
Interactive Media Strategies White Paper

Risk Management for Instant Messaging Series

Part 3: What Your Business Should Know about the Federal Rules of Civil Procedure

Paul Ritter
Vice President – Research
Interactive Media Strategies
May 2007

InterActive
Media Strategies

Sponsored by

Akonix[®] 
IM in CONTROL

Table of Contents

I. Executive Summary	3
Overview - Federal Rules of Civil Procedure.....	3
<i>Why the Rules Were Enacted</i>	<i>4</i>
<i>Who is Impacted by the New Rules.....</i>	<i>4</i>
<i>How May Companies be Impacted.....</i>	<i>4</i>
<i>How are Instant Messages Involved.....</i>	<i>5</i>
II. FRCP and the Implications for Businesses	6
<i>Business Use of IM is Increasing</i>	<i>6</i>
<i>With Increased IM Use Comes Increased Risk.....</i>	<i>6</i>
III. Steps Businesses Should Take	8
Procedural Controls.....	8
Technological Controls.....	9
Administrative Controls	10
On-Going Audits.....	10
V. Recommendations for Addressing FRCP Issues	11
<i>Understand the implications of the FRCP</i>	<i>11</i>
<i>Conduct an Audit of IM Use</i>	<i>11</i>
<i>Establish Explicit Policies Governing Retention of Communication Records.....</i>	<i>11</i>
<i>Implement Technology to Ensure Established Policies can be Enforced.....</i>	<i>11</i>
About Akonix Systems, Inc.	12

Abstract: This white paper, published by Interactive Media Strategies with sponsorship by Akonix Systems, examines how businesses should be taking steps to comply with the new Rules of Civil Procedure and discusses the need to manage, archive and retrieve instant messages.

To view an on-demand video webcast on the subjects addressed in this white paper, along with up-to-date information on threats, viruses, and spyware, please visit:

<http://www.Akonix.com/RiskMgmtforIM>

Important Note: This white paper is not intended to provide, and should not be relied upon for legal advice for any organization. It is intended to provide general information pertaining to a variety of regulations that govern the use and retention requirements pertaining to instant messaging and other communications. Any organization covered by regulations discussed herein, or any other compliance requirements should seek professional advice and counsel on strategies, procedures and technologies that may be required.

I. Executive Summary

This white paper is the third in a multi-part series of research reports by Interactive Media Strategies sponsored by Akonix Systems, and is accompanied by an on-demand webcast that includes a video presentation of information and related to the content in this report. The primary focus for this series is the importance for all organizations to examine the range of risks, compliance issues and organizational impact that the use of instant messaging can have and the steps that can be taken to manage the risks effectively.

In Part Two of this series, we examined a wide array of compliance regulations that companies face from state and federal agencies regarding the use of instant messaging as a communications medium. We touched briefly on the new regulations that had just taken effect called the Federal Rules of Civil Procedure. Since the potential impact of these new rules can be significant, and because they can affect virtually any size company in any industry, we have developed this report and the accompanying webcasts to help provide a detailed examination on the new rules and what companies should know in order to better prepare themselves for dealing with them.

Overview - Federal Rules of Civil Procedure

The new Federal Rules of Civil Procedure, which took effect on December 1, 2006, outline requirements for companies to find and produce relevant materials, documents and electronic communications related to court proceedings in Federal cases.

The impact on companies that use communications technology such as instant messaging will be significant, and it is important for organizations to understand the key elements of the new rules and to institute appropriate measures to control their risks and minimize the problems that can arise if involved in a Federal case. Some of the pertinent regulations are discussed below:

Rule 26(a)1 stipulates, *“A party must, without awaiting a discovery request, provide to other parties:*

(A) the name and, if known, the address and telephone number of each individual likely to have discoverable information that the disclosing party may use to support its claims or defenses, unless solely for impeachment, identifying the subjects of the information;

(B) a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment;

Rule 34(a) specifies, *“Any party may serve on any other party a request*

(1) to produce and permit the party making the request, or someone acting on the requestor’s behalf, to inspect, copy, test, or sample any designated documents or electronically stored information . . .” or

(2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b).

And 34(b) further states, *“The party upon whom the request is served shall serve a written response within 30 days after the service of the request.”*

At their core, the relevant aspects of the FRCP place several key requirements on businesses:

- Organizations need to know what types of communications employees are engaging in and how and where electronic records of such communications are stored.
- They should be prepared to locate and provide others any information covered by the FRCP within a specified time frame without waiting for a discovery request.
- Companies should understand that they cannot use an excuse of undue burden or costs for ensuring systems are in place for providing access to communications records.
- Organizations must face the music now and take proactive steps to put systems, policies and procedures in place to address the requirements of the FRCP.

Yes, this will place a significant burden on many, perhaps millions of businesses in order to comply. But, taking prudent measures to address the new requirements now will head off serious problems in the future. Furthermore, as we discuss in this report, instituting control measures designed for addressing FRCP issues will have enormous benefit for many other potential problems organizations are likely to face with regard to IM communications as well.

Why the Rules Were Enacted

The rules were enacted as a result of a confluence of incidents involving federal court cases where materials relevant to the proceedings were not made available (either not timely or not at all) to the other parties involved in the discovery process. One of the more highly publicized episodes was that involving then Vice President Al Gore whose fundraising activities were being examined in early 2000. At hearings where requests were made for access to e-mail records of the Vice President, the White House Counsel stated it would likely take as long as six months for the process of searching, retrieving and delivering the electronic communications.

Lawmakers determined that changes were needed that would compel parties involved in Federal cases to produce relevant materials, documents and communications in a timely manner.

Who is Impacted by the New Rules

Almost any organization can face the need to comply with the requirements of the FRCP and the unfortunate consequences of having to search, find and produce “*any designated documents or electronically stored information.*” In today’s world, electronically stored information covers so many different file types, communications records, and other documents or materials that it would be virtually impossible to comply with FRCP requirements unless a progression of proactive measures and technology solutions have been implemented. We’ll address this important issue in just a bit.

How May Companies be Impacted

Companies may find themselves having to comply with FRCP issues in a number of different ways. A lawsuit involving parties and issues that cross state lines may trigger FRCP requirements for discovery, retrieval of documents, etc. Other FRCP triggers are involvement in violations of federal compliance statutes such as Sarbanes-Oxley, HIPPA and other regulations.

(Readers are encouraged to download a copy of [Part Two in this series on Risk Management of Instant Messaging](#), by visiting the Akonix [website](#).)

The potential risk for non-compliance can be significant. Companies that fail to comply with discovery requests in a timely manner can face stiff penalties and fines. In the case *Serra Chevrolet vs General Motors*, the court levied fines amounting to \$50,000 per day. Although the amount of the fine was reduced significantly at a later date, the court placed a number of fairly onerous sanctions on the firm that had failed to comply with the discovery requests as required.

Although the rules pertain to federal court proceedings, companies should keep in mind two key points. First, state courts often tend to follow rules used in Federal court, and second, the requirement to produce copies of relevant materials may happen well into the future, or never, but without a crystal ball, all firms must anticipate the potential need to comply with the new regulations now, or risk the consequences later.

An important note from a risk management perspective is that documents deleted or purged “in the course of regular business” are not covered by the rules. Meaning, that a company can and should implement strict policies governing the storage, archiving and deletion of all sorts of files, documents and materials related to its business, whether governed by particular statute or not.

If a company can clearly show that it has a regular and well-established procedure for deleting certain materials at a specified time interval, such as one year for deleting instant messages or e-mails not covered by other regulations, then those electronic communications will generally not be included in the requirements to produce materials for a federal court proceeding within 30 days. (However, if the IMs or e-mails have not been deleted as per established policy, the company will likely have to provide them as a result!)

It is absolutely essential that a firm can prove that it had established and enforced its procedures well in advance of any request by a court to produce documents or communications relevant to a particular case.

How are Instant Messages Involved

Instant messages are now almost universally viewed as electronic communications in the same way as e-mail messages. The problem for organizations, however, is that while it is has been feasible to control, manage, archive and retrieve e-mail, instant messages pose a much more difficult challenge.

Due to the availability of a wide variety of software solutions, management technologies and hosted services that have been available for a decade or more, a vast majority of firms in our research have already implemented some form of technology for managing e-mail. Instant messaging poses a more difficult test in that it is often used on a totally unsanctioned and unmanaged basis.

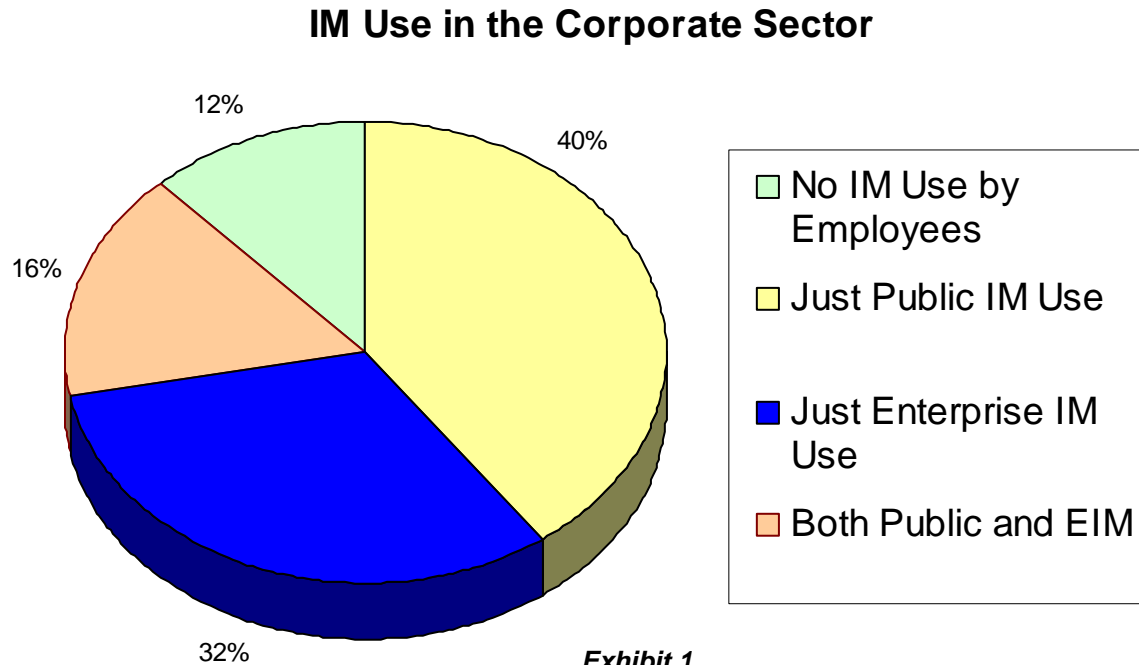
In surveys conducted by Interactive Media Strategies, many firms’ IT staff report that they do not have IM use taking place inside their organizations or that they actively block IM use altogether. The reality is that a majority of these firms are wrong on both counts. Employees will often utilize the public IM networks surreptitiously, even when their use is specifically prohibited by organization policy.

Furthermore, most firms that try to block IM use by employees discover that it is ineffective as a technology fix (since IM is an open port-seeking communications application) and a misguided business strategy (with many firms interviewed reporting outright revolts by employees who lose their access to IM.) The reality is that IM is being used extensively by a vast majority of companies and it is crucial to take steps to control it use and have a system in place to manage, store and retrieve any instant messages being sent or received by employees.

II. FRCP and the Implications for Businesses

Business Use of IM is Increasing

The use of instant messaging has exploded in the business sector over the past three years. According to research conducted by Interactive Media Strategies, more than 88% of businesses have some form of IM communications taking place inside the firm. (See Exhibit 1)



Source: Enterprise Communications Research Study of 300 IT Professionals conducted by Interactive Media Strategies; Q1 2007.

As stated before, many IT professionals, even the most senior of members of an organization, often believe no form of IM is taking place, when the reality is that employees have been using public network IM surreptitiously for many years. So the true extent of IM use in the business sector is likely even higher than reported in surveys.

So it is clear that IM use is becoming widespread, and with 40% of firms surveyed reporting that they allow employees to use the public IM networks, the potential for misuse is definitely present. Furthermore, since the majority of public IM use is completely unmanaged, untracked and not archived, the ability for those firms to take proactive steps to produce relevant communications for federal court cases as required by the FRCP is very limited.

With Increased IM Use Comes Increased Risk

One advantage of implementing technology solutions for addressing FRCP requirements is that the same solutions that provide granular control over the storage, archiving and retrieval of electronic communications such as instant messages can help firms to address a wider range of risks and threats such as spyware, malware and liability from IM use. Since control solutions for IM have been deployed to date at far fewer companies than similar solutions for e-mail, companies that have unmanaged IM use taking place face a plethora of threats. These threats are not simply theoretical – many firms have experienced problems arising from IM use that have negatively impacted the company network or the organization as a whole.

In a recent survey of 300 senior IT professionals conducted by Interactive Media Strategies in the first quarter of 2007, we analyzed the extent to which organizations have experienced

security breaches, identity theft and other security threats to their corporate networks. Although security breaches and other threats from e-mail are more widely seen, the data suggest that security issues from IM are greater than most would suspect. More than one-fourth of IT professionals surveyed report some sort of security breach into their corporate network as a result of instant messaging use. (See Exhibit 2)

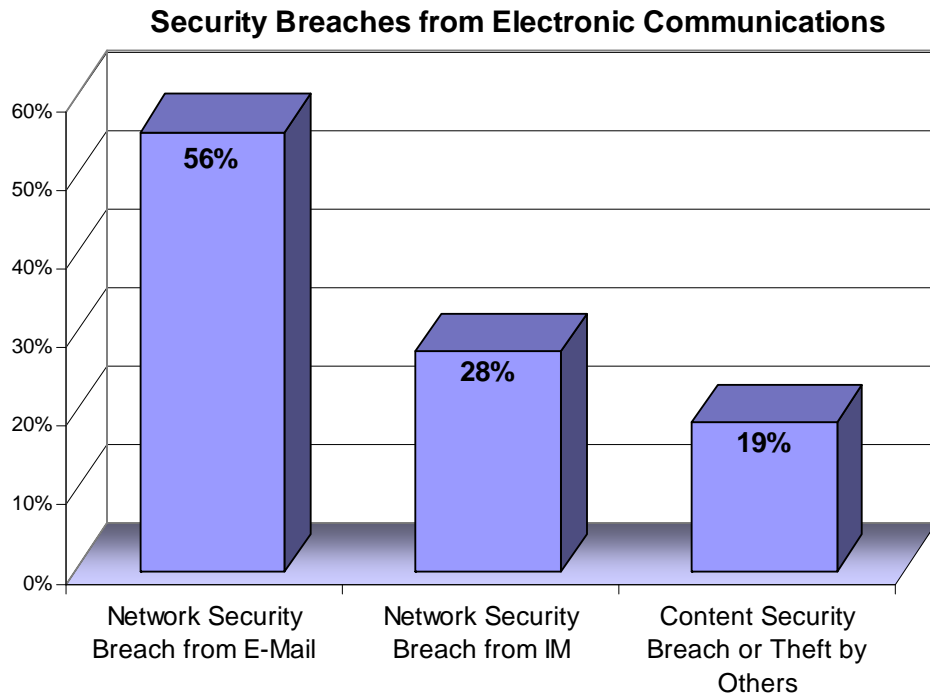


Exhibit 2

Source: Enterprise Communications Research Study of 300 IT Professionals conducted by Interactive Media Strategies; Q1 2007.

These data reveal deeper insight than what is seen on the surface. Since the use of e-mail is completely ubiquitous, reaching levels approaching 100% in companies of all sizes surveyed in the research study, the 56% of respondents reporting security breaches from e-mail is truly representative of the corporate sector as a whole. The 28% of respondents citing security breaches from IM is indicative of a growing problem for organizations, including those using the public IM networks as well as those using Enterprise IM (EIM).

It is interesting to note that in the survey of IT professionals, a higher percentage of firms using just EIM (39%) reported network security breaches from instant messaging use than firms using just the public IM systems (36%). The point here is that even commercial-grade IM systems are exposed to threats from viruses, worms, spyware and malware unless appropriate control measures and management solutions are deployed.

The very systems that allow firms to guard against security breaches are also able to provide the controls necessary to comply with the requirements of the FRCP. Instant messages from all types of IM clients, and across all kinds of IM systems and networks should be effectively managed, strictly tracked, and appropriately archived for later retrieval.

The control measures that firms can and should follow for protecting against IM threats are ideally suited for allowing firms the ability to comply with the Federal Rules of Civil Procedure, if and when necessary.

III. Steps Businesses Should Take

To manage the potential risks associated with FRCP effectively, organizations should implement a set of control measures that include procedural controls, technological solutions and administrative measures.

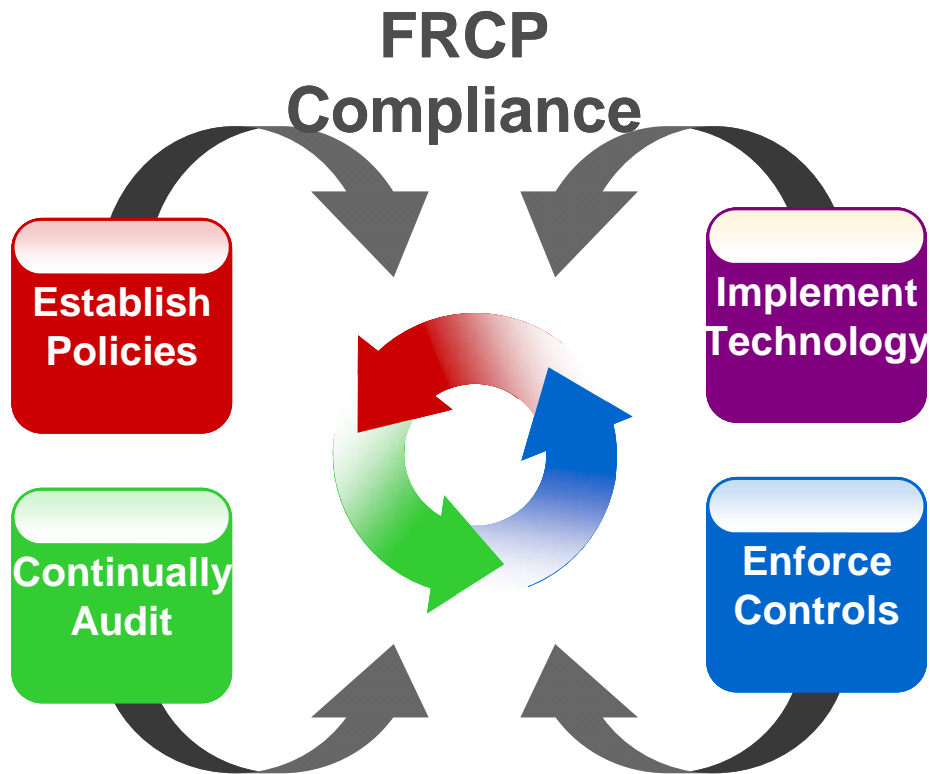


Exhibit 3

Procedural Controls

Companies should establish clear and consistent policies for the use of both email and instant messaging in the workplace. As most firms have existing email and internet use policies, it is not necessary to reinvent the wheel for instant messaging communication policies. In fact, it is recommended that similar policies for both forms of technology be instituted to help ensure consistency. However, there are inherent differences in how e-mail is used by most firms and how instant messaging is used as a communications tool, so an approach to establishing appropriate policies and procedures should be deployed to accommodate these differences.

For example, between the two forms of communication, e-mail is more generally used for formal internal and external business communications and IM is frequently used for short, informal communications of a more immediate nature (generally speaking). Firms establishing policies should take this into account. Many firms establish a shorter retention period for keeping instant messages (that are not covered by other regulatory requirements) than they do for e-mail. It is extremely important to note however, that all organizations should seek appropriate counsel when establishing procedures for record retention and destruction to ensure they comply with all relevant recordkeeping regulations. Sarbanes-Oxley, HIPAA, SEC Rule 17a-4, and many other statutes clearly outline the timing requirements for electronic records such as IM and e-mail.

Section 802 in the Sarbanes-Oxley act for example (Criminal Penalties for Altering Documents) imposes severe penalties and fines for altering, destroying, concealing, or falsifying records, documents or other materials with the intent to obstruct, impede or influence a legal investigation.

It is this fine line that all organizations must walk then – establishing retention procedures that are too short or not in keeping with regulatory requirements can place the firm in legal jeopardy, and having no formal policies, or just keeping records for indiscriminate or overly lengthy time periods exposes the firm to unnecessary risks that could otherwise be avoided.

So how is a firm supposed to establish and comply with the policies and procedures it establishes with regard to retention of electronic records such as instant messaging and e-mail. The answer is technology. Firms need a technology solution that permits a firm to establish very granular controls over who can use what IM client or network, when, what for, how, and where, and one that can, most importantly, capture, archive and retrieve messages according to a wide variety of parameters.

Technological Controls

The ability to intercept IM traffic, inspect for destination and source, review for content, and archive for compliance is something that technology vendors such as Akonix, with a focus on instant messaging, security, and compliance are best suited for. Without proper technology, a firm simply cannot implement all the necessary control measures to comply with the FRCP and to manage the risks associated with IM use by employees.

The diagram shown in Exhibit 4 depicts the manner in which instant messaging use by employees across any of the public networks of AOL, MSN, Yahoo, ICQ and Google can be logged, archived and reported on by a centralized management solution behind the firewall. Messages inbound and outbound can be managed via this system.

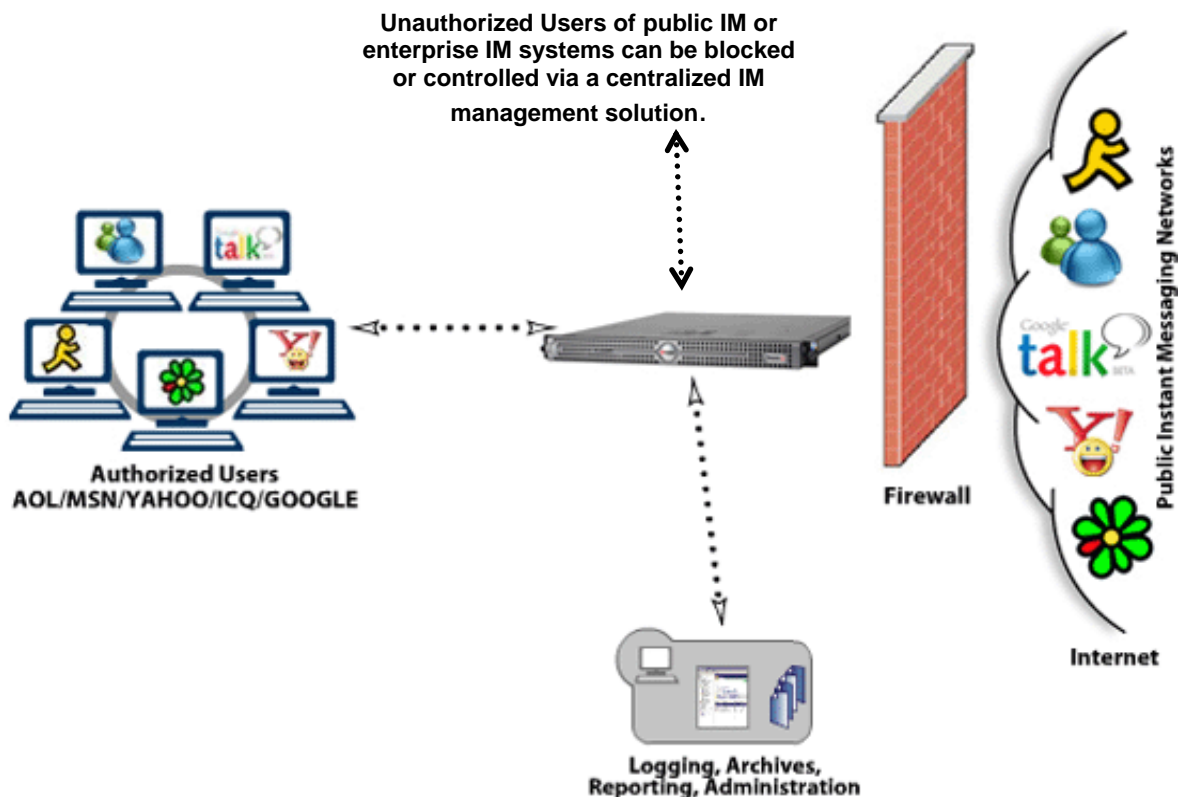


Exhibit 4

Source: Akonix Systems, Inc.

Administrative Controls

Once policies and procedures have been established and an appropriate technology solution for managing, archiving and retrieving IMs has been deployed, the work does not stop there. Administrative measures are needed to enforce the formal policies and procedures that are established, and to continually audit the program to ensure it is functioning as it should at all times.

Employees must be informed, and in most cases formally trained on the policies and procedures that have been established pertaining to the use of electronic communications. Most employees are fully aware that their e-mail communications are recorded and retained on the company's servers. Many, perhaps a majority of employees, are unaware that their IM communications can be logged, monitored and archived, even when using the public networks. Many people using IM do so without a care or concern about what they are typing, how it might be interpreted or misinterpreted by others, and how it might come back to haunt them in the future.

As has been seen in the past year or so with congressional personnel, Fortune 500 executives and leading political figures, the use of instant messaging is all too often viewed as a form of informal, personal communications that the senders believe will never be seen by any others once the message has been sent and the IM session has ended. It is not only a concern for firms to worry about the potential for IMs to be the focus of a federal court case where the Federal Rules of Civil Procedure come into play, but that instant messaging can and has been used in ways that put the organization at risk, not to mention the individuals sending the messages. Media reports are rife with accounts where IM has been used for purposes of sexual harassment, corporate espionage, and other illegal or immoral activities that caused serious harm to others and to the organizations from which the communications emanated.

Organizations must realize that they need to educate everyone, from the board of directors and senior management down to the most entry level employees on the proper use of all forms of electronic communications, including policies on the logging, archiving, retrieval and auditing of those communications. As with e-mail, employees should be informed that all IM communications are considered property of the company and can be monitored, stored, retrieved and destroyed as the company deems appropriate.

On-Going Audits

As with any set of policies and procedures, enduring success and effectiveness depends on rigorous audits being performed on an on-going basis. Audits of IM communications can and should be done on both a regular and on a random, unannounced basis.

First, it is recommended that firms audit the process of logging and archiving electronic communications to ensure that all messages are being logged appropriately by the system. Also, checks should be made to ensure that inadvertent or purposeful efforts have not been made to delete communications records from servers or archiving systems outside of the established policies for retention periods.

Audits should also be performed on the content of IM communications to ensure that no inappropriate use is taking place and that no messages are being sent that can place the company at risk. Steps should immediately be taken to address violations of established policy or breaches in the requirements for retaining or destroying records. Auditing should be done on the procedures, the training, the content and the systems used by the firm to comply with the FRCP as well as all other regulatory requirements.

V. Recommendations for Addressing FRCP Issues

IM use in the corporate sector is growing rapidly and will continue to grow well into the future. Likewise, state and federal regulations governing all forms of communication will certainly not decrease. The combination of both factors make it essential that companies take proactive measures for minimizing the risks associated with the ever increasing threats that non-compliance can bring.

Fortunately, there are several key strategies firms can pursue to enhance their risk management programs when it comes to instant messaging and FRCP compliance.

Understand the implications of the FRCP

It is important that key personnel involved in the efforts to comply with FRCP fully understand the aspects of the rules pertaining to the type of electronic communications that are likely to be considered relevant in such cases, and how and when such records must be produced as part of the discovery process.

Conduct an Audit of IM Use

The extent to which IM is currently being used by employees within a firm can drastically impact the degree of exposure an organization faces. Many IT departments believe that little to no IM use is taking place inside their firms. Others take proactive steps to block its use. However, it should be noted that all of the public IM networks change their protocols and firewall ports on a regular yet random basis, explicitly to outmaneuver the IT departments that seek to block them altogether. Audits can include informal inquiries of many different employees across different departments, but they are most effective when these inquiries are supplemented by technology that can identify, track and report on what type of IM clients in use, what public networks are involved, what types of content, URLs, attachments, etc. are being sent and received. Akonix is one of the leading providers of such technologies.

Establish Explicit Policies Governing Retention of Communication Records

Since the policies and procedures that a firm establishes must be appropriate across a wide range of regulatory requirements beyond the FRCP, it is essential that the firm take steps to appropriately classify different types of records and communications according to their purpose, relevance and retention periods. It is very important to clearly outline the rationale for establishing time periods for retention and destruction of electronic messages.

Implement Technology to Ensure Established Policies can be Enforced

It is important that companies put technology into place to identify instant messaging traffic and archive it as business records. Only a certified provider of IM management can legally redirect IM network traffic for inspection, archival, and security on the three major public IM networks of AOL, MSN and Yahoo! Whether public IM networks or used or not, it is essential that firms have technology in place that can automatically log and archive all IMs and enforce the policies and procedures that have been established.

Audit, Audit, Audit

In order to ensure the on-going effectiveness of the policies, procedures, training and technological controls that have been established, it is essential to continually audit all aspects of the use, logging, retention, retrieval and destruction of instant messages and electronic communications. Documentation that policies are being strictly followed and technology systems are working effectively will go a long way in managing the risks a firm faces and minimizing the liabilities that may arise from non-compliance with FCRP and other regulations.

About Akonix Systems, Inc.

Akonix is the most deployed IM security product in the world, enabling companies of all sizes to install productive, enterprise-wide IM that is secure, compliant and managed.



Over 1.9 million people around the world are protected by Akonix products. With more than 20 patent applications, Akonix's 360° Security provides the industry's only automatically-updated protection to block viruses and malware for both enterprise and public IM systems. Akonix is a Microsoft Gold Certified Partner, an IBM Business Partner and an HP Business Partner. The company is licensed and certified by America Online®, Microsoft and Yahoo! to inspect and archive IM traffic. Furthermore, Akonix has developed business alliances and integrated its technology with leading enterprise IM platforms, including Microsoft, Reuters, IBM, Jabber, Inc., Parlano, and Bloomberg, and message archiving products from EMC, HP, ZANTAZ and Intradyn.

An IM industry first, the Akonix IM Security Center (www.imsecuritycenter.com) provides real-time information about worms, viruses and other vulnerabilities that target IM and P2P networks. The company issues monthly and quarterly IM threat watch reports to track key trends and vulnerabilities.

For further information on the company, please visit www.akonix.com. To see related white papers and webcasts, visit www.akonix.com/RiskMgmtforIM

About The Author and Interactive Media Strategies



Paul Ritter is Vice President for Collaboration Research at Interactive Media Strategies. He is a veteran of the research industry, having worked for leading firms such as the Yankee Group and Wainhouse Research. He is the author of more than 100 research publications and has been featured in more than thirty webcasts, web seminars and industry conferences in his 20+ years of professional experience. He is frequently quoted in the press and media on topics related to instant messaging, real-time collaboration, and webcast technologies.

Prior to his work as a research analyst, he spent more than a decade in risk management consulting, and was the President and Founder of the Center for Risk Management & Safety, and Director of Risk Control Services at Albert Risk Management Consultants.

Interactive Media Strategies provides research and consulting services to help companies involved in the communications, collaboration and media distribution chains to recognize the potential of real-time communications and interactive multimedia. The company conducts extensive research deployment trends, spending plans and integration strategies firms follow for technologies that include instant messaging, collaboration tools and multimedia solutions such as webcasting, web conferencing and video conferencing. Interactive Media Strategies provides quantifiable analysis and market research of how business users, IT professionals and corporate executives perceive, use and deploy communications applications delivered via connected networks. For more information on Interactive Media Strategies, please contact:

Paul Ritter, Vice President – Collaboration Research
(508) 881-7149
ritter@interactivemediastrategies.com