

# BUSINESS TECHNOLOGY QUARTERLY

[www.technologygroupllc.com](http://www.technologygroupllc.com)

Brought to you by *The Technology Group, LLC* at Whittlesey & Hadley, P.C. (860) 524-4480 [technology@whcpa.com](mailto:technology@whcpa.com)

## MIP RELEASES NPS INTRO

By Deborah Swanson, MCSE

Micro Information Products, Inc. recently unveiled its latest product, Non Profit Series Intro. **NPS Intro** is based on MIP's original fund accounting software package NPS Pro. NPS Intro was **designed for the smaller non-profit organization** with a budget of less than \$1 million and no more than 3 concurrent users. It requires Windows 2000/Windows XP Professional. Like NPS Pro, it is a modular based software package. Its core General Ledger module **starts at \$1,295 for a single user**. Other modules include Accounts Payable, Accounts Receivable, Payroll, Bank Reconciliation, Budget and Forms Designer. The General Ledger module includes a built-in report writer and comes with pre-formatted financial statements. The chart of accounts is table-driven and allows for 2 user-defined segments in addition to a required General Ledger account segment and optional fund and restrictions segments. Like NPS Pro, NPS Intro **allows for cross-fiscal year reporting** and multiple open fiscal

periods. The Technology Group, LLC is a certified MIP service provider. For more information, please contact Deborah Swanson or Mark Torello.



## Choosing the Right Printer

By: Patricia Barnes

Choosing the right printer for your office or home can be a confusing process. There are many different printers on the market to choose from. Before making your printer choice there are a few key factors to take into consideration.

**The use:** Photos, letters, mass mailings, large paper, etc. Graphics printing requires more ram.

**The speed:** How many pages per minute needed.

Continued on Page 4

## Q & A ON: DISASTER RECOVERY AND WHY IT'S ONLY PART OF A GOOD IT SECURITY PROGRAM

By: Mark R. Torello, CPA, CFE  
(As printed in the Hartford Business Journal on December 17, 2001)

Q. WHAT ELSE COMPRISES GOOD IT SECURITY BESIDES DISASTER RECOVERY?

A. **Disaster recovery**, without a doubt, is one of the more critical components of a good IT security plan. The disaster recovery plan is the roadmap to restoring operations after a disaster. Without such a documented and tested plan, loss of data and critical processes as a result of a disaster can easily put a company out of business. Government offices are increasingly required to have documented disaster recovery plans as well as tested IT security plans. However, there are other equally important pieces to the IT security pie...

Access **Security** is one of those pieces. Access Security are those systems and processes (automated or manual) that ensure that only those individuals who have been authorized to access certain areas of information can gain access to that information. Components of designing a good access security plan include password protection, physical access rights, and a control process for granting approved rights. (see Security on Page 2)

## INSIDE

Technology Group News	pg. 3
Accounting System Industry News	pg. 3
Color Laser Printer Comparison	pg. 4

Security

Continued from Page 1

**Firewall protection** is another important piece of the IT Security pie that focuses on protecting internal systems from unauthorized public access. There are many different varieties of firewalls with varying associated costs. The firewall solution appropriate for your business should be determined by a security professional.

**Software Escrow**

**agreements** with mission critical software may also be part of a good IT security plan. Escrow agreements provide for the source code of software to be kept in a location available to the user upon disaster or dissolution of the software developer.

**Virus protection** that is up to date is also an important part of a balanced security diet. A virus can cause havoc to a network via lost data as well as lost "up time." More often than not, we find that a business's virus update process is either not automated or not kept up to date and verified. There are many virus protection programs that are very effective and employ a high level of automation for a corporate environment.

Q. DOES MY DISASTER RECOVERY PLAN HAVE TO BE IN WRITING?

A. Yes. When a disaster occurs, a documented plan allows people who are most likely not in their usual frame of mind to follow step-by-step directions. Further, in a worst-case scenario, the people who were involved in the creation of the plan may no longer be around,

which is the case with Espeed of Cantor Fitzgerald in the attack of September 11. Thanks to a detailed written disaster recovery plan, Espeed was able to have most mission critical processes back up in 47 hours after the attack and after losing 730 members of the company.

Q. HOW WOULD I KNOW IF SOMEONE WAS ATTEMPTING TO HACK INTO MY NETWORK?

A. If you have a firewall in place, the firewall product should generate automatic alerts to hack attempts. The firewall product should also generate a log, which will show hack attempts. If the hacker were to get past your firewall, his next step is to gain access to a server or PC behind the firewall. The un-automated process to find out if someone is attempting unauthorized access is to enable and review system security logs. Again, there are many products available to alert, detect, and prevent such unauthorized intrusion behind the firewall. As is typical, they range in price and functionality.

Q. ONCE IT'S DETECTED, WHAT DO I DO?

A. If you are suspect that you are the target of an unauthorized intrusion (a hacker), you will generally need the services of a high-level network security engineer to find and patch the holes. Resolving security holes entails a thorough review of the hacker's access into the system to determine where the hole exists and applying appropriate security enhancements. Enhancements can take the form of network infrastructure design, security patches, firewall updates, etc.

If you do not have your network engineer present and you or your firewall product detects and alerts you of intrusion, your best bet is to isolate your network from the source of the hack (usually the Internet). This can be done simply, by unplugging the router or dial-up connection to

the Internet. Immediately notify your network engineer or consultant of what you saw happening. This type of "what if" process must be planned with your network engineer or consultant to ensure when it is safe to unplug an internet connection since this can result in terminated applications, lost files, etc.

Q. WHAT IS PENETRATION TESTING AND DO I NEED TO DO IT?

A. Penetration testing is the authorized and planned attempt to hack into a network. Generally this level of prevention and assurance is not required as long as you are up to snuff on your security program. In some sensitive industries and businesses where data privacy and security are of the utmost importance, penetration testing is warranted and the benefits clearly outweigh the costs.

Q. HOW CAN I PREVENT A HACKER FROM GETTING INTO MY NETWORK?

A.

1. Make sure you have a properly configured firewall product installed that has been certified by ICISA (Internet Computer Security Association – [www.icsalabs.com](http://www.icsalabs.com).)
2. Have your network security evaluated by a qualified security professional (an IT Audit) These audits review the design of your network, firewall configuration sufficiency, as well as identify security holes.
3. Install latest security patches and updates for network operating systems, firewalls, virus protection, and Internet web

and email clients.  
4. Regularly review security logs.

**Q. HOW MUCH DO I HAVE TO SPEND ON A FIREWALL AND SECURITY?**

**A.** I hate responding with “it depends”, but it really does. Obviously you will most likely need to spend less than Microsoft (who has been found vulnerable in the past). Network firewall products for a small company generally range from \$500 – \$10,000 depending on the size of the network, number of users, etc. You will have to decide “how much” is enough protection based upon the type of data on your network and a cost-benefit analysis. Implementing a corporate network firewall can be much more costly than the product itself based on qualified network engineers rates, so the consulting costs must be included. Overall, a medium size medical practice of 50 users may spend \$15,000 for a network firewall solution while a manufacturer of the same size may only decide on spending \$6,000 based on a cost benefit analysis. A simple personal firewall can cost in the neighborhood of \$50.

What should you **spend on overall security**? Again, it depends on the data you keep and a cost benefit analysis. It is my opinion that a good budget should be developed that incorporates regular security reviews by a network security specialist. Regardless of your in-house qualifications, **an independent third party review** is guaranteed to find a chink in the armor because of their expertise and objectivity. I have found major security holes in \$600+ million dollar companies with IT departments of over 150

staff. These IT security audits can range from \$4,000 to \$50,000, depending on the size and complexity of the network.

**Q. WHAT ARE PERSONAL FIREWALLS?**

**A.** Personal firewalls protect an individual workstation from unauthorized intrusion. Some individual computers must dial-in to other networks directly (circumventing the network internet connection and any firewall security protection therein) and therefore need protection at that level. If you have an individual PC that has a network connection with a dedicated (or static) IP address and/or a full time Internet connection, a personal firewall is a must. Three personal firewalls just passed the ICSA’s stringent security tests and became certified as follows: 1) ZoneAlarm Pro, 2) Tiny Personal Firewall for Windows 2000, and 3) Norton Personal Firewall for Windows Me and 2000.

**Q. WHAT IS AN IT SECURITY AUDIT AND DO I NEED ONE?**

**A.** An IT Security Audit is a **review of the security and controls over your technology infrastructure by an independent third party qualified to perform such audits**. Certain governmental agencies, such as the National Credit Union Administration and Federal Deposit Insurance Corporation have required organizations under their control to have these audits performed.

The audits are designed to review all areas of security from firewalls to virus protection. If you have any data on your network or rely on your network for mission critical activities, you need an IT Security Audit.

Finding consulting firms qualified to perform such an audit is a more difficult task since it requires a blending skill set of an auditor and an IT engineer. Make sure that a written report is included that spells out what was performed, what was found, and most importantly, **clear** recommendations for improvement.

Mark Torello is the managing director of the Technology Group, LLC out of Hartford, CT (860-524-4433). The Technology Group specializes in IT Security, wide and local area network integration, and IT consulting.

**Technology Group News**

**Jennifer Boggs** has joined our team as a consultant. Jennifer comes with accounting systems experience from both the not-for-profit and manufacturing industries. Jennifer is a graduate of Central Connecticut State University with a B.S. in Accounting.

**The Technology Group, LLC** is now proud to be a reseller of the highly acclaimed not-for-profit software, MIP. In addition to providing stellar consulting and implementation services, as a certified service provider, The Technology Group can now help it’s clients save money on the purchase of their software.

**Accounting System Industry News**

On October 22, 2001 Best Software, the company that offers such brand names as Peachtree, MAS90 and One-Write Plus, acquired MIP. The expected benefits of this acquisition are numerous including an infusion of research and development to enhance the MIP stature including student billing and fundraising interfaces to name a few.

Choosing the Right Printer

Continued from Page 1

**The quality:** Usually measured in dots per inch (DPI)

**The duty cycle:** How many copies in a given period (usually monthly) the printer is meant to handle.

**The quantity:** The typical size of your printing job will determine the size and number of paper trays needed.

**Sharing:** Will the printer be shared? If yes, you can choose between a network ready printer with a built in network card or a separate network adapter, which is usually less costly.

**What's most important** in choosing the right printer is the end use:

What types of printing do you do "regularly"? Will the printer be used mainly for printing text or will you need to print images with high-quality graphics or photographs? Will there be one or two users, or will the printer be accessible to a network of users? Is there a consistent need to be able to print in color?

There are **three basic types** of printers a small to medium size business will choose from: Ink Jet, laser, and color laser.

**Ink jet printers** offer color image printing and good text printing at a very modest cost. These printers are predominantly used for personal printing such as draft reports, low quantity graphs and charts for reports, and low quantity images such as digital photographs.

**Black and white laser printers** offer the **best speed and quality text**. For medium high quantities of report printing, the laser is the best solution.

**Color lasers** offer **fine color image** and text reproduction at a higher cost. When running reports with color or larger quantity graphs and charts, a color laser will be the viable choice. **Color laser printers have recently come into an affordable range** for small businesses that wish to produce professional looking hand-outs without going to the offset printers.

Below is a comparison of **three of such color laser printers** with similar features:

**Color Laser Printer Comparison**

**Hewlett Packard  
Color LaserJet 4550n**

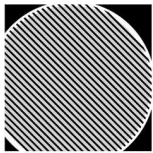
600 x 600 Dpi  
64 mb ram  
250 & 150 sheet paper trays  
16 pages/minute black  
4 pages/minute color  
Optional Duplex Printout  
Internal network card  
\$2,349.98

**Xerox  
Tektronix Phaser 750N**

1200 x 600 Dpi I  
64 mb ram  
250 Sheet paper tray  
16 pages/minute black  
5 pages/minute color  
Optional Duplex Printout  
Internal network card  
\$1,999.99

**Lexmark Optra C720**

1200 x 1200 Dpi  
32 mb ram  
250 Sheet paper tray  
24 pages/minute black  
6 pages/minute color  
Optional Duplex Printout  
Internal network card  
\$2,399.95



The  
Technology  
Group, LLC

at Whittlesey & Hadley, P.C.  
147 Charter Oak Avenue  
Hartford, Connecticut  
06106-5100

PR SRT STD  
U.S. POSTAGE  
**PAID**  
Hartford, CT  
Permit #2639

**VISIT OUR WEBSITE**  
[www.technologygroupllc.com](http://www.technologygroupllc.com)