2008 Annual Google Communications Intelligence Report

A Google white paper
February 2008

Executive Summary

At the end of 2007, Google conducted an annual online survey of messaging professionals. Providing insight into the major communications trends in the past year as well as the pressing issues and concerns for the coming one, this survey is the result of 575 global interviews with CEOs, CIOs, and CTOs in large, multinational enterprises as well as small organizations.

This report summarizes the key findings of the survey, including detailed statistical analysis of the key trends in business communications in 2007 and how these trends translate into priorities for business communications professionals in the year ahead. Following the summary of the research findings, the report touches on Google's expectations for the coming year as well as defines some best practices in business communication to help organizations address the expected challenges in the industry in 2008.

Key findings

1. The number of electronic messages increased in 2007, with spam still a huge issue for most organizations

Electronic communications – email, web, and instant messaging (IM) – continued to grow significantly in 2007, accompanied by a corresponding rise in the volume of spam. Based on data from Postini data centers (Postini, Inc. is a wholly owned subsidiary of Google Inc.) spam volume per user was up 57% in 2007 over 2006. What does this mean in real terms? It means that the average unprotected user would have received 36,000 spam messages in 2007, compared with 23,000 spam messages in 2006. Spam was – and still is – the top communication security issue facing companies.

2. Executives look to IT personnel – not end-users – to ensure security and compliance

According to survey participants, the burden of communications security and compliance rests squarely on the shoulders of IT personnel. In fact, 53% of all executives and messaging professionals surveyed indicated that they feel their IT department is the primary department responsible for communications security and compliance. Only 18% of survey participants felt that security and compliance accountability rests equally with IT as well as end-users.

3. IT professionals face serious challenges in reaching security and compliance goals

Respondents acknowledge that ensuring communications security and compliance is not a simple task and serious challenges exist in both areas. In communications security, respondents were most worried about protecting themselves against spam, viruses, and worms; securing their mobile workforce; ensuring the availability and continuity of the business – and handling the strain these challenges place on their IT resources. Similarly, the top challenges organizations face in meeting compliance goals are planning for disaster recovery, ensuring compliant business processes, preventing unintentional data leakage, and protecting internal systems from breach by hackers.

4. Security and compliance challenges negatively impact IT productivity

At the close of 2007, executives were extremely concerned about the impact of communications security and compliance on IT productivity. Time spent ensuring adherence to compliance procedures (46%), arranging system upgrades to enhance

security (44%), and overcoming network delays or outages due to security breaches (42%) were all high on respondents' lists of concerns.

5. Communications security and compliance solutions based on the Software-as-a-Service (SaaS) model can address these productivity issues

While different approaches exist to ensuring communications security and compliance, survey respondents acknowledged that the benefits of a solution based on the SaaS approach directly address the IT productivity issues with which they are most concerned, including ease of implementation, ease of maintenance and troubleshooting, and overall effectiveness of the solution. In fact, 31% of organizations surveyed already use some type of SaaS solution because of the benefits received.

6. In the year ahead, Google expects the number of threats to stabilize but the complexity of these threats to increase dramatically

Although Google does not expect the number of threats to business communications security to grow as rapidly in the coming year, we do anticipate that the complexity of these threats will increase. Businesses will be challenged to identify new and different types of malicious content as well as protect sensitive information against evolving social engineering techniques that circumvent security measures by manipulating or tricking users into disclosing or performing actions that divulge confidential data. To prevent these potential data leaks, we expect organizations to place increased emphasis on outbound security policies and content encryption in the year ahead.

Business Communications Trends in 2007

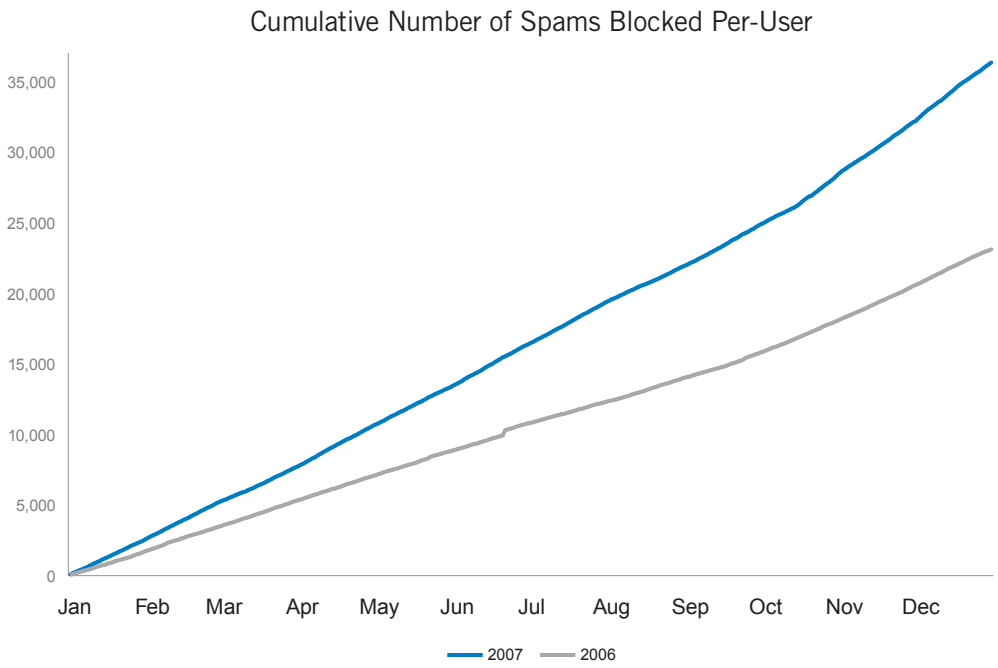
Google's online survey of business communications executives and professionals uncovered several key trends in communications over the past year. Further, the executives polled provided insight into how these trends will impact their key priorities for the coming year. The following sections detail the results of the survey as well as provide message statistics from Postini, a recent Google acquisition.

Trend #1: As the number of electronic messages increased in 2007, spam continued to be the biggest issue for most organizations

The proliferation of communications in 2007 – through email, web, and IM – brought with it a corresponding rise in the volume of spam. In 2007, Postini's data centers recorded the highest levels of spam and virus attacks in history. While overall email message volume per user grew 47% in 2007 over the prior year, spam volume was up 57% in the same time period, according to Postini's data center research. Much of this growth was fueled by an increase in the number of bot-net computers – networks of infected PCs with broadband internet connections – co-opted by hackers without the owner's knowledge to send spam messages and virus attacks.

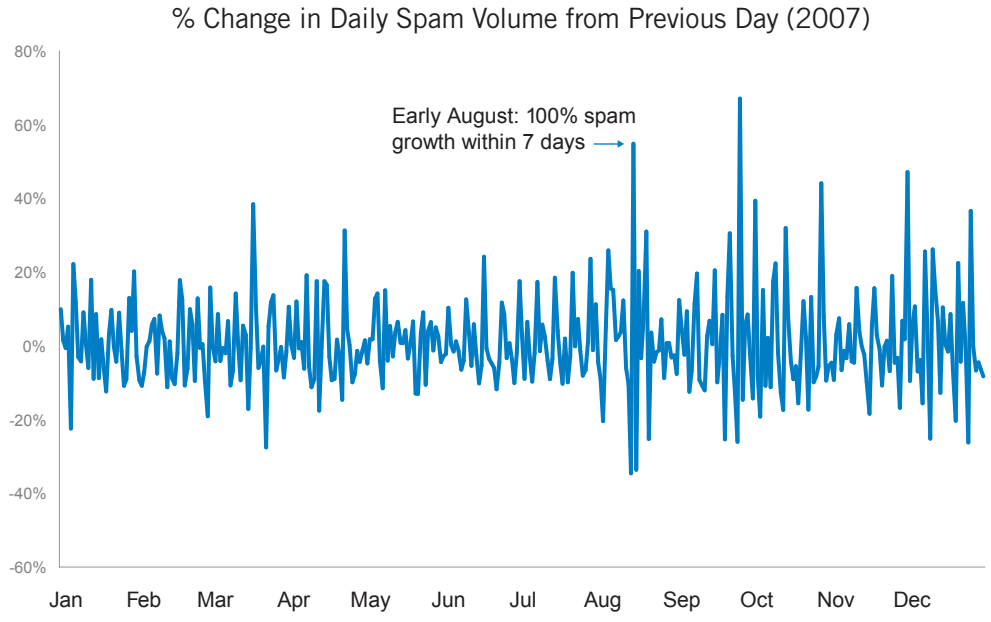
In 2007, Postini blocked 160% more spam messages than in 2006, even as spammers became more sophisticated in their attempts to evade detection by spam filters. The early part of 2007 was marked by the pervasiveness of image spam, where the spam content is contained in an image attached to the email message. Over the course of the year, image spam declined and was replaced by spam content contained in PDF, document, spreadsheet, and even multimedia attachments, such as MP3 files.

Figure 1
Spam volumes increased by 57% from 2006 to 2007.
Source: Postini



Although the increase in the overall volume of spam as well as innovations in the types of spam threats are causing organizations great concern, the volatility of spam is actually a bigger problem. According to Postini's data center research, the average volume of spam messages per user jumped significantly in August of 2007. In fact, it literally jumped 100% within a seven day period. It is extremely difficult for organizations to plan for an event like that.

Figure 2
Spam volatility increased in second half of 2007.
Source: Postini



Even more important – and less obvious in the graph – is that these spikes are virtually impossible to predict, meaning that organizations must either maintain large amounts of unused capacity to proactively prepare for these sudden spikes or

continually increase bandwidth in a reactive manner to keep up with unpredictable spikes. For example, if an organization had the appropriate level of bandwidth to handle its spam volume on January 1, 2007, it would have had to increase that bandwidth by 145% to deal with the volatility and spikes throughout the year.

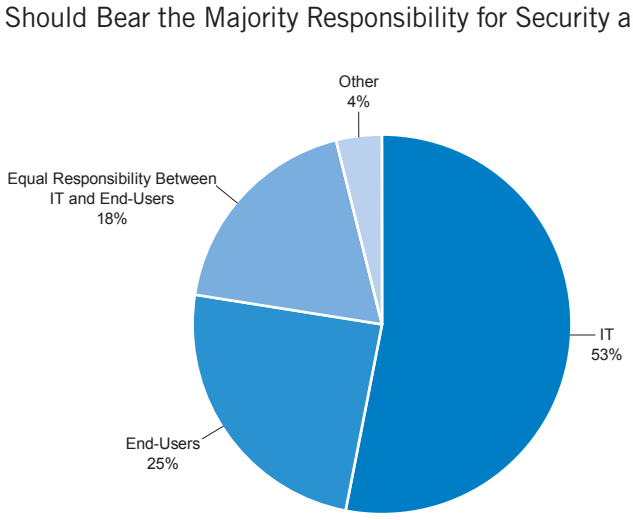
The bottom line

Concern about stopping spam and other forms of malware continued to be at the forefront of business communications professionals' minds (48% of respondents named it as their number-one concern) thanks to the escalating volume of spam as a percentage of all communications. Additionally, the volatility of spam – and the unpredictability of these sudden, sharp spikes in volume – place significant financial pressure on organizations that must increase capacity to deal with this uncertainty.

Trend #2: Executives look to IT personnel – rather than end-users – to ensure security and compliance

When asked what group holds ultimate responsibility for their organization's communications security and compliance, the majority of respondents to the online survey said their IT department (53%). Only 25% felt that their users should shoulder the responsibility of ensuring the safety and compliance of electronic communications. Interestingly, 18% of survey participants felt that security and compliance accountability lies equally with IT and users, and 4% said that other functional areas of the company – such as the executive staff, legal department, or even human resources – should be responsible for keeping the organization's business communications secure and compliant.

Figure 3
Respondents identified who is responsible for security and compliance within their organization.
Source: Google Research



The bottom line

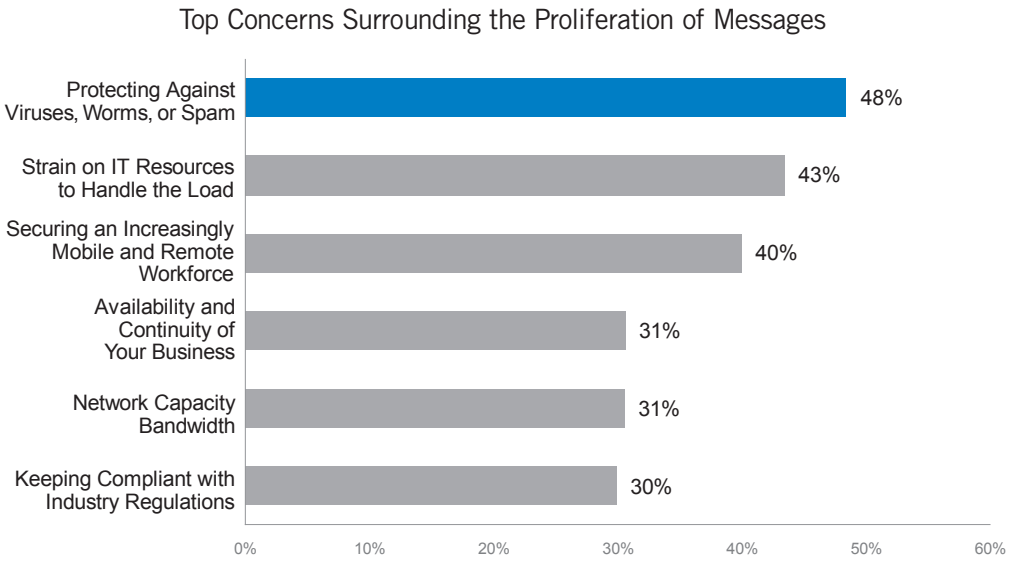
As with most aspects of enterprise security and regulatory compliance, the IT department is accountable for communications security and compliance in the majority of companies. While users certainly play a role in being aware of and vigilant about maintaining secure communications and ensuring compliance, organizations know that they need to have policy mechanisms in place to help users keep secure and compliant.

Trend #3: IT professionals face serious challenges in reaching security and compliance goals

The continuing proliferation of electronic messages and the corresponding increase in spam, viruses, worms, and other dangers present significant challenges for organizations – and their IT departments, in particular – in reaching their communications security and compliance objectives.

On the security side of the equation, the biggest concern among messaging professionals is protecting their organization against these threats (48% of respondents). Beyond that, executives are also worried about how their IT resources will continue to keep up with the exponential growth in messaging and the accompanying dangers (47%) and how to secure their increasingly mobile and remote workforce (40%). In a closer look at the survey data, respondents in the finance and healthcare industries sited IT resource strain as their top concern surrounding message management.

Figure 4
Respondents identified their top concerns regarding message volume growth.
Source: Google Research

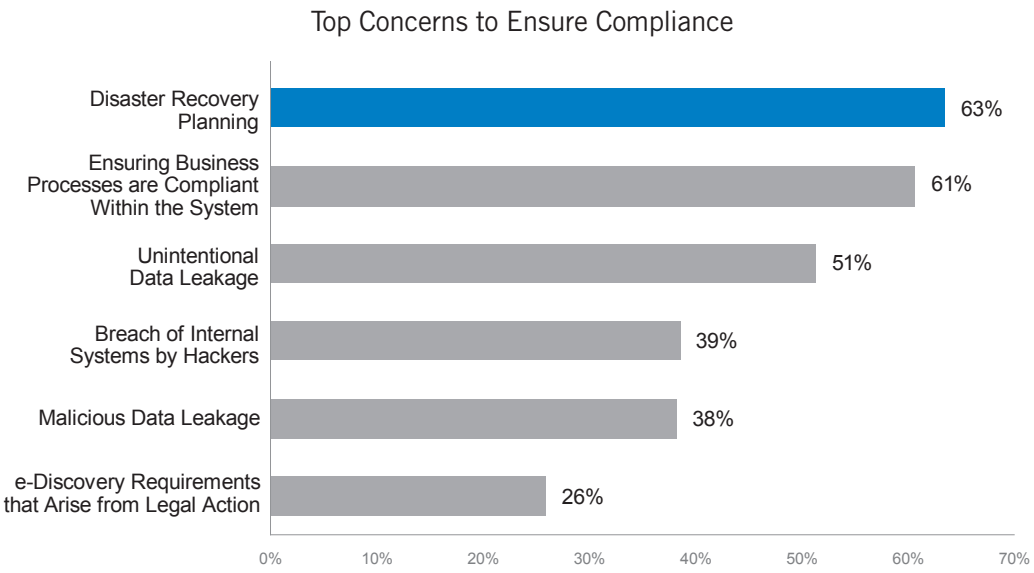


Ensuring business continuity in the event of a disaster (e.g., recovering data after a major system failure, terrorist act, or force of nature) and keeping business processes compliant with ever-changing regulatory requirements were clearly the most important issues for the organizations participating in the survey, with 63% of respondents concerned with disaster recovery and 61% focused on ensuring the compliance of business processes. Interestingly, companies are more worried about end-users unintentionally sending messages with confidential information or intellectual property (51% of respondents) than those same users maliciously violating corporate security and compliance, placing even more pressure on the IT organization to prevent breaches.

The bottom line

One of the key drivers of message proliferation is the explosion in the types and adoption of mobile technologies. Each day, users are becoming more comfortable sending email and IM and surfing the web using their laptops, cell phones, smart phones, and other mobile devices. All of these communications must be considered part of the overall organizational security plan – and IT personnel acknowledge their role in keeping these mobile communications secure.

Figure 5
Respondents identified their top concerns regarding message compliance.
Source: Google Research



With respect to compliance, the financial and legal ramifications of regulatory noncompliance are serious issues, and organizations are taking a more proactive and strategic approach to prepare themselves. To this end, companies are creating compliance organizations spearheaded by chief compliance officers (COO) and oversight from the chief executive. The result? These organizations are more likely to meet the challenge of maintaining regulatory compliance.

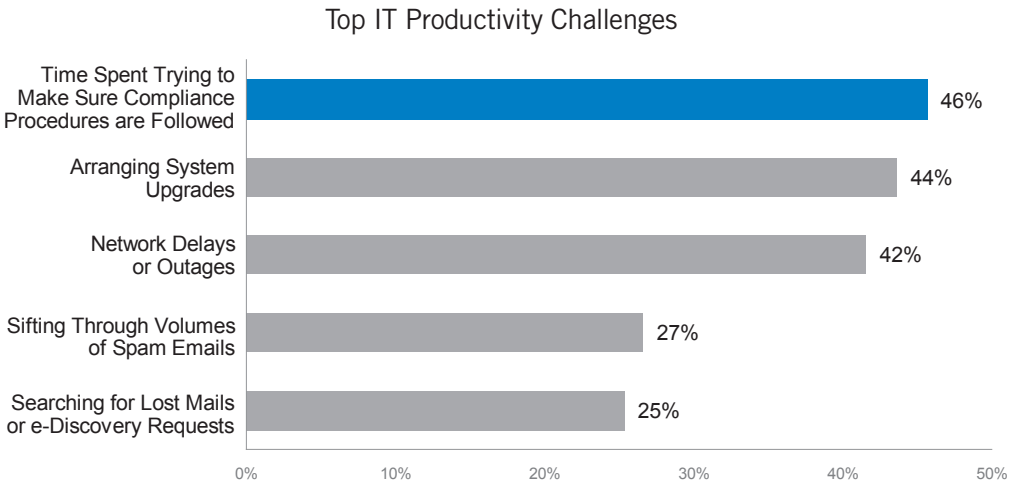
Trend #4: Ensuring communications security and compliance is a significant productivity drain on IT resources

Survey respondents emphatically agreed that ensuring communications security and compliance imposes significant productivity drains on their IT department. The three top productivity drains on IT personnel mentioned in the survey include ensuring adherence to compliance procedures (46%), arranging system upgrades (44%), and overcoming network delays or outages (42%). Less often mentioned, but no less impactful on productivity, were sifting through emails to determine its legitimacy or maliciousness (27%) and searching for lost email and other requests for electronic discovery (25%).

The bottom line

Ensuring the security and compliance of an increasing number of messages being sent via multiple communications channels is no easy task. IT departments in all sizes and types of companies were taxed by the effort – some to the point at which they had no time to work on new applications or other value-added activities that contribute to bottom-line revenue. Moving forward, organizations must find a way to reduce the productivity drain caused by communications security and compliance in order to remain competitive.

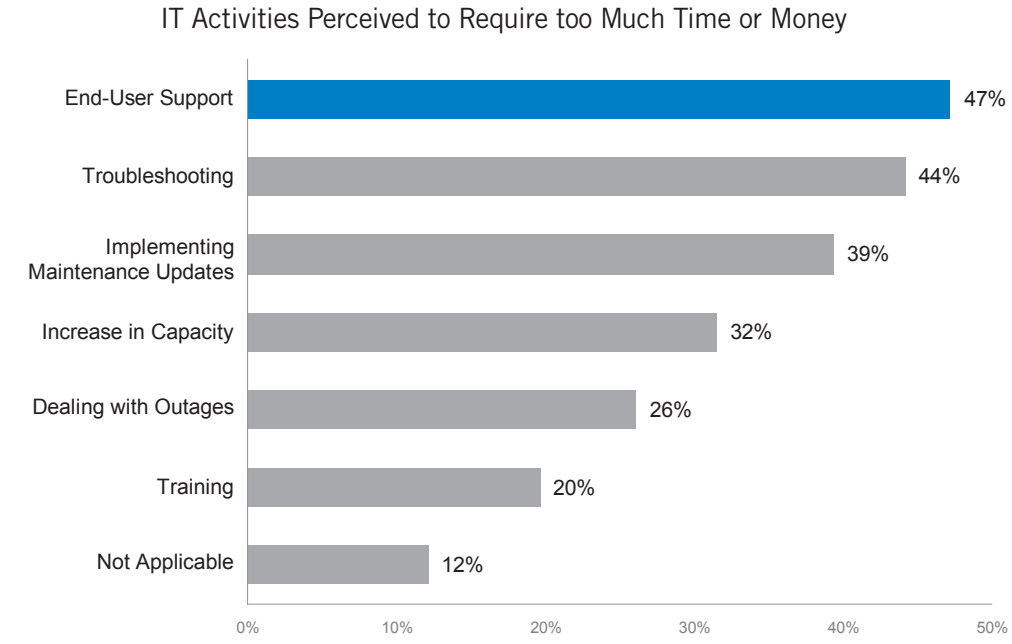
Figure 6
Respondents identified their top challenges surrounding productivity drains on IT.
Source: Google Research



Trend #5: Organizations felt they spent too much time and money on their current communications security and compliance solution and had several key requirements on their wish list for a solution that overcomes these financial and productivity drains

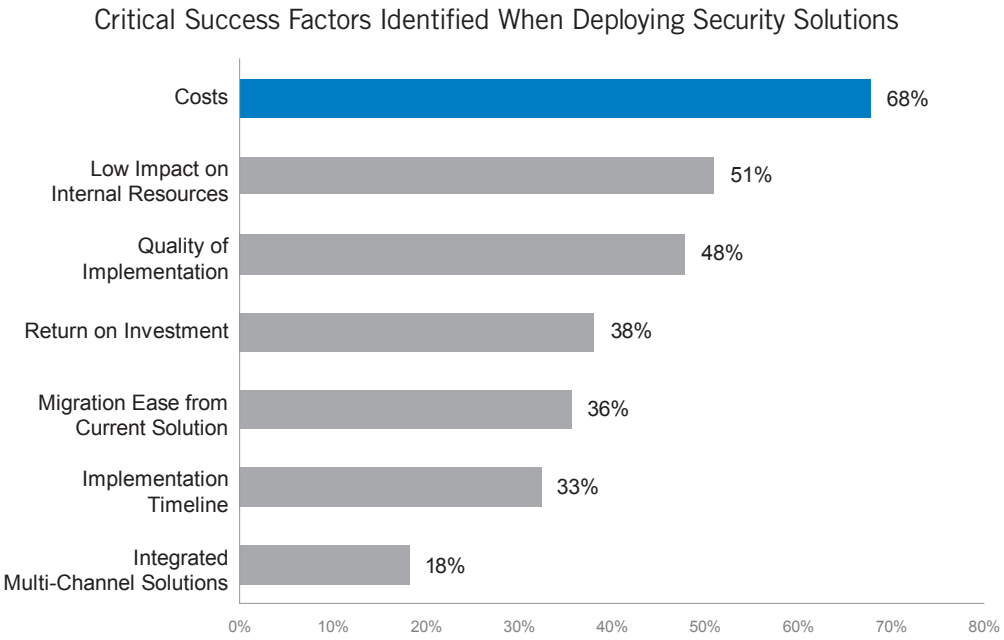
When asked whether they were satisfied with their current communications security and compliance solution, only 12% of respondents to the online survey answered in the affirmative. Even more telling, most said they spent too much time and money on end-user support (47%), troubleshooting (44%), implementing maintenance updates (39%), increasing capacity (32%), and dealing with outages (26%).

Figure 7
Respondents identified the areas they believe they spend too much time and money on regarding their existing security solution.
Source: Google Research



Digging deeper into the fact that so few respondents were satisfied with their existing solution, Google asked participants to list their key criteria for evaluating and deploying a new communications security and compliance solution. Respondents resoundingly said cost (68%) was the number-one factor they were looking for in a security and compliance solution. But, harkening back to the productivity drains

Figure 8
Respondents identified the critical success factors when deploying a security solution.
Source: Google Research



caused by many current solutions, survey participants also valued the solution having a low impact on internal resources (51%). Quality of the software (48%), fast return on investment (38%), and easy migration from the current solution (36%) were also mentioned by survey respondents as key criteria for a new communications security and compliance solution.

The bottom line

It's clear that organizations are concerned about the effectiveness of their current solution – and that most companies are not happy with the status quo. IT organizations are spending too much time managing and maintaining the communications security and compliance solution and not enough on revenue-generating activities that impact the bottom line. Many companies are actively searching for a new solution that will reduce the drain on IT productivity, can be easily and quickly deployed in their organization, and will give them a quick return on their investment.

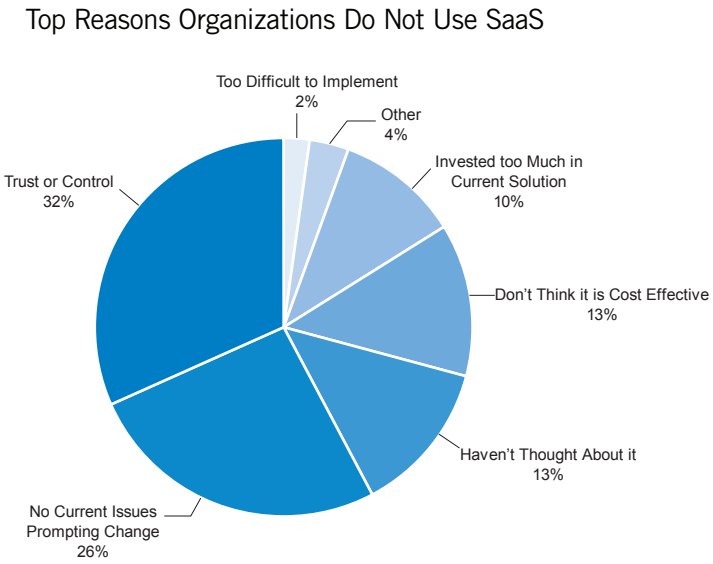
Trend #6: SaaS models are gaining in popularity – and market share – because they directly address key IT productivity pains

Thanks to the proven success of the SaaS approach in addressing critical financial and productivity issues prevalent in organizations today, many survey respondents were either currently evaluating or had already implemented SaaS solutions. Nearly 31% of organizations surveyed were using SaaS providers for some aspect of their technology infrastructure. When asked why they had chosen a SaaS solution, survey participants cited the reduced maintenance and troubleshooting requirements (30%), ease of implementation (23%), overall effectiveness (18%), and cost (12%) of the SaaS approach. Respondents listed the same benefits when asked for the critical success factions of a security implementation, which helps understand why SaaS is gaining in popularity in the IT industry.

Figure 9
Respondents with SaaS solutions identified their top reasons why they like SaaS.
Source: Google Research

However, not everyone surveyed was sold on the SaaS approach. Of the 53% of respondents indicating they did not use a SaaS solution, 32% said that it was because they did not feel comfortable giving up control of the specific function or process to an external party. Interestingly, 26% of those surveyed said they did not have a specific event or incident that prompted them to switch solutions. And 17% of all respondents were not familiar with the concept of SaaS at all.

Figure 10
Respondents top reasons why they do not use SaaS.
Source: Google Research



While 13% of respondents noted that they did not use a SaaS solution because they were not convinced of its cost-effectiveness, Google's internal research clearly illustrates the cost advantages of the SaaS approach. The following table, based on this research, compares the estimated cost of an appliance- or software-based email filtering solution with that of a SaaS-based solution in a typical 1,000 employee organization. The critical takeaway here is that many organizations only look at the up-front costs of the solution, rather than factoring in the total cost of ownership (e.g., maintenance, support, training, and other overhead costs). When these items are factored into the cost comparison, the advantage clearly rests with SaaS-based solutions.

Figure 11
A cost comparison between a tradition in-house solution verses a SaaS solution.
Source: Google Research

Cost Component	Appliance or Software Vendor	SaaS Vendor
Hardware		
Email appliance and/or server increase to scale with organization and spam growth	$2,000–$15,000	n/a
Email appliance and/or server increase for disaster recovery	$2,000–$15,000	n/a
Total fixed costs	**$4,000–$30,000**	**n/a**
Software		
License fees	$1,000–$5,000	$3,000–$12,000
Support fees	$1,000–$5,000	$0–$1,000
Maintenance		
Installation and upgrades	$3,000–$5,000	n/a
Administration and configuration	$4,000–$8,000	$1,000–$2,000
End-user support	$3,000–$6,000	$1,000–$2,000
Training	$2,000–$5,000	minimal
Fail-over and recovery efforts	$2,000–$5,000	included
Total variable costs (annual)	**$16,000–$39,000**	**$5,000–$17,000**
Total cost	**$20,000–$69,000**	**$5,000–$17,000**

The bottom line

The key advantages of the SaaS approach – ease of deployment and use, flexibility of administration and management, effectiveness, low total cost of ownership, and scalability and reliability – make it particularly well-suited for organizations looking to reduce the IT productivity pains of communications security and compliance as described above. Because of this, Google expects to see an increase in the number of organizations adopting and implementing communications security and compliance solutions based on the SaaS model in the coming year. The more businesses experience the benefits of SaaS first-hand, the more comfortable they will be with trusting SaaS vendors and relinquishing control of their communications security and compliance to a SaaS provider.

Business Communications Priorities for 2008

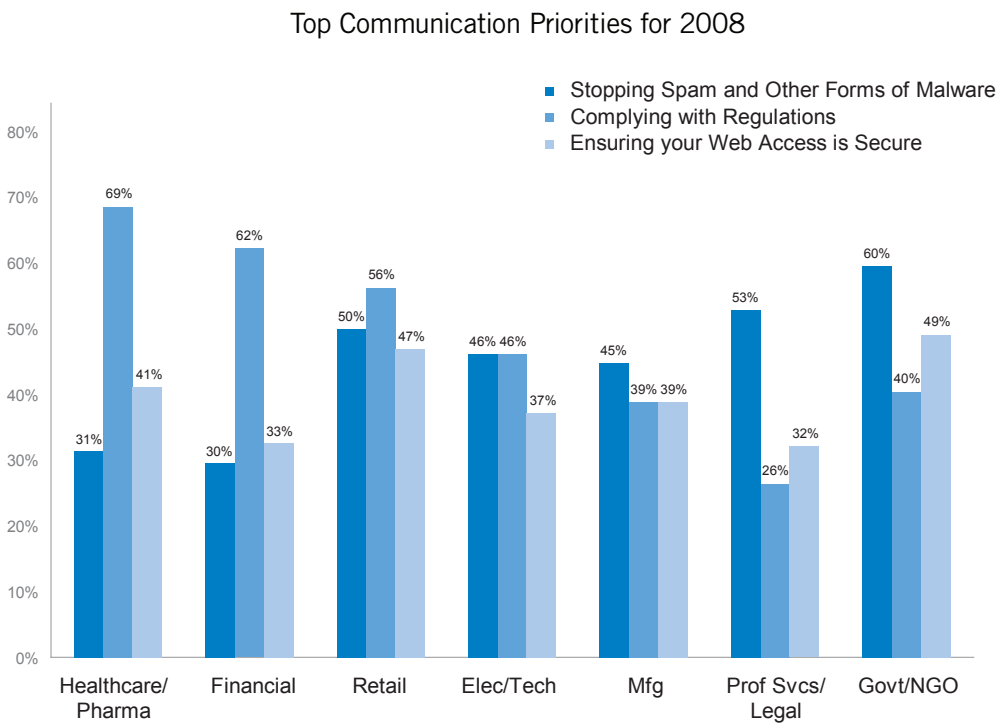
As part of the survey, Google also asked respondents to take look into the future and tell us their communications security and compliance priorities for the coming year. As expected, the majority of respondents listed priorities that are a direct result of the industry trends experienced in 2007, as outlined in the section above.

Of particular note is the difference in priorities among organizations in different vertical industry segments, e.g., finance, healthcare, retail, and government. We have chosen to highlight these industry differences in this section because they are so striking.

Top three priorities for business communications

While stopping spam and other malware is the clear, number-one priority in government and the professional services/legal industries, finance, and healthcare are more worried about ensuring their business communications comply with government regulations. This discrepancy is not surprising, as finance and healthcare are the industries most affected by regulations, including FINRA (Financial Industry Regulatory Authority) for finance and HIPAA (Health Insurance Portability and Accountability Act) for healthcare. Since these industries face significant compliance requirements, they tend to be the bellwether for how regulations will affect other industries. Of course, all public companies are subject to the transparency and record-keeping requirements of SOX (Sarbanes-Oxley Act).

Figure 12
Respondents identified their top communications priorities for 2008, segmented by industry.
Source: Google Research

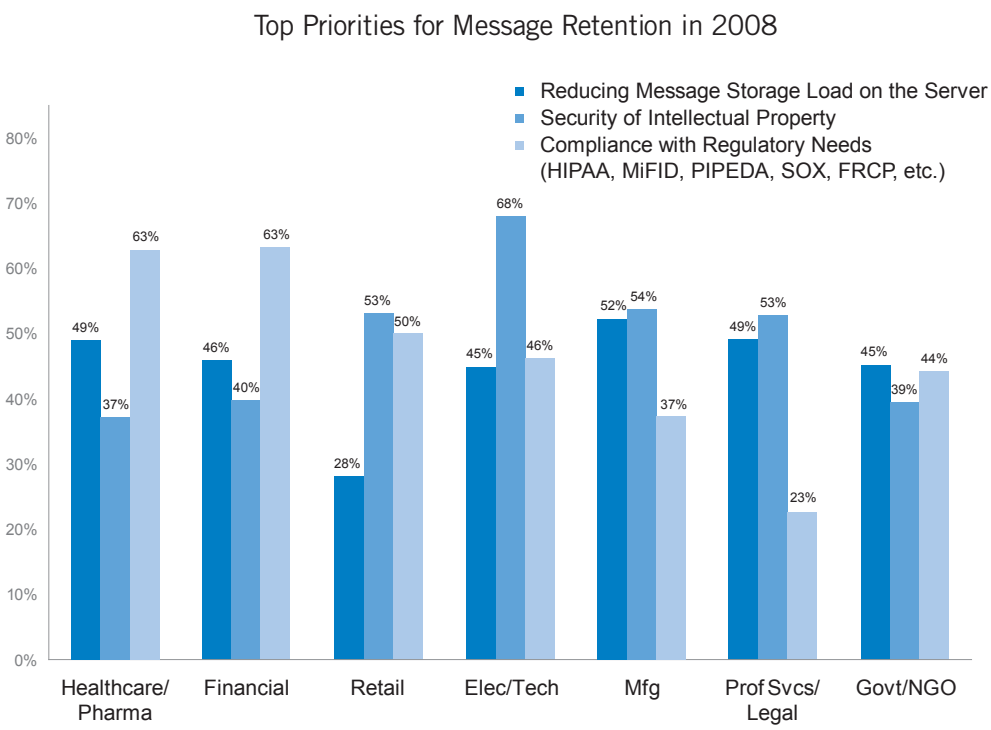


Also interesting to note is the fact that secure web access is, for the first time, one of the top three priorities for business communications professionals. This is likely a result of the increase in deployment of web-based customer interactions and the rise in malware attacks on the web communications channel.

Top three priorities for compliance

On the compliance side of the equation, again, industry differences are striking. In financial services and healthcare, ensuring message retention for compliance with government regulatory mandates is by far the most pressing priority for the coming year. However, among technology companies, the security of intellectual property to protect competitive advantage is the top-of-mind priority, with nearly 70% of technology companies listing it as their key focus for 2008.

Figure 13
Respondents identified their top priorities for message retention for 2008, segmented by industry.
Source: Google Research



Google Expectations for 2008

While the volume of threats to business messaging security and compliance may not grow in 2008 at the same rate as 2007, we do anticipate the complexity of these threats to increase. Businesses will be challenged to identify new and different types of malicious content as well as to protect sensitive information against evolving social engineering techniques. These techniques attempt to circumvent security measures by manipulating users into performing actions that divulge confidential data. To prevent these potential data leaks, we expect organizations to place increased emphasis on outbound security policies and content encryption in the year ahead.

Here are some additional challenges we expect businesses to face in 2008:

- Spam volume will stabilize and could actually decrease in 2008 as spam attacks become more targeted in nature. However, as more and more spam content is contained within email attachments, we expect that the overall size of spam will continue to be very volatile.
- Virus attacks will continue to blend with spam, with an increasing focus on identity theft utilizing ever-more-sophisticated social engineering techniques that will be related to specific current events, such as the Super Bowl, the Summer Olympic Games, yet-unknown natural disasters, and the like. Further, virus attacks will target executives at specific companies whose intellectual property is deemed valuable on the black market by the hackers. These attacks will appear to come from legitimate business agencies, such as the Internal Revenue Service, the Better Business Bureau, and the Securities and Exchange Commission. Google expects to see more of these types of attacks as the year progresses, leading to significant, high-profile data breaches at commercial enterprises and government agencies. We also anticipate that these data breaches will force

companies to modify their email practices, such as eliminating hot links in customer email communications.

- More businesses and organizations will implement specific policies that address outbound content in email and will deploy systems to monitor and enforce those policies to prevent sensitive or confidential data leaks.
- The growing need for managing consumer data privacy and retention policies globally will drive growth of encryption and archiving. In addition, hosted solutions (SaaS) will play a major role in reducing the cost and complexity of these products.
- Increasingly, identity theft attacks will be launched from websites, especially those that enable users to create their own content, such as social networking sites, blogs, and auction sites.
- As more states begin to revise rules governing civil procedure for state courts (similar to the Federal Rules of Civil Procedure), organizations will need to put in place a litigation readiness plan leveraging an electronic message archiving and discovery solution.

Best Practices for Business Communications for 2008

So how can you prepare your organization to face message security and compliance challenges outlined in this report? Based upon Google's experience and research, here are some best practices for weathering the storm this coming year:

Security best practices

1. **Protect your organization.** Deploy anti-spam and anti-malware solutions across your enterprise and keep them vigilantly updated. Where possible, leverage SaaS solutions to offload the burden of keeping the defenses updated. In many cases, you can lower costs and reduce the impact on IT resources by utilizing SaaS solutions.
2. **Keep current.** Keep all applications updated to the latest patch levels. This is especially true for operating systems, web browsers, file readers (e.g., Adobe Acrobat Reader), multimedia players, and other applications that are commonly launched from a web browser.
3. **Educate users often.** Constantly remind and educate users about external threats and about internal company policies regarding the use of email. If an outbreak occurs and is getting through our defenses, have a way to quickly communicate to your users to be aware of the threat.
4. **Define email usage policies with security in mind.** For example, decide how you will handle specific attachments such as executables, scripts, multimedia files, etc. Identify global policies and group exceptions. Communicate these policies on a regular basis to your employees and deploy flexible systems that can not only monitor and enforce these policies but also change as your policies evolve.
5. **Identify sensitive content.** Identify what content is contained in inbound and outbound email messages that might be sensitive, confidential, or private. Create email policies that address these types of data and deploy solutions that allow you to monitor and enforce content policies. For example, systems that can automatically encrypt sensitive emails can be useful for companies that may be

subject to privacy legislation. These systems should be especially flexible to react to constantly changing content that is contained in email.

6. **Evaluate your company's web usage.** Define policies for acceptable use of the web in your organization. Consider deploying solutions that can monitor web access and can provide real-time anti-malware protection, similar to what you have deployed for email security. Malware threats on the web are growing significantly faster than email-based threats and many companies have limited or no protection in place today.

Compliance best practices

1. **Plan ahead.** Don't wait for the lawsuit, hostile work environment complaint, trade secret leak, or confidential information loss to start managing your data.
2. **Know what is legally required.** Understand the legal requirements of your industry and jurisdictions in which your company operates. For instance, what are the data retention obligations for particular information in a country or state? What safeguards, if any, exist for restricting access or retention? Do you know what must be encrypted and what notification obligations exist if there is a breach of security? Are filters prudent in a jurisdiction to avoid hostile work environments or are filters deemed an invasion of privacy?
3. **One size might not fit all.** If you operate on a national or international scale, understand the sometimes conflicting obligations that your electronic data management system will have to address. Consider firewalls, access restrictions, and disabling particular functions in some jurisdictions that do not permit monitoring or filtering, for instance.
4. **Assign responsibility to manage the system.** Appoint personnel responsible for maintaining and managing electronic data. This might be a collection of people from legal and IT, with input from HR or other departments. Get the people involved early who will need to make the system work when legal demands arise.
5. **Locate the various forms and keepers of data.** Remember that data can be stored in a desk, personal digital assistants (PDAs), home computers, laptops, and elsewhere. Before you can manage data for which the law will hold the company accountable, you must first identify what and where it is to ensure that the systems you adopt will in fact capture the relevant data. Know what metadata you have.
6. **Don't be a pack rat.** Just because technology gives you the ability to store massive electronic data doesn't mean you should. Needless storage of data not only complicates data retrieval but also can increase hacking risks. For instance, don't keep sensitive customer financial data unless you need it. If you need it, encrypt it.

Conclusion

The continued growth in electronic messaging – and the accompanying surge in spam – is a consistent and increasingly painful thorn in the side of IT professionals. In most organizations, it is the IT department that is held accountable for ensuring the security and compliance of their electronic communications, but the obstacles to success are significant.

LEARN MORE

www.google.com/a/security

IT professionals today are not only facing the threat of spam, viruses, and worms, but they are also attempting to secure their increasingly mobile workforces, ensuring the availability and continuity of critical business processes, meeting compliance goals, planning for disaster recovery, preventing data leakage, and protecting their internal systems from hackers. It's no wonder IT professionals are feeling the pain most acutely in their productivity levels.

SaaS solutions in general, and Google's message security and compliance services in specific, address these IT productivity issues and help organizations tame the threats that lurk in electronic messaging. By deploying Google's services, organizations can reduce the pains of ensuring security and compliance – and improve the productivity of their IT professionals.

Google™