

# Email Security: A Holistic Approach for SMB

“

*Implementing the latest anti-virus software and security protection systems can prevent many internal and external threats. But these security solutions have to be updated regularly to keep up with new viruses and spam threats.*

”

“

*Microsoft's operating systems and applications have become a primary target for hackers and virus perpetrators because they have numerous vulnerabilities and command the greatest marketshare.*

”

**Many people call email the 'killer app' driving the growth of computer use and increased productivity among organisations of all sizes. However, an escalating array of Internet viruses and email spammers are generating a continuous stream of security threats that could seriously cripple operations. In fact, one email scanning company recently reported that 86.3% of the corporate email that it reviewed in June was spam, resulting in over 790 million messages being blocked.**

Small and mid-size businesses (SMBs) are especially vulnerable to these attacks because of their heavy reliance on Microsoft operating systems and applications that are the targets of many viruses. SMBs also have limited in-house security skills and resources to combat these threats. While many Internet service providers (ISPs) are responding to these email issues by adding a variety of anti-spam and virus features to their portfolios, these offerings haven't reduced the volume of spam for many end-users or created a fully effective firewall against the various viruses being launched on a daily basis.

Compounding these challenges are new government and EU regulations that are setting higher privacy and corporate financial reporting and storage compliance standards for SMBs. These regulations, along with the inability of ISPs to fully address the growing number and complexity of email issues, have convinced many SMBs it is time to take greater responsibility for protecting their information technology (IT) and business operations.

This white paper is intended to serve as a guide for SMBs seeking to improve their safeguards against today's email security threats. It will show how to acquire the right security technologies, and implement the right organisational policies, procedures and practices to strengthen your defense against external and internal attacks on valuable business data.





# Email Security: A Holistic Approach for SMB

## Today's Email Security Threats – How Serious Are They?

SMBs are increasingly reliant on email and the Internet to serve their customers, communicate with partners and meet their business objectives. Unfortunately, Gartner—a leading IT researcher—predicts that 40% of SMBs that manage their own network security and use the Internet for more than email will experience a harmful IT security attack before the end of 2005. And more than half of the affected SMBs won't even know they were attacked and will pass the viruses along to their customers, partners and others.

Email spam, or unsolicited commercial email, consumes an SMB's valuable network bandwidth and wastes precious employee time. The sheer volume of spam—now estimated to be over half of many people's daily email traffic—can be overwhelming. But it is more than just a hassle. It is also a vehicle for transporting computer viruses.



*Less than half of small enterprises and approximately a third of mid-size enterprises have a written security policy. This is generally due to a lack of in-house skills and experience establishing security goals, objectives, budgets and execution plans.*



In recent months, many new viruses have been hidden in spam messages that include ZIP files to fool anti-virus software. The ZIP files compress the viruses to evade the anti-virus software and deceive the email recipients into “unzipping” the attachments and infecting their computer systems.

For instance, a new version of the Bagle email worm, called Bagle.AG, was detected as it began to spread through shared file folders and in email messages. Email messages created by the new Bagle worm used forged or “spoofed” sender addresses and odd subject lines such as “Re:”, “Lovely animals” and “Screen.”

These messages also included worm-infected file attachments in ZIP, EXE, SCR and other common formats with names such as “Moreinfo,” “Details” and “Readme.” When opened, Bagle.AG harvests the recipient's email addresses stored on the infected computer's hard drive and installs its own SMTP (Simple Mail Transfer Protocol) engine, which is used to send out large volumes of infected email messages to other computers.

## Other Common Internet And Email Security Threats

### Spoofing

There are varying forms of spoofing. Email spoofing is when email is forged so the “From” address conceals the true address of the sender and permits the transmission of illicit messages. Internet Protocol (IP) spoofing is when a hacker creates packets that look as though they have come from an acceptable IP address to permit viruses to pass through firewall security and initiate an attack on a computer or local area network (LAN). IP spoofing attacks can be difficult to detect and often require specialised skills and systems to monitor and analyse IP traffic.

### Denial of Service (DOS) Attacks

These are systematic attacks intended to overload and disrupt a network service, Web or file server, or other computing devices. These programs probe IP addresses looking for unprotected systems to take control of address books and set off mass email transmissions.

### Phishing

Hackers use email to troll, or “phish” for email addresses that they can replicate, or forge, to direct other email users to illegitimate Web sites or compromised sites where the hackers can obtain personal information to commit identity fraud.

Although most of the IT security threats that are gaining attention today are associated with external email spam and Internet viruses, Gartner estimates 70% of all attacks that cause more than \$50,000 in damage involve a person working within an organisation. Disgruntled employees intentionally trigger some of these attacks, but most are caused unintentionally by loyal workers.



# Email Security: A Holistic Approach for SMB

The business costs to an SMB if an email spammer forges its Web domain or a hacker uses its domain name to phish for email addresses can be enormous. Not only is its corporate reputation harmed, but new government regulations could make companies liable for not properly securing their email and Internet systems. In addition, there are now examples of employees suing their employers if they believe the organisation intentionally ignored offensive email.

## Why Are SMBS Particularly Vulnerable?

Microsoft's operating systems and applications have become a primary target for hackers and virus perpetrators because they have numerous vulnerabilities and command the greatest marketshare. SMBs are disproportionately affected by these attacks on Microsoft operating systems because:

- **90% of SMBs are running Microsoft Windows on their desktops, laptops and servers**
- **80% of SMBs are using Microsoft Outlook and Exchange for email**
- **70% of SMBs are using Microsoft SQL databases**

SMBs also typically lack the technology skills and experience to keep pace with the continuous stream of new viruses and hacking techniques that threaten their operations.

SMBs are being compelled to combat spam not only because of its potential harm to their computer systems, but also because the explicit sexual content of many spam messages can be offensive to many people. Therefore, SMBs that fail to implement anti-spam measures can be seen as promoting a poor working environment.

Implementing the latest anti-virus software and security protection systems can prevent many internal and external threats. But these security solutions have to be updated regularly to keep up with new viruses and spam threats. This requires strong technical skills and stringent organisational processes governed by comprehensive security policies that reflect an SMB's business priorities.

## Technical Safeguards Against Email Security Threats

There are a number of technologies that can be acquired to protect SMBs from email spam and Internet viruses. The following are some of the most important technologies.

### Firewalls

Firewalls are aimed at establishing a protective shield around the perimeter of your corporate network or to partition portions of the network for security reasons. Firewalls hide the identities of computers within your network to make it harder for criminal hackers to target individual machines. A firewall is a system designed to prevent unauthorised access to or from a corporate network via the Internet. Some firewalls examine and filter information packets that flow in and out of the network to make sure that they are legitimate.



*Since most SMBs rely on their ISPs to supply them Internet access and email service, they have also become reliant on the ISP spam control and anti-virus capabilities.*



Firewalls can be implemented using hardware or software, and can vary in price from less than \$100 to over \$10,000, depending on size and complexity. SMBs can also outsource their firewall perimeter security to an outside-managed security service provider.

### Anti-Virus Software

Anti-virus software is also necessary to protect against infectious files moving within a corporate network and disrupting business operations, corrupting computer files or destroying valuable data. Most of the popular anti-virus software packages include update services to ensure organisations can combat the latest viruses. However, these software packages require continuous updating to be effective.



# Email Security: A Holistic Approach for SMB

And, although many of the anti-virus software packages can be relatively inexpensive, they can also be complicated to use. For instance, when the software identifies a potential problem it may not be clear about how an organisation should resolve the issue. Therefore, many organisations rely on their ISPs or independent email hosting services to handle their security requirements.

## Email Services

Since most SMBs rely on their ISPs to supply them Internet access and email service, they have also become reliant on the ISP spam control and anti-virus capabilities. Nearly every major ISP has implemented anti-spam technologies to block unwanted messages from their networks before they reach users. They have also recently taken measures to limit spam from originating within their networks.

ISPs have discovered that one of the important methods of cutting down the volume of outgoing spam is to filter email sent via Port 25, a gateway that pumps Internet email past an ISP's server. This approach forces users to send email through the ISP's mail server, allowing the ISP to monitor traffic flowing over its network.

New government regulations are placing more of the responsibility of controlling spam on ISPs. This regulatory movement may help to reduce unwanted spam or dangerous viruses, but they may also restrict email traffic as ISPs create filters that may block harmless messages that look suspicious.

## Organisational Safeguards Against Security Threats

Most IT security experts agree that implementing firewalls and anti-virus software is just a starting point. Another essential ingredient in combating spam and viruses is educating computer users about how to properly use email and avoid the various traps created by hackers on the Internet. This educational process needs to be supported by a set of security policies that clearly state an organisation's rules for utilising email and Internet access.

Yet, according to Gartner, less than half of small enterprises and approximately a third of mid-size enterprises have a written security policy. This is generally due to a lack of in-house skills and

experience establishing security goals, objectives, budgets and execution plans. Many SMBs don't know how to develop security policies that define the rules and responsibilities of staff when it comes to safeguarding against email or Internet threats.

In order to effectively combat these threats, SMBs must set policies to prevent their computer users from accepting email with potentially dangerous attachments or downloading dangerous files from the Internet. These policies should be re-enforced by properly configuring company email servers and security software.

Finally, the security policy should include a thorough education program to make employees aware of the organisation's security goals and objectives, the business benefits of maintaining a secure IT environment, the potential cost of IT disruptions, proper email behavior and computer techniques and employee penalties for security infractions.

## Leveraging Outside Experts Is The Best Protection

As we've seen, establishing and maintaining a secure IT environment is both a technical and organisational challenge. Having the right security skills and resources is as important as having the right security systems and software. It is for these reasons that many SMBs turn to outside IT security experts for help. But it takes more than a periodic visit from an IT contractor to combat the continuous threat and distraction of email spam and Internet viruses.

In addition to providing specialised security skills, IT security experts can also provide an independent, objective opinion regarding the right combination of security technology and policies to fit an SMB's business requirements. For instance, single-office SMBs with limited electronic interaction with their customers and business partners will have different security requirements than SMBs with multiple offices and regular communications with outsiders.

SMBs must also identify the right combination of outside security resources. It may be impractical for some SMBs to contract with individual security consultants, purchase various security products



# Email Security: A Holistic Approach for SMB

from multiple vendors and rely on separate ISPs to satisfy their email and Internet access needs. Therefore, many SMBs are establishing strategic sourcing agreements with solution providers that offer a combination of consulting skills, technology products and Internet services.

## **An Email Security Checklist**

The following steps can help an SMB establish an effective security program and select the right set of security products and services to satisfy their business needs.

- **Evaluate corporate email and Internet access requirements**
- **Determine business impact of current level of spam and virus disruption**
- **Measure the business benefits of reducing spam volume and virus threats**
- **Assess existing in-house security policies, skills and technology**
- **Evaluate security capabilities of current technology suppliers and ISPs**
- **Develop strategic sourcing approach for addressing ongoing security requirements**

## **Final thoughts**

Email security has become a serious concern for SMB executives, end users and IT managers. As the volume of email spam and Internet viruses escalates, it is nearly impossible for most SMBs to keep pace with today's IT security threats.

Implementing the latest security products alone to protect against these threats will not overcome this challenge. In fact, just keeping this technology current is an increasingly daunting task. In order to combat today's security threats on their own, SMBs must have dedicated and specialised staff with the right security expertise and business awareness to select, implement and fully utilise the security products and services, appropriate for their business.

Few SMBs can afford to hire this kind of staff on a full-time basis and contracting with individual security consultants won't ensure the continuity of security necessary to safeguard against email spam and Internet viruses on an ongoing basis.

The best approach is to develop a strategic sourcing arrangement with an IT solution provider with in-depth security expertise and the ability to implement the latest end-to-end security products to ensure that an SMB's entire set of IT security requirements are covered.

For more information about implementing the right security policies and technologies in your organisation to achieve your business objectives, contact your insight Account Manager or visit us at [www.insight.com/uk](http://www.insight.com/uk).