2003 Technology Update

Virginia Accounting & Auditing Conference
Roanoke, Virginia

September 29, 2003

2003 Technology Update

Edward K. Zollars, CPA
Henricks, Martin, Thomas & Zollars, Ltd.
Phoenix, Arizona

Why We Use Technology

- Not he who has the most toys wins...
- Rather technology is a tool to help us achieve other goals

Why We Use Technology

- Develop a decision making process for your technology budget
  - Prioritize your goals
  - Look at costs and benefits
  - Consider whether you are making the best use of your technology resources

Today's Topics

- Technology Trends and Developments
- Electronic Tax Return Filing
- Security Issues
- Wireless Networking
- Technology and Professional Standards

Technology Trends & Developments

- Growth of Laptops
- Flat Panel Monitors
- On the Road Connectivity

Growth of Laptops

- Sales surpassed desktop sales
- Should they be your standard?
- What to look for in a laptop—the trade-offs

Laptops – The Advantages

- Portable—your office can follow you anywhere
- USB and Firewire have reduced expansion problems
- Space saving designs—you can take back your desk
- Wireless networks built for laptops

Laptops—The Challenges

- Theft and Physical Security
  - Your client's data can literally walk off
  - Built to be easy to disconnect and move—so convenient to steal
  - Consider encrypting disks and using ROM based boot-up passwords
  - Educate users on the risks of losing a laptop

Laptops—The Challenges

- Remote Access and Security
  - Laptops are being connected to any and all networks
  - Need to have software firewall installed—as there may not be a hardware one in the network
  - Risk of "importing" worms/viruses into trusted network zone

Laptops—The Challenges

- Expandability
  - USB and Firewire don't solve all problems
  - Generally more expensive to expand
    - Memory
    - Hard drives
  - Additionally, options tend to be more limited
  - Proprietary nature of design may cause problems with upgrading or changing operating systems

Flat Panel LCD Monitors

- Conserves space on the desk
  - CRTs are big boxes
  - Flat panels don't have the wasted space "in back"
- Dropping in price (pushing down CRTs as well)
- Quality of display

On the Road Connectivity

- Growth of broadband on the road
- Access to information “back home”
- Portability of information

On the Road Connectivity

- The Issue of Email
  - Spam controls tend to block access to ports needed for SMTP servers
  - May find issues with configuration on the road, especially if using dial up
  - May find users will have easiest time using web based mail access systems

Electronic Filing

- Reasons pro and con
- Federal proposed incentives
- State issues

Extended Filing Due Date

- Proposed by President Bush
- Would allow efiled returns to be timely filed if filed by April 30

Extended Filing Date

- Bill introduced in the Congress
- So far, though, it's not become part of a bill that will become law—same fate as in 2002
- Note that it may still become law this year, though the likelihood appears small right now

Extended Due Date Issues

- If don't efile by April 30, cannot extend at April 30
- How to deal with returns that are found to be ineligible after April 15
- Practical issue—would need to file extensions at April 15 anyway
- What would the states do?
- Stay tuned

State Mandatory Efile

- States are looking for any money savings
- California has decided to mandate efiling
- Other states will watch and may follow suit

California Mandatory Efile

- If an income tax return preparer prepared more than 100 timely original individual income tax returns that were filed during any calendar year that began on and after January 1, 2003, and if in the current calendar year that income tax preparer prepares one or more acceptable individual income tax returns using tax preparation software, then, for that calendar year and for each subsequent calendar year thereafter, all acceptable individual income tax returns prepared by that income tax preparer shall be filed using electronic technology, as defined in Section 18621.5.

Efile Issues

- Qualifying and staying qualified
- State registration/notification issues
- Office processes
- Exposure on taking over filing matters
- The headaches of rejected returns

Registering for Electronic Filing

- Need to file Form 8633
- If want to qualify for next year, need to apply as soon as possible
- Also need to be sure to understand what you will need to do with your tax software to efile
- State of Virginia will accept you if IRS accepts you

Remaining Qualified

- Must meet all criteria and standards outlined
  - Revenue Ruling 2000-31
  - Publication 1345
- Note that violation can lead to immediate suspension
- While administrative appeal exists, are out until let back in

State Efile

- Certain states require additional steps
- See manual
- Have reproduced some forms in the appendix to apply for right to file in state
- Again, may have to jump through additional hoops with software provider

Benefits to Electronic Filing

- Electronic filing does provide increased certainty the return was received
- Some errors that would generate notices are corrected early
- Client with refund due will get it faster
- No waiting in line for certified mailing to prove filing

Issues with Electronic Filing

- Still not all forms
- SSN issues—dependents and taxpayers
- Preparer takes on added responsibilities
- Preparer can be suspended first, and only then have due process hearing
- IRS data mining opportunities improved
- Client comfort level

Security of Information Systems

- Always tops CPAs' lists
- Attest issue—is the client secure?
- Tax issue—is client data secure?
- Industry issue—is our data secure?

Security of Information Systems

- Forces driving security
  - Regulatory matters
    - Graham, Leach, Bliley
    - HIPAA
    - State laws (California)
  - Increased "connectedness" of computer systems
    - Stand alone system history
    - Legacy matters compromise security

Behaviorial Aspects of Security Systems

- Security systems generally
  - Make a process less efficient than it would otherwise be
  - Create incompatibilities that otherwise wouldn't exist
  - Often times are heavily guarded in the easy to guard places and completely open elsewhere
  - Has many similarities to issues that challenge internal control systems

Behaviorial Aspects of Security Systems

- Must understand these issues or your security system will fail
  - Often we design systems to be technically wonderful
  - However don't communicate reasons for actions
  - Don't anticipate how system will be evaded
  - Don't monitor or enforce compliance
- Why will it fail????....

Ever Seen a Password on One of These on a Monitor?

Security is a Balancing Act

- Systems always balance competing threats
- Threats include both
  - Technical threats
  - Compliance threats
- The threats are constantly changing
- Response must include multiple defenses and be constantly evaluated

Legal issues as well

- Graham, Leach, Bliley law and FTC regulations under it impose an obligation to protect privacy—and to protect such private data in your systems

15 USC §6801(a)

- It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.
- States a broad policy goal

15 USC §6801(b)

- The Goals of your System
  - Insure the security and confidentiality of customer records and information
  - Protect against any anticipated threats or hazards to the security or integrity of such records
  - Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

FTC Regulations

- 16 CFR Part 314 issued May 23, 2002
- Effective dates
  - Generally May 23, 2003
  - Pre-existing third service contracts must be in compliance by May 23, 2004
- In general, you need to be in compliance now and get responsible service providers with grandfathered contracts in line very soon

Standards for Safeguarding Information

- Found at §314.3 of the regulations
- Must develop, implement and maintain a comprehensive information security program
- It must be written
- Contain appropriate administrative, technical and physical safeguards, including elements found in §314.4

Standards for Safeguarding Information

- Found at §314.3 of the regulations
- Must develop, implement and maintain a comprehensive information security program
- It must be written
- Contain appropriate administrative, technical and physical safeguards, including elements found in §314.4

Standards for Safeguarding Information

- Reasonably designed to
  - Insure security and confidentiality of customer information
  - Protect against anticipated threats or hazards to the *security* or *integrity* of such information
  - Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer

Required Elements

- Must do the following (§314.4)
  - Designate an employee or employees to coordinate your information security program
  - Identify reasonably foreseeable internal and external risks to security, confidentiality and integrity of customer information
  - Design, monitor and test your safeguards
  - Require service providers to implement and maintain similar safeguards

Required Element of Risk Assessment

- At a minimum, your risk assessment must consider risks in each of the following areas:
  - Employee training and management
  - Information systems
  - Detecting, preventing and responding to attacks, intrusions or other system failures

Consequences of Noncompliance

- Little direct issue but...
- If there is a problem and you were not in compliance with GLB expect major problems defending against claims
- As well, the basic outline does “make sense” in setting a basic outline of looking at your security system overall

Who is the Threat?

- Major classes
  - Outsider looking for “easy pickings”
  - Outsider specifically interested in your organization or data
  - Organization insider
- More dangerous as you move down list
  - Increasing ability/motivation to get in
  - Increasing ability to “do damage”

“Easy Pickings” Outsider

- Wants to get into a system and will take the first available
- Possible Goals
  - Coordinated denial of service attack against another site
  - The “thrill” of getting in somewhere (script kiddies)
  - Spammer looking for open relay to send mail

Responses

- Practice basic safe computing
  - Close (or better yet, stealth) all ports that don't need to be open (Firewalls)
    - Hardware firewalls
    - Software firewalls for laptops
  - Anti-virus software
    - Install and activate
    - Keep it updated

Responses

- Update your software
  - Automated Windows Update
  - Check other software sites
- Consider advantage of using "nonstandard" software where appropriate
  - *Mozilla* for mail and browser
  - *OpenOffice.org*

Responses

- Do not install services that are not needed on a computer or network
- Train users about electronic mail
  - Do not open attachments unless expected
  - Do not send file formats that can be infected —use PDF where appropriate
- Disable default accounts in software and systems

Resources

- Steve Gibson's Shields Up! Site
  - http://www.grc.com
- SANS Institute Top 10 Windows and Linux vulnerabilities
  - http://www.sans.org/top20
- Windows Update
  - http://windowsupdate.microsoft.com

New Hardware/Software

- Assume all new hardware or software introduced in your system is intentionally configured by default as insecurely as possible
- You won't be wrong often...
- Vendors are looking to reduce or eliminate support costs

Interested Outsider

- Possible motivations
  - Identity theft through access to client/customer information
  - Industrial espionage
  - Simple theft using the computer system to get the company to do it for him/her
  - Revenge (ex-employee)
- Generally expects a higher benefit, therefore willing to incur higher costs

Responses

- Start with basics put in place for the random outsider—this guy will use an open door
- Disable accounts of former employees immediately
- Check access security policy
- Review logs (tedious, but the best way to find these guys)

Access Security Policy

- Passwords
  - Technical issues
  - Behavioral issues
- Access to Data
  - Does every account need access to every piece of data?
- Physical Security

Passwords—Technical Issues

- Easy to guess passwords are a real problem—and most users will default to them
- Words and dictionary attacks
- Best case—totally random long string of characters, changed very frequently
- Greater computing power has made "brute force" compromise more feasible

Passwords—Behavioral Issues

- A pure technical solution will fail
- Don't need brute force if you simply get the password
- Come up with reasonable compromises
  - Constructing a password
  - Changing passwords
- Educate users about tricks likely to be used to get password disclosed

The Insider

- Large source of major frauds
- Generally already has been granted access—so the major problem is already solved
- Motivations may be similar to outsider, though revenge is a more likely motivator

Responses

- More detailed access control
  - Consider time of access
  - Consider disabling for any period when account shouldn't be used
- Log issues again
  - When is this person on?
  - Activity when others not around?

Wireless Networking

- Growing Dramatically
- Very popular for home networks
- Speed is increasing
- Price is dropping
- Converging with laptop trend
  - Employee home network security issues
  - Possible “taint” of that network to yours

Wireless Networking Standards

- 802.11a
  - Less popular
  - Less area of coverage
- 802.11b
  - Most popular currently
  - Relatively low speed—good for web browsing, not so good for data intensive tasks
  - 2.4 Ghz band and interference

Wireless Networking Standards

- 802.11g
  - Most recent standard, though equipment based on proposed standard has been shipping for quite a while
  - Speed of 802.11a, but compatible with 802.11b
  - Still have 2.4 Ghz interference issues
  - Price is falling and will likely replace 802.11b

Wireless Advantages

- No wires need to be run, so adding a new node on the network is simplified
- Similarly, a home network that is entirely wireless becomes much easier to put together
- No need to hook and unhook portable computers from cables to the network

Wireless Issues

- Speed is slower than a wired network, and even slower if encryption turned on
- Security is a major problem
  - Defaults for most system give no security whatsoever
  - Even when “secured” most home systems can be breeched by someone with a moderate interest in doing so and some technical skill

Wireless Security

- Broadcast signals don't stop at the boundaries of your home or office
- Many security options grant greater access to machines that are part of the local network vs. those coming in from the Internet
- Essentially it's like having a network outlet sitting open on the street

Wireless Security Options

- SSID Broadcast
- MAC Address Filtering
- IP Address Control for Routers
- WEP Encryption

SSID Broadcast

- Wireless access point has an SSID that identifies it to clients trying to log in
- Most systems come with a “standard” SSID that identifies the maker
- By default, most access points broadcast that SSID “in the clear” so that any wireless equipped machine passing by will be told of the network's existence

SSID Broadcast

- Change away from default name
  - No reason to let everyone know the type of system you are using
  - As well, makes next option more useful
- Stop broadcast of SSID—will hide you from casual scanners
- Is not a perfect solution, as passive scanners will still find network

MAC Address Filtering

- Network cards and devices have unique MAC addresses to identify them
- Can limit most access points to only grant access to MAC addresses they know about
- Will only stop casual hackers—the MAC address can be easily "spoofed"
  - Many wireless routers offer the ability to "spoof" the address of device hooked to

IP Address Controls for Routers

- May wish to consider the advisability of using DHCP on wireless networks vs. using only static IP addresses
- If use DHCP, consider restricting the number of addresses automatically assigned to the maximum number of legitimate devices (many system default to over 100 possible devices)

WEP Encryption

- Encrypts transmissions between device and access point
- Each side must have the same "key" used to encrypt and decrypt the transmission
- Can be up to a 128 bit key
- For most "simple" systems is the most effective security option available

WEP Problems

- Slows down transmissions
- Worse, the key can normally eventually be derived if a hacker captures enough data
- For that reason, to be secure you need to change the WEP key regularly
- However, that generally means manually rekeying it into each device

Wireless Security

- Steps illustrated primarily remove you as a target of opportunity
- This may be good enough in many cases
- The majority of wireless sites have no security running whatsoever
- World Wide Wardriving Results from July

Sad State of Security

Category	*Total*	*Percent*	*Percent Change*
Total AP Found	88,122	100.00	71.68
WEP Enabled	28,427	32.26	4.34
No WEP Enabled	59,695	67.74	-4.34
Default SSID	24,525	27.83	-7.44
Default SSID and No WEP	21,822	24.76	-6.68

Source—World Wide Wardriving 2003
http://worldwidewardrive.org/stats.html

Security of Wireless

- Consider that there may be unauthorized access points in your network—scan for them
- Consider doing the same for clients where you are evaluating their controls —such as when performing an audit
- As well, consider risk from employee home wireless networks

Professional Standards

- New Revision to Ethics Interpretation 101-3
- Review of prior issues in this area

Ethics Interpretation 101-3

- Changes effective as of December 31, 2003 (though some engagements grandfathered until December 31, 2004)
- Revisits issues from last revision to Ethics Interpretation 101-3
- Adds new issues that will impact technology

Journal Entries Exception

- Propose standard, adjusting, or correcting journal entries or other changes affecting the financial statements to the client *provided the client reviews the entries and the member is satisfied that management understands the nature of the proposed entries and the impact the entries have on the financial statements*.

Other Technology Driven Issues

- SSARS and the trigger—apparently solved by modifications made in SSARS 8
- SAS changes
  - Responsibilities on understanding the information system
  - Issues related to changes in SAS 99 and fraud, coupled with required understanding of the information system

Interesting Websites

- FASB Statements
  - http://www.fasb.org/st/
  - Full text versions
  - Revisions are not incorporated into the text
  - Must check status of pronouncement
  - As well need to read main page (current notice about SFAS 149 and 150 status information not yet in other pronouncement links)

Interesting Websites

- Tax Sites
  - http://www.taxsites.com
  - Links to various tax related sites
  - Good point to get to state information
    - Full text of most state tax codes
    - Links to most state tax forms
  - Also organizes IRS site

Interesting Websites

- IRS Public Directory
  - http://www.irs.gov/pub/
  - Almost indecipherable—but worth a lot if you do decipher it
  - Full text of recent revenue rulings, revenue procedures, private letter rulings, etc.
  - Is essentially an old DOS directory listing of PDF files—have to decipher it

Interesting Websites

- IRS Public Directory
  - http://www.irs.gov/pub/
  - Almost indecipherable—but worth a lot if you do decipher it
  - Full text of recent revenue rulings, revenue procedures, private letter rulings, etc.
  - Is essentially an old DOS directory listing of PDF files—have to decipher it

2003 Technology Update

Any questions?