

realtimepublishers.comtm

The Definitive Guidetm To

Email Management and Security

 **singlefin**
e-mail protection services

Kevin Beaver

Introduction

By Sean Daily, Series Editor

Welcome to *The Definitive Guide to Email Management and Security!*

The book you are about to read represents an entirely new modality of book publishing and a major first in the publishing industry. The founding concept behind Realtimepublishers.com is the idea of providing readers with high-quality books about today's most critical IT topics—at no cost to the reader. Although this may sound like a somewhat impossible feat to achieve, it is made possible through the vision and generosity of corporate sponsors such as Singlefin, who agree to bear the book's production expenses and host the book on its Web site for the benefit of its Web site visitors.

It should be pointed out that the free nature of these books does not in any way diminish their quality. Without reservation, I can tell you that this book is the equivalent of any similar printed book you might find at your local bookstore (with the notable exception that it won't cost you \$30 to \$80). In addition to the free nature of the books, this publishing model provides other significant benefits. For example, the electronic nature of this eBook makes events such as chapter updates and additions, or the release of a new edition of the book possible to achieve in a far shorter timeframe than is possible with printed books. Because we publish our titles in “real-time”—that is, as chapters are written or revised by the author—you benefit from receiving the information immediately rather than having to wait months or years to receive a complete product.

Finally, I'd like to note that although it is true that the sponsor's Web site is the exclusive online location of the book, this book is by no means a paid advertisement. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100% editorial control over the content of our titles. However, by hosting this information, Singlefin has set itself apart from its competitors by providing real value to its customers and transforming its site into a true technical resource library—not just a place to learn about its company and products. It is my opinion that this system of content delivery is not only of immeasurable value to readers, but represents the future of book publishing.

As series editor, it is my *raison d'être* to locate and work only with the industry's leading authors and editors, and publish books that help IT personnel, IT managers, and users to do their everyday jobs. To that end, I encourage and welcome your feedback on this or any other book in the Realtimepublishers.com series. If you would like to submit a comment, question, or suggestion, please do so by sending an email to feedback@realtimepublishers.com, leaving feedback on our Web site at www.realtimepublishers.com, or calling us at (707) 539-5280.

Thanks for reading, and enjoy!

Sean Daily

Series Editor

Introduction.....	i
Chapter 1: A Look at Corporate Email Concerns.....	1
In the Beginning.....	1
Email Usage.....	2
Email Applications.....	3
Email is Maturing.....	4
Email Threats and Vulnerabilities.....	6
A Brief Look at the Malicious Software Problem.....	8
How Email is Affected.....	10
Malware.....	11
Vulnerability Exploits.....	12
Other Various Malicious Uses of Email.....	13
Spam.....	14
Why Email Must be Properly Managed.....	16
Why Be Concerned?.....	17
The Effect of Email on Employee Productivity.....	18
Looking at What Can Happen.....	19
Summary.....	20

Copyright Statement

© 2003 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.


If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

Chapter 1: A Look at Corporate Email Concerns

Email has long been hailed as the most popular Internet application. Although the Web tends to get the most attention and might be considered more useful and informational, there's no denying that most 21st century organizations couldn't function properly without email. And what a nice upgrade email is from the telegrams and telephones that we have solely relied on in the past! Email allows us to communicate more quickly and conveniently. What more could we want from something that gives us the ability to communicate when it's convenient and makes us more productive in the workplace?

In the Beginning

Way back in 1971, during the initial development of the U.S. Department of Defense (DoD) ARPANET network, the precursor to today's Internet, the @ symbol took on an entirely new meaning. Ray Tomlinson, an employee of Bolt, Beranek and Newman, the company contracted by the DoD to build ARPANET, didn't realize that playing around with his SNDMSG program and CYPNET protocol would spark such a revolution. Mr. Tomlinson sent a message to colleagues letting them know about the new email feature, with instructions for placing an @ in between the user's logon name and the name of his host computer. "The first use of network mail," said Tomlinson, "announced its own existence."

 To read more about this development, see Todd Campbell's article in the March 1998 issue of *Pretext Magazine* "The First E-Mail Message," online at <http://www.pretext.com/mar98/features/story2.htm>.

 The first email was sent over the ARPANET network by Ray Tomlinson in 1971.

As Ian R. Hardy argues in his thesis paper "The Evolution of ARPANET Email," ARPANET was originally developed as a medium more for sharing computer programs than for human communication.


 To read a draft of the entire paper, go to <http://www.ifa.org/documents/internet/hari1.txt>.

The development of email was more of a side benefit of ARPANET's evolution rather than a planned objective. However, it didn't take long for researchers at universities and other research centers to start collaborating via email. This method proved to be an efficient means of communication that could be used with minimal effort and cost involved, and email ended up as a significant application of ARPANET evolving into the email protocols as we know and use them today.

However, the utility and convenience of email comes at a price—a lack of security and management capabilities. Unfortunately, we're now paying the price for these two issues that really didn't matter several decades ago. This book will explore these issues in detail and will include practical advice about how you can effectively manage your organization's email system in order to get the most from it.

Email Usage

The initial fascination with email has worn off a little with the advent of the Web and other content-rich protocols and services on the Internet today. However, this certainly hasn't taken away any of the popularity and usefulness of email. What else is mostly free (at least to the end user) and is used by millions to accomplish both personal and business goals?

 Various surveys tout email as being the most widely used Internet application.

The numbers cited for email users around the world are staggering. According to IDC's Email Usage Forecast and Analysis 2001 through 2005, the number of worldwide email mailboxes is expected to increase from 505 million in 2000 to 1.2 billion in 2005. In addition, in IDC's Worldwide Email Usage Forecast 2002 through 2006, the company states that the total number of email messages sent daily is expected to exceed 60 billion worldwide in 2006, up from 31 billion in 2002. As Figure 1.1 illustrates, the Radicati Group estimates the number of daily emails will be 73.1 billion in the same timeframe.

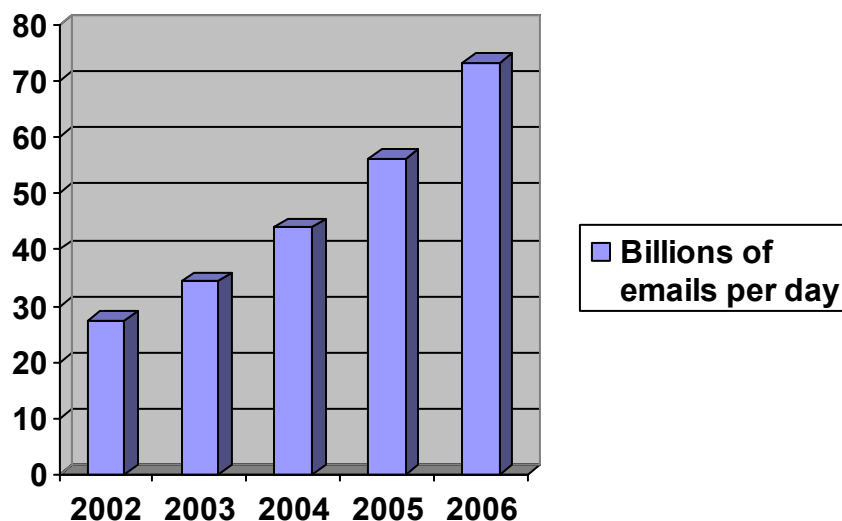


Figure 1.1: Worldwide email traffic according to the Radicati Group.

According to the April 22, 2003 edition of the Network World newsletter *Michael Osterman on Messaging*, a vendor-sponsored study about email usage by Osterman Research had some interesting results. It was determined that email usage is definitely on the rise, and some astonishing results were found. The following list provides highlights of the survey:

- Nearly 50 percent of the respondents receive more than 50 messages a day, and about one in six email users receives 100 or more emails daily
- About 52 percent of an average user's email is internal to the organization
- 38 percent of respondents have seen their organization's email volume grow more than 50 percent and an additional 30 percent of respondents have seen growth between 26 and 50 percent

- 55 percent of organizations have seen email storage grow more than 50 percent over the past 2 years, and nearly 10 percent of organizations have experienced email storage growth of more than 200 percent
- 50 percent of organizations have experienced business interruption or monetary loss because of email system downtime
- More than 33 percent of email users have lost email due to technical problems, hardware damage, virus attacks, or other problems

Ask practically anyone in today's business environment for his or her email address and odds are nearly perfect that the person will have one. And it's not just that most people have email addresses; we also have various methods for communicating via email:

- Through our desktop and laptop computers at the office
- Through dial-up, virtual private networks (VPNs), and the Web when we're out of the office traveling or working from home
- Through our PDAs and mobile phones when we're out at client sites or in those inevitable time-robbing meetings
- Through public libraries and cyber-cafes for those times when we must get away

We're highly connected and we like it. It's only natural to love the "human" benefits of email in a business setting such as being able to communicate when it's convenient for all parties or reduce the small talk that is typical in face-to-face conversations. Other benefits include not having to put people on the spot when asking them questions, and being able to more easily approach people about uncomfortable situations. All of these benefits add up to be some of the most valuable selling points for email communications.

Email Applications

Highlighting the importance of email in today's business environment, the Radicati Group expects demand for email software from companies such as Microsoft and Lotus to grow from \$2.6 billion in 2002 to \$4.4 billion by 2005. In addition, the Meta Group states that by 2005, 75 percent of all corporate knowledge will be communicated via email. These numbers are driven by the needs of corporations to conduct business at high speeds. Successful companies have recognized the demand from customers and partners for fast transactions and are relying more on applications such as email in their service delivery.



Email can help facilitate quick response times that are required in business today.

There are various applications for email in our business environments. The following list, although only a small sampling, shows how email communications is the backbone of most organizations:


- Internal business communications between managers and employees
- Information security awareness reminders
- Fulfill and track sales orders



- Customer service communications
- Research and development collaboration
- Business strategy planning among board members and upper managers
- Supply chain collaboration with business partners
- Software developers transferring files
- Doctors answering patient health inquiries
- Lawyers corresponding with their clients on legal issues
- Engineers and architects exchanging blueprints
- Instructors communicating with students about lessons and class assignments
- Owners and managers executing business contracts

The last bullet focuses on newer “digital” laws and deserves a little more attention. The U.S. Electronic Signature in Global and National Commerce Act (E-sign) combined with other state laws make certain emails legally binding contracts. Thus, organizations that have the proper technical systems in place—such as Public Key Infrastructure (PKI) or even individual digital signatures installed in their email software—can now use email communications to transmit official business documents and information that are legally binding. Such documents and data could include contracts, pricing, purchase orders, and so on. In fact, there are cases, dependent on the type of contract, in which simply exchanged emails can be considered legally binding contracts even without the use of digital signatures. This note isn’t meant as legal advice, so please consult with your attorney before attempting to transact legal documents via email. Either way, email allows organizations to have a permanent record of business documents, which can be very beneficial reference material in the future.

Remember that anything going across a public network in clear text should be treated as public information. In addition, just as these permanent records of email can be beneficial to your organization, they can also work towards the detriment of your organization if they contain material that should not have been sent out.

 In Chapter 5, I’ll discuss what actions you can take to protect those emails that need to remain confidential and intact.

Email is Maturing

Email is not what it once used to be. It has evolved into a newer line of technologies called groupware or “collaboration” applications. These applications support the essential need for humans to communicate more effectively in a business setting. At the same time, they can leverage current computer and networking technologies that support high-speed data retrieval and analysis. These technologies are even being integrated into business applications that corporations use in daily operations such as enterprise resource planning (ERP) and customer relationship management (CRM) software. This integration helps to eliminate the requirement of individual applications for each function including email, calendaring, and document sharing.

 Email is a perfect example of how computer networks can add business value.

The latest in messaging/collaboration technology—deemed unified messaging architecture (UMA)—not only combines business applications with messaging, but it also lets users have only one mailbox to manage. UMA combines email with voice mail, instant messaging, faxing, and document sharing. These technologies can help lower administrative costs and increase productivity and convenience for your users.

The UMA integration present in newer messaging platforms from the major vendors such as Novell, Lotus, and Microsoft is now aimed at using Web services and relational databases as the back-end technologies that will be more flexible and scalable. The intent is to support more transactions, enhance database querying and reporting, and improve integration of various databases. This functionality will help enterprises build a common messaging and collaboration infrastructure that's highly scalable for any size organization and possibly even platform independent so that it can work across many different operating systems (OSs).

In addition to the maturing collaboration software arena, the medium for message exchange is shifting as well. There is an increasing popularity in mobile messaging platforms. Pagers are out and handhels are in. In a market once dominated by the Research in Motion (RIM) Blackberry, newer players are stepping up to the plate providing various mobile messaging alternatives. Table 1.1 offers a listing of some of these vendors.

Vendor	URL	Application
Good Technology	http://www.good.com	GoodLink
Jarna	http://www.jarna.com	The Jarna Mobile Messaging Suite
Motient	http://www.motient.com	eLink
Palm	http://www.palm.net	ThinAir
Research in Motion	http://www.rim.net	Blackberry
SEVEN	http://www.seven.com	System SEVEN
Toffa International	http://www.toffa.com	SyncWisePro
ViAir	http://www.viair.com	Wireless Inbox

Table 1.1: Mobile messaging products.

These messaging products allow connectivity back to your regular email servers—providing users with mobile email, calendaring, and collaboration capabilities. Without getting into specifics, I can say that all of them support most of the popular messaging platforms and protocols to ease integration efforts with your existing systems. Although some compatibility, coverage, and data transfer speed issues still exist within mobile messaging infrastructures, these email access technologies will mature, proving themselves valuable in a business setting and further increase workplace productivity.

According to Giga Information Group, 87 percent of large U.S. enterprises will deploy mobile applications through 2005. The convenience and portability of email anytime and anywhere is quite appealing to a lot of business people. However, others see it as yet another way of preventing us from escaping from work. Regardless of one's stance, mobile messaging technologies are here to stay, and given enough time, will most likely change our way of doing business and our way of living life.

Email Threats and Vulnerabilities


The most widely used application on the Internet is arguably the most insecure one as well. Email allows us to communicate more effectively, but at the same time increases the risks to our information systems. A common entry point to an organization's network is via email—either through an insecure email server that can be compromised or through the actual email messages.

 Email systems provide malicious users and software one of the easiest ways into corporate networks.

Email has gained its insecure foundation as a result of various email protocol weaknesses. The Simple Mail Transfer Protocol (SMTP) and Post Office Protocol version 3 (POP3) were designed with some security features in place, but certainly not enough to keep prying eyes and malicious code away. The following list highlights some of the more significant weaknesses of these protocols:

- Emails are sent across open networks in clear text
- Weak user authentication requirements for receiving email
- No user authentication requirements for sending email

Additionally, there's a general misconception that if email is encrypted, it must be secure. That's not always the case. Encrypted emails can contain malicious code and even bypass certain server or perimeter antivirus protection measures. Also, just because email is encrypted doesn't mean that you know or can trust the sender and his or her intentions.

 Refer to Chapter 5 for more details about email encryption.


Computer and network security incidents are on the rise stemming from both internal and external attackers. There are various reasons for the rise in cyber crimes:

- Lack of upper management buy-in on information security initiatives
- General lack of awareness of security threats and vulnerabilities
- General belief that firewalls and antivirus software are all that's needed
- Not having solid information security policies and procedures in place
- Having information security policies that are not enforceable or enforced
- Global reach of the Internet
- Increasing complexity of our information systems
- Software written without security in mind


- Lack of information security integration into software projects
- Widespread availability of attack scripts source code on the Internet
- Ease of carrying out attacks
- Anonymity provided by computers and the Internet lowering the chances of getting caught committing a cybercrime

Before we talk about some specific threats and vulnerabilities to email, let's look at the definition of these words in the context for which we are using them:

- **Threat**—An indication or expression of intent to cause disruption or damage to a computer or email system.
- **Vulnerability**—A weakness that can be exploited either maliciously or accidentally to cause disruption or damage to a computer or email system.


 Threats are *indications* and vulnerabilities are *weaknesses*.

There are numerous threats and vulnerabilities associated with our information systems, particularly with email. Table 1.2 contains a partial list of threats and vulnerabilities that you should consider when evaluating your information security infrastructure. Keep in mind that these threats and vulnerabilities will affect every organization differently. Some might not even be a factor for your environment. As we'll see later in Chapter 5, these threats and vulnerabilities can be used in the calculation of your overall email security risks.


 See more about assessing your email risks in Chapter 5.

Threats	Vulnerabilities
<ul style="list-style-type: none"> —Hackers breaking into exposed email servers —Malicious software (viruses, worms, and so on) —Spam —Current or former disgruntled employees —User error —Environmental (fire, tornado, and so on) —Attacks that subvert antivirus software —Denial of service attacks —Mobile device-specific attacks 	<ul style="list-style-type: none"> —Unpatched applications and OSs —No antivirus software —Unprotected network shares —Email not filtered for content —Systems with default configurations —Untrained users opening email attachments —No viable data backup system —Unreasonable policies —Sloppy or careless administrators —Auditors and consultants with nothing to lose —Passwords that are easy to guess

Table 1.2: Email system threats and vulnerabilities.

 According to Gartner, through 2005, 90 percent of cyber attacks will exploit known security flaws for which a patch is available or a solution known.


As you can see, the threats and vulnerabilities listed in Table 1.2 are nothing new or complex. With a little time, effort, and good business practices, a lot of the security threats that your email systems are up against can be reduced. Some of them can even be prevented altogether. The email management and security techniques, tools, and resources presented later in this book can help you in doing so.

 Email threats and vulnerabilities can be significantly reduced or even eliminated when the proper systems are put in place.

A Brief Look at the Malicious Software Problem


Before we start, we need to define some key malicious software (malware) terms that we will be using in this chapter and throughout the book:

- **Virus**—A program, which is typically self-replicating, that attaches itself to executable files and is propagated via email or some form of storage media such as diskette or CD-ROM. Viruses are designed to cause computers to crash, erase data, and even drain batteries in PDAs!
- **Worm**—A type of self-propagating program, similar to a virus, but instead travels across computer networks. They typically do not affect files and data like viruses do. Instead, worms load themselves in memory and exploit known system vulnerabilities causing computers and even entire networks to stop working.
- **Trojan horse**—A program (named after the hollow wooden horse used by the Greeks to sneak into the city of Troy during the Trojan war), typically delivered by email, that masquerades as a legitimate executable file such as a screen saver, a game, or a graphics file. The file often works as advertised, but also contains embedded malicious code that can harm the local computer or network such as delete files, steal passwords, or even install keyboard logging or network analysis programs to be used for malicious purposes.

 I'll provide more in-depth coverage for these types of malicious code and more in Chapter 2.

Long ago (as far as Internet time is concerned), back in the mid-1980s, the first Intel/Microsoft computer virus named Brain was introduced. It took 5 years to create \$50M worth of damage. In 1993, the July/August issue of NCSA News stated that “viruses cost U.S. computer users over a billion dollars over the last three years with the average computer site spending \$176,000 on computer virus cleanup this year.” My, how times have changed! Studies now show that malware affects most businesses. In fact, according to the 2002 Computer Security Institute and FBI Computer Crime and Security Survey, the average annual cost for virus infections in a company was \$283,000.

Compounding the problem, malware infection times are shortening. The months and years required for malware infections, such as macro and floppy disk-based viruses, has been drastically reduced thanks to newer methods of malware distribution. Now email and Internet servers are the prime targets in helping to facilitate faster infections. With newer malware such as the Melissa virus and the SQL Slammer worm, the time is down to less than a day for hundreds of thousand—even several million—infections to occur.

 The time required for widespread malware infections has dropped from years to minutes.

Computer Economics has found that malware had a worldwide economic impact of \$13.2B in 2001 alone. According to the market intelligence firm Mi2g, the SQL Slammer worm caused between \$950 million and \$1.2 billion in damage worldwide in its first 5 days of spreading! Figure 1.2 shows the world economic impact that malicious code has had since the mid-1990s.

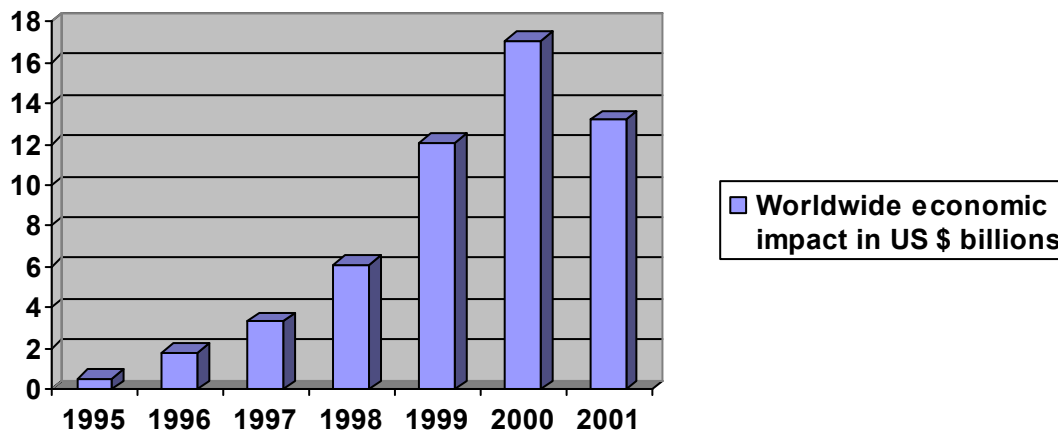



Figure 1.2: The increasing cost of malicious code on the business world based on figures from Computer Economics.

Table 1.3 shows some specific malware outbreaks that the world has experienced along with their estimated costs.

Virus/Worm	Estimated Cost
Nimda	\$635 million
SQL Slammer	\$1.2 billion
Klez	\$9 billion
Code Red	\$2.62 billion
Melissa	\$1.10 billion
SirCam	\$1.15 billion
LoveBug	\$8.75 billion
Explorer	\$1.02 billion

Table 1.3: The cost of malware infections—Source: Mi2g and Computer Economics.

A lot of the newer malware relies less on social engineering—a term used to describe the act of attackers acquiring information from trusting people and using it for malicious purposes.

 An example of social engineering used in viruses is how the LoveBug and AnnaKournikova viruses “convinced” users to open their email thinking that someone had truly sent them something of interest—either a love letter or a picture of the famous tennis star. Once the unsuspecting user opened the email attachment, there was no prize, but instead a rather nasty infection that began to spread.

Instead, malware has become more automated and can exploit known software vulnerabilities without any user intervention. This increased ability has the added “benefit” (for the attacker at least) of not having to wait on people to view their email. When attacks can be automated electronically, infection speeds and accuracy are increased exponentially. Figure 1.3 shows viruses’ effects compared with other problems faced by IT personnel.

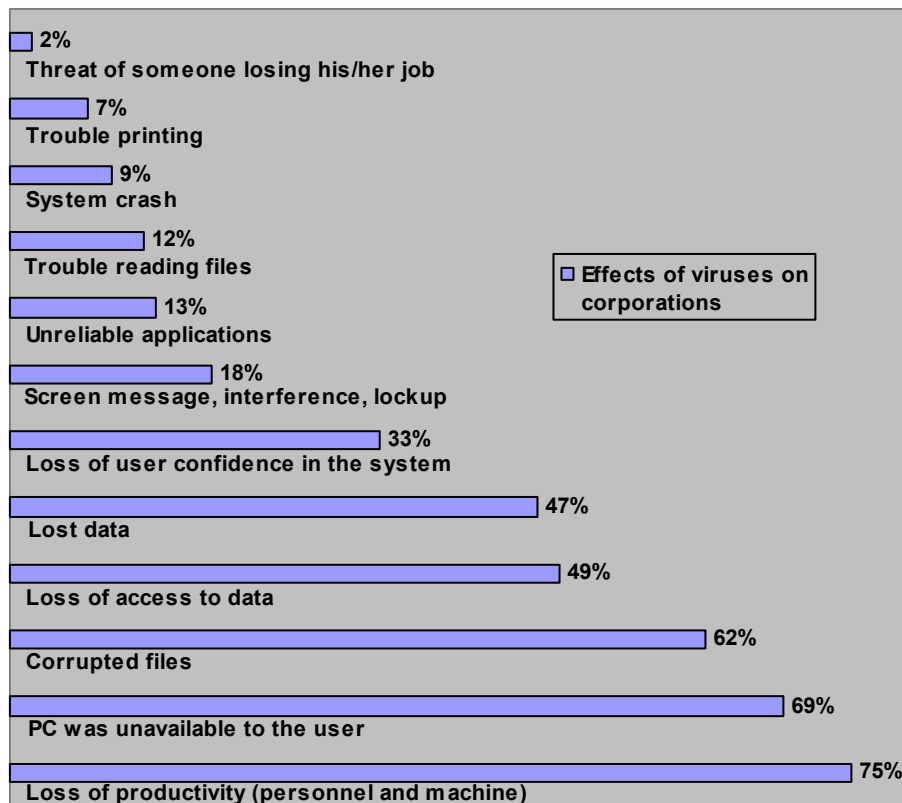


Figure 1.3: Effects of viruses on corporations (based on figures from the 2002 ICSA Labs Virus Prevalence Survey).

How Email is Affected

Email is affected in many different ways by the various threats and vulnerabilities our systems face. In the past, the only thing we had to worry about regarding email was not getting enough of it, or maybe ensuring that it was backed up and we didn’t lose anything. Now we not only have to ward off all the possible attacks, but we now also have to worry about having *too much* email to deal with! We’ll take an initial look at the spam epidemic later in this chapter.



Ferris Research estimates that spam cost \$8.9 billion in 2002 for U.S. organizations alone—and the problem is only getting worse!


Some specific negative side-effects that email threats and vulnerabilities can generate include:

- System crashes
- Lost productivity as a result of computers and networks running slowly
- Lost productivity as a result of computers and networks being unavailable
- Partial loss of information due to file corruption
- Complete loss of information
- Loss of privacy

It used to be that a stray floppy disk was enough to make a security-conscious email administrator cringe, now it's email—something that everyone has—and a lot of it too! Email management, from both the end users' and email administrators' perspective, is becoming a heavy burden that is consuming a lot of time and effort. Trying to balance user demand for email availability and administrative requirements of fighting malware and other attackers as well as attempting to find enough storage space for everyone's Inbox is becoming very difficult. Let's take a look at these issues more in-depth.

Malware

Viruses, worms, and Trojan horses seem to be dominating our networks. From lost data to lost productivity, individuals and the organizations they work for are losing out. Malicious code no longer needs to be attached to emails to quickly take down thousands of systems within a few minutes; however, the malware attacks on email haven't stopped, and I don't suspect they will anytime soon.

 Want to see if your antivirus software is working? Not sure if you even have antivirus software loaded? Download the eicar virus test file from the following site—it's not a real virus that will cause damage, but it's a neat way to test your software: http://www.eicar.org/anti_virus_test_file.htm.

First it was desktops taking the malware hits. Next it was the servers—either dedicated antivirus servers or email servers—whose resources were being hogged by these attacks. Now, at least for the security-minded administrator, it's the perimeter devices such as firewalls, content filtering systems, and even intrusion detection systems (IDSs) that are getting hit. It seems as if any new hardware upgrades—from new processors in desktop computers to Ethernet switches on the network—are futile.

As the malware traffic increases and the antivirus software, “pest” software, personal firewalls, and whatever else is needed to fight off the bad stuff becomes more complex, it's hard to tell that anything new has been installed because of all of the bottlenecks that packets must go through! Sure, if you break out the benchmark software and network analyzers, the numbers will most likely prove it. However, based on my non-scientific studies I, nor the average end user, can really tell that much of a difference in the computing power over the old equipment—thanks to the all the new security armor that must be in place just so we can get our work done.


This grumbling doesn't even take into consideration the dreaded hard drive fragmentation that starts occurring—thanks in part to all the log file writes that the security armor is making! OK, realistically, this factor might not be a major issue to the average enterprise, but it's still a frustrating annoyance we must deal with.

One other issue we're up against is the fact that signature-based antivirus software can provide only so much protection. In our ever-growing electronically connected world, "zero day" attacks, or attacks that start causing damage immediately, are occurring more often than not. This speed of development truly hampers the ability for antivirus products to keep up. Newer, more sophisticated, behavior-based malware analysis programs are emerging that could be the next big thing to help fight the malware war.

 In Chapter 2, we'll look at the newer behavior-based applications in detail.

Vulnerability Exploits

As if viruses and worms aren't enough to have to fight off, we're also faced with various email server and client vulnerabilities that can be exploited very easily if the proper patches are not applied on a constant basis. At the time of this writing, a simple search on the word "email" turned up 106 email vulnerability results in the National Institute of Standards and Technology (NIST) ICAT Metabase and 69 vulnerabilities in the CERT/CC Vulnerability Notes Database. These numbers will surely continue to grow as email software becomes more complex and more people use these applications.

 If you'd like to find out more about the known vulnerabilities in your existing systems, check out the following searchable security vulnerability databases:

CERT/CC Vulnerability Notes Database at <http://www.kb.cert.org/vuls>

NIST ICAT Metabase at <http://icat.nist.gov/icat.cfm>

There are various ways for email systems to be compromised. The following list provides some general possibilities:

- Logons susceptible to password-sniffing utilities
- Rogue administrators that read other people's emails
- Messages in transit susceptible to network analyzers, man in the middle attacks, session hijacking, and message re-routing
- Misconfigured email servers susceptible to extremely large attachments and too many emails coming in at once
- Vulnerable Web servers hosting Web mail applications susceptible to buffer overflows, malformed URLs, directory traversals, and other various denial of service attacks

By exploiting some specific well-known vulnerabilities, malicious users can


- Send a malformed email that could cause the user's email client to stop working
- Create hostile Web pages that, when viewed through an email client, will allow emails to be read or deleted and calendar items to be changed in the email client
- Send forged emails to a user and run just about any command on their systems without the users ever knowing it
- View the local directory structure and files after the user views a specially crafted HTML email

- Create hostile Web pages that allow a user's email address to be copied without the user's knowledge, which can lead to spam and privacy issues
- Create hostile Web pages that can initiate an outgoing email or FTP session from the user's computer back to the originating site, which can, again, lead to spam and privacy issues

 Check out <http://www.emailsecuritytest.com> for a quick way to assess some of your email vulnerabilities.

Let's take a look at the steps involved in a typical email vulnerability exploit. This example illustrates how easily an activity that occurs all the time on the Internet with advertising and behavior monitoring companies can go awry:

1. An unsuspecting user downloads what he thinks is a regular HTML-formatted email.
2. His email client displays the email in HTML format, and at the same time, downloads a 1-pixel high by 1-pixel wide graphic file called a Web bug.
3. Behind the scenes, this Web bug download then logs the user's IP address and possibly even his client software version on the originating site.
4. The malicious user then cross-references the user's IP address to the malicious user's email address.
5. At the same time, the malicious user can then determine how quickly the user opened the email after receiving it.
6. The malicious user can take this information and:
 - a. Best-case scenario—put the user on a spam list based on how quickly the user opened his email
 - b. Worst-case scenario—email the user a virus or Trojan horse that could exploit a particular software vulnerability on the user's computer
7. Anyone that the user forwards the email on to could also fall victim to this privacy (and potentially security) invading scheme.

 For some interesting and independent insight into specific email and other vulnerabilities, check out <http://www.guninski.com>.

Other Various Malicious Uses of Email


In addition to the danger posed by viruses, there are many malicious uses of email. The following list highlights a few of these:

- Child pornography
- Cyber stalking—The electronic equivalent of improper or illegal pursuit of someone
- Harassment—Electronically annoying someone
- Libel and slander—Improperly conveying an unfavorable message about another entity

- Extortion—Electronically intimidating another entity for ill-gotten gains; this happens quite a bit in hacking scenarios in which a malicious user will demand money in exchange for information on the “newly discovered” computer or information system vulnerabilities that the organization should know about
- Forgery—Electronically sending an email that appears to have come from someone other than the true sender, or making or altering a document while posing as someone else
- Fraud—Electronically tricking or deceiving for ill-gotten gains; this happens quite a bit in online auctions

Spam

Spam is a complete nightmare that no one asked for! According to the Coalition Against Unsolicited Commercial Email (CAUCE), spam is the leading Internet complaint. I’ve heard it called everything from free-enterprise advertising to postage-due marketing. The spammers are basically placing collect calls to practically everyone that has an email address, and it’s the end user organization’s that have to foot the bill.

 According a European Commission study in 2002, spam costs Internet users \$8.7B.

Once you make it onto a spam list, your Inbox is permanently doomed to spam hell. Well, not quite. There are various spam filtering solutions for email clients from vendors such as SpamAssassin and McAfee, for servers from vendors such as NetIQ and Tumbleweed, and as an application service provider (ASP) model from vendors such as Singlefin.

You probably recognize the scenario presented in the screen capture that Figure 1.4 shows. These are actual spam messages captured by a Eudora-specific spam filter called Spamnix by Spamnix Software. This Inbox is not what you want for yourself or end users in your organization to deal with, is it?

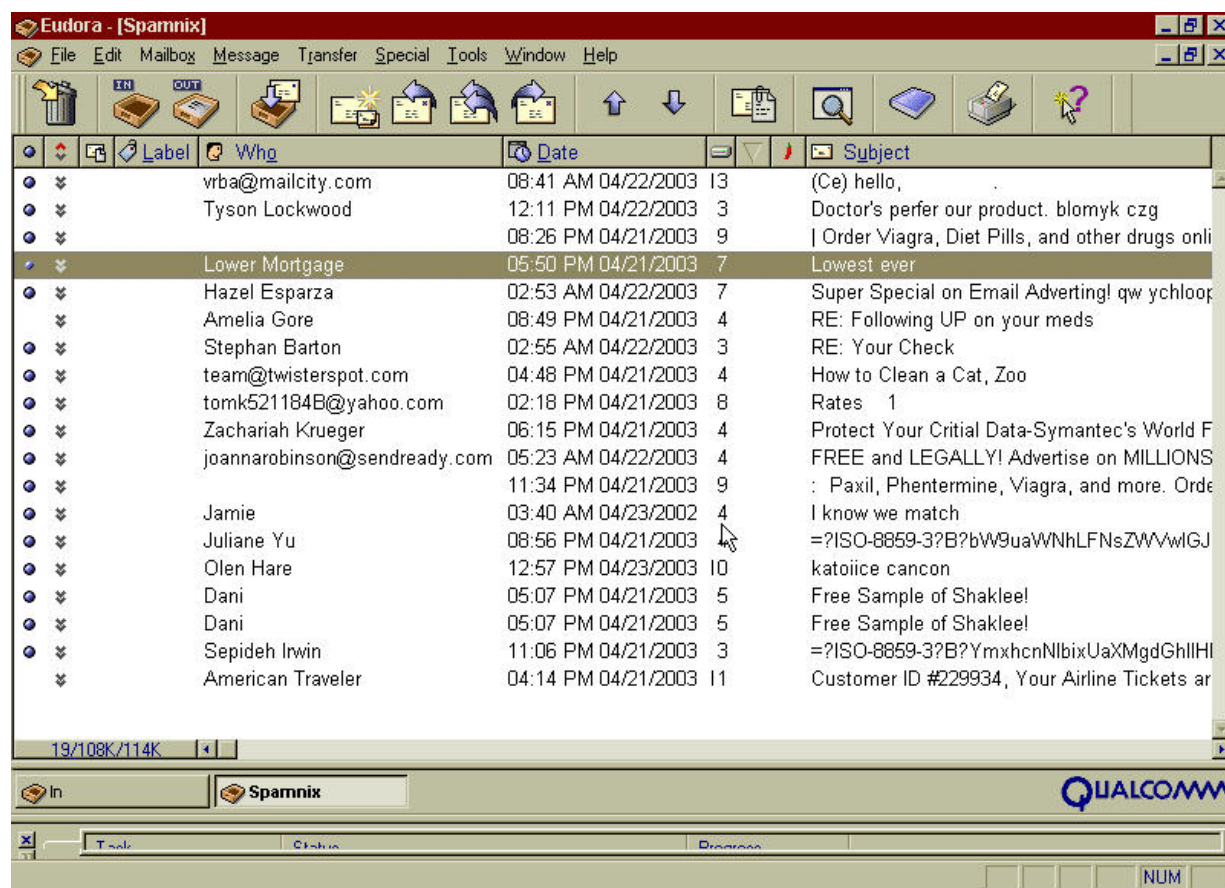


Figure 1.4: Screen capture of some filtered spam over a 3-day period.

Internet service provider (ISP) Earthlink estimates that 10 to 30 percent of all email is spam. In addition, according to Jupiter Media Metrix, the average email Inbox will be congested with 1400 spam messages per year by 2006. That's 27 spam emails per user per week!


So why do we have such a huge spam problem? There are three main factors that play into this situation:

- Spamming is simple—It's easy to hide behind false email addresses and email servers that aren't secured against someone sending emails through them.
- Spamming is cheap—For less than \$100, a spammer can buy an entire spam email database and software to reach potentially millions of victims.
- Spamming can have huge payoffs—Because there are so many spam recipients, even if only a tiny fraction of a percentage of people that receive spam reply and end up buying the products or services offered, the profits can be huge.

All in all, spam is a nuisance and a money and time waster. The following list offers additional considerations about spam:

- It can contain malicious code
- It can be a threat to the confidentiality, integrity, and availability of your information systems
- It diverts resources away from other, more serious, IT and security issues
- Spam is expensive to support—you must consider the resources it uses up, such as the communications (Internet) link, storage space, content filtering software, and most importantly, the administrators' time and efforts

Perhaps the spam issue could be resolved if there weren't so many open email relays—but that's not going to diminish any time soon. Perhaps the spam issue could be resolved with new laws forbidding it. In fact, some organizations, including the European Union, have banned spam. Just like with the junk faxes that were banned in the U.S. more than a decade ago, it's next to impossible to enforce these laws. For now, we'll simply have to fight spam with technical solutions and general email usage best practices.

 We'll look at the spam problem along with various detailed solutions to it in Chapter 3.

Why Email Must be Properly Managed

We've already touched on some of the issues that can arise when email is not managed properly, but it deserves more discussion. There are myriad issues that organizations must address to ensure that one of their most mission-critical business applications is maintained properly and remains secure and available (almost) 100 percent of the time. Figure 1.5 shows the foundation of a solid email infrastructure.

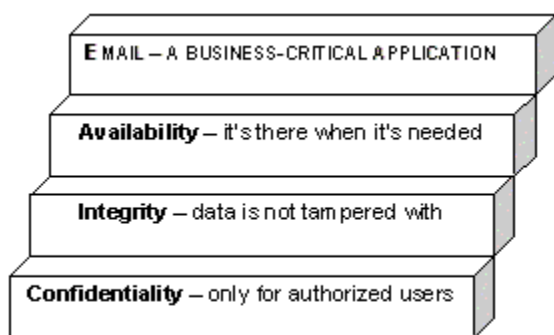


Figure 1.5: The essential elements for a functional and secure email system.

Keep in mind that before email can be properly managed, the proper staff or outsourcing firm must be in place to do so. The person typically responsible for email management might be very good at that specific job. However, there are other areas in which they must be knowledgeable such as network architecture, security, or storage management. Whether this person is you or another colleague, it's imperative to ensure that these skills exist somewhere within the organization or in an outsourcing firm that can be readily called upon.

There is also an important characteristic for successful email management—that of having the skills to be able to communicate effectively to users everything they need to know about using email on a daily basis. These communications must include but aren't limited to

- How to use existing email software features
- How to use new features when software is upgraded
- Email etiquette
- Email policies and their consequences
- The need to clean out your mailbox periodically


Again, as with the other skills I mentioned earlier, the ability to communicate and manage your end users needs to be (preferably) in-house or readily available as an outside resource.

Why Be Concerned?

Why should you be concerned about how email is managed in your organization? Personal privacy and corporate intellectual property are at stake here. It's not a matter of if, but when and how many times an email security incident will occur within an organization. Given how essential email is to business survival, it's imperative that you properly manage its associated risks.

Starting with privacy, you, your upper management, and human resources (HR) need to communicate the expectations associated with employee privacy to all users:

- Who has what access to the email system
- How much monitoring will be done
- Why and how to use passwords in email software
- Why and how to log off to prevent other users from sending emails to others from your computer on your behalf

 We will cover privacy and employee monitoring in detail in Chapter 4.

There is a watchful eye on certain corporate fiduciary responsibilities. At the same time, there is a growing need to reduce corporate liabilities. In addition, there are certain federal regulations that require information security responsibilities. Examples of such regulations include the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach Bliley Act (GLBA), which mandate strict controls on confidential health and financial information, respectively. There are even some aspects of the USA PATRIOT Act that affect how email is managed.

Although we won't explore the specific details of these regulations, I strongly suggest that you and your organization study them (and others) carefully and consult with an attorney to determine whether they apply to your business. Regardless of the specific regulation, there are harsh personal fines and penalties that affect everyone from end user to IT managers to the board of directors.


There are direct financial impacts that organizations must be concerned with regarding email threats and vulnerabilities. Keep in mind that a lot of the cost estimations we hear regarding malware infections and spam only consider productivity losses or cleanup costs. Other cost factors need to be considered as well. There are both tangible and intangible losses as Table 1.4 shows.

Tangible Losses	Intangible Losses
<ul style="list-style-type: none"> —Direct financial losses —Costs as a result of increased bandwidth, storage space, and administrative requirements —Employee productivity —Corrupted or deleted data —Time, money, and effort spent cleaning up and restoring systems after an email incident —Legal costs required for any investigation or prosecution of the email attackers —Legal costs involved with defending lawsuits —Potential public relations costs —Replacement costs for compromised systems and information —Insurance premium increases —Intellectual property losses 	<ul style="list-style-type: none"> —Customer confidence and loyalty —Shareholder value —Brand image —Opportunity costs as a result of information systems unavailability —Diminished trust by upper management —Failure to meet state or federal privacy and security regulations —Corporate officer and upper management liabilities —Employee morale —Diversion of information to unintended recipients —Goodwill

Table 1.4: The various types of losses that can result from email incidents.

The Effect of Email on Employee Productivity

Finally, and perhaps most importantly, email has a strong effect on employee productivity. There are productivity issues that involve everything from the actual usage of email to facilitate business communication, to the potential downtime resulting from a malware attack, to the effort involved in sifting through spam. Regardless of the cause, the last thing any organization can afford is for their employees' jobs to be impeded as a result of something that could have been prevented had the proper technologies, policies, or procedures been put in place initially.


 We will cover employee issues such as monitoring and policies in Chapter 4 and Chapter 6.


As we explored earlier in the chapter, email downtime can really keep people from getting their jobs done. When half of all organizations surveyed experienced business outages or financial losses, and over a third of all email users have lost emails in the past as a result of email problems, it's obvious that email is a critical business asset.

We'll discuss email management best practices throughout the book, but while we're on the topic of employee productivity, I want to take this opportunity to stress a couple of important points: It's absolutely critical to have carefully crafted security incident plans and email contingency plans.

On the same note, it's equally important to ensure that there is a solid communications plan between the various departments responsible for email, telephones, HR, and so on. I can't tell you how many times I've been involved with or seen from the outside various organizations' email systems that have been taken down either intentionally or unintentionally without effectively communicating what's going on to the end users.

In particular, I've seen instances in which email access goes down and yet no one has communicated that fact to the end users via telephone (or some other method). In turn, no one knows what has happened, what to do, when it will be up, and so on. This snowball effect can wreak havoc in larger organizations. It's absolutely critical to ensure that everyone's expectations have been set, including timeframes and alternative methods for email so that downtime has minimal impact on the business.

 We'll cover the essential policies and procedures required for effective email management in Chapter 6.

 Effective policies and procedures are essential to minimize the impact of email disruptions.


Looking at What Can Happen

There are various employee productivity issues that can arise from both the usage and lack of usage of email. A lot of these issues are HR related, so be sure to get the appropriate people involved. Here are some productivity increases that email can provide:

- Provides almost real-time communications
- Helps eliminate the dreaded game of phone tag
- Saves time sending documents to coworkers, customers, and partners
- Facilitates remote collaboration on projects
- Facilitates and can even speed decision making within an organization

Of course, with these productivity gains come some productivity losses. According to Ferris Research, the average corporate email user spends an average of 5 minutes dealing with each email! Gartner estimates that the average American worker spends 4 hours per day writing, reading, and forwarding emails. Based on my experience, these numbers seem very accurate. The following list offers a few additional considerations regarding the negative side of email productivity:

- Wasting time filtering out the good email from the spam
- Fighting off malware, which requires end user time and effort
- Utilization of IT and Help desk resources
- People handling personal business while at work

 A recent study by Vault indicated that 76 percent of respondents stated that they use company systems for personal email.

All in all, there's a general belief that the benefits of email outweigh its risks. That's ultimately a business decision that your organization will have to make. Email is already engrained in many of today's business processes, and organizations without it will most likely be left behind. Given this situation, it's best to embrace email, educate yourself and upper management about ongoing email and messaging issues, and integrate email as part of your organization's overall system of policies, procedures, and processes.

Summary

In this chapter, we've briefly touched on email usage and applications, the changing face of email, the threats and vulnerabilities involved with using it, and the effect of email on employee productivity. This is just the tip of the iceberg. We will cover these topics in much more detail throughout the rest of the book.

New messaging technologies are coming and so are new threats and issues revolving around employee usage. To make the most of this essential method of communication, you and your upper management must learn and embrace what it takes to manage and secure your organization's email while still using it to its utmost capabilities.

Time is of the essence. Time is money. The more quickly you get a handle on and streamline your email management, the more effective organizational communications will be. This effectiveness can, in turn, result in increased employee productivity and morale. This business value is what upper management will notice and understand. How's that for return on your email investment.