

# *Securing the Information Workplace: Managing Threats to Enterprise E-Mail, IM, and Document Sharing Environments*

Joe Licari

**C**ustomer satisfaction. It is what we all want, but it can be difficult to ensure, even under the best conditions. Especially when your information workplace is under attack. The Radicati Group estimates that threats to the information workplace will cost companies over \$54 billion by 2006. The writers of new viruses are much better at infiltrating corporate networks; they exploit system vulnerabilities, use sophisticated programming techniques, and constantly change subject lines and attachment names.

Let us take a look at the information workplace, the impact and scope of threats to the enterprise, and some security best practices and recommendations.

We consider the “information workplace” as the environment where enterprise messaging and collaboration take place. There is a critical need to protect this space

from threats to e-mail, instant messaging, and document sharing. Why? Because this is the place within any enterprise, regardless of size, where business information is exchanged among employees, partners, customers, and other stakeholders. Access security, identity management, verification, and intrusion detection are also important parts of any enterprise security system, but the integrity of shared data is critical and reflects directly on the perception of a company as a trusted and valued partner or supplier.

Taken in the aggregate, an organization’s e-mail, instant messaging, and document collaboration systems have the ability to touch nearly every document of importance and relevance to an organization. Again, if it is all about customer satisfaction, then it must also be all about protecting the information workplace.

---

*JOE LICARI, Sybari director of product management, is responsible for the management and implementation of Sybari’s product development and marketing initiatives. He is a messaging and collaboration security industry veteran and a frequent security conference speaker. Joe can be reached at [joe\\_licari@sybari.com](mailto:joe_licari@sybari.com).*

*Phishing schemes continue to progress beyond social engineering techniques; they modify host files so that users unknowingly provide password and account information to criminals running imposter sites.*

When looking at the elements that comprise the information workplace — e-mail, certainly, but also the growing use of IM and now, document collaboration — one can see that it is a dynamic, ever-changing environment. And often, there is a lack of guidance on how to use these elements correctly.

#### **E-MAIL SECURITY**

The trust and value placed in our e-mail systems is enormous. Early enterprise e-mail systems served primarily as vehicles for brief company communications. These quickly morphed into transport mechanisms for critical, often confidential business communications. At first, we e-mailed information and opened documents with confidence. That was until we got hit with viruses and spam; attachments once viewed with nonchalance and anticipation are now a cause for concern and dread.

The type and intent of malicious e-mail threats have evolved significantly from those viruses that attacked computers just a few years ago. Motivation appears to have shifted as well — new attacks are combining multiple virus and spam techniques and distribution methods to bypass filters and infect as many systems as possible. Virus writers are using spam to plant Trojans onto the systems of hundreds or thousands of unknowing users, forming Zombie networks or botnets. That way, an army of systems can carry out attacks, instead of just a few. Phishing schemes, meanwhile, continue to progress beyond social engineering techniques; they modify host files so that users unknowingly provide password and account information to criminals running imposter sites.

#### **INSTANT MESSAGING ADOPTION**

Now, instant messaging (IM) is quickly taking hold in the enterprise and its value is recognized by businesses. IM serves a function far beyond simple jotted notes and an excuse to abandon good grammar and spelling. IM provides immediacy, presence, and access. We use it to reach out to a colleague,

check status or availability with a vendor, and exchange information quickly and easily with others.

IM is unquestionably a great method for businesses to quickly and easily enrich employee, customer, and partner communications. It has not, however, been fully embraced or supported by IT departments. The Gartner Group forecasts that IM will represent 50 percent of all business-to-client communication in 2005. And although more than 90 percent of enterprises are using IM, sanctioned IM enjoys less than a 17 percent corporate penetration rate, according to researchers.

Most IM installation and usage is unmanaged and employee driven. Further, employees often use IM to get around policies that have been established for e-mail usage. For example, if the transfer of executable (EXE) application files is prohibited via e-mail, employees will use IM to transfer these files into and out of the organization.

Enterprise IM is vulnerable to the same threats as e-mail — viruses, spam (or spIM), and worms. It also presents a challenge for organizations concerned about corporate liability and compliance. In a recent survey of our European, Middle East, and Africa (EMEA) customers, across a variety of industries, we found that 75 percent of businesses surveyed said the threat of viruses and worms through IM is a primary concern. This was closely followed (68 percent) by information theft and loss of sensitive data — information that would have an “extreme impact” on their businesses. This was especially true among those aware of compliance requirements based on government and industry regulations and legislation. Moreover, 54 percent of the companies surveyed were concerned that IM could be used to expose employee computers to remote controlling “hijackers,” while 40 percent were concerned about IM conversation spying.

It is clear that businesses need to consider how to best address the growing presence and status of IM in the enterprise.

## **COLLABORATION**

Document collaboration is a goal for many organizations. It began with one person who took ownership over a document and incorporated others' comments and changes. It then evolved into routed e-mail document attachments. Today, document collaboration allows for multiple users to access the same document with complete tracking and version control. Using programs such as Microsoft SharePoint, companies can take advantage of a single point of access to multiple applications such as Microsoft Office programs, business intelligence and project management systems, and existing line-of-business applications, including third-party and industry-specific programs. However, as users share documents, they also share the capacity to proliferate harmful viruses, corrupt valuable data, and compromise corporate networks.

## **THREATS**

Analysts indicate that the number of security threats will continue to increase alongside adoption of new technologies, such as enterprise IM and document collaboration. And, as the types of threats change and evolve, they also appear to be more targeted and harmful in nature. For example, a recent review of the top 50 viruses and worms over one recent six-month period showed a nearly 400 percent increase in malicious code submissions using P2P and IM applications.

Regarding spam, we recently witnessed the most active week of spam attacks all last year during the December 2004 holidays. We have seen the volume of unique spam attacks rise at a rate of 150 percent greater than the average of just months earlier. We expect that as IM growth and use in corporations continues in 2005, it will very likely attract a greater volume of attacks and other miscreant behavior.

According to the enterprise IM customer data from our partners, approximately six percent of IM traffic today can be categorized as spIM. Although not as prevalent or pervasive as spam over e-mail, spIM can

actually be more disruptive when encountered within an enterprise because it is a generally disruptive communication medium and often contains offensive content. This can potentially introduce human resource and legal risks to an organization.

## **COMPLIANCE AND LIABILITIES**

Companies must ensure that their systems enable compliance with recent regulations like the Sarbanes–Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), or the Gramm–Leach–Bliley Act (GLBA). Many of these reforms rose in the wake of recent corporate accounting scandals. Some regulations are designed to stop sources of spam and viruses, but others have a more chilling effect for businesses; they are intended to make companies more responsible for the protection of customers' privacy and more accountable for the substance of their financial reports. Compliance often requires that the processes used to keep records are consistent, reliable, secure, and accurate.

In addition to compliance, many companies find that they are in need of preventing the creation of hostile work environments by restricting inappropriate content and filtering confidential data.

## **SECURITY CONCERNS**

So, what are some of the challenges facing network managers as they provide security?

In the messaging environment, we look at three main challenges to security: (1) removing the single point of failure, (2) closing the window of vulnerability, and (3) increasing the response to new types of viruses and spam.

The single point of failure is often a concern for companies that rely on a single virus scanning solution that is deployed throughout an organization. By using a layered approach and by scanning at multiple points in the infrastructure (i.e., at the gateway, SMTP relays, Exchange front ends, etc.), administrators can reduce risks. However, if the same virus scanner is used at every location, a single point of failure

*As the types of threats change and evolve, they also appear to be more targeted and harmful in nature.*

*Spam levels will continue to grow in 2005, and companies will begin recognizing the need to replace first- and even second-generation solutions with more effective tools.*

looms large. If a virus penetrates a single scanning engine, or if it is offline during an update, it often becomes a vulnerability to the organization and can cause slowdowns that can derail entire operations.

The window of vulnerability is the delay between the outbreak of a new virus in the wild and the release of signatures created to combat and thwart the threat. This process is usually measured within a matter of hours, but it is of critical concern to IT managers.

The ability to respond to new viruses and spam is another top worry. Spam levels will continue to grow in 2005, and companies will begin recognizing the need to replace first- and even second-generation solutions with more effective tools. These will include integrated solutions that provide anti-spam, anti-virus, content-filtering, and compliance and policy management and will enable companies to meet new challenges while uniformly managing their messaging hygiene throughout their networks.

One last concern that many organizations fail to address is the lack of end-user messaging security training and monitoring. According to Ferris Research, while virtually all organizations have some type of virus protection in place, only half provide training, monitor e-mail, or automatically filter attachments to encourage and enforce compliance with e-mail content policies. This must be addressed as a part of overall corporate best practices through policy creation, education, and enforcement.

#### **SECURITY BEST PRACTICES**

Security solutions are not without their costs. Based on our research, we estimate that the global market for anti-virus products that protect Internet gateways and e-mail servers will reach approximately \$1.6 billion by 2007. In addition, based on our research, we estimate that the global market for messaging security applications, which includes anti-spam and content filtering products but excludes anti-virus products, will reach approximately \$1.1 billion by

2007. The numbers indicate the seriousness that enterprises are placing on securing their information workplaces.

Response to information workplace threats must be proactive, not reactive. And they must provide peace of mind for end users to foster trust in their messaging and collaboration environments. To accomplish this, organizations must:

- Provide a layered anti-virus security approach focused on server-level Internet gateways before information reaches the desktop and is shared with other users.
- Conduct an internal audit of communication applications running in the network, such as IM.
- Enable real-time, next-generation anti-spam protection.
- Establish appropriate policies and procedures for protecting non-public information.
- Continually educate employees on potential security risks.
- Use best-of-breed solutions to maintain proactive content filtering for consistent policy.

Let us take a look at each of these recommendations.

Organizations must take an approach that comprises the deployment of multiple anti-virus and anti-spam solutions throughout their messaging environment to ensure the highest level of protection against threats. These systems must scan incoming e-mail and data before threats can reach the messaging and collaboration servers. This approach avoids the single point of failure scenario and increases productivity by guaranteeing more system uptime. During a virus outbreak or a scanning engine upgrade, additional anti-virus engines remain up-and-running, continually scanning for threats. As independent virus labs update their signatures or heuristics engines, they can be deployed more quickly to improve detection rates faster than when a single engine is used.

Unfortunately, according to our research, too many companies still rely on a single, stand-alone proprietary anti-virus engine. This is likely a result of companies purchasing suites of solutions from a single vendor. Although good at catching known viruses in the wild, this approach leaves messaging servers exposed to a single point of failure, especially during new virus outbreaks. Should the engine be taken offline or fail, e-mail often stops or goes through unscanned. Late engine and signature file updates also increase the window of vulnerability.

Organizations should be aware that programs such as IM can be downloaded, installed, and run without IT consent and knowledge. These companies must know which applications are running, as well as their function. For this, we recommend an internal audit of communications applications running in the network. IT managers should consider users' needs — in terms of internal and external use — and see if these programs improve worker productivity and communication. If these tools do enhance communication, then the IT managers can look into universal distribution, monitoring, and use.

Regarding spam, the second best practices approach calls for IT managers to enable real-time, next-generation anti-spam protection.

It is neither acceptable nor fiscally viable to wait for spam to arrive on the network and then filter based on content. This approach was fine in the past, but as the volume and nature of spam grows and changes, it becomes increasingly difficult to filter based on known content alone.

The recommended anti-spam approach must not rely entirely on typical spam detection technologies that can be fooled by spammer tactics. The anti-spam security deployed should provide continuous and automatic updates, integrate at the Simple Mail Transfer Protocol (SMTP) or Internet Mail Connector (IMC) level, and allow integration with Exchange 2003 and Intelligent Mail Filter (IMF) compatibility. Additionally, signatures should include combinations of unique attributes of particular

spammers, not simply rely on content recognition. And, an increasingly global information workplace also requires the ability to provide anti-spam protection in multiple languages.

When it comes to corporate compliance and liability, organizations must embrace technology that protects non-public information, such as employee and customer data, corporate projections, and financial information. A security system must provide centralized management; enable the creation and enforcement consistent policies throughout the enterprise; and also provide tools for content and file filtering, keyword scanning within documents, and customizable notifications and disclaimers.

Performance issues, specifically the ability to fine-tune based on needs, are also of crucial importance to network security. Although e-mail-borne viruses remain the largest problem, individuals inside and outside the organization often have position-dependent policy and document sharing requirements. For example, the marketing department might have the need to share JPEG and GIF images, while accounting may need to share spreadsheets containing macros for complex formulas. The ability to tune for individual requirements, based on policies, is key for balancing performance needs against security enforcement.

Organizations cannot rely solely on employee filtering and maintenance to protect against viruses and other malicious attacks. Instead, IT managers should provide continual education on new and emerging security threats. Many virus writers and spammers try to attract users with appealing or familiar messages: jokes, fan access to music and film stars, and credit information. By educating employees on these possible threats, the organization can raise the level of awareness and prevent additional security threats from propagating through the network.

In addition to using next-generation spam solutions to block unwanted e-mail from entering the network, companies should use consistent content filtering for

*Programs such as IM can be downloaded, installed, and run without IT consent and knowledge.*

*A layered approach to anti-virus, the use of multiple scan engines, and the deployment of anti-spam and content filtering solutions can help companies thwart these malicious threats.*

every e-mail that enters or exits the network. By utilizing a best-of-breed solution that allows administrators to filter based on specific keywords, file extensions, or size, companies are ensuring that inappropriate or potentially harmful materials are not being sent and received via the company network. Files such as EXE or MP3 files can be blocked before they even enter a user's inbox. An organization can quickly and easily reduce the amount of time users spend on reading or sending personal, inappropriate, or harmful communications. When combined with a comprehensive e-mail policy, this can be an effective tool for maintaining consistent HR and commu-

nication policies throughout the organization.

To be sure, vigilance is required by IT and security professionals to protect their users and environments from these evolving attacks. A layered approach to anti-virus, the use of multiple scan engines, and the deployment of anti-spam and content filtering solutions can help companies thwart these malicious threats. By combining these techniques, organizations can become much more proactive while ensuring optimal uptime, increased end-user productivity, and increased corporate profitability in the face of these ever-increasing threats to the information workplace. ■

# FINSEC 2005



The International Leader  
in Audit & Information  
Security Training

**December 6-7, 2005** The Roosevelt Hotel / New York, NY **Optional Workshops: December 5 & 8**

## ***Two Intensive Days Devoted to the Targeted Information You Need Most:***

- ***Pinpoint the top security risks*** your organization faces today: phishing, identity theft, instant messaging, network security, patch management, virus protection, and more
- ***Protect your security assets*** from data leakage, fraud, and hackers
- ***Prevent damage*** by developing top-notch customer authentication, forensic analysis, and outsourced/third-party verifiable security controls



**KEYNOTE SPEAKER** *Dave Cullinane*  
Chief Information Security Officer,  
Washington Mutual, Inc.

**For more information and to register visit [www.misti.com/finsec](http://www.misti.com/finsec) or call 508-879-7999**