

CORPORATE PARTNER SPOTLIGHT

As part of the new "Friends of ILCMA" Corporate Partnership Program, partners at the highest level get the opportunity to submit a one page written promotional piece in the ILCMA newsletter. This article is the seventeenth in a series that will highlight ILCMA's newest corporate partners.

Use Your IT \$ Wisely –

Increase Performance While Increasing Security

By Jerry Irvine, CIO & COO, Prescient Solutions

Making decisions on IT purchases today are more important and more difficult than ever. It seems that every IT article lists more and more security risks, viruses and general vulnerability issues. Although the costs of security breaches can be substantial (systems down, loss of data, productivity loss, etc.), it's difficult to measure their real cost and equally difficult to justify taking extra steps to prevent them. As a result, the diligent Administrator needs to reduce security risks while, at the same time, increasing productivity of their users.

From a high level, maintaining security of a network deals with three types of access:

- Unauthorized access from outside the network to internal devices
- Unauthorized access between internal devices on the same network
- Unauthorized access from internal devices to external resources

The first category, unauthorized access from outside the network to internal devices, deals with threats coming from the Internet or private networks (i.e. vendor or partner networks). Devices designed to provide security for this category of risk include Firewalls, Gateways, and Routers, as well as other tools for detection and prevention. These are generally the first level of defense from external threats and are extremely important in developing a secure environment.

As you may already know, the greatest threats to internal computers with external access originate from, and are propagated through, email. SPAM/Antivirus Firewalls, Gateways and other solutions protect the organization from the crippling effects of viruses and other malicious applications, but they can also bring measureable improvements in network performance and employee productivity. For example, some SPAM/Antivirus Firewall devices can actually stop some Spam even before it is sent, which is a great breakthrough for Internet Bandwidth. Some statistics claim that as much as 96% of all email is spam, so stopping it before it is sent greatly increases your overall Internet speed and bandwidth availability. Additionally, blocking spam increases overall server availability and performance while decreasing storage requirements for thousands of unnecessary (and potentially malicious) emails. Finally, the most overlooked increase in performance is in user productivity: fewer SPAM- and virus-laden emails directly results in less time wasted by users.

As for the second category of risk, unauthorized access between internal devices on the same network, the most logical solutions for protection are anti-virus applications and systems updates. Although anti-virus solutions can sometimes hinder overall network performance, productivity can be brought to a halt without them. As a result, existing without them is unrealistic. As for systems updates, in many cases these updates provide corrections to the operating systems and applications and,

therefore, they often enhance performance. Because these updates are provided free by operating system and application vendors and, in most cases, can be installed automatically, it is important to implement them as soon as they become available. Still, directly-related increases in performance are hard to measure for these security methods.

An easy and cost effective way to increase performance while increasing security within this category is through network segmentation. Most, if not all, network devices (firewalls, gateways switches) allow for virtual segmentation of the network. This segmentation is called a VLAN (Virtual Local Area Network). VLANing allows facilities to group devices into smaller, more manageable workgroups which can then have separate security policies configured for them. This would allow segmenting resources like financial servers and data repositories away from users who do not require (and should not be allowed) access to them. At the same time this segmentation occurs, increased performance can be achieved due to the smaller amounts of traffic and requirements for individual VLANs. As a result, networks will see increased bandwidth availability, increased server performance and higher data availability, all while making the network easier to manage.

The final category, unauthorized access from internal devices to external resources, is largely disregarded. Many filtering applications and devices exist to reduce and/or block access to inappropriate websites, instant messaging, file sharing and downloading sites, etc. These applications provide significant security advantages because all of these types of activities have the potential to infect local devices with viruses and malicious applications. Additionally, these sites and applications may have the ability to gain access to local information or to actually gain control of the local machines.

Still, many facilities fail to implement filtering systems and simply try to control local users' access to the Internet via "Acceptable Use Policies" or other employee practices. Nevertheless, filtering applications provide great performance increases. Consider that a single user downloading large media files can slow down or even stop all Internet traffic completely. Reducing or blocking access to audio/video streaming sites keeps the Internet bandwidth available for its required functions (e.g., email, remote access, site-to-site connections and web services). These same applications can be used to block excessive traffic on the internal network as well increasing overall performance and availability of local server and data resources.

While it is my belief that the implementation and deployment of network security tools is essential, overall network performance does not have to suffer and, in many cases, can be enhanced. As a result, consideration should be given when implementing any new IT technologies in order to obtain the largest return on their feature sets. Increased Security, Performance and even Reliability can be achieved through advanced configuration methods and design of any IT device.

City/County Management in ILLINOIS

5

Jerry Irvine is CIO/COO of Prescient Solutions, a virtual Information Technology services company that helps global business clients, local municipalities, schools and governmental agencies maximize technology resources and minimizes IT expenditures. He holds many technical designations, including MCSE, CNE, CCNA, CCNP, CCDA, CCDP.

Contact him at jirvine@pswetakecareofit.com

PS We take care of IT

Is Your Network at Risk?

FREE Vulnerability Scan for ILCMA members*

*Some restrictions apply

Prescient Solutions

Schaumburg Corporate Center
1515 Woodfield Rd., Suite 880
Schaumburg, IL 60173

847-240-3900
www.pswetakecareofit.com

: April 16-17, 2009 –

Boulder, Colorado; St. Julien Hotel

Think Pink: The Manager's Role in Moving from the Information Age to the Conceptual Age

Building on concepts from the conversation between Daniel Pink and Bob O'Neill, captured on DVD, this workshop will focus on the manager's role in a new world of work where the era of "left brain" dominance is giving way to a new world in which "right brain" qualities—inventiveness, empathy, and meaning—will govern. Pink's examples show how the forces of affluence, globalization, and automation are altering the competitive logic of organizations and putting a premium on abilities that have often been overlooked and undervalued. Bob O'Neill will illustrate how smart organizations are using the arts to pull ahead of the competition; and how Pink's six essential right-brain aptitudes now mark the fault line between success and failure.

Young Professionals Leadership Institutes

Please note that in 2009, each Regional Summit event will be