



GFI White Paper

*Your network environment
is the key to the success
of your business*

By Lynn Lunik

Contents

Introduction: What's the key?.....	3
Share the terms, share the success!.....	5
We are on the journey together now, so: What's our plan?.....	5
Summary.....	7
About GFI®	8

Introduction: What's the key?

Your network environment is one of the keys to the success of your business. Most business people don't fully believe this, even after long discussions and mounds of evidence to the contrary. As an IT professional focusing on security for the Windows platform, I have the pleasure of working with and for other IT professionals, supporting the day-to-day operations of businesses of various sizes. So, why do businesses still look at safe and secure networks as a "nice-to-have" rather than a "need-to-have?"

First let's outline the terminology for our discussion. These may sound a little "geeky," but the sooner you accept "geeky" terms as a business owner, the sooner you will share success with your IT professional (to some this is an IT administrator or perhaps a team of IT professionals). Shared success is what all ITpros really work for at the end of the day! Here's our shared vocabulary list for our discussion:

Term or expression	Definition
Workstation	PC hardware used to run a PC operating system (OS) and associated applications.
Workstation image	The exact copy of one workstation which can then be transferred to one or more other "blank" workstations, allowing for easy creation and/or recovery of computers. The image contains the entire operating system plus all applications and data.
Server	Hardware used to run an operating system that "serves" applications, data, print functionality and other business functions to users and workstation. On occasion, the term "server" may refer to just the software component of the system rather than the hardware. For example, Microsoft Windows Server and Microsoft Exchange Server are both software applications.
Server image	This is the same concept as a workstation image. The only difference is that the copy is made of a server rather than of workstations.
Firewall	A hardware device or an application that permits or denies network traffic based on a defined rule set.
Gateway	The defined "edge" where one network meets another network. For example, this might occur where the corporate network connects to the Internet. Each is a distinct network.
Router	A hardware device or an application that transfers, or "routes" data between two networks. For example, a router moves data from your corporate network to the Internet, and vice versa.
Wireless router	A router that also accepts data through wireless connections rather than just through cables.
Network jack or port	The connector typically built into the wall but also a part of many other devices, into which you plug Ethernet (twisted copper) cables.
Network switch	Hardware device designed to aggregate network connections and properly route network traffic from source to target. The network switch is the modern day equivalent of telephone switchboards, directing traffic when and where needed.

Term	Definition
IP address	Numbering system used on computer networks to uniquely identify each device, including workstations, servers, printers, routers and firewalls.
Operating system	Designed software that permits communication between PC hardware and the end-user.
Patching	The act of installing operating system or application updates.
Reboot	The act of restarting a computer or other network device.
Reinstallation	The act of reinstalling an operating system or application.
Logoff	The act of ending a user's session on a computer.
Malicious software	Software that is purposely destructive in nature.
Antivirus software	Software that continuously monitors, quarantines and/or removes viruses.
Anti-malware software	Software that continuously monitors, quarantines and/or removes software determined to be of malicious nature. Anti-malware may include antivirus, anti-spam and anti-spyware software.
Anti-spam software	Software that continuously monitors, quarantines and/or removes unsolicited email messages.
Patch management	The centralized management of operating system and application updates. Patch management is typically handled at the server, and then "pushes" the updates down to workstations.
Network scanning software	Software that automatically or manually scans a computer network to search for vulnerabilities. The network scanner compares the results with a baseline configuration or a database of known vulnerabilities.
Backup	The act of making a duplicate of specific data files.
Restore	The act of recovering data files from a backup.
Disaster recovery	The aggregate procedures of recovering network services to a functional state after a disaster.
Database	Specialized software designed to store connected data in tables and rows.
Query	The act of searching a database based on a specific "question."
Search	The act of researching a technical issue using an online repository of data.
Password	A string of unique characters matched to a user ID to gain access to a network or other data.
Passphrase	A logical sequence of words or characters easily memorized. Passphrases are used in place of passwords to enhance security, since they can be more difficult to guess or "crack" when properly chosen.
Local administrator	A user account within an operating system with complete access to and control of the system.
Local user	A user account within an operating system with limited access to applications and/or data.
Original equipment manufacturer (OEM)	The manufacturer accepting responsibility for a hardware product.
Backup software	Software that enables the creation of backups and the restoration of data.
USB or thumb drive	Portable hard disk media (disk drive) in a miniature form factor.
Technical security audit	The act of performing a network audit focused on defined security variables.
Hosting provider	The organization or data center that maintains an environment designed to securely, economically and reliably host Web sites, servers or other network systems.
Network outage	A planned or unplanned interruption in network services.

Share the terms, share the success!

Initially and for a variety of reasons, most IT pros find it difficult to communicate with business professionals. Some of these reasons are as simple as “It takes a lot of time to explain network routers,” or “I’m not sure if my explanation will be clear enough,” or even, “Explaining networking to a business professional means they might need to explain more about the business to me!” IT pros therefore typically keep quiet about the requirements to perform their jobs in a way that supports business functions. However, as IT pros gain understanding of the expectations from the business pro, the terms listed in the previous section become a shared vocabulary. Once we arrive at this phase, we begin a different journey to improve network services.

We are on the journey together now, so: What’s our plan?

IT pros (like business pros) always have a plan to improve the network environment. The limitation (for both the IT pro and the business pro) is resources. Resources can be time, money or the availability of skilled labor. As an IT pro, I focus on specific fundamentals of building, growing, optimizing and securing a network environment. If a business pro were to ask me for the fundamentals that translate into the largest return on investment (ROI), I would begin with the following list:

Invest in antivirus software	Install antivirus software on all servers and workstations. The price of the software is insignificant compared to the expense of recovery and lost productivity that will occur if a virus infects an unprotected network.
Invest in anti-malware software	Similar to antivirus software, install the more generic “anti-malware” software on all servers and workstations to protect the systems and the business from downtime and/or legal problems in the event that the network is compromised.
Invest in patch management software for workstations and servers	Patch the workstation and server operating systems and applications monthly or “as needed”. This ensures that “exploits” written to take advantage of weaknesses in the operating system or applications do not compromise the workstations or network in general.
Use passphrases instead of passwords	Modern operating systems require passwords to access the system or specific data. The complexity of this password may be the difference between “stolen” and “secure” data. Instead of making passwords the norm, use a passphrase. For example: 1) “Light\$3” might be a typical password, while 2) “Light-@-WatEr-GrOw-Pl@ntz” (a variation of “Light and Water Grow Plants”) is a passphrase. When you use a passphrase, you commit to memory 1) the phrase, and 2) the Special Characters in that phrase (such as using hyphens, the @sign, the use of “0” instead of “o”, and the “z” instead of “s” in the word “plants.” The use of a passphrase dramatically increases the technical requirement to “crack” into a user account.
Logoff or lock your workstations when you step away	Access to a network occurs through workstations, servers or network device sessions. Reduce access to the network by unapproved users by logging off or locking your desktop even if for a brief break away from your desk. This decreases the likelihood that confidential data can be viewed by unauthorized users.
Don’t make every user a local administrator on his/her workstation	Most employees do not need local administrator access in a well-managed network. Prevent users from logging in as a local administrator. This helps to prevent the installation of unauthorized or malicious software.
Don’t share passwords	If we plan to guard critical business data, then we need to define who can access this data. Passwords or passphrases should be kept confidential. IT pros trying to track down unauthorized access will be severely restricted if individuals are logging on with other users’ accounts or if there is a “shared” account that multiple individuals use.

Provide access to the Internet only to those requiring access and when appropriate	Not all job functions require Internet access. Improve productivity by providing Internet access through a proxy server (see the section "Invest in quality edge devices such as firewalls and proxy servers" later in this table) and only to individuals whose job function requires access. Alternatively, provide Internet access only at certain times of the day, such as during lunch breaks. This will improve productivity and provide an incentive for work completion.
Invest in workstation and server imaging software	Imaging software provides the ability to "create" a single workstation or server "image," and then "duplicate" that image to new computers as they are purchased. This reduces administrative overhead, since all new workstations will now have the software pre-installed and you will not need to update and/or manage software that may have been pre-installed by the hardware vendor.
Always image workstations and servers purchased from an original equipment manufacturer (OEM)	Workstations purchased with the operating system and applications pre-installed are typically loaded with unnecessary software. This software requires maintenance to patch and can provide a real distraction to employees if left on workstations. The same holds true for server software. In addition, you may have had to purchase additional licenses from the OEM just to obtain the hardware. This OEM software may take a long amount of time to remove manually, and failure to do so will typically lead to poor system performance. Instead, use imaging software and deploy the company "image" that contains only approved software. Creating an image is a one-time process with maintenance of an image considerably less costly than uninstalling OEM software on every workstation upon arrival.
Invest in server backup software and hardware	Data critical to business success necessitates being backed up to an alternate storage location for safe-keeping and disaster recovery. Typically, a combined software and hardware solution is required. Move away from portable USB drives. Data on portable USB drives is easily duplicated by unauthorized users and the disks are lower quality than those purchased in servers or specialized disk arrays. This ensures a higher likelihood of data recovery in the event of any type of disaster.
Reduce or eliminate use of USB hard drives (thumb drives or flash drives) and portable USB drives	Although these devices prove extremely valuable they consistently prove to be liabilities. Consider investing in file server storage or a Storage Area Network (SAN) instead. Also invest in the software and services necessary to restrict/eliminate use of portable USB devices. A skilled IT Professional configures the system to make sure that data remains with your company rather than finding its way into your competitors' hands. This also improves data retention and reduces the likelihood of data theft.
Reduce the number of workstations and servers to as few as possible	Only purchase workstation hardware as required. This reduces the number of devices that need to be maintained on a regular basis. This further reduces costs and ensures the proper use of company assets.
Consider investing in server virtualization technology	This relatively new technology is now extremely viable to let you run several "virtual" servers from one physical or "real" server. This is accomplished using specialized software to run these "virtual" machines. From the point of view of users and other systems, the virtual servers are no different from the real ones: they run their own operating system, contain their own applications and process their own data. This also provides excellent disaster recovery functionality (virtual servers can be copied and saved elsewhere) and a reduction in physical space requirements, power consumption, and maintenance costs.

Invest in quality edge devices such as firewalls and proxy servers	Purchase and maintain a good quality firewall and proxy server. The firewall should be configured with both inbound (common) and outbound (not common) rules to restrict or permit only certain types of network traffic. The proxy server role should include data caching and packet inspection (just like the firewall) to permit or deny access to specific web sites and payload content.
Invest in a security audit focused on the fundamentals and take action based on the results	Identify a professional consulting firm or consultant to perform a technical security audit of the fundamentals listed in this document. Review the results and take action when appropriate. This is a documented and proven method to mitigate risks. It also builds your IT pro's confidence by providing a "shared vision" of discovered goals.
Invest in one or more IT professional on staff or augmented through a professional consulting firm	Incorporate an IT professional or team of professionals into your business plan. Invest the effort to communicate your business goals. Conversely, request an IT plan from the IT professional that meets your business goals.
Consider hosting services with a hosting provider	Skilled IT pros can assist in determining which services are good candidates for being hosted in dedicated data centers (frequently referred to as the "cloud," as the servers'/developers'/system engineers' fees are included in the monthly service fee). Examples of the common services that many businesses are moving to the cloud include: 1) the company website, 2) offsite backup storage, 3) email and email archiving, 4) email antivirus/anti-spam filtering and others. Using hosting from dedicated data centers improves fixed costs, reduces complexity and may improve service availability for specialized services.
Integrate a disaster recovery plan into your business plan	Disaster recovery for servers and workstations requires preparation, practice and constant planning. Request that your IT Pro includes a disaster recovery plan into your business plan and then execute business decisions based upon that plan. This provides a higher likelihood that your business will recover from a disaster with the network services necessary to stay in operation.
Budget for IT expenditures in your business plan	Understand that every dollar spent regarding information technology (IT) is more than triple that earned. Expect to spend money on licenses, renewals, hardware replacement, hardware upgrades, and new hardware and services every year.
Plan for occasional "outages" of services	Maintaining server and workstation hardware, printers, scanners and the associated software is a challenge. Add demanding users to this equation and this is a typical day for an IT pro. Occasionally, services will not be available during business hours. This should be the exception and not the norm (see "Invest in an IT professional on staff or augmented through a professional consulting firm" earlier in this table). Communicate expectations regarding availability and integrate this availability into your business plan. Adapt when the circumstances require non-availability on an expected basis for network services. This shows your leadership and understanding for circumstances beyond the control of even seasoned IT professionals.
Communicate with your IT pros	Understand as a basic consideration that IT pros genuinely want to provide quality services to support the business objectives. This communication provides the leadership, encouragement and accountability all aspiring IT professionals require!

Summary

In this brief excerpt from the thoughts of an IT professional (IT pro), I have outlined several important considerations regarding communication between an IT professional and a business professional (business pro) jointly working toward the same business goals. Additionally, I have outlined what could be considered “fundamentals” that business pros should consider regarding services provided within a business by IT pros. I have also indicated that business pros and IT pros should speak a common vocabulary and work towards shared objectives. In the end, business pros will likely become more like IT pros, while IT pros continue to grow in business acumen. With that in mind, why don't you give it a try?

Lynn Lunik, Chief Security Architect

IT Pro Secure Corporation | <http://itprosecure.com/blogs>

Founder of IT Pro Secure Corporation (ITPS), Lynn has over 22 years of information technology experience. Prior to ITPS, Lynn worked as a senior consultant for Microsoft Consulting Services, a platform strategy advisor for Microsoft Corporation, as a principal consultant for a Microsoft Gold Certified Security Partner, and as an executive director of information technology for an international medical equipment and services organization. Additionally, Lynn holds a Master in Business Administration (MBA), a number of Microsoft certifications (including MCSE+I) and the Certified Information Systems Security Professional (CISSP) designation.

About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMBs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at <http://www.gfi.com>.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com



Disclaimer

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.