WHITE PAPER

Messaging and Web Security Best Practices for 2011 and Beyond

An Osterman Research White Paper

Published March 2011

SPONSORED BY

websense®
ESSENTIAL INFORMATION PROTECTION™

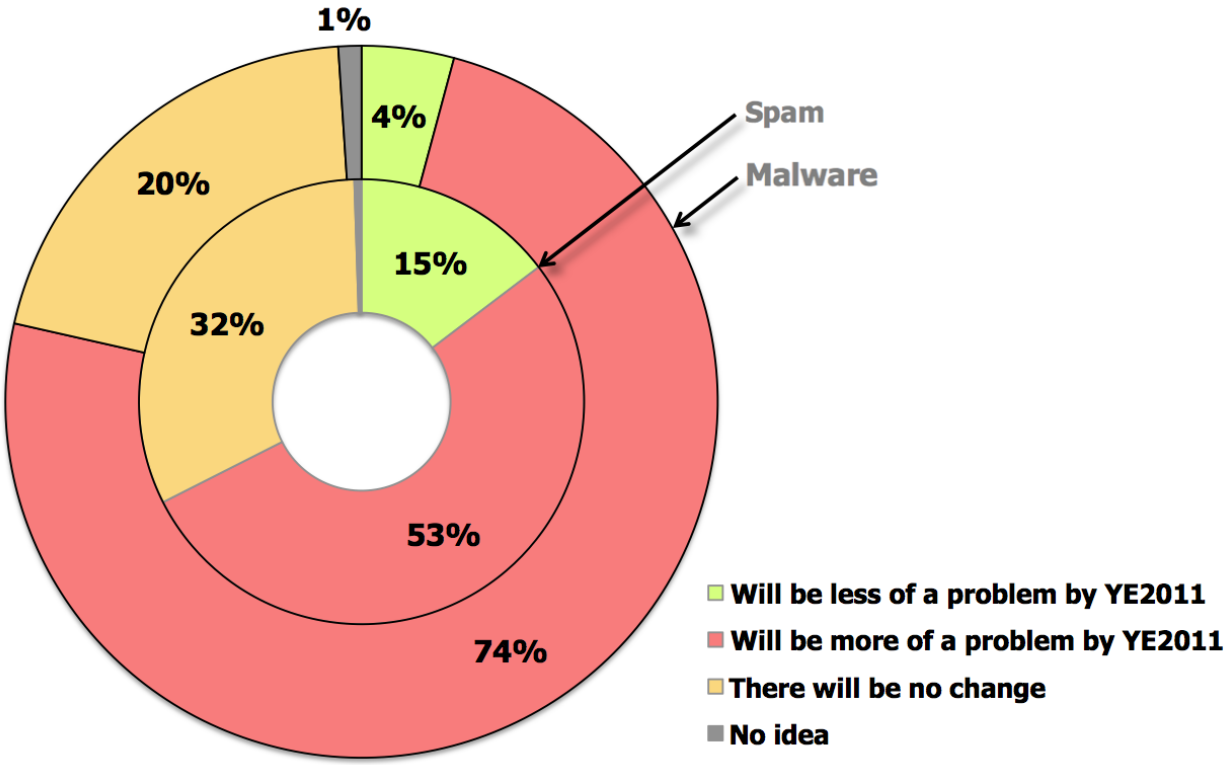
OSTERMANRESEARCH

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

Executive Summary

In an Osterman Research survey conducted during January 2011, decision makers and influencers demonstrated that they are decidedly pessimistic about the future of spam and malware problems for 2011, as shown in the following figure.

Predictions About Global Spam and Malware Problems in 2011



They have little reason to be optimistic: despite recent, albeit temporary good news – such as reductions in the number of spam messages traversing the Internet – there has been relatively little good news in the context of threats directed against messaging and Web users. Further, while many decision makers are taking messaging and Web security threats quite seriously, a soft economy coupled with threats that are rapidly increasing in sophistication and severity means that many organizations are not keeping pace with the threats they face. For example:

- Symantec.cloud reported that 41.1% of all of the malicious domains they blocked during January 2011 were new, representing an increase of 7.9% from the month before[i].

- The Rustock botnet was more or less shut down during the 2010 Holiday season. However, GFI Software reports that in January 2011 Rustock was reactivated and its spam volume increased by 98%[ii] almost overnight. As of late March 2011, Rustock has been silenced once again, but has the potential for coming back online.

- SpamTitan reported results from a 2010 survey that found that 49% of small- to mid-sized businesses had not taken even basic steps toward crafting a social media policy[iii].

- Edgewave reported that during the month ending February 23, 2011, there were anywhere from 49 to 352 new spam campaigns launched every day[iv].

- In 2010, Websense Security Labs found that 61% of all data stealing attacks occurred over the Web or email[v].

KEY TAKEAWAYS

There are five key points that readers of this white paper should understand and appreciate:

- **Spam is still a major problem**
  Despite some recent good news on the spam front, spam volumes continue to increase and are expected to do so for many years to come. Because it saps storage, bandwidth and employee productivity; and is increasingly used as part of malware-distribution campaigns, spam continues to be a very serious problem.

- **Malware is a rapidly growing threat**
  Malware infiltration continues to be a vexing issue for IT management because of a) the increasing sophistication of the threats, b) the financial and other damage they can cause, and c) the sheer volume of new malware that is being distributed across the Internet.

- **There are more places for spam and malware to enter an organization**
  The number of venues for unwanted content to enter an organization is growing. In addition to the normal email channel, this content now increasingly enters an organization through social media tools like Twitter and Facebook, personal Webmail accounts used for work-related applications, Web-enabled smartphones, other mobile devices like iPads, the growing number of cloud-based applications used in the workplace, voice-over-IP systems, real time communication tools like instant messaging, flash drives, applications that users download that are not sanctioned by IT, and normal Web surfing to legitimate Web sites.

- **The network perimeter is disappearing, making organizations more vulnerable**
  Related to the point above is that the network perimeter is rapidly disappearing. Where there used to be a clear distinction between the corporate network and the outside world, the growing number of employees who work from home, coupled with the increasing number of mobile devices used for both work and personal applications, means that the network perimeter often does not exist.

- **Data loss is becoming a greater risk**
  The granularity and thoroughness of the policies to manage messaging and Web applications have not kept pace with the threats that organizations face. This makes organizations more vulnerable to data loss, financial loss, damage to corporate reputation, higher remediation costs and other problems. The risk of data loss through the Web has been exacerbated dramatically with the rapid growth of social media and other Web 2.0 applications.

ABOUT THIS WHITE PAPER

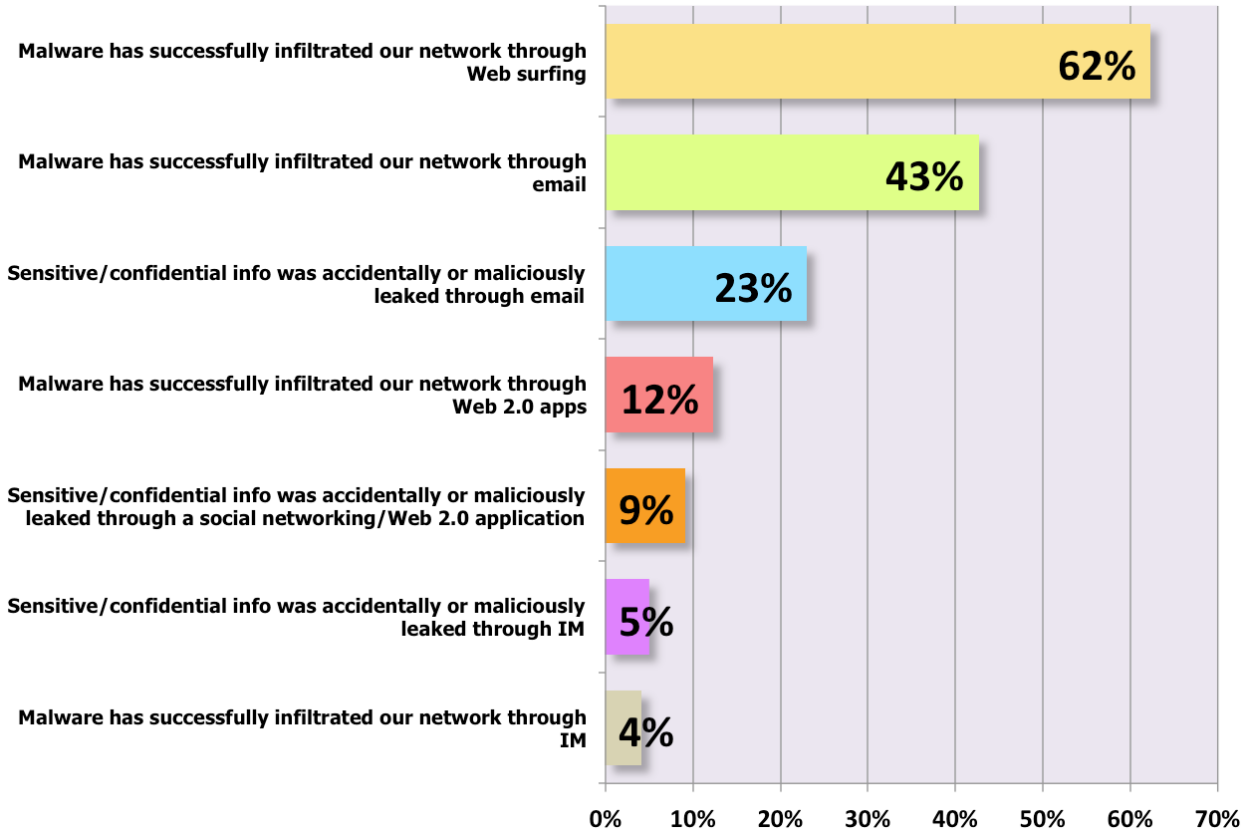
This white paper discusses the threats that organizations face from spam, malware and other threats directed at their messaging and Web capabilities. It uses research from recent Osterman Research surveys, as well as information from a variety of other data sources. It was sponsored by a leading vendor of messaging and Web security capabilities – Websense; information about and contact information for the company is included at the end of this white paper.

Electronic Communication and Collaboration is Dangerous

MOST ORGANIZATIONS HAVE EXPERIENCED MALWARE INFILTRATION

Most organizations have experienced some sort of malware infiltration through a variety of sources, as shown in the following figure from an Osterman Research survey[vi] conducted during 2010.

Security Problems That Occurred During the Previous 12 Months



The occurrence of malware infiltration has become decidedly worse over the past several years. For example, in a 2007 survey conducted by Osterman Research[vii], we found that malware had infiltrated through email in only 25% of organizations surveyed, while only 22% had

experienced malware infiltration through the Web – decidedly fewer than in the more recent survey noted above. McAfee reported that their identification of new malware increased from roughly 16,000 new samples per day in 2007 to 29,000 in 2008 to 46,000 per day in 2009 to 60,000 in 2010[viii] – an increase of 275% in just three years.

SPAM CONTINUES TO BE A SERIOUS PROBLEM

In addition to the rapid increase in malware penetration over the past few years, the spam problem continues to vex organizations large and small. For example, Symantec.cloud reported that spam accounted for 89.1% of email in 2010, or roughly 130.5 billion spam messages sent on a typical day[ix]. While spam levels have dropped significantly in recent months – in part due to the closure of pharmaceutical affiliate seller Spamit and botnets Xarvester, Rustock and Lethic in 2010[x] – there continue to be more than 100 billion spam messages traversing the Internet each day – a figure that will increase over the long term.

WHERE DO THE PROBLEMS COME FROM?

There are a large and growing number of platforms and venues from which malware and spam can enter an organization:

- **Email**
  Email was the dominant method for distributing malware from the early 2000s to roughly 2009 before it was overtaken by the Web as the primary attack vector. However, email continues to be the primary method for distributing spam through a variety of venues – desktop email, mobile phones using SMS, etc.

  Today, email is used largely for "blended threats" – spam messages that contain links to malware-hosting sites. Blended threats are a more sophisticated form of attack because they require a greater level of security integration by combining traditional email and Web security capabilities. Websense found that 89.9% of all unwanted emails in circulation during 2010 contained links to spam sites or malicious websites[xi].

- **User mistakes**
  Users will sometimes install malware or compromised code on their systems, mostly often inadvertently. This occurs when they install ActiveX controls, download codecs or various applications that are intended to address some perceived need (such as capability that IT does not support or that a user needs when working from home), or when they respond to scareware and fake anti-virus (Rogue AV or Fake AV) software.

  Rogue AV is a particularly dangerous type of malware, largely because it preys on users who are attempting to do the right thing – to protect their computers from threats. Even users who are reasonably experienced can be fooled by a well-crafted Rogue AV message. Underscoring the seriousness of the problem, Symantec found that in the year ended June 2009, there were 43 million Rogue AV installation attempts from more than 250 different programs[xii].

- **Various Web site threats**
  There are a number of ways for malware to enter an organization through Web surfing or the use of Web-based applications:

- Cross-component attacks occur when two innocuous pieces of malware code appear on the same Web page. Separately, they are harmless and difficult to detect; however, when they appear simultaneously on a single page, they can infect a user's machine with malware.

- With Cross Site Request Forgery (CSRF) attacks, innocent-looking Web sites generate requests to different sites. CSRF attacks have exploited vulnerabilities in Twitter, enabling site owners to acquire the Twitter profiles of their visitors.

- As Web 2.0 applications often leverage XML, XPath, JavaScript and JSON, Adobe Flash and other rich Internet applications, those applications are frequently vulnerable to injection attacks using these environments. These technologies are often used to evade anti-virus defenses, motivating attackers to leverage them.

- Cross-site scripting attacks embed tags in URLs – when users click on these links, malicious Javascript code will be executed on their machines.

- SQL injection attacks occur when SQL commands and meta-characters are inserted into input fields on a Web site, the goal of which is to execute back-end SQL code.

- **Smartphones**
  Another source of Web threats is the growing use of Web-enabled smartphones. Osterman Research has found that few organizations require any sort of malware protection on these devices, making networks vulnerable to malware that enters through a mobile device when users surf the Web, access email or social media, etc. Compounding the problem is the fact that mobile devices are widely used (more than 90% of corporate information workers also have an employer-provided mobile device[xiii]) and a large proportion of email users employ their mobile device as their primary client for checking work-related email from home.

  The growth and importance of smartphones is being exploited by criminals. For example, ING customers in Poland have been hit with a man-in-the-middle attack (a variant of Zeus) that will install malware designed to intercept passcodes sent to Blackberry and Symbian devices via SMS as part of a two-factor authentication scheme[xiv]. The first malware that targets the Google Android OS was discovered in August 2010. McAfee reported a 46% increase in mobile-focused malware during 2010 compared to the year before.

- **Compromised search engine queries**
  Compromised search engine queries are another method for criminals to distribute malware. This form of attack relies on users making typographical errors when typing search queries, resulting in the presentation of malware-laden sites during Web queries. Search engine poisoning is particularly effective for timely and popular search terms, such as the latest celebrity gossip. Websense reported that searching for breaking trends and current news represented a higher risk (22.4%) than searching for objectionable content (21.8%)[xv].

- **Drive-by downloads**
  Related to the blended threat is a "drive-by" download that occurs when a user visits a Web site and has malware automatically downloaded to his or her computer. In some cases, a user will visit a Web site and see a popup window – upon clicking the "OK" button in the

popup, a Java applet, an ActiveX control, etc. will be installed on the user's computer without their consent.

- **Direct hacker attacks**
  Direct hacker attacks can include a variety of exploits, including hackers attacking a known vulnerability in a Web browser, or exploiting an older version of a browser or ActiveX control.

- **Compromised, legitimate Web sites**
  Many legitimate Web sites have been hacked and have served up malware to unsuspecting visitors. Kaspersky found that one in every 3,000 Web sites served up some sort of malware in 2010[xvi], while the Online Trust Alliance reported that in excess of 10 billion advertising impressions in 2010 contained malware[xvii], with a dramatic increased noted during the last quarter of 2010[xviii]. Websense reported that 79.9% of Web sites with malicious code in 2010 were legitimate sites that had been compromised[xix].

- **Geolocation**
  A growing number of applications use individuals' real-time location, permitting criminals to execute more targeted attacks – phishing attacks that employ geolocation may be more difficult for users to discern as a threat. Many users seem unaware of the malware and other threats they face from revealing their location, and often will freely share this information without considering the consequences.

- **Other problems**
  Off-network users, such as employees who work from home, are another source of Web-based threats. An unprotected user of a corporate asset, such as Outlook Web Access that is not accessed via a VPN, or a laptop computer that becomes infected and later is connected to the corporate network, can constitute a serious threat.

  Insufficient authentication controls will sometimes enable cyber-criminals to crack administrative accounts in order to gain access to sensitive information. For example, BitDefender found in a check of randomly verified email accounts that three-quarters of users employ the same password for their email and social media accounts.

GROWING USE OF SOCIAL MEDIA, WEB 2.0 INCREASES THE PROBLEM

Social networking tools are exploding in popularity. For example, Facebook had 153.9 million unique visitors in December 2010 in just the United States, an increase of 38% from December 2009[xx]. December 2010 also saw 26.6 million US visitors to LinkedIn and 23.6 million visitors to Twitter, representing increases of 30% and 18%, respectively, compared to a year earlier[xxi]. Further, not only the access to social media, but their penetration is growing: for example, while the number of unique visitors to Facebook increased by 38% during the year ended December 2010, total minutes spent on the site increased by 79%[xxii].

The growth in popularity of social media tools has not been lost on hackers and other criminals, leading to active targeting of social media tools across a wide spectrum. For example:

- While phishing sites that target social media account for less than one percent of current phishing sites worldwide, these sites received 62.4% of all phishing impressions in the six months ended June 2010[xxiii].

- Roughly 20% of the news feeds on Web sites contain some sort of malware infection[xxiv].

- The criminal organization that operates Koobface maintains, as of late 2010, nearly 22,000 Facebook accounts (with 935,000 friends), more than 350,000 Blogger accounts, and more than 520,000 Google accounts[xxv].

- Websense found that 10% of links posted in Facebook are either spam or malicious[xxvi].

One of the fundamental problems with social media is that many more organizations allow the use of social media (often doing nothing to protect the organization from its threats) than consider it to be legitimate for use in their organizations, as shown in the following table from a recent Osterman Research survey.

Organizational Views About Various Social Media Tools[xxvii]

Tool	Allow Use	Consider to be Legitimate	Difference
LinkedIn	70%	64%	6%
YouTube	52%	35%	17%
Twitter	50%	34%	16%
Facebook	48%	31%	17%
MySpace	35%	17%	18%
Peer-to-peer file sharing	22%	21%	1%

Another important consideration, albeit not directly a security issue per se, is that strictly personal use of social media can represent an enormous productivity cost to an organization. For example, if users are updating their personal status on Facebook, looking for a new job on LinkedIn, or simply surfing for funny comments on Twitter, that represents an enormous loss of productivity. Using SpamTitan's calculator, an organization of 100 users, each of whom spends 20 minutes per day on personal Facebook use at work and whose average annual salary is $45,000, will cost the organization nearly $186,000 in lost productivity each year.

What this demonstrates is that social media use is allowed in more organizations than actually consider it to be legitimate, indicating that many in IT departments may not accept its use, but they are doing little or nothing to prevent it from being used, resulting in both productivity losses and excessive exposure to malware.

The Consequences of Poor Communication Security

USERS NEED CONTINUOUS ACCESS TO COMMUNICATIONS

Organizations have long struggled with how they should – or should not – manage the use of various communication tools like email, the Internet in general, the Web and Web 2.0 tools. The emergence of social media applications and services makes that question more relevant and also more difficult. Given the range of security threats that can be received by email and the Web, as well as launched from social media sites, organizations need to be extremely careful about their employees' use of those sites in a work environment. The problem is exacerbated by the growing trend for employees to work from home, at times on unprotected or inadequately protected systems that can easily introduce threats into the corporate network. These are problems that must be addressed. Continuing growth in the use of email, the Web, cloud-based applications, and the growing variety of Web 2.0 tools make employees more productive and efficient. Further, these capabilities support the greater concept of mobility – allowing employees to work from home or on the road with the same capabilities they would have in the office. Mobility in its larger context will become increasingly important as organizations look to drive down the cost of real estate, taxes and power by operating with the same number of employees, but with less office space.

The last point is one that cannot be underestimated: as companies seek to reduce their cost of operations, they will focus more on having employees work remotely. Highly reliable communications and information access will be critical to supporting these employees – and robust security will be even more important to enable these employees to work remotely.

THE CONSEQUENCES OF POOR SECURITY

The problems associated with security exploits impact just about every aspect of an organization:

- **Decrease in employee and IT staff productivity**
  Employees waiting for malware to be removed from their computers will be significantly less productive during these downtime periods – in some cases, 100% less productive. Further, any sort of messaging or Web exploit will require IT staff to address the issue as soon as possible after the problem is discovered. This can lead to IT staff working on weekends, the delay of various IT projects, rebuilding desktops, and other costs that may be difficult to estimate. Security exploits can also lead to extended email or other service outages that can have serious ramifications on user productivity.

- **Financial losses**
  Loss of funds that arise from the use of malware like Zeus that is designed to steal money from victims' financial accounts can have a devastating impact on an organization. Just one of the many examples of Zeus' victims is Parkinson Construction, a firm with $20 million in annual revenue that lost $92,000 – nearly 0.5% of its annual revenue – simply because the owner of the firm clicked on email claiming to be from the Social Security Administration[xxviii].

- **Loss of customer data**
  Data breaches can result in the need to remediate them in expensive ways, such as notifying customers via postal mail that their data was lost, provision of credit reporting services to the victims for a year or longer, loss of future business, embarrassing press

coverage and loss of goodwill. The Ponemon Institute has determined that the cost of a single data breach ranges from $98 in the United Kingdom to $204 in the United States[xxix].

- **Loss of internal data**
  Trade secrets, confidential information and other intellectual property can be lost as a result of poor security. These losses can occur across a wide range of venues and activities, including sensitive content that is mistakenly sent in an email or an unencrypted file transfer, data that is lost on an unencrypted mobile device or flash drive, or data that is taken home by employees and stored without any IT controls.

- **Violation of statutes and compliance requirements**
  If adequate security defenses are not maintained, organizations can run afoul of a wide variety of statutes that require data to be protected and retained. However, one study found that decision makers in one out of five organizations do not know which compliance laws apply to their organization[xxx]. A small sampling of these statutes – but by no means an exhaustive list – include the following:

  - The Payment Card Industry Data Security Standard (PCI DSS) encompasses a set of requirements for protecting the security of consumers' and others' payment account information. It includes provisions for building and maintaining a secure network, encrypting cardholder data when it is sent over public networks and assigning unique IDs to each individual that has access to cardholder information.

  - The Gramm-Leach-Bliley Act (GLBA) requires financial institutions that hold personal information to transmit and store this information in such a way that its integrity is not compromised. GLBA requires financial institutions to comply with a variety of Securities and Exchange Commission and NASD rules. A keystroke logger or cross-site scripting attack, for example, that permits sensitive financial data to be exposed to a third party could potentially violate GLBA.

  - The UK Data Protection Act imposes requirements on businesses operating in the United Kingdom to protect the security of the personal information it holds.

  - Japan's Personal Data Protection Law is designed to protect consumers' and employees' personal information. It includes provisions for ensuring the security and disclosure of databases that contain this information, among other requirements.

  - The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian privacy law that applies to all companies operating in Canada. Like many other privacy laws, it requires that personal information be stored and transmitted securely.

  - California's SB1386 (the Database Security Breach Notification Act) is a far reaching law that requires any holder of personal information about a California resident – regardless of where they are located – to notify each resident whose information may have been compromised in some way. Since California passed this groundbreaking data breach notification law, most other US states have passed similar laws. These laws require

organizations to notify customers and others for whom sensitive data is held if their data is exposed to an unauthorized party – an expensive proposition in almost every case.

- **Other issues**
  There are a number of other problems that can occur from malware and other threats delivered via email, the Web, Web 2.0 applications and other capabilities, including:

  - Internet service outages, which can create serious problems for core business services such as email, collaboration, and cloud-based CRM systems. Related to these outages are the potential for data leakage, and lack of compliance with monitoring capabilities and archiving requirements when employees use personal Webmail systems to send corporate data.

  - Web sites being taken down for long periods in order to patch the code to eliminate an exploit.

  - The exposure of FTP and other login credentials to attackers and other cybercriminals.

  - The download of malware that can turn corporate and home-based computers into zombies used as part of a bot network.

  - Users downloading illegal content, such as copyrighted works or pornography using corporate assets. For example, a study published by Cisco ScanSafe found that the number of employees who had attempted to download MP3 files and illegally obtained software has recently increased[xxxi]. A BitDefender study found that 63% of users seeking pornography online had been infected with malware at least twice[xxxii].

What Should You Do to Address the Problem?

DEFINE WHAT YOU MUST DO

It may sound obvious, but IT and business decision makers must determine exactly what they must protect today, and what they can reasonably expect that they will need to protect over the next few years. For example, this list should include things like:

- On-premise, IT-deployed corporate email systems, smartphones, iPads and other capabilities from spam and malware.

- Threats introduced by employee devices that are brought into the workplace and that are used to access corporate resources. This should include iPads, personal smartphones, personal laptops, etc.

- Monitoring and/or preventing what leaves the organization via corporate email, personal Webmail, laptops, smartphones and other mobile devices, social media posts, flash drives, portable hard drives, etc. to protect against data loss. Consider how your data policies can be applied across all channels.

- Encryption of sensitive communications to remain in compliance with both regulatory requirements and best practices.

- Monitoring internal communications for sexually or racially offensive content, as well as sensitive information that could be stored on desktops, servers or other systems without appropriate access controls.

- Monitoring employees' activities when accessing corporate resources from personally owned devices when working from home or remotely.

- Archiving business records that should be retained. While archiving may not seem like a security issue per se, archiving systems should be considered along with spam- and malware-filtering systems because of the ramifications that each has on the other.

- Non-traditional security threats, such as confidential information that might be left on PCs at a hotel's business center. For example, a senior manager at a leading anti-virus company recently reported that he found the itinerary for a general's visit to a military installation on a hotel business center's PC.

DETERMINE WHAT NOT TO DO

As important as establishing what must be done is to establish what must not be done. For example, a blanket prohibition on the use of social media tools like Facebook or Twitter, or preventing users from employing personal Webmail systems at work can have negative ramifications on a number of levels. Employee morale may suffer as a result, as well as user productivity if employees are not permitted to use certain consumer-focused tools that can help them get their work done. Plus, employees will probably use these tools anyway unless IT imposes draconian controls that will most likely have the side effect of impairing employee productivity.

ESTABLISH DETAILED AND THOROUGH POLICIES

Any organization that seeks to protect their users, data and networks from Web-based threats must establish detailed and thorough policies about acceptable use of all of their online tools: email, instant messaging, Web 2.0 applications, collaboration tools, smartphones, flash drives and the Web itself. Successfully addressing these problems must start with an acknowledgement of the threat landscape and the corresponding policies about how tools will be used before technologies are deployed to address the problems.

Further, there must be buy-in across the organization in order for policies to be effective. For example, a policy against the use of social media tools may seriously impact a marketing department's effectiveness at building the corporate brand; similarly, not allowing the use of unauthorized file transfer tools may prevent users from sending large files to prospects or customers in a timely manner.

It is important to note that communication policies must be appropriate and not so broad as to prevent employees from participating in lawful activities. For example, the National Labor Relations Board has taken the position that policies focused on social media are appropriate – to a point. However, corporate policies that prevent employees from discussing their employer on their own time, sharing comments about union organization, etc. may not be legal[xxxiii].

DEPLOY A MULTI-LAYERED, MULTI-LEVEL DEFENSE STRATEGY

It is also important to deploy a multi-layered, multi-level defense strategy. This is becoming increasingly critical as the network perimeter becomes less well defined over time as noted earlier. For example, a traditional security architecture had a clearly defined firewall that separated internal IT-managed resources from the outside world. However, the increasing use of personal devices that can connect as easily to a Starbucks Wi-Fi network as they can to a corporate network, Web 2.0 applications like Twitter, or employees using their personal smartphones to access corporate email on weekends means that the network perimeter is rapidly disappearing. This has made security a much more difficult proposition for IT decision makers, largely because there are so many more devices and data sources to protect. Consequently, any organization should consider deploying:

- Email-based defenses that include anti-virus, anti-malware, anti-spam and DLP capabilities.
- Web content monitoring capabilities that include basic URL filtering, granular remediation capabilities that allow more sophisticated threat management, and real-time security capabilities that will determine if requests from users and applications comply with security policies.
- Integrated Web and email security as a way to defend against more sophisticated blended threats and reduce the cost of managing multiple systems.
- Endpoint capabilities that include anti-virus capabilities on client machines, removable media scanning capabilities, and protection for employees' personal, home-based platforms.
- Cloud-based threat intelligence, such as reputation services, that can determine if content is likely to be acceptable or unacceptable before it is delivered to the corporate network.
- Real-time monitoring and reporting capabilities that will provide visibility into employee activity in order to reduce overall risk exposure.
- Feedback loop systems that will enable community-watch defenses and reports on threats like spam and phishing attempts.

CONSIDER VARIOUS DELIVERY MODELS

There are a variety of ways in which messaging and Web security capabilities can be managed, including:

- **Server-based systems**
  On-premise solutions deployed at the server level, where most data typically resides, resolve many of the problems associated with client-side systems by allowing easier deployment and management capabilities, as well as the ability to more easily enforce corporate policies and changes through a centralized management interface.
- **Gateway-based systems**
  Gateway security stops threats at the earliest possible point in the on-premise infrastructure and is a best practice for organizations that manage on-premise defenses.

- **Client-side systems**
  Client-based systems, such as URL filtering tools, anti-virus tools, spyware blockers and the like provide useful capabilities and can be effective at preventing a variety of threats – client-side anti-virus tools, for example, are an important best practice for any organization to prevent malware from being introduced via flash drives or other local sources. It is important to note here that most traditional, consumer-oriented anti-virus products are client-based tools.

  Client-side capabilities can be relatively inexpensive and are often provided as part of desktop protection suites that include anti-virus, anti-spam and other capabilities. While client-side systems are effective in smaller organizations, they often do not scale well. They are time-consuming to install and update for large numbers of users and can be quite expensive to deploy in larger organizations. Centralized management and deployment capabilities are essential to cost-effectively install, update and enforce corporate policies using client-based systems, particularly for larger organizations.

- **SaaS/cloud-based services**
  SaaS and hosted services are increasing in popularity and offer another option for organizations to implement a variety of threat-protection capabilities. The primary advantages of this model are that no investments in infrastructure are required, up-front costs are minimal, ongoing costs are predictable, and all management and upgrades of the system are provided by the SaaS or cloud service.

  A potential disadvantage of SaaS or cloud services, particularly for Web traffic, is proxying all traffic to the host and addressing latency issues. Their costs can be higher than for on-premise systems in some situations, although they will not necessarily be more expensive. For example, SaaS vendors merely rent space on a server, providing a very inexpensive method for accessing software and infrastructure technologies. Although organizations may pay more to a SaaS or hosted security vendor than they would for an on-site solution, the value of the hosted infrastructure and administration provided by the third party vendor can provide a lower total cost of ownership in many cases.

- **Managed services**
  Managed services are similar in concept to hosted services, but a third party – either with staff on-site or via a remote service – manages the on-premise infrastructure, installs upgrades, updates signature files and the like. Costs can vary widely for managed services depending on the size of the organization, whether third-party management personnel are located on-premise or in the third party's data center, and other factors.

- **Virtual appliances**
  Another option, and one that is finding significant uptake in security applications, is the virtual appliance model – a pre-configured combination of a dedicated operating system and security software that runs in a virtualized environment. Advantages of the virtual appliance approach include the ease of deploying new capabilities, the ability to move virtual appliances from one physical server to another for purposes of maintenance or failover protection, very high availability, reduced power consumption and minimal IT staff time to manage.

- **Hybrid offerings**
  A newer approach that is increasingly offered by vendors is to combine on-premise infrastructure with hosted or cloud based services. For example, an email security vendor may provide a malware-filtering appliance on-site, but couple this with a hosted filtering service that acts as a sort of pre-filter; or they may rely on a hosted anti-virus service and desktop anti-virus tools.

  The fundamental advantage of this approach is that the on-premise infrastructure is protected from spikes and overall increases in the volume of malicious traffic over time, thereby preserving the on-premise investment and maintaining acceptable performance of messaging.

  A hybrid approach may also be deployed for Web security, where on-premise infrastructure is used to secure larger offices and cloud-based services are used to secure smaller sites where on-premise infrastructure is too expensive to support.

Enterprises still prefer in-house over hosted solutions, although this is changing over time. Hosted solutions tend to be more accepted in small- to medium-sized business with less developed IT staff and fewer resources. These organizations often need external expertise and can benefit from the CAPEX and OPEX savings of cloud solutions. Similarly, appliances also tend to offer the SMB the convenience of an integrated solution.

Larger organizations tend to have well-staffed IT departments, and so gain less from the benefits of appliances, unless those appliances are for remote or branch locations where there may be a lack of local expertise. Plus, large organizations tend to have extra server hardware enabling them to realize the CAPEX cost savings afforded by service providers. Evidence to this point is the popularity of in-house managed server software. Given the size of their requirements, large organizations can also justify internal personnel and so may not be realize the OPEX savings of cloud services.

Having said that, while large organizations may not have been the ideal play for cloud service providers in the past, the market is definitely shifting. As IT continues to downsize and outsource, cloud providers are gaining traction in larger organizations precisely because of the savings they can offer. This is particularly true when the buy discussion is conducted at the CIO level.

When evaluating security capabilities, it is important to keep in mind three key questions:

- Will there be the resources available to continually maintain the infrastructure, either through IT staff continually updating capabilities or via an automated update process? If not, anti-malware and anti-spam capabilities can become outdated and leave organizations more vulnerable to infiltration by unwanted and damaging content.

- Related to the question above, will the in-house personnel have the training and time available to manage the infrastructure? This is a particularly important consideration for SMBs that may lack the personnel, training or time to properly manage the security infrastructure. Organizations whose "IT staff" may consist of a few hours per week from

the office manager can end up with security capabilities that are not properly configured because they are simply are too complex not to be managed by a full-time IT staff member.

- Organizations need to consider the cost of managing multiple layers of defense and multiple delivery models. Do IT resources exist to manage everything? If not, consider solutions that consolidate security capabilities, as well as delivery models.

Sponsor of This White Paper

Websense
10240 Sorrento Valley Road
San Diego, CA 92121
USA

+1 858 320 8000
www.websense.com

Websense, Inc., a global leader in unified Web, data and email content security solutions, delivers the best security for modern threats at the lowest total cost of ownership to tens of thousands of enterprise, mid-market and small organizations around the world. Distributed through a global network of channel partners and delivered as software, appliance and software-as-a-service (SaaS), Websense content security solutions help organizations leverage new communication, collaboration and Web 2.0 business tools while protecting from advanced persistent threats, preventing the loss of confidential information and enforcing Internet use and security policies.

[i] Symantec.cloud MessageLabs *January 2011 Intelligence Report*

[ii] http://www.allspammedup.com/

[iii] http://www.irishpressreleases.ie/2010/06/16/spamtitan-report-that-lines-between-personal-and-company-data-becoming-increasingly-blurred/

[iv] http://www.redcondor.com/threat-center/

[v] Websense *2010 Threat Report*

[vi] *Messaging and Web Security Market Trends, 2010-2013*, Osterman Research, Inc.

[vii] *Messaging, Web and IM Security Market Trends, 2007-2010*, Osterman Research, Inc.

[viii] http://news.softpedia.com/news/Number-of-New-Daily-Malware-Samples-Reached-All-Time-High-167141.shtml

[ix] Symantec.cloud MessageLabs *January 2011 Intelligence Report*

[x] http://www.informationweek.com/news/security/management/showArticle.jhtml?articleID=229100295&cid=RSSfeed_IWK_News

[xi] Websense *2010 Threat Report*

[xii] http://www.symantec.com/connect/blogs/fake-av-talking-enemy

[xiii] *Mobile Messaging Market Trends, 2010-2013*, Osterman Research, Inc.

[xiv] http://www.pcworld.com/businesscenter/article/220223/advanced_zeus_trojan_hits_polish_ing_customers.html

[xv] Websense *2010 Threat Report*

[xvi] http://www.bbc.co.uk/news/technology-12539993

[xvii] http://www.bizreport.com/2011/02/ota-10-billion-ad-impressions-carried-malware-in-2010.html

[xviii] http://www.clickz.com/clickz/news/2025413/billions-web-ads-carried-malware-2010

[xix] Websense *2010 Threat Report*

[xx] *U.S. Digital Year in Review 2010*, comScore

[xxi] *U.S. Digital Year in Review 2010*, comScore

[xxii] *U.S. Digital Year in Review 2010*, comScore

[xxiii] *Microsoft Security Intelligence Report*, Volume 9, January through June 2010

[xxiv] http://www.eschoolnews.com/2010/11/23/at-least-20-of-facebook-users-exposed-to-malware-in-their-news-feeds/

[xxv] *Koobface: Inside a Crimeware Network*, November 12, 2010

[xxvi] Websense *2010 Threat Report*

[xxvii] *Messaging and Web Security Market Trends, 2010-2013*, Osterman Research, Inc.

[xxviii] http://voices.washingtonpost.com/securityfix/2009/12/who_says_pay-per-click_revenue.html?wprss=securityfix

[xxix] *Five Countries: Cost of a Data Breach*, Ponemon Institute LLC

[xxx] Source: Webroot Software, Inc.

[xxxi] *Illegal internet downloads at work skyrocket*, IT Pro, January 13, 2010

[xxxii] http://news.bitdefender.com/NW1965-en--BitDefender-survey-reveals-Internet-pornography-remains-a-major-e-threat-source.html

[xxxiii] *How to Stay on the NLRB's "Friends" List*, Bullivant Houser Bailey PC