# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Business Use of Email</td>
<td>4</td>
</tr>
<tr>
<td>Keeping the Email On</td>
<td>4</td>
</tr>
<tr>
<td>Sensitive Data in Company Emails</td>
<td>5</td>
</tr>
<tr>
<td>Email Security Issues</td>
<td>6</td>
</tr>
<tr>
<td>A Killer App is a Killer Target</td>
<td>6</td>
</tr>
<tr>
<td>Spam</td>
<td>9</td>
</tr>
<tr>
<td>Phishing</td>
<td>12</td>
</tr>
<tr>
<td>Spyware &amp; Viruses</td>
<td>13</td>
</tr>
<tr>
<td>Denial-of-Service Attacks</td>
<td>16</td>
</tr>
<tr>
<td>Employees</td>
<td>18</td>
</tr>
<tr>
<td>Regulatory and Legal Compliance</td>
<td>21</td>
</tr>
<tr>
<td>Retention, Retrieval and Archiving</td>
<td>22</td>
</tr>
<tr>
<td>Protecting Business Email</td>
<td>24</td>
</tr>
<tr>
<td>Integrating Multiple Types of Protection</td>
<td>24</td>
</tr>
<tr>
<td>Integrating Multiple Layers of Protection</td>
<td>26</td>
</tr>
<tr>
<td>Leveraging a Remote Management Model</td>
<td>27</td>
</tr>
<tr>
<td>Conclusion</td>
<td>30</td>
</tr>
<tr>
<td>About Webroot</td>
<td>31</td>
</tr>
<tr>
<td>Appendix</td>
<td>32</td>
</tr>
<tr>
<td>Sources</td>
<td>36</td>
</tr>
</tbody>
</table>
Email is vital in business communications. Companies worldwide are dependent upon it. It is used to communicate with customers and employees on a daily basis. At the same time that companies are generating huge volumes of email, cyber criminals are targeting email knowing that it is a data form rich in valuable personal and corporate information.

In spite of measures taken by companies and organizations to protect against spam, viruses, spyware and other online threats, most of these efforts have only been partially successful at best. It is a constant challenge to stay ahead of the spammers and malware writers. Fortunately, there are new methods available to help companies more effectively secure their email and other valuable data.

In February 2008, Webroot® conducted a survey of 1,494 email security decision-makers to explore their views about email-related threats and the latest methods to protect business email. The survey revealed that email security threats are having a significant impact on businesses worldwide, underscoring the need for a multi-layered approach to Internet security. Highlights of the study include:

Email is Business Critical

- According to IDC, over 6.62 trillion business emails will be exchanged in 2008.
- Three-fourths of Webroot survey respondents rely on email for communicating with customers and providing customer support.
- Over 60 percent of respondents had at least one email outage in 2007.
- One out of three survey respondents said that the hourly cost of an email outage is over $1,000; and approximately seventeen percent of the survey respondents estimated that an email outage costs $5,000 or more per hour.

Risks to and from Email were Prevalent in 2007

- More than half surveyed experienced spyware and virus attacks via email.
- Over 40 percent experienced a phishing attack.
- About one out of four dealt with a denial-of-service attack.

Employee Behavior Increases Email Security Risks

- Individual email users open messages before realizing they are spam, open messages in junk folders and even make purchases from emails marked as spam.
- One out of five Webroot survey respondents estimated that employees in their organization spend an hour or more per day doing personal email at work.
- One out of three organizations reported employee misuse of email resources.
- Less than a third of organizations surveyed have key employee email security policies in place.
Legal Compliance Drives Email Security Requirements

- Over a third of Webroot survey respondents were very or extremely concerned about compliance with email archiving requirements.
- Close to 40 percent of respondents were required to retrieve emails for compliance reasons.
- There was a noteworthy difference in retrieval requirements between regulated and unregulated industries. Fifty-six percent of organizations in regulated industries were required to retrieve email for compliance reasons. In contrast, only about 32 percent of organizations in unregulated industries were required to retrieve email for compliance reasons.

Spam had Serious Impacts on Organizations in 2007

- One out of three organizations experienced slowed system performance as a result of spam.
- Spam drained IT resources and disrupted business activities for about one out of four organizations.
- About one out of five organizations reported that sensitive online transactions were threatened and confidential information was compromised as a result of spam.
INTRODUCTION

“As their dependence on email grows, some firms find ever-bigger problems.”

The timeliness of this headline might lead readers to think it was in this morning’s paper, yet the Herald Tribune story that accompanied this headline was published in 2001. While information technology and the Internet have rapidly evolved in many respects over recent years, there are at least two things that have remained constant:

→ The efficient running of businesses around the world – and thus the global economy – depends upon online communications, in particular email.
→ There is an ever-present risk of online communications being compromised.

For some, email may seem like yesterday’s news, however business dependence on email is greater than ever before, and the number of people seeking to misappropriate and misuse company email for financial gain is ever greater as well. While email is certainly not new in 2008, the volume of email, the types of sensitive data contained in business email, and most importantly, the creative methods that would-be thieves devise to steal business email have changed over time. These online criminals use sophisticated tools to find unprotected and vulnerable networks and computers. In addition, many of today’s online security threats are much more difficult to detect and remove.

As a result, companies need to be ever-vigilant in their efforts to protect business email. This is particularly true for small and medium-sized organizations that have fewer financial and personnel resources than larger companies, and thus rarely have the same level of expertise and technological protection.

Fortunately, the tools and methods available to protect this business-critical application continue to evolve, providing more effective email security than ever before. Companies need to have comprehensive, layered approach. One of the newest developments is software-as-a-service (SaaS) email security that can provide enterprise class protection to every size company.

This edition of the State of Internet Security, published quarterly by Webroot, concentrates on current email related threats, and the latest methods to protect business email. In conjunction with the publication of this report, Webroot conducted an Email Security Survey of 1,494 email security decision makers in companies across seven countries: Australia, Canada, France, Germany, Japan, the United Kingdom and the United States. The results of the February 2008 survey are interspersed throughout this report.
Keeping the Email On

For many companies, email has become as essential as electricity to running the business. According to the study, “Growing Business Dependence on the Internet,” issued by the Business Roundtable in September, 2007:

“By 2010, the Internet is expected to save U.S. businesses approximately $500 billion… A significant portion of these savings can be attributed to productivity gains that the Internet confers on businesses, by reducing time and effort involved in communicating ideas and information and consequently, workers can accomplish more during a given period of time.”

In March 2007, industry analyst firm IDC issued a report by Mark Levitt entitled, “Worldwide Email Usage 2007–2011 Forecast: Resurgence of Spam Takes Its Toll,” estimating that 6.62 trillion person-to-person business emails will be exchanged in 2008. In comparison, the report estimates 1.68 trillion business emails were sent in 2000; and 7.15 trillion business emails will be sent in 2011.

According to the Webroot Email Security Survey, email is critical to communicating with customers and providing customer support. The majority of companies and organizations surveyed also rely on email as a communication and collaboration tool among employees and to process sales transactions.

<table>
<thead>
<tr>
<th>Business Task</th>
<th>Overall (N=1494)</th>
<th>Australia (N=200)</th>
<th>Canada (N=208)</th>
<th>France (N=205)</th>
<th>Germany (N=200)</th>
<th>Japan (N=206)</th>
<th>UK (N=201)</th>
<th>US (N=274)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communicating with customers</td>
<td>74.1%</td>
<td>79.8%</td>
<td>75.4%</td>
<td>78.0%</td>
<td>68.0%</td>
<td>68.5%</td>
<td>71.2%</td>
<td>81.8%</td>
</tr>
<tr>
<td>Providing customer support</td>
<td>63.6%</td>
<td>71.7%</td>
<td>73.5%</td>
<td>60.0%</td>
<td>53.0%</td>
<td>43.3%</td>
<td>68.2%</td>
<td>75.7%</td>
</tr>
<tr>
<td>Communication and collaboration among employees</td>
<td>61.6%</td>
<td>72.5%</td>
<td>70.2%</td>
<td>61.0%</td>
<td>50.5%</td>
<td>45.6%</td>
<td>54.2%</td>
<td>77.1%</td>
</tr>
<tr>
<td>Processing sales transactions</td>
<td>55.8%</td>
<td>60.9%</td>
<td>63.0%</td>
<td>56.2%</td>
<td>46.0%</td>
<td>53.4%</td>
<td>46.9%</td>
<td>64.2%</td>
</tr>
<tr>
<td>Communicating with investors</td>
<td>39.9%</td>
<td>44.1%</td>
<td>51.5%</td>
<td>44.0%</td>
<td>29.4%</td>
<td>22.3%</td>
<td>32.8%</td>
<td>55.5%</td>
</tr>
</tbody>
</table>

Sensitive Data in Company Emails

Account numbers and sensitive information are often included in email correspondence since it is a primary method of communication with customers, among employees and when processing sales transactions and providing customer support. Some of the types of company data that may be transmitted and stored in email include:

- Customer support personnel collecting or providing account information, credit card numbers and customer personal data.
- Terms of partner arrangements and discussion about terms for partner agreements.
- Sales team exchanging information about competitors, progress with prospects, sales revenue targets, sales forecasts, responses to proposal requests, distribution rights and profit margins.
- Finance staff information about cash flow, customer accounts, debts, taxes, shareholder information and company results.
- Engineering department online conversations about product roadmaps, product development progress, patent issues, intellectual property and industry standards.
- Marketing information about company strategy, messaging, lead generation, events, advertising, media releases and time-sensitive market announcements.

In March 2007, the National Federation of Independent Businesses and Visa USA announced the results of a survey of companies with fewer than 250 employees. Fifty-two percent said they keep at least one type of sensitive customer information, such as social security numbers or credit card numbers. Often this information may be collected or inadvertently stored in emails. Yet, an alarming 61 percent said they have never sought information about how to properly handle and store customer information. In the same survey, 57 percent did not see securing customer data as something that requires formal planning, and 39 percent said they simply rely on “common sense” to keep data safe.
EMAIL SECURITY ISSUES

A Killer App is a Killer Target
Most businesses, large and small, around the world cannot function without email. With so many people accustomed to doing business via email, and so much data transmitted and collected via email, it’s an obvious target for scammers and thieves. The Business Roundtable’s September 2007 report reinforced this point: “Continually increasing reliance on the Internet now places technology at the center of many fundamental business operations, making them more vulnerable.”

A significant factor in numerous email attacks is the “black market” economy operating to buy and sell government issued identification numbers (like social security numbers in the United States and driver’s license numbers in most countries), credit card numbers, bank account numbers, personal identification numbers and other highly sensitive and/or personally identifiable data.

According to the most recent report of the Internet Crime Complaint Center, a partnership between the U.S. Federal Bureau of Investigation and the National White Collar Crime Center, of all the fraudulent acts reported in 2006, 73.9 percent used email as the mechanism of contact. CSO Magazine, the U.S. Secret Service, the Carnegie Mellon University Software Engineering Institute’s CERT Program and Microsoft collaborate to produce the annual eCrime Watch report. In the most recent release, issued in September 2007, one third of respondents reported that the number of security events experienced by their organizations increased over the previous 12 months. In the same report, 57 percent said they are more concerned about cyber security threats facing their organizations in the coming year.

Of all the fraudulent acts reported in 2006, 73.9 percent used email as the mechanism of contact.

With so many people accustomed to doing business via email, and so much data transmitted and collected via email, it’s an obvious target for scammers and thieves.
This trend was reinforced in the Webroot Email Security Survey findings. Over 40 percent of respondents anticipate a moderate to substantial increase of spam in 2008, and approximately one third of respondents expect a moderate to substantial increase of spyware and viruses in 2008.

<table>
<thead>
<tr>
<th>Expecting a Moderate to Significant Increase in 2008</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam</td>
<td>43.7%</td>
</tr>
<tr>
<td>Spyware</td>
<td>34.5%</td>
</tr>
<tr>
<td>Viruses</td>
<td>30.8%</td>
</tr>
<tr>
<td>Denial-of-Service (DoS)</td>
<td>19.9%</td>
</tr>
</tbody>
</table>

Source: Webroot Email Security Survey, February 2008 (N = 1494)

The survey also evaluated specific areas of concern related to email security:

- Spam
- Infections from viruses and spyware
- Employees sending sensitive company information externally
- Data breaches
- Compliance with email archiving requirements
- Legal liability of offensive incoming emails
- Losses from email outages
- Denial-of-service attacks
- Inaccurately blocking legitimate emails
- Ensuring email confidentiality

Of these, infections from spyware and viruses was the greatest concern in every country surveyed.

<table>
<thead>
<tr>
<th>Concerns About Email Security Issues</th>
<th>Very or Extremely Concerned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infections from viruses and spyware</td>
<td>70.0%</td>
</tr>
<tr>
<td>Data breaches</td>
<td>59.1%</td>
</tr>
<tr>
<td>Spam</td>
<td>59.9%</td>
</tr>
<tr>
<td>Ensuring email confidentiality</td>
<td>58.1%</td>
</tr>
<tr>
<td>Inaccurately blocking legitimate emails</td>
<td>52.0%</td>
</tr>
<tr>
<td>Losses from email outages</td>
<td>50.2%</td>
</tr>
<tr>
<td>Denial-of-service attacks</td>
<td>48.4%</td>
</tr>
<tr>
<td>Employees sending confidential or internal-only company information externally</td>
<td>48.5%</td>
</tr>
<tr>
<td>Legal liability of offensive incoming emails</td>
<td>43.6%</td>
</tr>
<tr>
<td>Compliance with email archiving requirements</td>
<td>36.4%</td>
</tr>
</tbody>
</table>

Source: Webroot Email Security Survey, February 2008 (N = 1494)
These concerns are rooted in their experiences over the past year. More than half of the survey respondents experienced spyware and virus attacks in 2007. Close to 80 percent dealt with spam, and over 40 percent were confronted with a phishing attack.

<table>
<thead>
<tr>
<th>Attacks on Business Email in 2007</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of Attack</strong></td>
</tr>
<tr>
<td>Spam</td>
</tr>
<tr>
<td>Viruses or Worms</td>
</tr>
<tr>
<td>Spyware (Trojan horse, key logger, system monitor or root kit)</td>
</tr>
<tr>
<td>Phishing or Pharming</td>
</tr>
<tr>
<td>Employee misuse of email resources</td>
</tr>
<tr>
<td>Denial-of-Service</td>
</tr>
</tbody>
</table>


More than half of the survey respondents experienced spyware and virus attacks in 2007.
Spam

The IDC study, “Worldwide Email Usage 2007–2011 Forecast: Resurgence of Spam Takes Its Toll,” cited earlier, estimates that there will be 11.95 trillion spam (unsolicited bulk email) messages in 2008. IDC estimates that in 2000 there were 4.02 trillion spam messages and in 2011 there will be 33.07 trillion spam messages. According to Webroot tracking data, spam has accounted for about 90 percent of all email managed by its Software-as-a-Service (SaaS) Email Security Solution over the past year.

In a survey conducted by the Pew Internet & American Life Project from February to March 2007, 29 percent of email users said spam in their work email accounts is increasing. When the same question was asked by Pew two years earlier, only 21 percent said spam in their work email accounts was increasing. The growing volume increases the likelihood that an email user can inadvertently open spam. In fact, 27 percent of the Pew survey respondents said they occasionally open an email message before realizing it is spam.

Even when there is strong antispam protection in place, human behavior often undermines the effectiveness of the technical solutions. Endai Worldwide, an Internet marketing company, issued results of a survey in December 2007 that found half of email users check their junk mail folder on a daily basis. Spammers use social engineering techniques to create ‘from’ identities and subject lines that are very compelling. Thus the more frequently users look over emails marked as junk, the more often they will be driven by confusion or curiosity to open a spam message. Particularly concerning is that 16 percent of the Endai survey respondents reported making a purchase from a message tagged as spam. Even a small percent of people clicking and buying generates a significant incentive for spammers to expand their businesses.

Ironically, the better the spam filtering tools and the savvier email users become, the more spam that is generated. This is because in order to increase or maintain the chances for a spam message to be opened, spammers must continuously increase the amount of spam they send. The premise is that if they send enough spam then they can be successful even if only a very small percent of the messages they send are opened.

Another facet driving an increase in the volume of spam is its use to proliferate more spam. Initially, spam messages abused open SMTP relays. Then as those became less common, spammers began relying on proxy servers to deliver their spam. Today, spammers often hijack computers and create botnets (networks of compromised computers controlled by a single master) to generate and deliver spam across the Internet.

This ever growing volume of spam hits most companies around the world. According to the Webroot Email Security Survey, approximately 80 percent of companies and organizations dealt with problems associated with spam in 2007.
All of this spam is far more than just a nuisance for companies. It has direct business impacts including:

- Slowing system performance
- Reducing employee productivity
- Draining IT resources
- Increasing help desk time to repair damage
- Disrupting business activities
- Threatening sensitive online transactions
- Compromising confidential information
- Causing loss of sales

In the Webroot Email Security Survey, approximately one third of the respondents said they experienced a moderate to major impact on system performance and employee productivity as a result of spam in 2007. Spam drained IT resources and disrupted business activities for about one out of four organizations. About one out of five organizations reported that sensitive online transactions were threatened and confidential information was compromised as a result of spam.
Sixty percent of the Webroot survey respondents are very or extremely concerned about spam.

The risks and impacts associated with spam are clearly on the minds of many company personnel in charge of email security. Sixty percent of the Webroot survey respondents are very or extremely concerned about spam, and in Japan that number was closer to 70 percent. In contrast, a much smaller percent (37%) of respondents in Germany were very or extremely concerned.

Fighting spam is particularly tricky because of the risk that legitimate email can be falsely identified as spam. Given companies’ dependence on email to communicate with their customers, this can be particularly concerning. In fact, half of the Webroot survey respondents are very or extremely concerned about inaccurately blocking legitimate emails. Concerns about false positives will make the selection of a very sophisticated antispam solution even more important to these companies.

### Moderate or Major Spam Impact in 2007

<table>
<thead>
<tr>
<th>Type of Impact</th>
<th>Overall (N=1494)</th>
<th>Australia (N=200)</th>
<th>Canada (N=208)</th>
<th>France (N=205)</th>
<th>Germany (N=200)</th>
<th>Japan (N=206)</th>
<th>UK (N=201)</th>
<th>US (N=274)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slowed system performance</td>
<td>34.3%</td>
<td>42.1%</td>
<td>42.6%</td>
<td>46.1%</td>
<td>23.9%</td>
<td>7.8%</td>
<td>33.9%</td>
<td>44.0%</td>
</tr>
<tr>
<td>Reduced employee productivity</td>
<td>29.4%</td>
<td>36.2%</td>
<td>38.0%</td>
<td>33.7%</td>
<td>23.5%</td>
<td>3.9%</td>
<td>26.5%</td>
<td>44.1%</td>
</tr>
<tr>
<td>Drained IT resources or increased help desk time to repair damage</td>
<td>27.9%</td>
<td>32.0%</td>
<td>37.1%</td>
<td>39.8%</td>
<td>21.0%</td>
<td>5.4%</td>
<td>29.1%</td>
<td>30.9%</td>
</tr>
<tr>
<td>Disrupted business activities</td>
<td>24.9%</td>
<td>27.0%</td>
<td>33.2%</td>
<td>29.6%</td>
<td>18.7%</td>
<td>5.8%</td>
<td>22.7%</td>
<td>37.5%</td>
</tr>
<tr>
<td>Threatened sensitive online transactions</td>
<td>19.3%</td>
<td>21.8%</td>
<td>30.1%</td>
<td>22.7%</td>
<td>13.3%</td>
<td>3.4%</td>
<td>15.9%</td>
<td>27.6%</td>
</tr>
<tr>
<td>Compromised confidential information</td>
<td>18.7%</td>
<td>19.8%</td>
<td>27.7%</td>
<td>29.3%</td>
<td>14.9%</td>
<td>1.5%</td>
<td>13.2%</td>
<td>24.2%</td>
</tr>
<tr>
<td>Caused loss of sales</td>
<td>14.5%</td>
<td>15.1%</td>
<td>25.8%</td>
<td>12.3%</td>
<td>15.2%</td>
<td>1.9%</td>
<td>10.9%</td>
<td>20.2%</td>
</tr>
</tbody>
</table>

Phishing
Phishing is a particularly harmful type of spam. In 2005, the Financial Services Technology Consortium defined phishing as the fraudulent acquisition of personal information by tricking an individual into believing the attacker is a trustworthy entity. The U.S. Federal Trade Commission calls phishing “a scam where Internet fraudsters send spam or pop-up messages to lure personal and financial information from unsuspecting victims.”

Phishing attacks are often designed to gain valuable, personal information from individuals. Stories about people whose money or identity have been stolen as a result of a phishing attack have become all too common. Yet, phishing also has a significant impact on organizations doing business online and communicating with customers via email.

Some phishing attacks, often called “spear phishing,” are targeted at individual companies, government agencies or organizations, and rather than an individual credit card, these ploys attempt to steal whole files of valuable information, customer data or intellectual property. As recently as December 2007, large, highly visible U.S.-based organizations such as the Oakridge National Energy Lab and Salesforce.com shared publicly that they had been the targets of two separate spear phishing attacks. In both cases, files containing sensitive information were stolen including social security numbers from Oakridge and customer lists from Salesforce.
Four out of ten respondents in the Webroot Email Security Survey saw some form of a phishing attack at their organization in 2007. Japan was the one country where the phishing incidence was significantly lower at only 13 percent.

**Spyware and Viruses**

The number of malicious programs has risen steadily in recent years. In a February 8, 2008 article entitled “Malicious Programs Hit New High,” BBC News reported 5.49 million unique samples of malicious software. There are several factors that explain the explosive growth in malicious programs over the past year:

- Greater volume of higher quality malware programs
- More complex, sophisticated attacks
- Continuously evolving threats
- Derivatives and blended threats designed to bypass detection

Ultimately, all these factors demonstrate that this has clearly become a very big business. Successful spyware writers reap significant financial rewards, usually in the form of bank passwords and personal information, such as social security numbers, credit card information, as well as Web site and e-mail usernames and passwords. Beyond individuals chasing these financial gains, there has also been greater involvement from organized crime groups in recent years. The deputy chief of the computer crimes and intellectual property section of the U.S. Department of Justice, has said, “There are still instances of ‘lone-gunman’ hackers but more and more we are seeing organized criminal groups.” Cybercrime has become a top priority for the law enforcement agencies as it overlaps organized crime, as well as state-sponsored and terrorist organizations.

Of all the email security issues included in the Webroot Email Security Survey, infections from spyware and viruses were the most concerning. Seventy percent of survey respondents were very or extremely concerned about infections from spyware and viruses. In Japan this number was over 80 percent, and in the U.S. and Australia it was more than three fourths of respondents. Respondents in Germany stood out as the least concerned, with fewer than half of respondents saying they are very or extremely concerned about spyware and viruses.
The high level of concern about spyware and viruses is not surprising given the high rates of attack that companies experienced in 2007.

In every country but Japan (only 29%), over half of the companies surveyed dealt with spyware in 2007. In contrast to viruses, which typically make their presence known by spreading across many systems simultaneously and impacting machine functionality, the success of spyware programs depends on their stealth nature. Given the significant financial incentives to stealing sensitive data or serving nuisance advertising, spyware program writers are adept at covertly infiltrating a system and installing programs deep within a computer or network. The potential for financial reward is a strong incentive for the ongoing proliferation of spyware at higher rates than viruses or other types of malware.
Email is a common delivery mechanism for spyware and viruses. One type of spyware that can be delivered via email are Trojan horses, intended to run undetected on a computer and grant the spyware sender access to the data stored on the machine. Trojans can be used to steal confidential business information and intellectual property, as well as valuable customer and employee data files that include personally identifiable information.

Webroot conducted a survey of small and medium-sized businesses in six countries in September 2007 which gathered information about the effects that spyware and viruses have on businesses. Over half of the respondents experienced slowed system performance, reduced employee productivity, disrupted business activities and increased use of help desk resources as a result of spyware and viruses in the first half of 2007.

<table>
<thead>
<tr>
<th>How SMBs are Affected by Spyware and Viruses</th>
<th>US</th>
<th>Canada</th>
<th>France</th>
<th>Germany</th>
<th>Japan</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>SpYware Virus SpYware Virus SpYware Virus SpYware Virus SpYware Virus SpYware Virus</td>
<td>47.2%</td>
<td>47.5%</td>
<td>32.9%</td>
<td>32.9%</td>
<td>24.4%</td>
<td>33.0%</td>
</tr>
<tr>
<td>Caused Lost Sales</td>
<td>47.7%</td>
<td>52.5%</td>
<td>43.1%</td>
<td>40.3%</td>
<td>37.8%</td>
<td>39.4%</td>
</tr>
<tr>
<td>Compromised Confidential Info</td>
<td>79.1%</td>
<td>73.4%</td>
<td>67.5%</td>
<td>60.6%</td>
<td>66.4%</td>
<td>62.6%</td>
</tr>
<tr>
<td>Disrupted Business Activities</td>
<td>80.7%</td>
<td>74.2%</td>
<td>74.0%</td>
<td>67.2%</td>
<td>54.4%</td>
<td>51.8%</td>
</tr>
<tr>
<td>Drained IT Resources</td>
<td>82.6%</td>
<td>74.1%</td>
<td>77.5%</td>
<td>67.2%</td>
<td>58.0%</td>
<td>55.0%</td>
</tr>
<tr>
<td>Reduced Employee Productivity</td>
<td>86.5%</td>
<td>76.4%</td>
<td>82.9%</td>
<td>73.2%</td>
<td>68.3%</td>
<td>62.6%</td>
</tr>
<tr>
<td>Slowed System Performance</td>
<td>61.0%</td>
<td>53.4%</td>
<td>40.9%</td>
<td>39.7%</td>
<td>35.6%</td>
<td>32.9%</td>
</tr>
</tbody>
</table>

Source: Webroot SMB Survey, September 2007 (N=1842)
Denial-of-Service Attacks

According to the United States Computer Emergency Readiness Team (US-CERT) Web site, a denial-of-service (DoS) attack is when an attack successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. By targeting computers’ network connections, an attacker may be able to obstruct access to email, Web sites, online accounts (banking, etc.), or other services that rely on the affected computer(s). In a distributed denial-of-service (DDoS) attack, an attacker uses one computer to attack other computers. The attack is “distributed” because the attacker is using multiple computers to launch the denial-of-service attack.

Denial-of-service attacks can effectively shut down an organization’s Internet connection and result in email outages among other problems. One particularly noteworthy denial-of-service attack occurred in April 2007 against the government of Estonia. According to an article in the May 10 issue of The Economist, the attack was launched by a group or groups within Russia who were furious about the removal of a Soviet war monument from the center of Tallinn, Estonia’s capital. The attacks continued for several weeks and government officials in Estonia said it caused significant harm to the country’s economy.

These same types of attacks are sometimes launched against specific companies. Reasons for these attacks range from disgruntled customers, to groups with various political or personal agendas, to financially motivated cyber criminals who request a ransom to end the attack.

About one fourth of all the respondents to the Webroot Email Security Survey said they experienced a denial-of-service attack in 2007. This number was closer to one third in Canada, Australia and Germany, but significantly lower (10%) in Japan.

Organizations Reporting a Denial-of-Service Attack in 2007

<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td>31%</td>
</tr>
<tr>
<td>Australia</td>
<td>30%</td>
</tr>
<tr>
<td>Germany</td>
<td>30%</td>
</tr>
<tr>
<td>UK</td>
<td>28%</td>
</tr>
<tr>
<td>USA</td>
<td>23%</td>
</tr>
<tr>
<td>France</td>
<td>19%</td>
</tr>
<tr>
<td>Japan</td>
<td>10%</td>
</tr>
</tbody>
</table>

Source: Webroot Email Security Survey, February 2008 (N=1494)
These types of attacks clearly raise serious concerns for IT security experts. The number of survey respondents that said they are very or extremely concerned about a possible denial-of-service attack was double the number of respondents that had actually experienced such an attack in 2007. Interestingly, respondents in Japan expressed the greatest amount of concern, even though they reported the lowest number of denial-of-service attacks.

<table>
<thead>
<tr>
<th>Very or Extremely Concerned about Denial-of-Service Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall (N=1494)</td>
</tr>
<tr>
<td>48.4%</td>
</tr>
</tbody>
</table>


It is understandable why concerns would be greater than experience, given the impacts an email outage can have on a company. Over 60 percent of the companies that participated in the Webroot Email Security Survey experienced at least one email outage in 2007, and almost 15 percent experienced more than eight email outages during the year. This number was considerably higher in Australia, where almost 30 percent of respondents had more than eight email outages in 2007.

<table>
<thead>
<tr>
<th>Number of Email Outages in 2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Outages</td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2 to 3</td>
</tr>
<tr>
<td>4 to 7</td>
</tr>
<tr>
<td>8 or more</td>
</tr>
<tr>
<td>Don’t know</td>
</tr>
</tbody>
</table>


Each outage can be very costly. One out of three survey respondents said that the hourly cost of an email outage is over $1,000; and approximately seventeen percent of the survey respondents estimated that an email outage costs $5,000 or more per hour.
Employees

In addition to spammers, spyware purveyors and information thieves, companies also face a threat from within when employees either intentionally or unintentionally compromise sensitive business data or intellectual property.

In the 2007 eCrime Watch report, sponsored by CSO Magazine, the U.S. Secret Service, the Carnegie Mellon University Software Engineering Institute’s CERT Program and Microsoft, current employees were second only to hackers as groups that posed the greatest cyber security threat to the organization in the past 12 months. According to the UK Department of Trade and Industry’s Information Security Breaches Survey 2006, inappropriate Web and email usage is the second largest cause of reported security incidents.

One out of three organizations reported employee misuse of email resources occurred in 2007. In Australia, Canada and the United States over 40 percent of organizations reported dealing with employee misuse of email last year.
Employees accessing personal emails and non-work related Web sites can inadvertently put company information at risk when they open emails and files infected with spyware. Employees can also use email to inappropriately send internal documents to recipients outside the organization. Approximately half of the Webroot survey respondents are very or extremely concerned about their employees sending sensitive information externally.

Excluding any malicious acts of sabotage on the part of employees, the unintentional acts of individuals within a company can pose a significant email security risk, particularly when they are using company computers to access personal email accounts. One out of five Webroot survey respondents estimated that employees in their organization spend an hour or more per day doing personal email at work. Assuming these estimates approximate the actual time spent, employees are spending over one full work week a year on personal email.
The Office of the Inspector General at the U.S. Department of Interior conducted an investigation in 2006 and found that the personal Internet use of their 80,000 employees was costing the Department almost $39,000 per week and over $2 million a year.

In spite of all the concerns about employees and the risks their personal email use can present to organizations, fewer than one third of organizations reported having key employee email security policies in place.

<table>
<thead>
<tr>
<th>Amount of Time</th>
<th>Overall (N=1494)</th>
<th>Australia (N=200)</th>
<th>Canada (N=208)</th>
<th>France (N=205)</th>
<th>Germany (N=200)</th>
<th>Japan (N=206)</th>
<th>UK (N=201)</th>
<th>US (N=274)</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>3.1%</td>
<td>0.5%</td>
<td>2.4%</td>
<td>4.4%</td>
<td>3.5%</td>
<td>5.8%</td>
<td>3.0%</td>
<td>1.8%</td>
</tr>
<tr>
<td>1-9 minutes</td>
<td>17.6%</td>
<td>16.0%</td>
<td>11.1%</td>
<td>26.8%</td>
<td>20.5%</td>
<td>25.2%</td>
<td>15.4%</td>
<td>8.0%</td>
</tr>
<tr>
<td>10-29 minutes</td>
<td>33.8%</td>
<td>32.0%</td>
<td>37.2%</td>
<td>35.1%</td>
<td>35.0%</td>
<td>35.0%</td>
<td>31.8%</td>
<td>34.9%</td>
</tr>
<tr>
<td>30-59 minutes</td>
<td>19.1%</td>
<td>18.5%</td>
<td>23.6%</td>
<td>14.6%</td>
<td>15.0%</td>
<td>13.1%</td>
<td>25.4%</td>
<td>23.3%</td>
</tr>
<tr>
<td>1 hour</td>
<td>11.0%</td>
<td>16.5%</td>
<td>12.0%</td>
<td>9.3%</td>
<td>11.5%</td>
<td>6.8%</td>
<td>11.4%</td>
<td>9.5%</td>
</tr>
<tr>
<td>2 hours</td>
<td>6.5%</td>
<td>7.0%</td>
<td>9.6%</td>
<td>4.9%</td>
<td>6.5%</td>
<td>1.0%</td>
<td>6.0%</td>
<td>10.2%</td>
</tr>
<tr>
<td>3 or more hours</td>
<td>4.7%</td>
<td>6.0%</td>
<td>3.8%</td>
<td>1.0%</td>
<td>5.0%</td>
<td>2.4%</td>
<td>5.0%</td>
<td>9.8%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>4.3%</td>
<td>3.5%</td>
<td>4.8%</td>
<td>3.9%</td>
<td>3.0%</td>
<td>10.7%</td>
<td>2.0%</td>
<td>2.5%</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Email Security Policy</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prohibit access to personal (non-business) email accounts</td>
<td>31.9%</td>
</tr>
<tr>
<td>Require global confidentiality signature (auto signature included in all outbound email stating confidentiality policy)</td>
<td>25.0%</td>
</tr>
<tr>
<td>Prohibit sending emails to personal accounts</td>
<td>29.2%</td>
</tr>
</tbody>
</table>

Source: Webroot SMB Survey, September 2008 (N=1494)
Regulatory and Legal Compliance

In addition to the business risks associated with email security issues, companies also face regulatory compliance issues as a result of their email dependence.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Overall (N=1494)</th>
<th>Australia (N=200)</th>
<th>Canada (N=208)</th>
<th>France (N=205)</th>
<th>Germany (N=200)</th>
<th>Japan (N=206)</th>
<th>UK (N=201)</th>
<th>US (N=274)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data breaches</td>
<td>59.1%</td>
<td>63.5%</td>
<td>63.5%</td>
<td>63.4%</td>
<td>36.5%</td>
<td>65.1%</td>
<td>54.2%</td>
<td>67.3%</td>
</tr>
<tr>
<td>Ensuring email confidentiality</td>
<td>58.1%</td>
<td>65.0%</td>
<td>64.9%</td>
<td>60.0%</td>
<td>35.0%</td>
<td>63.1%</td>
<td>50.2%</td>
<td>68.4%</td>
</tr>
<tr>
<td>Legal liability of offensive incoming emails</td>
<td>43.6%</td>
<td>48.5%</td>
<td>50.5%</td>
<td>39.5%</td>
<td>20.5%</td>
<td>56.8%</td>
<td>39.8%</td>
<td>49.8%</td>
</tr>
<tr>
<td>Compliance with email archiving requirements</td>
<td>36.4%</td>
<td>41.0%</td>
<td>43.8%</td>
<td>37.1%</td>
<td>15.5%</td>
<td>39.8%</td>
<td>28.9%</td>
<td>48.4%</td>
</tr>
</tbody>
</table>


Governments in many parts of the world have instituted additional data protection measures to compel companies to adequately protect the sensitive customer data in their possession. One of the most well known measures in this regard is the European Union’s Data Protection Directive. This Directive sets out the guidelines on which European countries have crafted their laws. Article 17 of the Directive requires:

> Member States shall provide that the (data) controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, alteration, unauthorized disclosure or access, in particular where processing involves the transmission of data over a network.

Japan enacted a similar measure, the Personal Information Protection Law, in May 2003. In the United States several laws set out data protection requirements. For example, the U.S. Health Insurance Portability and Accountability Act (HIPAA) requires that the privacy of medical records be adequately protected against unauthorized access and misuse. In the financial sector, the Gramm-Leach-Bliley Act requires that organizations which maintain credit information for customers be held accountable if that data is accessed or compromised by an unauthorized third party. Incidents of unauthorized network access and spyware, such as system monitors or Trojans, raise concerns about noncompliance.

In the United States, government offices responsible for protecting consumer interests, such as the U.S. Federal Trade Commission (FTC) and several U.S. state Attorneys General have become increasingly proactive in filing complaints against companies for lax computer security measures. For example, the FTC filed a case against DSW, Inc. (FTC File No. 052-3096) stating the company created unnecessary risks to the personal information collected about consumers in its stores by failing to use readily available security measures to protect its computer networks, nor employing sufficient measures to detect unauthorized access. Additional regulatory compliance information is included in the Appendix.
One way companies can significantly minimize the impacts of data breaches is to encrypt email data. Under some laws, such as California SB 1386, use of encryption can provide an exemption from data breach notification requirements. Further, encrypting emails, especially when archiving, can offer much greater security for the sensitive information contained in business emails.

Another important resource that outlines how companies can protect data is the Payment Card Industry (PCI) Data Security Standard that details these data protection objectives:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

The PCI standard provides details about how to best fulfill each of these objectives. Specific elements of the standard, such as ensuring that antivirus programs can protect against other forms of malicious code such as spyware and adware, offers important guidance for all companies, even those that do not accept credit cards as a form of payment.

Retention, Retrieval and Archiving

In addition to the legal and compliance issues associated with data protection, there are also many laws that detail requirements for data retention and retrieval capabilities. In most jurisdictions, emails have come to be viewed as business documents, making them subject to retention and discovery requirements. In the U.S., amendments to the Federal Rules of Civil Procedure went into effect in 2006 making e-discovery capabilities mandatory for businesses. There are also industry specific requirements about data retention and access. For example, Article 51 of the Markets in Financial Instrument Directive, implemented by the European Commission in 2007, requires organizations to retain details of trades for five years. In the U.S., Securities and Exchange Commission rules and National Association of Securities Dealers requirements dictate that broker/dealer organizations retain all emails pertaining to trading activity for six years.

<table>
<thead>
<tr>
<th>Required</th>
<th>Overall (N=1494)</th>
<th>Australia (N=200)</th>
<th>Canada (N=208)</th>
<th>France (N=205)</th>
<th>Germany (N=200)</th>
<th>Japan (N=206)</th>
<th>UK (N=201)</th>
<th>US (N=274)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>38.5%</td>
<td>44.0%</td>
<td>47.1%</td>
<td>32.8%</td>
<td>34.5%</td>
<td>21.4%</td>
<td>43.0%</td>
<td>46.4%</td>
</tr>
<tr>
<td>No</td>
<td>44.2%</td>
<td>42.5%</td>
<td>34.6%</td>
<td>43.9%</td>
<td>40.5%</td>
<td>64.1%</td>
<td>40.3%</td>
<td>43.6%</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>17.3%</td>
<td>13.5%</td>
<td>18.3%</td>
<td>23.4%</td>
<td>25.0%</td>
<td>14.6%</td>
<td>16.9%</td>
<td>9.8%</td>
</tr>
</tbody>
</table>

Even more important than retaining and storing emails to meet regulatory requirements is the ability of companies to search and retrieve files when necessary. Approximately 40 percent of the companies in the Webroot Email Security Survey had to retrieve emails for a compliance reason in 2007. This is particularly relevant for companies in regulated industries, such as banking, finance, healthcare and telecommunications, where 56 percent were required to retrieve emails for a legal or compliance reason. In contrast, only about a third of companies in non-regulated industries needed to retrieve emails for a legal or compliance reason.

Approximately 40 percent of the companies in the Webroot Email Security Survey had to retrieve emails for a compliance reason in 2007.
PROTECTING BUSINESS EMAIL

Integrating Multiple Types of Protection
In selecting the types of protection needed, companies should consider these business and technical requirements.

Antispam
With spam levels regularly running between 65 and 90 percent, companies need to find antispam solutions that help manage the sheer volume of unwanted email being delivered. Selecting technical solutions that are expertly integrated to provide multiple best-of-breed filters will effectively block the maximum quantities of spam with the lowest number of false positives.

- Greater than 98 percent removal of spam
- Less than .001 percent false positives
- Constantly updated spam definitions
- Spam messages quarantined outside of company network
- Optional custom notifications
- Black lists / White lists
- Real-time control of service via web control panel
- Full logging of all messages in real-time
- Rapid search and audit capabilities
- Real-time graphic reporting about volume, source and target

Antispyware
To accurately detect, block and remove spyware and prevent damage to the network and other computers in the company, organizations need specialized antispyware protection to be part of an overall, centrally managed enterprise solution.

- Comprehensive, automated threat detection that:
  • prevents installation of unauthorized software
  • monitors network use and abuse
  • blocks inappropriate Web content
- Removal of useless files to free up disk space (temp files, memory dumps)
- Custom policies to manage employee Internet, network and application use
- Proactive, accurate threat detection that minimizes false positives
- Minimal impact on desktop performance
- Seamless, scalable deployment
- Flexible, centralized management
- Laptop and remote user management

Respondents’ answer to the question: “What challenges to maintain email security do you foresee in 2008?” are included on this and subsequent pages.

“Spam, spam and more bloody spam!”
- Business Manager, Wholesale Trade Co., Australia
Antivirus
A company’s antivirus solution should include multiple best-of-breed identity-based engines to maximize virus detection. As mass-outbreak viruses tend to replicate and distribute at high speed, the time taken by identity-based antivirus vendors to capture, analyze and release tested updates to the antivirus engines leaves organizations exposed to the threat of virus infection for a period of time. This window has been dubbed the ‘Zero Hour’ syndrome. To meet this challenge, antivirus protection needs to include heuristic filters to seek out new, unknown viruses.

- 100 percent removal of known viruses without false positives
- Multiple antivirus engines scanning every email
- Zero-hour protection against new outbreaks
- Outbound virus filters to protect company reputation
- Constantly updated virus definitions
- Full logging of all messages in real time
- All virus infected messages neutralized and logged
- Custom notifications
- Visibility and control via a Web dashboard
- Rapid search and audit capabilities
- Real-time graphic reporting about volume, source and target

Content Control
Increasingly, employers recognize that they have a duty to minimize users’ exposure to emails that contain distasteful images. Additional content controls to filter these messages and specifically address image analysis should also be included in companies’ email security solution.

- Inbound and outbound message monitoring
- Effectively enforce best practice email use policies
- Filtering based on size, words, identity, time, source, destination and attachment type
- Quarantine, delete, copy or redirect messages to meet any legal requirements
- Workflow systems to trigger notifications to appropriate company departments
- Web control panel to manage reporting and audit

Encryption
Increasingly, companies are instituting encryption technologies and policies to further protect company email from misuse. Historically, reliable encryption has been unachievable for many organizations due to complexity, incompatible standards and the threat of intellectual property leakage and malware infiltration through unscannable encrypted channels. There are now email encryption services that use Transport Layer Security (TLS), making this technology more accessible to a broader range of companies.

- Reliable encryption
- Transport Layer Security (TLS), a transparent mechanism for encrypting data on a peer-to-peer basis, such as between messaging servers
- Filtering of email sent via encrypted channel
- Open, interoperable SSL standard
- Supported by all messaging server vendors

Top email security challenges in 2008:
“Continuing growth in sophistication and subtlety of attacks.”
- CEO, Prof. Services Firm, Canada
Additional Types of Protection
A complete email security solution should also include protection against denial-of-service attacks (DOS) and Directory Harvest attacks (DHA).

Integrating Multiple Layers of Protection
In addition to implementing a combination of different types of protection, companies also need to ensure there are layers of protection, starting at the gateway or perimeter and carrying through to the desktop. Perimeter protection is the first line of defense and offers companies a way to keep much of the problem email from even entering their servers.

Incorporating a layered security approach to the email security solution protects this valuable business application and all the data associated with it. In a layered security solution, if one layer fails to fully neutralize an attack, then the next layer exists to stop the attack or limit damage.

A layered approach to security includes perimeter and endpoint protection, to effectively defend against email and Web threats.

Top email security challenges in 2008:
“Trying to stop staff using the computer at work (for) games and personal use.”

- CEO, Manufacturing Co., Australia
Leveraging a Remote Management Model

How companies manage their protection systems is closely tied to the need for layered protection. At the perimeter, companies can install a gateway appliance or software on their servers, or they can actually move the perimeter further out by using a managed security software as a service (SaaS) perimeter. This approach puts an even larger boundary between the company network and all the spam and malware coming from the Internet.

In addition to placing a greater distance between the “bad stuff” and the company servers, a SaaS model lessens the burden on company resources, eliminates the need for managing constant software updates, and virtually eliminates the IT time required to manage a comprehensive email security solution.

Top email security challenges in 2008:
“People are working from home and it’s hard to deter them from using their work email for personal use.”
- IT Director, Healthcare Company, USA

### Business Benefits of SaaS

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective and Reliable</td>
<td>→ Protects against 98% of spam and 100% of known viruses</td>
</tr>
<tr>
<td></td>
<td>→ Multiple antivirus engines scanning every email</td>
</tr>
<tr>
<td></td>
<td>→ Zero-hour protection against new outbreaks</td>
</tr>
<tr>
<td></td>
<td>→ Outbound virus filters to protect company reputation</td>
</tr>
<tr>
<td>Low Cost</td>
<td>→ No hardware or software installation or maintenance</td>
</tr>
<tr>
<td></td>
<td>→ Predictable, low-risk operating costs</td>
</tr>
<tr>
<td>Fast, Easy Implementation</td>
<td>→ Fast, low-risk deployment</td>
</tr>
<tr>
<td></td>
<td>→ No user disruption</td>
</tr>
<tr>
<td></td>
<td>→ Deployment usually completed within one to four days</td>
</tr>
<tr>
<td>Save Time and Resources</td>
<td>→ Integrated suite of email protection, management and compliance services</td>
</tr>
<tr>
<td></td>
<td>→ No training or in-house expertise required</td>
</tr>
<tr>
<td>Real-Time Reporting</td>
<td>→ On-demand, customizable reports demonstrate effectiveness and ROI</td>
</tr>
<tr>
<td></td>
<td>→ Query anytime</td>
</tr>
<tr>
<td></td>
<td>→ Web-based administration panel and summary dashboard offers total visibility, control and flexibility</td>
</tr>
</tbody>
</table>
Leveraging a SaaS model to increase email security manageability also provides the additional benefit of providing a business continuity solution. By having company email filter through external servers before coming into the company network, security SaaS also provides the opportunity to store and manage email remotely. If an email outage occurs at the company, email remains secure and accessible on the service provider’s system.

Combining the reliance on email for customer communications with the legal and regulatory requirements to retain email presents a significant email security risk in itself. Half of the respondents to the Webroot Email Security Survey are very or extremely concerned about the potential for losses from email outages.

<table>
<thead>
<tr>
<th>IT Benefits of SaaS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage and Bandwidth</td>
<td>Less use</td>
</tr>
<tr>
<td>Email Infrastructure</td>
<td>Prolonged life and increased capacity</td>
</tr>
<tr>
<td>IT Administration</td>
<td>No personnel costs and no more upgrade headaches</td>
</tr>
<tr>
<td>IT Help Desk</td>
<td>Fewer calls, fewer issues</td>
</tr>
<tr>
<td>Hardware</td>
<td>No hardware required</td>
</tr>
<tr>
<td>Software License or Maintenance</td>
<td>No software, no patches, no compatibility issues</td>
</tr>
</tbody>
</table>

Combining the reliance on email for customer communications with the legal and regulatory requirements to retain email presents a significant email security risk in itself. Half of the respondents to the Webroot Email Security Survey are very or extremely concerned about the potential for losses from email outages.

<table>
<thead>
<tr>
<th>Very or Extremely Concerned about Losses from Email Outages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall (N=1494)</td>
</tr>
<tr>
<td>50.2%</td>
</tr>
</tbody>
</table>


Top email security challenges in 2008:
"Enormous increase in spam challenges our systems and wastes a great deal of time."

- Business Manager, Vehicle Supply Co., Australia
Using a SaaS email security solution provides additional business continuity benefits for companies to avoid email outages, including:

- Ensures email is available in times of disaster
- Current and historical email available
- Accessible from remote sites
- Ability to re-route email if organizations’ mail servers are down or damaged
- Rolling message capture
- Browser webmail access

In addition to the security and business continuity benefits, implementing a SaaS model also lowers the total cost of ownership for email security.


Top email security challenges in 2008:
“For employees to remain productive and not spend time with problem emails.”

- CEO, Personal Services Co., USA
CONCLUSION

Email has proven to be a revolutionary productivity and communication tool that companies around the world have come to rely upon to conduct business, and more specifically to facilitate customer and employee interactions. Spam, spyware and viruses transported via email represent a serious data security threat to these companies. Managing these concerns translates into a significant investment in time and money for IT departments. Appropriate technology and business practices are essential to secure business email. A robust perimeter SaaS solution, coupled with best-in-class desktop protection, is the best combination to effectively protect business email.

Top email security challenges in 2008:
“Keeping ahead of the ‘bad boys’.”
- CFO, Arts/Entertainment Business, UK
ABOUT WEBROOT

Webroot provides industry-leading security software and services to consumers, enterprises and small to medium-sized businesses worldwide. The Boulder, Colorado based company’s newest software-as-a-service (SaaS) offerings, Webroot E-Mail Security SaaS and Webroot Web Security SaaS, provide better manageability, better value and better protection than any other e-mail or web security solutions. Webroot’s award-winning endpoint products, Webroot AntiSpyware Corporate Edition and Webroot AntiSpyware Corporate Edition with AntiVirus are comprehensive, centrally-managed solutions that aggressively block, detect and eradicate malware on desktops across the network.

To find out more visit www.webroot.com or call 800.772.9383.

About the Research

In February 2008, Webroot sponsored online surveys of organizations with 5 or more PCs or laptops in Australia, Canada, France, Germany, Japan, the United Kingdom and the United States. Survey Sampling International invited panel members who are email security decision-makers. Two hundred or more responses were received from each country. With a total of 1,494 respondents, the margin of error is ±2.5 percentage points. Findings within each country have a margin of error of ±7.0 percentage points.

© 2008 All rights reserved. Webroot Software, Inc. Webroot, the Webroot icon and the Webroot tagline are trademarks or registered trademarks of Webroot Software, Inc. in the United States and/or other countries. All other trademarks are properties of their respective owners.

NO WARRANTY. Analysis based on research conducted by Webroot Software, Inc. The information is provided AS-IS. Webroot makes no warranty as to its accuracy or use, and nothing contained in this document constitutes legal advice. Any use of the technical documentation or the information contained herein is at your own risk. Documentation may include technical or other inaccuracies or typographical errors. Webroot reserves the right to make changes without prior notice.

Certain data is available upon request.
APPENDIX

Resources for Additional Information about Legal Compliance*

Multi-Country

**Asia-Pacific Economic Cooperation (APEC) Privacy Framework**
APEC members, which include 21 countries in the Asia-Pacific region of the world and the United States, established a common Privacy Framework to enable regional data transfers in ways that benefit of consumers, businesses and governments. The Framework also provided technical assistance to those APEC economies that had not yet addressed privacy from a regulatory or policy perspective.
http://www.apec.org/content/apec/about_apec.html

**BASEL II Accord**
Basel II is a European-developed standard for the way financial institutions ensure the privacy of financial information when it is transferred across international borders. It also encourages financial institutions to lower operational risks by requiring a lower capital allocation when strong risk management policies are in place. As part of the risk mitigation plan, financial institutions must ensure that data and communication is secure, accessible and accurate.
http://www.bis.org/publ/bcbsca.htm

**EU Markets in Financial Instrument Directive (MiFID)**
MiFID, part of the European Commission’s Financial Services Action Plan, went into effect November 1, 2007. It includes requirements about retention for emails that document client orders.
http://ec.europa.eu/internal_market/securities/isd/mifid_en.htm

**EU Data Protection Directive**
Often referred to as the EU Privacy Directive, the Data Protection Directive is one of the most well known legal standards requiring companies to protect sensitive information in their possession.
http://ec.europa.eu/justice_home/fsj/privacy

**International Organization for Standardization Standard (ISO) Number 15489**
ISO 15489 sets guidelines for the classification, conversion, destruction, disposition, migration, preservation, tracking and transfer of records.
http://www.iso.org/cate/d16387.html

**Organization for Economic Cooperation and Development (OECD) Privacy Guidelines:**

**Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**
The OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data were agreed to by the member countries (Austria, Belgium, Canada, Denmark, France, Germany, Iceland, Luxembourg, the Netherlands, Norway, Spain, Sweden, Switzerland and the United States) in 1980 to clarify the manner in which personal data is used.
http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

**Organization for Economic Cooperation and Development (OECD) Privacy Guidelines:**

**Ministerial Declaration on the Protection of Privacy on Global Networks**
In 1998, the OECD affirmed their commitment to the 1980 Guidelines and made additions and revisions to reflect new technologies.

**Payment Card Industry (PCI) Standard**
The PCI standard for data security includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
https://www.pcisecuritystandards.org/
Australia

Federal Privacy Act of 1988
The Australian Privacy Act of 1988 is the country’s federal privacy law setting guidelines for how business, government, individuals and health organizations handle information.
http://www.privacy.gov.au

National Health Act of 1953
Under the auspices of the National Health Act of 1953, the Medicare and Pharmaceutical Benefits Program Privacy Guidelines were issued in 1997 that provide rules for the collection, use, disclosure and retention of personal medical information.

This Australian Telecommunications Acts of 1979 and 1997 prohibit, among other things, access to stored communications (i.e. email, SMS and voice mail messages stored on a carrier’s equipment) except where authorized in specified circumstances.

Canada

Personal Information Protection and Electronic Documents Act (PIPEDA)
PIPEDA protects personal data during commercial transactions, not just inside Canada but internationally. It also directs how information can be gathered and how it should be stored.
http://www.privcom.gc.ca/legislation/02_06_01_e.asp

France

Data Protection Act
France was the first member of the EU to enact data protection legislation in 1978.
http://www.cnil.fr/index.php?id=4

Germany

Federal Data Protection Act
The Federal Data Protection Act was the end result of this process in 2001. It satisfies the requirements of the Directive, but there is still a feeling that the problems of unnecessary data use have not been adequately addressed.
http://www.bfdi.bund.de/

Japan

The Law on the Protection of Personal Information
Japan enacted a measure similar to the EU Data Protection Directive in 2003 called the Personal Information Protection Law. It details the requirements for companies to adequately protect sensitive information in their possession.

METI Guidelines for Personal Information Protection
These guidelines, revised by the Ministry of Economy, Trade and Industry in 2007, summarize the ways that personal information protection laws should be applied. The guidelines use specific examples to explain what businesses should do to protect personal information.
http://www.meti.go.jp/english/information/data/IT-policy/privacy.htm#01
United Kingdom

Data Protection Act of 1998
This is the best-known of the UK acts. It specifies the storage, retention and destruction of electronic personal information and security pertaining to the transfer of personal data.
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

Companies Act
The UK Companies Act states the accounting records and other paperwork requirements to demonstrate accuracy in company transactions. As records are increasingly created in electronic form, and email often constitute the business record of a transaction, retention policies must be fulfilled.
http://www.opsi.gov.uk/acts/acts2006/ukpga_20060046_en_1

Freedom of Information Act
The UK Freedom of Information Act allows anyone to request information from a government agency. Thus, agencies must retain email and other electronic documents and ensure a reasonable method for retrieval exists.
http://www.opsi.gov.uk/acts/acts2000/ukpga_2000036_en_1

Regulation of Investigatory Powers Act (RIPA)
RIPA details the allowable methods of surveillance and information gathering to help the prevention of crime, including terrorism. Its provisions for acquisition and disclosure of data relating to communications and access to electronic data protected by encryption or passwords has implications for corporate email retention and retrieval capabilities.
http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1

Financial Services Act
Administered by the Financial Services Authority (FSA), the Act sets guidelines for storing, retrieving, or deleting electronic files, including email, Web pages and other e-documents.
http://www.uk-legislation.hms.o.gov.uk/acts/acts2000/ukpga_20000008_en_1

United States

Disposal of Consumer Report Information and Records Regulations
The Federal Trade Commission issued these regulations in 2004 detailing compliance with the Fair and Accurate Credit Transactions Act of 2003 (FACTA) and the Fair Credit Reporting Act (FCRA). FACTA and FCRA specify retention and disposal guidelines for certain types of consumer credit information.
http://www.access.gpo.gov/nara/cfr/waisidx_07/16cfr682_07.html

Federal Information Security Management Act (FISMA)
FISMA requires that Federal government agencies develop information risk assessments and mitigation strategies. These programs need to include methods for tracking outgoing emails.

Federal Rules of Civil Procedure (FRCP)
FRCP amendments detailing electronic discovery requirements and obligations to preserve and produce electronically-stored information were implemented in 2006.
State of Internet Security: Protecting Business Email

Food and Drug Administration GxP
The FDA’s GxP (Good x Practice; x can mean Clinical, Laboratory, Manufacturing, Pharmaceutical, etc.) sets guidelines for record management in the industries regulated by the FDA, including pharmaceuticals, medical devices, cosmetics and edible goods.
http://www.fda.gov/opacom/morechoices/industry/guidedc.htm

Freedom of Information Act (FOIA)
FOIA requires federal agencies to respond to citizens’ requests to disclose their records. E-government initiatives have resulted in many government records existing in electronic only formats, including email, making data retention and retrieval capabilities central to fulfilling FOIA requirements.
http://www.usdoj.gov/oip/foiastat.htm

Gramm-Leach-Bliley Act (GLBA)
GLBA requires organizations that maintain credit information for customers be held accountable if that data is accessed or compromised by an unauthorized third party. It also governs the handling of nonpublic personal information about consumers.
http://www.ftc.gov/privacy/glbact/glbsub1.htm

Health Insurance Portability Act (HIPAA)
HIPAA applies to all paper and electronic records that contain information relevant to an individual’s medical history. Specific retention requirements vary from five years to the life of the patient.

Sarbanes-Oxley Act of 2002 (SOX)
SOX compliance has become a central focus of corporate governance initiatives. SOX requires that all publicly-traded companies include specified risk assessment and audit controls that cover such areas as data security policies.

Securities and Exchange Commission (SEC) Rule 17
SEC Rule 17 includes requirements for broker-dealers organizations to retain all emails pertaining to trading activity for six years, and that these emails are preserved in a way that maintains access to them.
http://www.sec.gov/rules/final/34-44992.htm

Telecommunications Act of 1996
Section 222 of the Telecommunications Act of 1996 outlines requirements related to the privacy of customer information.
http://www.fcc.gov/telecom.html

*This is not an all-inclusive list, but rather a summary of some of the most discussed laws and regulations that have impacts for business email security efforts. The list, summaries, descriptions and links: (i) are provided “as is” with all faults and with no warranty whatsoever; (ii) are provided for informational purposes only; and (iii) do not constitute legal advice.*
SOURCES

Government
Avoiding Social Engineering and Phishing Attacks
United States Computer Emergency Readiness Team (US-CERT)
Washington, D.C. USA
July 19, 2007
http://www.us-cert.gov/cas/tips/ST04-014.html

Official Journal of the European Communities
Brussels, Belgium
October 1995
http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

Decision and Order in the Matter of DSW, Inc.
File Number 052-3096
Federal Trade Commission
Washington, D.C. USA
March 2006
http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWDecisionandOrder.pdf

Excessive Indulgences: Personal Internet Use at the Department of Interior
Office of the Inspector General
U.S. Department of Interior
Washington, D.C. USA
September, 2006

Information Security Breaches Survey 2006
UK Department of Trade and Industry
London, UK
April 2006

Internet Crime Report 2006
Internet Crime Complaint Center
Federal Bureau of Investigation
U.S. Department of Justice
Washington, D.C. USA
January 2006
http://www.ic3.gov/media/annualreports.aspx

Spam Summit: The Next Generation of Threat and Solutions
Staff Report by the Federal Trade Commission
Washington, D.C. USA
November 2007
http://www.ftc.gov/bcp/workshops/spamsummit

Private Sector

2007 E-Crime Watch Survey
Conducted by CSO Magazine in cooperation with the U.S. Secret Service, CERT Coordination Center and Microsoft Corp.
Framingham, Massachusetts USA
September 2007
www.cert.org/archive/pdf/ecrimesummary07.pdf

California Senate Bill (SB)1386
Sacramento, California USA
September 2002
http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

Computer Security Institute
Manhasset, New York USA
October 2007
http://www.gocsi.com/forms/ksi_survey.html

Definitions
Anti-Spyware Coalition
Washington, D.C. USA
June 2006

Digital Fear: The Internet as a Tool for Crime and Terrorism
Business Roundtable
Washington, D.C.
September 2007

Effective E-marketing: New Study Shows Shoppers Respond to Email Marketing
Endai Worldwide Marketing
New York, New York USA
December 11, 2007

Growing Business Dependence on the Internet
Business Roundtable
Washington, D.C.
September 2007

NFIB and Visa partner to educate small businesses on security in 2007
National Federation of Independent Businesses
Washington, D.C. USA
March 8, 2007
http://www.nfib.com/object/IO_32561.html
Payment Card Industry (PCI) Data Security Standard
PCI Security Standards Council, LLC
Wakefield, Massachusetts USA
September 2006
https://www.pcisecuritystandards.org/tech/index.htm

Pros and Cons of SaaS Secure Web Gateway Solutions
by Peter Firstbrook
Gartner, Inc.
Stamford, Connecticut USA
April 16, 2007

Software-as-a-Service: A Comprehensive Look at the Total Cost of Ownership of Software Applications
Software & Information Industry Association
Washington, D.C. USA
2006

Spam Volume
Data Memo by Deborah Fallows
Pew Internet & American Life Project
Washington, D.C. USA
May 2007

Worldwide Email Usage 2007–2011 Forecast: Resurgence of Spam Takes Its Toll
Mark Levitt
IDC
Framingham, Massachusetts USA
April 2007
http://www.idc.com/getdoc.jsp?containerId=206038

News Stories
“A Cyber-Riot”
The Economist
May 10, 2007
http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598

“As Their Dependence on Email Grows, Some Firms Find Ever-Bigger Problems”
Herald Tribune
August 30, 2001
http://www.iht.com/articles/2001/08/30/email_ed3_.php

“Data Security and Tort Liability”
Journal of Internet Law
January 2008

“Malicious Programs Hit New High”
BBC News
February 8, 2008
http://news.bbc.co.uk/2/hi/technology/7232752.stm

“Oak Ridge Speared in Phishing Attack Against National Labs”
eWeek
December 7, 2007

“Phishing-Based Breach of Salesforce.com Customer Data is More Evidence of Industry’s Need to Act on Spam”
ZDNet
November 6, 2007
http://blogs.zdnet.com/Berlind/?p=880

“Rules About to Change in e-Discovery Game”
Enterprise Storage Forum
November 7, 2006
http://www.enterprisestorageforum.com/continuity/features/article.php/3642421