

Email, Small Businesses and the Hostile  
Exchange Environment  
**Rick Caccia, Product Management**

## **Securing Email for Small Businesses in a Hostile Exchange Environment**

*By Rick Caccia, Sr. Director, Product Management*

As the volume of e-mail continues to escalate dramatically each year, e-mail will likely continue its dominance as the hub of the corporate communications infrastructure. In fact, the Enterprise Strategy Group estimates that 75 percent of corporate intellectual property is stored in e-mail.

Despite obvious advantages, e-mail poses a number of serious security and availability risks to small businesses such the ability to steal, destroy, or distribute confidential information; or being subject to malicious attacks such as spam.

Not only do many small businesses believe they are not vulnerable to malicious attacks, thinking they are too small to be noticed, but they also lack the resources—budgetary and staffing—to effectively address information security. They often neglect taking security precautions larger businesses often adopt to protect themselves. Attackers recognize this vulnerability and use it to their advantage.

Moreover, today's hackers want to stay unnoticed, their goal being to gather as much personal and financial information as possible while remaining undetected. Not surprisingly, they use email as the path of least resistance.

With this in mind, small businesses ought to rethink their e-mail protection and management strategies to ensure confidential information stays within the organization. Keeping up-to-date with security solutions can help them quickly and easily implement an effective e-mail security policy.

### **Inventory of Business Assets**

Small businesses should create an in-depth sketch of their information assets and access rights to that information. Without this understanding, assets that should be protected may be left vulnerable to attacks.

Furthermore, understanding the current threat landscape also helps small businesses understand how they should spend their time and budget, ensuring they're taking the right protection measures to address their individual needs. For example, risks that may be of concern for a small bank or credit union, may not be the same as risks posed to a small construction firm.

Once risks have been identified and evaluated, the next step is to develop a security policy. A team of managers from separate departments should be assembled and involved in developing the policy.

## Multiple Layers of Defense

To stay secure in today's highly connected world, small businesses need layered security. Multiple layers of security around computers and valuable data help keep the compromise of one level from causing a general compromise of the entire network. This layered defense is necessitated by the advent of blended threats and a blurred network perimeter.

The most important layers that should be part of any effective security program are:

- Antispam software
- Antivirus software
- Firewalls
- Intrusion detection/prevention software
- Virtual Private Networks
- Disk imaging applications

By doing all of the above, small businesses can be protected from growing security and availability risks, and feel much more secure in leveraging the use of e-mail in their business.

## Employees Education

Employees also play a critical function in ensuring that e-mail is secure and safe. Intentional or not, user error is behind many of the security problems small businesses face. Along with technical setup, policy execution should include employee education and training.

The most important ideas to keep in mind with employee education and training are ensuring every employee is included in the training and reviewing the training regularly. When new employees are hired, e-mail security training should be included in their new-employee orientation.

A major discussion point should be creating strong passwords. Passwords are the most common method of authenticating users to provide system entry for hackers. Hackers can gain unauthorized access to the network by cracking passwords. Using a strong password is a layer of protection every business can use to secure their network.

A recent study by global research firms Nucleus Research and KnowledgeStorm found that one in three employees are still writing down passwords and leaving them either on a piece of paper or in a text file on a PC or mobile device, compromising the security of their computer and network.

Part of the program should also include training on how to be smart e-mail users and following guidelines such as not using the preview pane in e-mail programs, being alert to phishing scams, refusing e-mail attachments from unknown senders, and discarding and refusing to proliferate spam. Also, responding to spammers verifies an e-mail address and increases the amount of spam sent to that address.

After the policy has been introduced to employees, perform a regular IT audit of employees to ensure proper security measures are being practiced.

### **Best Practices**

Some best practices small businesses can employ to ensure they are covering their bases in terms of preventing and addressing potential security issues are:

- Remove unnecessary tools and utilities, and updating patches as fixes to newly discovered security vulnerabilities are offered
- Configure e-mail servers to block or remove e-mail containing file attachments commonly used to spread viruses
- Isolate infected computers immediately to prevent further network compromise
- Disable or block access to services that have been exploited by a threat until a patch is available and applied
- Have a backup and restore solution ready in case of an attack
- Put an incident-response plan in place to recover quickly and easily
- Keep server equipment in a secure location

The security landscape is never static. Conducting a semi-annual review of the security policy helps ensure that it is being followed and up-to-date with the current landscape.

### **Conclusion**

As small businesses conduct more and more business via e-mail, they face the ever-present challenge of keeping their IT systems and information safe. E-mail threats have the potential to be even more dangerous to small businesses because of their generally limited IT infrastructure and resource base.

Although they may not have the time and resources many large enterprises have at their disposal, every small business can protect itself from e-mail and other Internet threats by keeping up-to-date on antivirus, firewall and other security technologies; creating a security policy; and educating and training employees on these security policies. Following these guidelines can help each small business establish a secure e-mail infrastructure and internal network.