text chat) through to the Internet.

However, this protection will only be effective if the blocking and enabling solution is applied to all internal network users, otherwise business units still run the risk of losing confidential data outbound and importing malware of various kinds inbound. Files imported over ports 80, 443 and others are generally not scanned for malware due to the latency effect on browsing traffic. Within Banks and Securities houses many trading applications require continuously updated market data flows from the internet whose value will be severely degraded by the introduction of even sub-second latency delays.

The solution to this, of course, is to import these market data feeds via dedicated lines through a completely separate and dedicated market data feed firewall and proxy gateway, but this can be an expensive proposition which will not be cost effective for smaller organizations. Also, in order to accommodate the requirements of Investment Banking teams who need to exchange files during deal negotiations the best solution is to enable file sharing for specified individuals through the enabling gateway. Needless to say anti-virus software on all of the individuals workstations needs to be fully updated when using this solution.

Some additional protection against malware has recently been provided by recent legislation in California (The Consumer Protection Against Spyware Act) and Washington (HB 1012) both of which ban spyware and penalize suppliers of such software. The US House of Representatives has just approved a similar bill (H.R. 29) on March 9th for the whole country with much larger penalties[13].

5) Vulnerability risks

Once again, the main risk relating to vulnerabilities relates to external IM facing clients, rather than Enterprise IM services. Given the fact that nearly all of these clients and services are supplied as Freeware, users must realize that the "vendors" or "Service Providers" are under no obligation to support these products or the businesses that rely upon them. There is no Service Level Agreement in place at all. Users have to agree to this as one of the terms in the EULA but rarely read these clauses and fewer understand the implications.

This means that users (or their IT support groups) are under an obligation to support and control these products themselves. So when IM product vulnerabilities are announced, users had better have this support function adequately resourced to provide a quick turnaround on the necessary patching and testing activities involved. This means that somebody within the IT support group needs to be tasked with monitoring the IM Service Provider websites and other sections of the IT press to identify these vulnerabilities as soon as they are announced and then to react swiftly.

A properly configured enabling gateway can help in this regard as it can be set to allow access only to the latest (or patched) versions of the IM clients and block any others. The first reactions to a vulnerability announcement should include:

- Find out when and from where the patch will be made available. This should be from the IM Service Provider's website.
- Download, scan and test the patch.
- Load the patch onto an intranet server from which it can be accessed by internal users.
- Communicate with users to let them know from where and how to download and install the patch. Specify a date after which the old version will be blocked.
- Finally block the old version by specifying that as a disallowed version on the IM enabling gateway.

Conclusion

As with all other types of Internet enabled services, there are risks and rewards in using Instant Messaging. In the Banking and Securities industry the rewards were quickly associated with the "Instant" part of the messaging service by those business units where time is of the essence in executing transactions. These are the lines of business associated mainly with exchange traded products relating to markets in equities, bonds and other fixed income products, foreign exchange products, commodities and derivative products.

Other types of P2P services, such as file sharing, are of great value between teams of negotiators conducting complex investment banking deals in which large files need to be exchanged between various parties during deal negotiations.

For this reason simply blocking all IM or P2P services would place these businesses at a competitive disadvantage in the marketplace. The preferred solution is to allow properly controlled use of these services. This is best achieved by blocking all of these services at the proxy servers using a blocking product and then to selectively allow properly controlled and authorized IM and P2P services to take place through an IM enabling gateway.

References

[1] **First AIM Vulnerability:**

AOL Inc: Online Safety/Security FAQ: http://www.aim.com/help_faq/security/faq.adp?aolp=

Hulme, George V. AOL Warns Of Another Instant Message Vulnerability Jan. 15, 2002 Information Week Magazine: http://www.informationweek.com/story/IWK20020115S0002

[2] **Second AIM Vulnerability:**

Graeme Wearden, and Dawn Kawamoto, CNET News.com ZDNet News: August 10, 2004: http://netscape.com.com/2100-1009_22-5303636.html

[3] **Other AIM Vulnerabilities:**

Internet Security.com: http://www.all-internet-security.com/aol_vulnerability_messenger.html

[4] **Yahoo IM Vulnerability:**

Roberts, Paul IDC News Service Article in Computer Weekly December 2003: http://www.computerweekly.com/Article127018.htm

[5] **MSN Messenger Vulnerability:**

Microsoft Technet March 2004:http://www.microsoft.com/technet/security/Bulletin/MS04-10.mspx

[6] **The next big threat:**

Metz, Cade PCMAG.COM June 2004: http://www.pcmag.com/article2/0,1759,1616266,00.asp

[7] **SEC Regulation 17a-4:**

U.S. Securities and Exchange Commission: http://www.sec.gov/rules/final/34-44992.htm (See Section V – Rule 17a-4)

U.S. Government Printing Office: PDF file of SEC 17a-4(b)(4) containing record retention requirement:

http://a257.g.akamaitech.net/7/257/2422/12feb20041500/edocket.access.gpo.gov/cfr_2004/aprqtr/17cfr240.17a-4.htm

[8] **NASD Rule 3010:**

NASD: http://nasd.complinet.com/nasd/display/display.html?rbid=1189&record_id=1159001315

[9] **Fines for breaching SEC 17a-4:**

U.S. Securities and Exchange Commission: http://www.sec.gov/news/press/2002-173.htm
http://www.sec.gov/news/press/2004-103.htm
John Mark Ministries May 2002 : http://jmm.aaa.net.au/articles/1285.htm

[10] Following the expansion of some IM clients to include anti-spyware code, it is now necessary to have System Administrator access rights when installing these clients in order to add the programs to the registry.

[11] **Gramm Leach Bliley Act:**

Senate Banking Committee November 1999: http://banking.senate.gov/conf/confrpt.htm

[12] **CA SB 1386:**

California State Senate February 2002:

http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

[13] **H.R. 29:**

Library of Congress; Thomas Jefferson database via govtrack.us:

http://www.govtrack.us/congress/bill.xpd?bill=h109-29

Tech Law Journal; March 9th 2005:
http://www.techlawjournal.com/topstories/2005/20050309.asp