

TBC Church Administration Conference
April 27-28, 2009
Hermitage Hills Baptist

“Personal Security / Database Integrity”

Ron M. Chandler

ChurchAdminPro.com

Director, Shelby Systems

- I. Introduction
 - a. www.shelbyinc.com
 - b. www.churchadminpro.com

- II. You are not as safe as you think
 - a. Where do you keep information about
 - i. Your church membership
 - ii. Your donors
 - b. Do you?
 - i. Use laptops?
 - 1. With ChMS databases downloaded?
 - 2. Excel files of membership data
 - ii. Do any of your pastors have Cell PDA's
 - iii. Is your desktop vulnerable to hacking
 - 1. Church lists
 - 2. Access to your ChMS
 - iv. Do you use your accounting software:
 - 1. To do ACH transactions?
 - 2. Scan checks for contributions entry?
 - 3. Retain images of scanned documents?
 - v. Do you have a bookstore, café, or do in-house transactions as commerce?
 - 1. Accept credit / debit card transactions onsite?
 - 2. How is credit card information stored in the system?
 - vi. Issue church-owned credit cards to your staff?
 - vii. Conduct online banking transactions for the church in the accounting office?
 - 1. Browser security
 - 2. Password storage

- III. Keeping your church membership donor and personal information secure is
 - a. A matter of integrity
 - b. A legal matter

- IV. Common gateways for hacking personal information
 - a. Email
 - i. HTML formatting issues
 - 1. HTML heavy emails can contain malicious program code that can infect your computer

2. Simplest way to eliminate vulnerability is to eliminate HTML by:
 - a. Turning off HTML preview or formatting
 - b. Turn off HTML formatting completely
 - c. Regularly upgrade to your email provider's latest updates
- ii. Email attachments
- iii. Web based email
 1. Login pages are sometimes not encrypted
 2. Look for the "lock" symbol in your browser
- iv. Spam
- v. Phishing

b. Other areas of vulnerability

- i. Web surfing
 1. Malicious code web pages
- ii. Pharming
 1. Similar to Phishing...sends the user to a non-legitimate website to collect personal information that looks legit
 2. Check the certificates by double clicking on the lock at the bottom of the browser
- iii. Chat rooms and other "public" areas

V. Lines of defense

- a. Firewalls – first line of defense against unwanted attacks on your system
 - i. Software
 - ii. Hardware
 - iii. Legislation
- b. Antivirus Software
- c. Laws and Liability
 - i. States have laws that allow individuals whose personal data has been compromised to file a civil suit to recover damages resulting from that compromise.
 - ii. Tennessee
 1. <http://www.creditreport.com/identitytheft/statistics/Tennessee-identity-theft.asp>
 2. <http://www.idtheftcenter.org/map.html>

Tennessee Identity Theft Deterrence Act of 1999, T.C.A. § 47-18-2101 et seq., while not expressly imposing liability on businesses or banks for solely failing to prevent identity theft, also does not expressly immunize businesses or banks from civil suits under the Tennessee Consumer Protection Act of 1977 (TCPA) for failing to prevent or minimize the harm resulting from identity theft; accordingly,

3.
 - a. Link for above:
 - <http://www.state.tn.us/consumer/documents/CPAandRelatedLaws2007.pdf>

- iii. Federal

1. Gramm-Leach-Bliley Act

- a. Requires companies to protect against unauthorized access and anticipated threats or hazards to security and integrity of personal records. Requires that organizations implement systems that will detect, prevent, and respond to attacks, intrusions, and system failures.

- iv. Church Membership

1. Violation of these laws can spell financial ruin for a church or ministry trying to defend itself against a civil suit.
2. Loss of loyalty and trust of membership / donors

VI. Best Practices for security and to avoid liability

- a. End user security for email

- i. Delete emails from unknown users
- ii. Discontinue previewing email messages in HTML format
- iii. Do not open unknown attachments
- iv. Do not run unfamiliar macros in documents

- b. System security

- i. Prevention

1. Use firewalls
 - a. Software firewalls, especially on laptops
 - b. Hardware firewalls for systems

- ii. Detection

1. Good Antivirus system to:
 - a. Clean, leave alone, quarantine, delete

- iii. Eradication

1. The ability to safely delete any virus or worm from an entire system

- iv. Loss prevention




1. Reinstalling systems if virus / worm cannot be eradicated

c. *“The best approach for companies that are serious about avoiding security breaches is to protect the data itself and to provide protection that stays with the data, wherever it travels. Encryption is the single most effective solution for protecting data and the only security solution that travels with the data on your network, your service provider’s network or any other network in the world.” Jim Doherty, chief marketing officer, CipherOptics*

d. Personal Identity Theft protection systems

i. Free credit reports

ii. [Online Service enrollment:](#)

Services:	Our Ratings:	Bottom Line:
	Rating: ★★★★★ Go to Site Review	Best overall value, especially for families; Exclusive 30 day free trial & 15% off; Call 800-234-6611 to sign up by phone
	Rating: ★★★★★ Go to Site Review	Great value for identity theft protection; 30 days free & 10% off
	Rating: ★★★★★ Go to Site Review	Most complete ID theft detection service; Free Internet Security Suite; 30 Day Free Trial

iii.

iv. Online Backup Service, OBS, Remote Data Backup

1. Examples

a. Carbonite, Mozy, Idrive, HP Upline, Norton

2. Pros

- a. Off-site security for your data, at multiple locations
- b. May not be as expensive as on-site hardware solutions
- c. No user intervention
- d. Secure Sockets Layer (SSL) encryption ensuring off-site security

3. Cons

- a. Trusting your data to a 3rd party
- b. On-site hardware solutions are becoming cheaper, easier to operate, and more portable
- c. Can be very expensive depending on size of data
- d. Online backups cause a drag on your bandwidth and processor time
- e. Most providers do not archive data longer than 30 days – if you deleted something and don’t discover it for 31 days, you are out of luck
- f. Restoring off-site files can take days
- g. Many OBS companies do not guarantee their services or your data

4. Creative solutions

a. Use OBS for major databases and local hardware for total backups

- b. Use a simple offsite storage schedule for backup tapes and Ext HDs
 - c. Use a service like Amazon S3
 - d. With cheaper prices for mega storage, portable backup hardware should continue to be an acceptable off-site solution for most churches for some time to come
- e. Policies and procedures for Information Technology
 - i. Information Security Policies
 - 1. A well written and implemented policy contains sufficient information on what must be done to protect information and people in the organization.
 - 2. They establish computer usage guidelines for staff in the course of their job duties.
 - 3. The objective: improved information availability, integrity and confidentiality, from both inside and outside the organization.
 - 4. One approach:
 - a. Identify all the assets to protect
 - b. Identify all the vulnerabilities and threats, likeliness of the threats happening
 - c. Decide how to protect the assets in a cost effective manner
 - d. Communicate finds and results to the appropriate parties
 - e. Monitor and review the process continuously for improvement
 - ii. (Kee 2009)**SANS - SysAdmin, Audit, Network, Security** (www.SANS.org) examples
 - 1. [Top 25 papers on Information Security](#)
 - 2. [Top 20 Systems Security List](#)
 - 3. [Best Practices for Preventing Top 20 List](#)
 - iii. **Professional Practices in Church Administration**, NACBApress, July 2009
 - 1. Rules for using the internet responsibly.
 - 2. Rules for the proper use and etiquette for email.
 - 3. Rules for personal use and personal data stored on church-owned systems, including email ownership.
 - 4. Software licensing, installation, and support.
 - 5. Hardware standardization, configurations, and support.
 - 6. Prohibitions for downloading and installing software.
 - 7. Prohibitions for personal software on church systems.
 - 8. Statement of church ownership of all system components including software.
 - 9. Rules for use of security passwords and logins.
 - 10. Privacy of information.
 - 11. Rules for file management and file sharing.
 - 12. Rules for purchasing hardware and software.
 - 13. Rules for system use by volunteers and temporary users.
 - 14. Rules for use of copyrighted material, including digital music.
 - 15. Repairs and maintenance.
 - 16. Updates.

17. Rules for power conservation.
18. Rules for personal websites and blogs, including disclaimers that the views you express are yours alone and do not necessarily reflect the views of your church. It is suggested that these rules be provided and reviewed by legal advisors.
19. Rules for private and public wireless access.
20. Structure, procedures, and workflows for the information management system data entry and data management.
21. Using common sense.

VII. Backup and Disaster Recovery

- a. Causes
 - i. System failure
 - ii. Hacking
 - iii. Natural disaster
- b. Options
 - i. Built-in backup and recovery tools in the operating systems
 - ii. Dedicated software from a different vendor
 - iii. Backup service, usually 3rd party and offsite
- c. Facts to consider
 - i. How frequently you have to backup data
 - ii. Best time to backup
 - iii. How much data to backup
 - iv. Off-site storage in event of catastrophe
 - v. How long the backup data to be stored
 - vi. Security of the backup data
 - vii. Good documentation for backup and recovery procedure
 - viii. Test it!

VIII. PCI Compliance – avoiding fraud when accepting online payments

- a. What is “PCI”
 - i. Payment Card Industry Security Standard
 - ii. A set of rigid guidelines meant to protect from security breaches where cardholders would be open to identity theft or payment fraud via stolen credit card and personal data.
 - iii. Result of the collaboration between Visa USA, MasterCard, and other companies to establish universal security requirements within the industry to ensure that service providers and merchants employ the highest standard of information security to protect cardholder data.
 - iv. Regulates the security and business processes of service providers and merchants that store, process, or transmit consumer credit card data, customers making payments through a PCI-compliant establishment can feel safe that their bank card account information will be secure under all circumstances.
- b. Why is PCI compliance important to you and your church?
 - i. Many churches are not conducting transactions for

1. Online donations
 2. Live and online credit / debit registrations for
 - a. Events / ticketing
 - b. Classes
 - c. Conferences
 - d. Retreats
 - e. Camps
 - f. Sports teams and classes
 3. Conducting a business or trade through
 - a. Bookstores
 - b. Café / coffee shops
 - c. Media (CD, cassette, DVD, etc) sales
- ii. Church is responsible
1. To insure that cardholder info is protected according to industry guidelines
 2. [This includes this list of criteria](#)
(Link)

PCI Data Security Standard	
Build and Maintain a Secure Network	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none"> 3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security

c. New Standards

- i. Under the new PCI regulations, all merchants that accept credit cards are required to comply with requirements that call for the following security measures to be in place:
 - 1. Encrypted transmission of cardholder data
 - 2. Periodic network scans
 - 3. Logical and physical access controls activity monitoring and logging
 - ii. Very difficult, if not impossible for a church to meet these standards
 - 1. Takes 2-3 years to implement compliance
 - 2. Costs thousands of dollars
 - d. Options for churches and non-profits
 - i. Choose to use a vendor that offers a PCI-compliant solution – online payment service providers are becoming compliant so that their customers don't have to
 - ii. [List of PCI-compliant service providers is published by VISA USA](#) (pdf)
 - iii. [Cardholder Information Security Program Link](#) (go to)
 - e. When selecting a service provider
 - i. Make sure that you can seamlessly integrate them with your existing Web site
 - 1. Ability to customize payment processing pages to look and feel like your Web site
 - ii. Look for a provider that accepts a variety of payment methods
 - 1. Credit cards
 - 2. Checks / ACH
 - 3. Debit cards
 - 4. Paypal
 - iii. Robust Reporting abilities: verify the reports available to aid in reconciling your payments and bank statements
 - f. Benefits of using a service provider
 - i. Industry compliant security – verify before signing up
 - ii. Merchant account setup
 - iii. Comprehensive and customizable reporting functionality
 - iv. Targeted support for churches and non-profits
 - v. Transfer of identity theft liability to the service provider

IX. Auditing Standards

- a. Statements on Auditing Standards (SASs) 104-108
 - i. Effective for audits of fiscal years ending 12/15/2007 or later
 - ii. Changes the focus of audit somewhat from financial statement balances to an assessment of risk in key business processes and the environment in which we operate.
 - iii. Appropriately named "Risk Assessment Standards", although really not a new emphasis, but a return to an audit basis of determining the areas of greatest risk, whether caused by error or fraud.
 - iv. Specifically relates to the information technology (IT) used in financial accounting and reporting
 - v. Audits must ensure that IT-related risks are appropriately evaluated and considered in the audit
- b. Specifically, SASs 105 & 109

- i. Require your auditor to gain an understanding of your key risks and evaluate your internal controls, including those in IT
 - ii. Audits will require the input of your IT staff or out-sourced IT contractor
 - iii. Will evaluate the effectiveness of your internal controls within your IT and Financial policies and procedures
- c. Auditing standards established by the Committee of Sponsoring Organizations (COSO)
 - i. Standards are categorized for IT as follows
 - 1. “less complex”
 - 2. “more complex”
 - a. Have custom developed software
 - b. Have packaged software that’s been modified or supplemented
 - c. Rely on the internet to transmit transactional data (more than just email and browsing)
 - d. Heavily rely on spreadsheets with complex calculations and macros
- d. Questions auditors will be asking to CBAs, IT Directors, and independent IT contractors:
 - i. *Are there controls over system design and implementation?* The focus will be on the role senior management plays in the process of setting and approving of IT strategies and changes
 - ii. *Are updates tested before installation?* Not many churches have the ability to test updates.
 - iii. *Is system security adequate?*
 - 1. Standards will call for a minimum 8-digit alphanumeric password that is un-guessable.
 - 2. Multiple failed login attempts should automatically lock a user’s account for a period of time.
 - 3. Anti-malware should be in place and current
 - 4. Servers and wiring closets should be locked with a limited number of keys
 - 5. Data should be backed up, regularly, stored off-site, and regularly tested
 - 6. Firewalls should be in place and current and vulnerability assessments should be regularly performed
 - iv. *Are operational errors identified and corrected in a timely manner?* A reference to user help desk activity.
 - v. *Do applications ensure complete transactions?* This includes folder and file naming conventions to ensure that only the latest files are being used.
 - vi. *Additional IT risk management steps*
 - 1. Identify / inventory your hardware
 - a. List of your IT infrastructure including
 - b. Switches
 - c. Routers
 - d. WiFi router security settings
 - e. internet connection providers / IP addresses
 - f. Servers
 - g. Desktop computers
 - h. Notebook computers
 - i. Printers

- e. Virtualization security – role-based access control, virtual server ID management, virtual network security
- f. Secure software development – software companies will be forced to embrace secure software development efforts
- g. Information-centric security – new ways to classify sensitive information, apply security policies, and enforce policies throughout the network
- h. Ubiquitous encryption – cryptographic processors on hard drives will become common
- i. Entitlement management – XACML language (XML Access Control Markup Language)
- j. Business Process Security – basically building and securing private portals for company execs

References and Cited Sources

- AICPA, Inc. "Statements on Auditing Standards (SASs) No. 104-111." <http://pcps.aicpa.org/>. 2007.
http://www.google.com/search?q=Statements+on+Auditing+standards+no.+104-111&sourceid=navclient-ff&ie=UTF-8&rlz=1B3GGGL_enUS302US303 (accessed March 2009).
- Byron Acohido, USA Today. "Website-infecting SQL injection attacks hit 450,000 a day." www.usatoday.com. March 16, 2009. <http://usatoday.printthis.clickability.com/pt/cpt?action=cpt&title=Website-infecting+SQL+injection+attacks+hit+450%2C000+a+day+-+USATODAY.com&expire=&urlID=34770985&fb=Y&url=http%3A%2F%2Fwww.usatoday.com%2Fmoney%2Findustries%2Ftechnology%2F2009-03-16-sql-> (accessed March 17, 2009).
- Diver, Sorcha Canavan. "Information Security Policy - A Development Guide for Large and Small Companies." www.sans.org. 2007.
http://www.sans.org/reading_room/whitepapers/policyissues/information_security_policy_a_development_guide_for_large_and_small_companies_1331 (accessed March 2009).
- Dr. J.D. (Doc) Watson, Christian Computing Magazine. "The Online Backup Service (1): The Pros and Cons (Pages 14-17)." www.ccmag.com. December 2008. http://www.ccmag.com/ccmag_issues/view_issue2.php?recordID=14 (accessed March 2009).
- . "The Online Backup Service (2): The Alternative (Pages 15-21)." www.ccmag.com. January 2009.
http://www.ccmag.com/2009_01/ccmag2009_01.pdf (accessed March 17, 2009).
- Drinnon, David. "Best Practices: Governing Staff Use of Second Baptist Technologies." <http://www.equipthem.net/>. 2009. <http://www.equipthem.net/2008/02/policies-proced.html> (accessed March 23, 2009).
- ECCU. "Is Your Data Secure? (ECCU Whitepapers)." <https://www.eccu.org/resources/whitepapers>. Unknown.
https://www.eccu.org/assets/white_paper_pages/7/pdfs.pdf (accessed March 2009).
- Elky, Steve. "An Introduction to Information System Risk Management." www.sans.org. 2006.
http://www.sans.org/reading_room/whitepapers/auditing/an_introduction_to_information_system_risk_management_1204 (accessed March 2009).
- Ford, Douglas. "8 Simple Rules for Securing Your Internal Network." www.sans.org. 2003.
http://www.sans.org/reading_room/whitepapers/bestprac/8_simple_rules_for_securing_your_internal_network_1254?show=1254.php&cat=bestprac (accessed March 2009).
- Heare, Sean. "Data Center Physical Security Checklist." www.sans.org. 2001.
http://www.sans.org/reading_room/whitepapers/awareness/data_center_physical_security_checklist_416 (accessed March 2009).
- Kee, Chaiw Kok. "Security Policy Roadmap - Process for Creating Security Policies." www.sans.org. 2001.
http://www.sans.org/reading_room/whitepapers/policyissues/security_policy_roadmap_process_for_creating_security_policies_494?show=494.php&cat=policyissues (accessed March 2009).

Lauren Hunter, Church Executive Magazine. "How PCI Compliance Will Protect Your Congregants." *www.churchexecutive.com*. May 2008. <http://www.churchadminpro.com/Articles/PCI%20Compliance%20-%20What%20is%20it%20.pdf> (accessed March 2009).

Manen, Godert Jan Van. "Looking Ahead at Security Trends for 2009 - Lost in the Noise." <http://blogger.xs4all.nl/gjvm>. February 10, 2009. <http://blogger.xs4all.nl/gjvm/archive/2008/12/31/434923.aspx> (accessed March 2009).

Milford, David. "A System Security Policy for You." *www.sans.org*. 2002. http://www.giac.net/certified_professionals/practicals/gsec/734.php (accessed March 2009).

Nick Nicholaou, MBS, Inc (*www.mbsinc.com*). "CPA Audits Now Focusing on IT! (Pages 13-16)." *www.ccmag.com*. October 2008. http://www.ccmag.com/2008_10/ccmag2008_10.pdf (accessed March 17, 2009).

Poffenberger, Karen C. "Computer Security and The Law: What You Can Do To Protect Yourself." *www.sans.org*. 2004. http://www.sans.org/reading_room/whitepapers/bestprac/computer_security_and_the_law_what_you_can_do_to_protect_yourself_1430?show=1430.php&cat=bestprac (accessed March 2009).

Press, The Associated. "Cybercrooks' website spotlights extent of identity theft." *www.usatoday.com*. March 15, 2009. http://www.usatoday.com/money/industries/technology/2009-03-15-identity-theft-is-your-computer-infected_N.htm (accessed March 17, 2009).

Saddington, John. "Bridging the Gap - Supporting Your Leaders Technology." <http://churchcrunch.com>. March 12, 2009. <http://churchcrunch.com/2009/03/12/bridging-the-gap-supporting-your-leaders-technologically/> (accessed March 17, 2009).

Securosis, L.L.C. "The Business Justification for Data Security." *www.sans.org*. January 2009. http://www.sans.org/reading_room/whitepapers/dlp/the_business_justification_for_data_security_33033 (accessed March 2009).

Setty, Harish. "System Administrator - Security Best Practices." *www.sans.org*. 2001. http://www.sans.org/reading_room/whitepapers/bestprac/system_administrator_security_best_practices_657?show=657.php&cat=bestprac (accessed March 2009).

Steve Hewitt, Christian Computing Magazine. "100 Million Credit Card Accounts Stolen (Pages 13-14)." *www.ccmag.com*. January 2009. http://www.ccmag.com/2009_01/ccmag2009_01.pdf (accessed March 17, 2009).

SysAdmin, Audit, Network, Security (SANS). "Top 20 Year 2007 Security Risks." *www.sans.org*. 2009. http://www.sans.org/top20/?utm_source=web-sans&utm_medium=text-ad&utm_content=Free_Resources_Homepage_top20_free_rsrcs_homepage&utm_campaign=Top_20&ref=27974 (accessed March 2009).

—. "Top 25 Papers." *www.sans.org*. 2009. http://www.sans.org/reading_room/top25.php (accessed 2009).

University of Illinois. "Section 19.5 - Information Security Policy - The University of Illinois." *www.obfs.uillinois.edu*. 2004. http://www.obfs.uillinois.edu/manual/central_p/sec19-5.html (accessed March 2009).

—. "Section 19.8 - Software Copyright Compliance." www.obfs.uillinois.edu. 1999.
http://www.obfs.uillinois.edu/manual/central_p/sec19-8.html (accessed March 2009).

NACBA Resources

[The ePolicy Handbook](#)



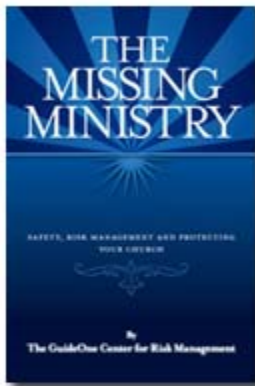
Second Edition

Price: \$ 19.50

by Nancy Flynn

Rules and best practices to safely manage your company's email, blogs, social networking, and other electronic communication tools. *The e-Policy Handbook* gives you everything you need to develop clear, complete e-policies. Packed with electronic rules, step-by-step guidelines, sample policies, and e-disaster stories.

[The Missing Ministry](#)



GuideOne's New "The Missing Ministry" Book Shows You How

Price: \$ 17.00

As a devoted leader or volunteer at your church, the Bible calls upon you to shepherd the flock and keep it from harm. To help you safeguard the people, property and gifts God has entrusted to your church, the GuideOne Center for Risk Management and Group Publishing are proud to present "The Missing Ministry." This informative guide provides you with a step-by-step approach to creating a ministry of safety and security — one that can help prevent child sexual abuse, vehicle accidents, fires and a host of other tragedies. Plus, with a [free resource packet](#), you'll have access to a wide variety of documents to put your plans into action. Make your church safer and more secure with the "Missing Ministry

Biographical

Workshop Leader: Ron Chandler, FCBA

Division Director, Customer Development
Shelby Systems, Inc.



Before joining Shelby Systems in 2007, Ron Chandler served as a church administrator for 30 years. He was the Pastor for Administration at the Germantown Baptist Church in the Memphis, Tennessee metro area, where he served for the last 24 years of his church ministry. He continues to serve as a church administration consultant, conference speaker, and writer. His pre-ministry business background includes accounting and auditing for various companies. Ron is the author of **Thy Kingdom Clean**, a popular NACBA Press resource for over 15 years. In 2002 he founded the popular website, www.churchadminpro.com, a website for church administration resources, used widely by volunteers and professionals. Ron was the 2002 recipient of the NACBA Maurice Saucedo Award, the 2006 recipient of the Southern Baptist Taylor Daniel Award, and a 2008 inductee into the SBCBAA Hall of Honor. He has been a member of the NACBA since 1986, FCBA certified in 1990, has served as the president of the Southern Baptist Church Business Administration Association. Ron is married to Renee and they reside in Germantown, TN. They have two grown daughters and one granddaughter.

Contact:

ron@churchadminpro.com

Ron.Chandler@shelbyinc.com

800.654.1605 x1300

www.churchadminpro.com

