

Scaling New Heights
 An Advanced Training Conference
 for ProAdvisors and Intuit Solution Providers
 May 24-26, 2010 – Atlanta Georgia
 www.ScalingNewHeights.com

“The Most Secure Way to Run QuickBooks”

Presenter: Joe Woodard – The Woodard Consulting Group
Panelist: Wendy Rohrssen – The Woodard Consulting Group
Panelist: Robin Hall, President – VARC Solutions
Panelist: Eric Pulaski, President – Smart Vault
Contributor: Mario Nowogrodzki – Mendelson Consulting



Scaling New Heights 2010
 www.ScalingNewHeights.com

About this Year’s Conference

- **General Information**
 - Conference Sessions: May 24-26, 2010 – Atlanta, Georgia
 - Stone Mountain Climb, Picnic and Laser Show: May 23
- **Your Investment in the Conference Provides You with:**
 - Practice Marketing, Management & Development Training
 - In-Depth, Intuit-Centric Professional Education
 - Networking Opportunities
 - Exhibition Floor
 - Professional Distinction



Scaling New Heights 2010
 www.ScalingNewHeights.com

About this Year’s Conference

- **In Depth Professional Education Focused on Each of the Following:**
 - **Expanded!** Advanced QuickBooks & QuickBooks Enterprise Solutions
 - **New!** Intermediate QuickBooks Training
 - **New!** QuickBooks Point of Sale
 - **Expanded!** Intuit Warehouse Management ES
 - **Expanded!** Intuit Field Service Management ES
 - **New!** Method
 - **New!** Fishbowl Inventory
 - **New!** “QuickBooks & The Mid Market” – a Practice Development Track
 - Intuit QuickBase



Scaling New Heights 2010
 www.ScalingNewHeights.com

Upgraded Venue
 Evergreen Marriott Resort & Spa
 \$109/Night





Scaling New Heights 2010
www.ScalingNewHeights.com

"The Most Secure Way to Run QuickBooks"

- Minimizing Security Issues around the Company's QB Users
- Protecting Your Clients from Unauthorized Admin Password Resets
- Maximizing Security on a Local Area Network
- Leveraging the Web to Increase QuickBooks Security
- Increasing QuickBooks Security through Business Processes and Internal Controls

Scaling New Heights 2010
www.ScalingNewHeights.com

The Over-Arching Security Measure

- Awareness: Make Your Clients Aware of Potential Issues
- Anti-Awareness: Do Everything Possible to Keep Your Clients' QB Users *Unaware* of Potential Issues

Scaling New Heights 2010
www.ScalingNewHeights.com

Security Concerns within QuickBooks

- Access Rights in QuickBooks Pro & Premier
 - Problem: Access Rights are Too General
 - Solution 1: Upgrade to QuickBooks Enterprise Solutions
 - Solution 2: Leverage the Web
- Editing the Payee on Printed Checks
 - Problem: Print and Edit Post Printed Check or Print and Edit "Print on the Check As" Field
 - Solution 1: Protect Your Clients through Internal Controls
 - Solution 2: Leverage the Web
- Printable Signatures on Checks in QuickBooks 2010
 - Problem: There is no ability to restrict users from adding e-signatures to checks – if they have the rights to print checks
 - Solution 1: Provide a written document to your bank stating that you do not authorize the use of facsimile signatures
 - Solution 2: Wait to Upgrade?
 - Solution 3: Leverage the Web

Scaling New Heights 2010
www.ScalingNewHeights.com

Security Concerns within QuickBooks

- Static Bank Reconciliation Reports?
 - Problem: The Acrobat/Static QuickBooks Reports are Not Necessarily Static
 - Solution: Print and Save Bank Reconciliation Reports as Paper or Acrobat Documents Outside QuickBooks
- Printing Documents for Customers with No Audit Trail Presence
 - Problem: You Can Print a Document (e.g. an invoice) and Then Exit without Saving
 - Solution 1: Set Company Preferences to Save Transactions When Printing/Previewing
 - Solution 2: Leverage the Web (More on this Later in the Webinar)
- Weak Logins and No Requirement to Change Admin Passwords
 - Problem: QuickBooks does not require "strong" passwords or changes to admin passwords
 - Solution 1: Turn on Credit Card Protection
 - Solution 2: Leverage the Web (More on this Later in the Webinar)

Scaling New Heights 2010
www.ScalingNewHeights.com

Increasing Security on the Local Area Network

- **Issue: QuickBooks Users Must Have "Power User" Access to the Server**
 - Solution 1: Use a Dedicated QuickBooks Server
 - Solution 2: Use a Linux Server
 - Solution 3: Leverage the Web
- **Issue: Workstations/QB Installations Do Not Have Protected DLL Files**
 - Solution 1: Use Trend Microsystems for your Antivirus/Firewall Application
 - Solution 2: Leverage the Web
- **Tip: Look at the IBM Smart Cube for Local QuickBooks Hosting**
 - Linux System - More Restrictive for LAN Users and Less Prone to External Attack/Viruses
 - Indigenous, Integrated Firewall Called Proventia Server for Linux
 - Internet Protocol Security (IPsec) for Built in Remote Access Capabilities
 - Very Tight Security Protocols Configured by Default During Smart Cube Setup

Scaling New Heights 2010
www.ScalingNewHeights.com

Intuit's Password Recovery Service

Step 1: Click Forgot Password



Scaling New Heights 2010
www.ScalingNewHeights.com

Intuit's Password Recovery Service

Step 2: Click "Download the Free Password Reset Tool"



Scaling New Heights 2010
www.ScalingNewHeights.com

Intuit's Password Recovery Service

Step 3: Complete the Form Shown Below.



Scaling New Heights 2010
www.ScalingNewHeights.com

Intuit's Password Recovery Service

Step 4: Accept the License Agreement and Click Download.
Step 5: Run the Utility to Reset the Password – Using the Emailed "Token"

Scaling New Heights 2010
www.ScalingNewHeights.com

Intuit's Password Recovery Service

Key Issues:

- You Can Enter Any Email Address for the Emailed Token.
 - Solution: Use a Fake Phone Number as a Secondary Password
- You Can Reset the Admin Password for Any QuickBooks File – Even if the File is Not Tied to the Company's License Number
 - Solution: Leverage the Web

Scaling New Heights 2010
www.ScalingNewHeights.com

Third Party Admin Reset Utilities

- One Example – Passwre at www.lostpassword.com
- Solution: Leverage the Web

Note: Third Party Utilities Can Cause File Damage. If you need to reset admin passwords for legitimate reasons it is best to use the downloadable Intuit utility.

Scaling New Heights 2010
www.ScalingNewHeights.com

Increasing Security through Business Processes & Internal Controls

- Segregate Duties – For Example
 - AP Payments and Check Printing
 - AR Receipts and Creating Deposits
 - Receipts/Disbursements and Bank Reconciliation
 - Invoicing and Customer Receipts/Credits
 - Inventory Receipts/Shipments and Physical Inventory Counts
 - Approval/Management of Employee Time and Creation of Employee Paychecks
- De-Face Documents (e.g. Bills) to Avoid Double-Processing
- Maintain/Monitor Employee Morale
- Review the Voided/Deleted Transaction Detail Report at Least Weekly
- Track Petty Cash as a Fixed Balance – Reconcile When Replenished and Spot Check the Available Cash Against Receipts Regularly

Scaling New Heights 2010
www.ScalingNewHeights.com

Increasing Security through Business Processes & Internal Controls

- Reconcile All Sensitive Balance Sheet Accounts – Including Non-Bank Accounts
- Review AR/AP Reports for Negative Balances and Confirm Accuracy
- Do Not Track Pre-Payments from Customers as Negative Receivables
- Do Not Track Pre-Payments from Vendors as Negative Payables
- Watch for Skewed Costs on Inventory Products → User-Inflated Pricing → Kickbacks from Vendors
- Run Reports to Track “Buried” Postings
 - Find for Posts to Income that are not Invoices, Sales Receipts or Credit Memos
 - Find for posts to Expenses that are not Bills/Credits, Checks, Credit Card Charges/Credits
 - Double-Click Total Income and then Total by Customer. Look for “No-Customer” Activity
 - Double-click Total COGS (Inventory-Related) and Total by Customer. Look for “No-Customer” Activity
 - Double-click Total Expense and Total Costs (Non-Inventory) and Total by Vendor. Look for “No-Vendor” Activity

Scaling New Heights 2010
www.ScalingNewHeights.com

Increasing Security through Business Processes & Internal Controls

- Create a Paper-Trail around Employee Reimbursements
- Use Corporate Credit Cards for Employee Expenses Whenever Feasible
- Create a Per-Diem for Traveling Employees Whenever Feasible
- Establish Physical Controls for Inventory
- Install Traceable GPS Devices in Company Vehicles
- Use GPS Tracking for Field Service Reps (e.g. on Phones)
- Safeguard and Limit Access to Keys – Especially Keys that Access Sensitive Areas
- Pay Employees Using Direct Deposit Whenever Feasible
- Perform Criminal Background Checks before Hiring Employees
- Process I-9 Forms Quickly (e.g. within a week of any hire)
- Check for Date Sensitive Terms Consistently Not Applied → Vendor Kickbacks

Scaling New Heights 2010
www.ScalingNewHeights.com

Cloud Security vs. Local Security – An Overview

Eric Pulaski – President, Smart Vault

Scaling New Heights 2010
www.ScalingNewHeights.com

Securing Data Inside Your Office

- What steps should you be taking to make sure your data is safe and secure inside your office?
 - 3A's: Authentication, Authorization and Audit
 - External (Internet) Security
 - Patch Management
 - Physical Security (who has access to your servers?)
 - Disaster Protection and Planning (backup and restore)
 - Safely sharing your data with external users
- You typically need a pretty savvy IT department, with security expertise, to manage all of the above on an ongoing basis.

Scaling New Heights 2010
www.ScalingNewHeights.com

Securing Data Inside Your Office

- **User login credentials (authentication)**
 - What kind of password complexity rules do you enforce?
 - What kind of training do you provide to users re: passwords?
- **Internal data security (authorization)**
 - Who has right rights and permissions to data?
 - Do you check to make sure roles are being allocated properly?
- **Monitoring access to data (audit)**
 - Turn on audit trails (access to data, invalid login attempts, etc.)
 - Periodically review audit reports
 - Prune audit files (they can get very big, depending on what you are auditing)

Scaling New Heights 2010
www.ScalingNewHeights.com

Securing Data Inside Your Office

External data security (Internet security)

- Firewalls, routers, and Internet scanners
- Vulnerability assessments and Intrusion detection/prevention
- These require a high level of expertise – beyond typical “IT”. Do you in-source or out-source the above functions?

Patch Management

- All servers should be maintained at recent patch levels
- This includes your internet security components, such as routers, firewalls... and internet scanners and intrusion detection systems.

Scaling New Heights 2010
www.ScalingNewHeights.com

Securing Data Inside Your Office

Physical Security

- Are your servers behind lock and key? Who has the keys?
- Does cleaning staff have access? Are cables secure?
- What would happen in case of power loss? Or Fire? Or flood?
- Do you have backup Internet access? (reliability issue)

Disaster Protection and Planning

- Do you backup your data?
- Do you store backups offsite?
- Do you periodically perform “test restores”?
- What do you do in case of a security breach?
- What is your customer notification policy?

Scaling New Heights 2010
www.ScalingNewHeights.com

Securing Data Inside Your Office

- **Safely sharing data with outside users**
 - Internet email is very unsafe – content travels around the internet in “clear text”, and may reside in multiple “temporary” holding servers (who knows where).
 - MS Office and QuickBooks password protection can be cracked.
 - PKZip-type encryption is much safer.
 - Access to internal servers should be secured by a VPN, with a hardware device required (this is best) for remote access.
 - Terminal servers and remote access to machines without VPN software may not be as safe, and also requires setup and maintenance (patch management & vulnerability scanning).
 - You can forgo a VPN for access to web servers by setting up a “DMZ” (complicated firewall setup) and using properly configured web servers that do not have access to your internal servers behind the DMZ. [this can be complicated to setup and manage.]

Scaling New Heights 2010
www.ScalingNewHeights.com

Securing Data in "The Cloud"

You (or your users) still have to manage (3 A's)

- User login credentials (some may warn of weak passwords)
- "Internal" data security (you still have to set access policies)
- Reviewing audit logs (you still probably want to review these)

Cloud platform, ASP or SaaS application vendors, manage

- External (Internet) Security
- Patch Management
- Physical Security (SAS 70 facilities are very safe and reliable)
- Disaster Protection and Planning (backup and restore)
- Safely sharing your data with external users

Scaling New Heights 2010
www.ScalingNewHeights.com

Benefits of Hosting and SaaS Model

- **Definitions**
 - Hosting: Desktop software provided by a "hosting" provider (ASP)
 - SaaS: Software-as-a-Service designed to work over the web
 - Offers automated provisioning; other advantages may vary
- **Benefits from a security point of view**
 - You probably get better security from your hosting/SaaS vendor
 - Do you have full time IT and security staff?
 - Security is probably managed by professionals 24x7
 - Reduced costs: Costs of managing security is spread across thousands of customers

Scaling New Heights 2010
www.ScalingNewHeights.com

Leverage the Web and Remote Systems to Increase Security

Option 1: QuickBooks Portal Services (e.g. Method)


- Create Access Privileges at the Transaction and Even Field Level (All QB Editions)
- Prevent Access to the .QBW File for Selected QB Users
- Prevent the Ability for Selected QB Users to Create Copies of the QuickBooks File
- Password Protect Specific Screens
- Filter Drop-Down Menus
- Create Approval Processes for Transactions Prior to QuickBooks Import/Sync
- Track Changes to List Information in the Method Audit Trail
- Track Login Times by User Name and Computer IP Address

Scaling New Heights 2010
www.ScalingNewHeights.com

Leverage the Web and Remote Systems to Increase Security

Option 2: Hosted QuickBooks Services (e.g. Right Networks)

- Avoid "Power User" Level Access to the Server on Which QuickBooks Operates
- Limit Access to the Folder in which the .QBW File is Stored
- Limit the Running of Executables to an "Approved" List
- Limit Access to Third Party Websites
- Require Strong Passwords and Require Users to Change Password Regularly

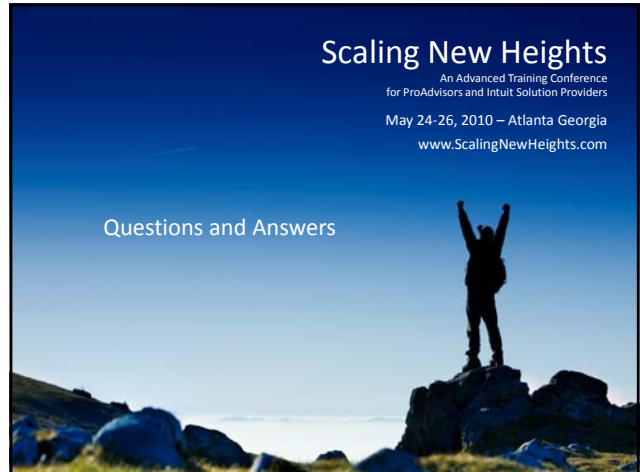


Scaling New Heights 2010
www.ScalingNewHeights.com

January "Taste of the Conference" Webinar

"Professional Billing – QB Tips, Tricks and Workarounds"

- Tracking Client Retainers
- Making Timesheets Posting without Creating Paychecks → True Project-Level Profitability
- Setting Billing Rates by Timekeeper, Service and Client – What QB Will and Will not Do
- Tracking Employee Receivables (e.g. Expense Reports)
- Write-Downs and Write-Off's – Best QuickBooks Practices
- Adding an Auto-Populating "Professional" Column to Invoices
- Determining Which QuickBooks Integrated Professional Billing Solution Is Best for Your Client



Scaling New Heights

An Advanced Training Conference
for ProAdvisors and Intuit Solution Providers

May 24-26, 2010 – Atlanta Georgia
www.ScalingNewHeights.com

Questions and Answers