

Realtime  
publishers

"Leading the Conversation"

# The Essentials Series

# IT Compliance Volume II

*sponsored by*

**SECURE**<sup>®</sup>  
COMPUTING

*by Rebecca Herold*

---

# Preventing Data Leakage Through Email and Instant Messaging

by Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI

February 2007

## Incidents Occur Easily and Often

Incidents continue to accumulate and hit the daily headlines. Many of them involve the loss of sensitive information through some type of messaging activity. The losses can have devastating impacts to business.

A large financial organization I once did work for was going through downsizing. They notified their systems administrators 2 weeks in advance of their impending layoff, but allowed them to continue performing their job responsibilities as usual until their last day. Indeed this was not a good idea; 2 weeks following the last day, one of the terminated administrators accessed the internal Web site remotely using the admin ID he was once responsible for, changed the passwords for all the remaining admin IDs, then sent messages to all the other email accounts with a very explicit rant about how horrible the company's security was in addition to posting copies of all email messages on the email server to multiple Internet sites. Although this incident happened several years ago, copies of the email messages still continue to pop up on miscellaneous sites from time to time, much to the embarrassment of the organization, which estimated significant lost customers and associated revenues as a result.



It is very difficult, and usually impossible, to completely recover information once it has been posted on the Internet.


Insiders pose significant threats to organizations. It is particularly easy to leak sensitive company information and secrets along with personally identifiable information (PII) through messaging technologies such as email and instant messaging (IM).

*From the 2005 CERT/Secret Service Insider Threat Study Report*  
[http://www.secretservice.gov/ntac/its\\_report\\_050516.pdf](http://www.secretservice.gov/ntac/its_report_050516.pdf):


*"An application developer, who lost his IT sector job as a result of company downsizing, expressed his displeasure at being laid off just prior to the Christmas holidays by launching a systematic attack on his former employer's computer network. Three weeks following his termination, the insider used the username and password of one of his former coworkers to gain remote access to the network and modify several of the company's web pages, changing text and inserting pornographic images. He also sent each of the company's customers an email message advising that the website had been hacked. Each email message also contained that customer's usernames and passwords for the website. An investigation was initiated, but it failed to identify the insider as the perpetrator. A month and a half later, he again remotely accessed the network, executed a script to reset all network passwords and changed 4,000 pricing records to reflect bogus information. This former employee ultimately was identified as the perpetrator and prosecuted. He was sentenced to serve five months in prison and two years on supervised probation, and ordered to pay \$48,600 restitution to his former employer."*

It is so easy to lose information through messaging paths.

---

 In February 2006 it was widely reported that the names and Social Security numbers of about 27,000 Blue Cross and Blue Shield of Florida current and former employees, vendors, and contractors were sent by a contractor to his home computer in violation of company policies. The contractor had access to a database of identification badge information and transferred it via email to a home computer.

Messaging systems are vulnerable to hacking from outsiders if not configured appropriately and can be purposefully used for sending sensitive data to outside entities and storage areas. There are also many mistakes made that have resulted in inadvertently sending sensitive information to people and/or systems that should not get such information.


 In November 2006, the personal information and Social Security numbers of 561 Virginia Commonwealth University (VCU) students were accidentally included in two attachments in an email sent to 195 students to inform them about their eligibility for scholarships from Phi Kappa Phi, a national honor society. The information included names, Social Security numbers, local and permanent addresses, and grade-point averages. This was the second time in 2006 that VCU had an incident exposing PII; in September, the names, Social Security numbers, and email addresses of about 2100 current and former students had been online for 8 months because of human error.

The growing use of IM within the business enterprise also opens business to a vast array of threats.

## Consider IM Vulnerabilities

IM is increasingly being used within businesses. The implementation and use of IM can create huge vulnerabilities within the enterprise if not implemented appropriately. According to a February 2006 survey of more than 200 U.K. businesses done jointly by Peapod and FaceTime Communications, most organizations are not managing IM and are not protecting their networks from spyware threats that exploit IM vulnerabilities. The survey reported:

- 73 percent of the survey participants had experienced a spyware attack through IM in 2006
- 19 percent of the survey participants could not identify the source of the spyware
- Of 57 percent that had banned IM in the workplace, 70 percent used obsolete, easy-to-defeat, or ignored methods to try and enforce the IM ban

 W32/Rbot-GFL is a spyware worm that spreads through IM and network shares. It can:


- Allow others to access the infected computer
- Steal data
- Download code from the Internet
- Degrade systems security
- Be installed within the registry
- Exploit systems and software vulnerabilities
- Help facilitate Denial of Service (DoS) attacks

Most IM solutions use a centralized infrastructure. Centralized servers must handle capabilities such as routing messages and authentication. Because of the expenses and resources required in building and maintaining these infrastructures, many organizations choose to use outside services such as AOL, Yahoo!, and Microsoft. Each of the IM services typically offers many features. The features offered change quickly, but Table 1 shows what was in place with commonly used IM services at the time this paper was written.

	AIM	Google Talk	ICQ	Jabber	MSN	Skype	Trillian	Yahoo!
Application Sharing					X			
Audio Chat	X	X	X		X	X	X	X
Encryption	X			X		X	X	
File Sharing	X							
File Transfer	X	X	X	X	X	X	X	X
Group Chat	X	X	X	X		X		X
Mobile Messages	X		X	X	X			X
Multi-Network							X	
Text Chat	X	X	X	X	X	X	X	X
Video Chat	X		X		X		X	X
VoIP	X		X	X		X		X
Web Services Integration	X		X		X		X	X
Whiteboard					X			

**Figure 1: IM services and capabilities.**

As you can see from the capabilities listed, each of these services brings with it many, and often unique, vulnerabilities that must be addressed to appropriately reduce the risks of using IM within a business enterprise. Business leaders must address those risks now; IM usage within organizations, both sanctioned use and use against policy requirements, is rapidly growing. The exploits for IM vulnerabilities have grown right along with the popularity of IM. The FaceTime Communications and Peapod study mentioned earlier revealed security incidents through IM types of networks were up 2200 percent in 2005 over 2004. These incidents often involve leakage of sensitive corporate information and PII. For example, IM worms can install programs on your enterprise systems that will copy usernames, passwords, credit card numbers, PayPal account details, and other financially useful data.

 The Heartworm worm tricks users into clicking a link to receive a virtual greeting card. When clicked, data-theft malware is downloaded and the worm propagates to the user's IM contacts. The interesting aspect of this worm is that it looks like a hoax. The goal is for the victims to believe that they are victims of a hoax, not an actual malware infection.

---

There are many risks related to data leakage; IM:

- Opens new holes within the network infrastructure through which information can easily and unknowingly leak out, creating privacy and intellectual property loss concerns.
- Creates invisible communications channels that typical information security measures do not address, making it difficult to comply with legal, regulatory, and contractual requirements and exposing the organization to breaches.
- Creates new paths into end-user computers and networks for the stealth distribution of malware such as viruses, worms, spyware, rootkits, and SpIM. Fighting these increasing malware outbreaks, and even just trying to protect against them, can drain business productivity and resources.



Spam over IM (SpIM) typically occurs through a link appearing to come from someone on your buddy list. If the link is clicked, malicious code can be installed on your computer.

Many business leaders direct the IT folks to just block IM. However, in most organizations, simply blocking IM is not an option:

- Every IM network provider has a unique set of IP addresses for client connections. The IP addresses often change without notice, so firewalls and proxies cannot apply blocking policies using the typical black list of IP addresses.
- IM clients use port crawling—the ability to exploit open ports on the firewall. Blocking specific ports for the particular IM application will not work.
- IM protocols are proprietary and constantly change to deliver new and enhanced features. Firewalls, proxies, and most other security technologies within enterprises do not evolve at this pace. Likewise, IT organizations cannot realistically be constantly updating protocol signatures on the firewall to prevent IM use.
- IM connections are synchronous. This is much different from asynchronous Web browsing and email traffic. Firewalls and proxies are not designed to inspect and analyze real-time communication traffic such as IM, so network performance can suffer when trying to configure them to prevent IM.
- In a very short time, large numbers of employees have embraced and become, from their perspective, dependent upon IM communications with business colleagues. Blocking IM will likely result in unhappy employees, many of whom will find ways to bypass the IM blocks, possibly causing more problems.


Instead of curtly declaring no IM use is allowed within the enterprise, business leaders must look at all the issues involved and make a decision that will work best to prevent critical information from being leaked through these pathways while supporting the business benefits IM may provide.

---

## Consider Email Vulnerabilities

Email has been used within organizations for a comparatively long time. It can be very beneficial and support business. However, there are many inherent vulnerabilities with email that organizations must continue to diligently address:


- Email messages are vulnerable to unauthorized access through misconfigured mailservers and end user errors
- Email messages are vulnerable to modification by those intercepting them, and by recipients who make changes within them before forwarding them on
- Email messages are vulnerable to spoofing. Just because an email message looks like it came from someone does not mean it actually did come from the indicated sender
- Email systems are vulnerable to DoS attacks from error or from malicious intent
- Email messages can easily contain PII and other sensitive information that is unsecured and should not be sent outside the organization
- Email messages are vulnerable to user errors, such as incorrect addressing, misdirection, inappropriate forwarding, and the unreliability of the Internet

 The Internet cannot be considered 100% reliable. Just because you send an email message does not mean that it will reach the intended recipient; it could end up being misdirected to inappropriate recipients, or be sidetracked for a significant period of time within one of the relay points along the way.


There are many issues involved with using email for business. A few significant ones include:

- Legal issues, such as potential need for proof of origin, dispatch, and receipt
- Uncontrolled remote user and Internet access to email accounts
- Email sent between organizations by individual members of staff may lead to unauthorized exposure of confidential or sensitive information and a breach of confidentiality, leading to bad publicity and possibly legal action

History demonstrates that organizations are exposed to legal actions for inappropriate use or mistakes made with email.


 Business can be exposed to libel writs as a result of what an employee has written in an email message, even if it was written in jest and intended only for internal distribution.

Organizations must not only ensure the confidentiality of PII but also that confidential corporate information that could impact brand value and share prices is not leaked. U.S. Stock Exchange regulations must be observed, along with federal data protection laws such as the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA). Business leaders must continue to diligently address email vulnerabilities and ensure appropriate use to protect PII, business intellectual property, and the business from regulatory fines and costly legal actions.

 It is not possible to establish a 100% secure email system—there are too many protocols, evolving technologies, and unpredictable human factors. However, business leaders MUST evaluate the involved risks and establish email systems in ways to address and reduce the risks to a level acceptable to the business while being in compliance with legal and regulatory requirements.

## **Policies and Education Are Very Important**

No organization can absolutely prevent unauthorized transfer of data through messaging solutions; trusted users with authorized capabilities will sometimes make mistakes, and some will make conscious decisions that will result in sensitive data leakage and subsequent incidents. The human element is the weakest in the information security equation. This makes the establishment and enforcement of clear and comprehensive policies, along with ongoing education and awareness, so very important.

 Personnel must be given ongoing training and awareness for messaging policies to make the policies effective.

### ***Implement policies, procedures and standards***

There are many policies, procedures, and standards that must be implemented for messaging use within the business environment. Incorporate the following into your policies and practices to specifically help prevent corporate information loss:


- Require encrypted channels for messaging. Doing so will mitigate packet-sniffing attacks and other man-in-the-middle attacks that unscrupulous third parties may try against you.
- Do not send PII within IM communications.
- Block outbound Direct Client Connection (DCC) to help prevent intentional or accidental leakage of files to third parties.
- Use security tools to hide the hostname/IP address from other messaging system users.
- Do not allow personal messages to be sent using the enterprise messaging systems.
- Use spam filters on all types of messaging systems.
- Require emails that must contain sensitive information and PII to be encrypted. Provide a transparent or easy-to-use encryption solution to help ensure employees do this.
- Monitor and log email use to help prevent sensitive information from leaving the enterprise. Check for PII and other sensitive data going out from the enterprise.
- Monitor and log IM use to help catch inappropriate access before intruders can get to sensitive data. Most of the popular IM systems provide the capability to log online conversations with other users. However, this information is stored in a text file on the local workstation. A malicious user who has access to this workstation can retrieve this file and have access to all information that was exchanged during an online conversation. Be sure to implement messaging logging in a centralized location.



---

## **Awareness and Training**

When you have your policies, procedures, and standards established, you must communicate them to personnel; not only once but also through periodic training and ongoing awareness messages. More reports of incidents occurring through mistakes or malicious actions appear all the time. You must educate the individuals using your messaging systems about how to use them correctly to help prevent sensitive business information and PII from being leaked out to criminals, competitors, and the general public.

 You cannot expect personnel to use messaging systems appropriately and successfully protect PII and other sensitive information if you do not tell them, often and in many ways, what appropriate use is and how to secure related information.

Include the following topics and communicate the associated messages—tailored for your business environment—within your awareness and training efforts to specifically address the prevention of data leakage through messaging systems.

## **Social Engineering**

Social engineering is pervasive on IM services. Buddy lists allow users to add contacts that they are familiar with to their lists. The assumption is that if someone contacts you, they have received your name from a friend, when in fact it could have been gained through a simple dictionary attack. Beware of social engineering attempts.

## **Identity Theft**

Identity theft can occur in many ways and puts you and the business at risk. For example, by posing as an employee of an IM service, a malicious user can trick someone into giving information such as usernames, passwords, and credit card information. This information can be used to compromise other systems and services and can lead to theft. Another method of identity theft involves obtaining usernames or passwords through decryption on the local workstation or through a packet capture utility. Programs such as dsniff are able to decrypt passwords for some IM services over a network on the fly. Other utilities, such as Cain and Able, can monitor network activity and decrypt passwords.

## **File Transfers and Messages Spread Malicious Software**

One of the most dangerous security risks for IM and email is the ease with which Trojans, viruses, and other malicious code can be spread. IM in particular is vulnerable to these threats through the file transfer feature. Sending files in this manner creates a direct connection between users, bypassing the centralized network scanning used to provide malware protection. Once these pieces of malware infect a machine, they can spread to other machines, creating massive amounts of network traffic and overloading a network. Depending upon the configuration of IM, it is possible for files to be transferred without your knowledge. This could allow sensitive information to be transferred from your workstation, or a file you have access to on the network, without your permission.



---

## **Worms and File Transfer Through IM Get Around Enterprise Security Devices**

Worms are capable of spreading over IM and typically appear as a uniform resource locator (URL). These messages will usually come from what appears to be someone on your buddy list, so it is more likely that you will click them. Once clicked, the worm will infect your computer and spread to everyone on your buddy list. Some worms and viruses that spread via IM send an infected file to users and are able to avoid being detected by the network antivirus system. Do not click URLs if you did not expect to receive one, even if it looks like it came from one of your buddies.

## **IP Address of Workstation May Be Revealed**

Some IM features, including file transfers, reveal the IP address of the workstation being used. This can allow for unauthorized access and capture of sensitive files and PII on your computer and the enterprise network.

## **Encrypt Messages and Files**

When communicating sensitive information, such as PII and company intellectual property, encrypt your messages and any files attached to them. This applies not only to email but also to IM. And never discuss sensitive information over IM unless the conversation is encrypted and you know for sure who the buddy is you are communicating with.

## **Watch out for SpIM and Offensive Material**

SpIM is becoming quite common and is carried out by automated bots to collect data from IM users' systems. For example, they can copy IM names and send marketing messages to those users. SpIM typically contains URL links that go to sites with malicious code, pornographic material, or other inappropriate or dangerous sites. Do not click on URLs within your IM messages to help prevent being a victim of SpIM. Help prevent unwanted SpIM messages by changing the settings in your IM client to ignore messages from unknown users.

## **Follow Email and IM Compliance**

Know and follow the company's email, IM, and other messaging policies and requirements. If you do not, you will not only put yourself and your job at risk, you can also put the business at risk along with the PII of customers and your fellow coworkers.

## **Don't Trust Unsolicited Instant Messages**

If you receive a suspicious IM, such as a message containing only a URL link with a brief or vague phrase from a friend, verify that your friend, and not an IM bot or virus, sent you the link. Do this by typing something back to the person who sent it asking something such as, "What is this? Why should I go there?" If no one responds, it is likely a bot sent it.

---

## **Use BCC Within Email Messages**

When you send a message to a group of people, consider putting their email addresses within the blind carbon copy (BCC) field. Definitely do this if the members of the group are from different organizations or do not know each other. Not only would putting a large number of email addresses in clear text in the TO field leave the message open for spammers to harvest email addresses, it also protects the privacy of the people to whom you are sending the message. You should not provide someone's email address to others, particularly strangers, without permission.

## **Be Very Careful When Forwarding Attachments and Email Messages**

Except in a work environment where it might be expected within your internal network, check with your intended recipient before sending attachments. If it is a large file, consider that sending it may block their account from receiving additional email because they exceeded their disk space quota. You need to avoid inadvertently sending a file with PII or other sensitive company information that your recipient should not have.

## **Be Very Careful When Opening Attachments**

Use great care when opening email and IM attachments, even if they appear to come from someone you know. If you receive an attachment that you are not expecting, don't open it. First read the message and make sure that the attachment is most likely legitimate. If you're still not sure, get in touch with the sender to be sure. If the sender's computer has a virus, it may be attaching trojans to all outgoing emails from them. If you're opening spam, it could direct floods of it to your inbox, multiplying the time you're chained to email by an order of magnitude. Web bugs (one pixel GIFs) may be embedded and could send a signal back to a remote system, sending sensitive information from your computer or the network to fraudsters and criminals.

## **Be Careful**

Remember that email and IMs can be intercepted anywhere en route to the recipient. Remember that these messages could exist for years in recipient email boxes, later coming back to haunt you with inappropriate information or sensitive information you sent. Stop and think before sending email you will later regret.

## **Use 'Reply All' With Care**

Do not use "reply all" if other recipients of a group email do not need your response. There may be information you are replying with that all recipients should not receive. You may be inadvertently sending sensitive information outside the organization by using "Reply All."

## **Proofread Your Messages Carefully**

Proofread your messages carefully before sending them. Make sure you are not sending information that should not be going out to your recipients. Make sure you have the correct recipient email addresses and have not accidentally included an address for someone who should not receive your message. Make sure you have removed sensitive information if you are forwarding another message that you received.

---

## **Don't Unsubscribe Blindly**

If you start receiving “subscription” emails from some source to which you did not subscribe, do not use their “unsubscribe” link. If you do, you might just find yourself getting even more emails. You’re better off just adding the email address (or the entire domain) to your inbox blacklist.

## **Don't Be Hooked**

Phishing messages, such as those commonly claiming to be Paypal, Western Union, eBay, numerous banks, and many other organizations, typically indicate account closure and balance forfeiture if you do not click on included URL links to “verify” your account details, or they warn you that your account has been compromised and that you must click the URL link provided to address the “serious” situation. The URL links look legitimate but will instead direct you to a lookalike site set up to collect your login and password information, credit card, and/or bank account details, and so on. Never click links in these types of messages. Honest companies never send this sort of email; they will never send an email where they tell you to click on an enclosed URL link to save your account from shut down or to verify your ID and password.

## **Implement Messaging Security in Depth**

The most effective way to reduce the inherent risks associated with messaging is to implement a combination of technical protections along with effective management strategies and policies and ongoing awareness and training.