Data Security Compliance: Regulation to Implementation

1:00 – 2:00 p.m.

Dama Brown, Regional Director, Southwest Regional Office, Federal Trade Commission
Matthew Froning, Chief Information Officer, Security Compliance Associates
Christopher Gulotta, Founder and Chief Executive Officer, Real Estate Data Shield, Inc.

FEDERAL TRADE COMMISSION

Dama J. Brown, Director

Southwest Region

What is the Role of Regulation?

The FTC seeks to prevent business practices that are anticompetitive or deceptive or unfair to consumers without unduly burdening legitimate business activity.

Consumer Protection Laws:

-Gramm-Leach-Bliley Act (GLB)
    -The Privacy Rule
    -The Safeguards Rule
    -The Pretexting Rule
-Fair and Accurate Credit Transactions Act (FACTA)
    -The Disposal Rule

Gramm-Leach-Bliley Act (GLB):

Requires “financial institutions” to adopt policies and procedures concerning the collection, disclosure, and protection of consumers’ nonpublic personal information or personally identifiable information.

The Financial Privacy Rule:

Requires financial institutions to provide customers/consumers with a "**clear and conspicuous**" notice that accurately states what personal information is collected, where it is shared, how it is used, and how it is protected; and informs of the right to "opt out" of the sharing of information.

The Safeguards Rule:

Requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information.

A Safeguards Rule Plan must include:

-Denoting at least one employee to manage the safeguards;

-Constructing a thorough risk analysis on each department handling the nonpublic information;

-Developing, monitoring, and testing a program to secure the information; and

-Changing the safeguards as needed with the changes in how information is collected, stored and used.

In addition, an effective Safeguards Rule Plan:

Includes an effective process for managing the risks of third party service providers;

(1) Due diligence to verify that the service provider understands and is capable of complying with applicable laws;

(2) Periodically reviewing the services provider's policies, procedures, training materials and controls to ensure compliance.

The Pretexting Protection Rule:

A well-written plan under GLB's Safeguards Rule should also include a section on training (and testing) employees to recognize and deflect inquiries made under pretext.

The Disposal Rule:

Any business, large or small, that uses consumer reports must dispose of this sensitive information “properly.” The rule also applies to individuals who use consumer reports for business.

Reasonable Measures could include:

-Burning, pulverizing or shredding papers so that the information cannot be read or reconstructed;

-Destroying or erasing electronic files or media so that the information cannot be read or reconstructed;

-Hiring a reputable document destruction contractor to dispose of material consistent with the Rule.

FTC's Guiding Principles for Enforcement:

1. Information security is an ongoing process.

2. A company's security process must be reasonable and appropriate in light of the circumstances.

3. A breach does not necessarily show that a company failed to have reasonable security measures – there is no such thing as perfect security.

4. A company's practices may be unreasonable and subject to FTC enforcement even without a known security breach.

FTC's Enforcement Actions:

-*FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. 2008)

-*In Re Premier Capital Lending, Inc*., No. 072 3004 (FTC 2008)

-*In Re Nationals Title Agency, Inc.*, No. 052 3117 (FTC 2006)

-*In Re Superior Mortgage Corporation*, No. 052 3136 (FTC 2005)

-*In Re Nationwide Mortgage Group, Inc*., No. 9319 (FTC 2005)

-*In Re Sunbelt Lending Services, Inc*., No. 042 3153 (FTC 2005)

FTC's Enforcement Actions:

FTC v. Wyndham Worldwide Corporation, No. 12-01365 (D. Az.)

-Alleges that Wyndham's privacy policy misrepresented the security measures taken to protect consumers' personal information, and that its failure to safeguard personal information caused substantial consumer injury.

-According to the FTC's complaint, the alleged failures included not using complex user IDs and passwords, firewalls and network segmentation between the hotels and the corporate network; and having improper software configurations which resulted in the storage of sensitive payment card information in clear readable text.

Wyndham:

The court concluded that:

(1) the FTC has authority to regulate cybersecurity under Section 5 of the FTC Act to address unfair practices regardless of the existence of any other cybersecurity law or regulation;

(2) the FTC does not need to issue regulations prescribing cybersecurity practices prior to taking action;

(3) sufficient potential injury was demonstrated to initiate such an action, and

(4) that Wyndham statements of its cybersecurity practices prior to the breach were sufficient for the FTC to initiate an action.

BUREAU of CONSUMER PROTECTION
BUSINESS CENTER

Federal Trade Commission
Protecting America's Consumers

Search this Site GO

ADVERTISING & MARKETING | CREDIT & FINANCE | PRIVACY & SECURITY | SELECTED INDUSTRIES | LEGAL RESOURCES | BUSINESS CENTER BLOG

- Multimedia
- En español

- Behavioral Advertising
- Children's Online Privacy
- Credit Reports
- Data Security
- Gramm-Leach-Bliley Act
- Health Privacy
- Red Flags Rule

er Privacy
hange
s a new

2 3 4 5 6

BUSINESS CENTER BLOG

LOANMOD TXT MSGS VIOL8 LAW, SEZ FTC

February 23, 2011

The FTC has gone to court in an effort to shut down an operation that allegedly blasted consumers with more than five million illegal spam text messages, including many pitching loan modification help, debt relief, and other services. The... READ MORE

VIEW BLOG

TOPICS

Jewelry Non-Profits Credit Reports Advertising and Marketing Red Flags Rule Online Advertising and Marketing Credit Health Claims Advertising and Marketing Basics Alcohol Franchises and Business Opportunities Real Estate and Mortgages Selected Industries Gramm-Leach-Bliley Act Clothing and Textiles Telemarketing Children's Online Privacy Tobacco Funerals Behavioral Advertising Finance Human Resources Data Security Health Privacy Privacy and Security Appliances Credit and Finance Automobiles Debt

ADVERTISING & MARKETING

The CAN-SPAM Act: A Compliance Guide for Business

Do you use email in your business? The CAN-SPAM Act establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.

TOPICS: ADVERTISING AND MARKETING, ONLINE ADVERTISING AND MARKETING, PRIVACY AND SECURITY

CREDIT & FINANCE

Complying with the Credit Practices Rule

If your company is a creditor subject to FTC jurisdiction, the Credit Practices Rules applies to you. Read this guide to find out what the Rule requires and what transactions are covered.

TOPICS: CREDIT, AUTOMOBILES, FINANCE, CREDIT AND FINANCE, SELECTED INDUSTRIES

PRIVACY & SECURITY

How to Comply with the Children's Online Privacy Protection Rule

The Children's Online Privacy Protection Act (COPPA) sets out guidelines about the online collection of personal information from children under 13. If you run a website targeting this age group – or know you're collecting information from kids – is your site COPPA compliant?

TOPICS: ADVERTISING AND MARKETING, CHILDREN'S ONLINE PRIVACY, ONLINE ADVERTISING AND

Data Security/Best Practices Awareness and Implementation

Christopher J. Gulotta, Esq.
Founder & CEO
Real Estate Data Shield, Inc.
271 Madison Avenue Suite 700
New York, NY 10016
☎212-951-7302
✉cgulotta@redatashield.com

Terminology & NPPI Defined

- **Non-public Personal Information ("NPPI"):**
  - Personally identifiable data such as information provided by a customer on a form or application, information about a customer's transactions, or any other information about a customer which is otherwise unavailable to the general public.

  - NPPI includes first name or first initial and last name coupled with any of the following:
    - Social Security Number
    - Driver's license number
    - State-issued ID number
    - Credit or debit card number
    - Other financial account numbers

The Assets to be Protected

Common "Settlement" Documents Containing NPPI	Common "Title" Documents Containing NPPI
Uniform Residential Loan Application (Form 1003) (**NPPI includes:** SSN, bank account numbers, loan numbers, work, address, etc.)	Identification (Driver's License, passport, etc.) (**NPPI includes:** address, Birthdate, ID number, Passport number)
Borrower Tax Returns (**NPPI includes:** SSN, financial information, address)	Title Order Form (**NPPI includes:** SSN, address, loan numbers)
Lender Engagement Letter (**NPPI includes:** SSN, address, loan numbers)	Payoff Letter (**NPPI includes:** Bank account numbers, loan number, address)
Identification (Driver's License, passport, etc.) (**NPPI includes:** address, Birthdate, ID number, Passport number)	Escrow Agreements with Tax Searches (**NPPI includes:** SSN, address)
Settlement Statement (HUD-1) (**NPPI includes:** loan number, address)	Real Estate Transfer Tax Forms (**NPPI includes:** SSN, financial information, address)
IRS Form 4506-T, Request for Transcript of Tax Returns (**NPPI includes:** SSN, address)	Affidavits (**NPPI includes:** SSN, address)
IRS Form W-9, Request for Taxpayer Identification Number and Certification (**NPPI includes:** SSN, address)	Recordable Docs (**NPPI includes:** loan numbers, address)
Payoff Letter (**NPPI includes:** Bank account numbers, loan number, address)	Title Bill (**NPPI includes:** address)

Relevant Sources

1. Gramm-Leach Bliley Act (GLBA)
2. Federal Trade Commission (FTC)
   - Privacy Rule (1999)
   - Safeguard Rule (2003)
   - Disposal Rule (2005)
3. Consumer Financial Protection Bureau (CFPB)
   - April 2012 Bulletin
   - Supervisory Highlights (2012)

Relevant Sources (cont'd.)

4. Office of the Comptroller of the Currency (OCC)
   - Interagency Guidelines Establishing Standards for Safeguarding Customer Information (2001)
   - Third-Party Relationship Bulletin (Oct. 2013)
5. American Land Title Association (ALTA)
   - "Best Practices" for Title Insurance and Settlement Companies Version 2.0 (Jan 2013)
6. State Agencies & Regulators (State Attorney General, Department of Insurance, Attorney Professional Codes of Conduct)
7. Lender mandates

Gramm-Leach Bliley Act (GLBA)

- Enacted date: November 12, 1999
- Effective date: November 18, 2000
- Compliance date: July 1, 2001

- Tasks the FTC and other agencies that regulate Financial Institutes to implement regulations to carry out GLB's financial privacy provisions.

- Covers "financial institutions"
  - Real Estate Settlement Service Providers (*e.g.*, Title and Settlement companies) included in definition of "financial institutions" as they are "significantly engaged" in financial activities.

Federal Trade Commission RULES:

- **1999 – FTC Privacy Rule (16 C.F.R. § 313)**

  Financial Institutions are required to provide "**a clear and conspicuous notice**" (*i.e.*, a "Privacy Notice") to customers/consumers that accurately states the company's privacy policies and practices

- **2002 – FTC Safeguards Rule (16 C.F.R. § 314)**

  Financial Institutions are required to develop a **written information security plan** that describes their program to protect customer/consumer information

  Preamble to Rule identifies "**employee training and management**" as one of the three areas essential to ensuring information security within a business

- **2005 – FTC Disposal Rule (16 C.F.R. § 682)**

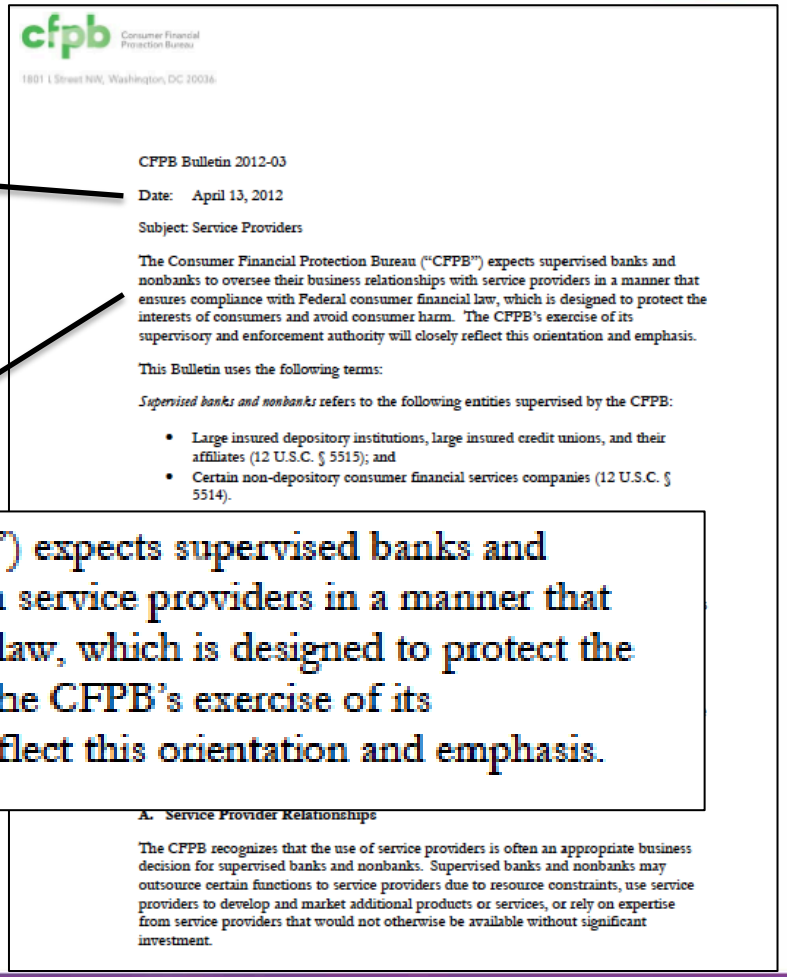
  Financial Institutions are required to properly dispose of all customer/consumer information by taking **"reasonable measures"** to protect against unauthorized access to/use of the information

  – Reasonable measures = burning/pulverizing/shredding papers so that the information cannot be read or reconstructed; destroying or erasing electronic media

CFPB Bulletin 2012-03

Date: April 13, 2012

Subject: Service Providers



cfpb Consumer Financial Protection Bureau

1801 L Street NW, Washington, DC 20036

CFPB Bulletin 2012-03

Date: April 13, 2012

Subject: Service Providers

The Consumer Financial Protection Bureau ("CFPB") expects supervised banks and nonbanks to oversee their business relationships with service providers in a manner that ensures compliance with Federal consumer financial law, which is designed to protect the interests of consumers and avoid consumer harm. The CFPB's exercise of its supervisory and enforcement authority will closely reflect this orientation and emphasis.

This Bulletin uses the following terms:

Supervised banks and nonbanks refers to the following entities supervised by the CFPB:

- Large insured depository institutions, large insured credit unions, and their affiliates (12 U.S.C. § 5515); and
- Certain non-depository consumer financial services companies (12 U.S.C. § 5514).

A. Service Provider Relationships

The CFPB recognizes that the use of service providers is often an appropriate business decision for supervised banks and nonbanks. Supervised banks and nonbanks may outsource certain functions to service providers due to resource constraints, use service providers to develop and market additional products or services, or rely on expertise from service providers that would not otherwise be available without significant investment.

The Consumer Financial Protection Bureau ("CFPB") expects supervised banks and nonbanks to oversee their business relationships with service providers in a manner that ensures compliance with Federal consumer financial law, which is designed to protect the interests of consumers and avoid consumer harm. The CFPB's exercise of its supervisory and enforcement authority will closely reflect this orientation and emphasis.

OCC Bulletin OCC 2013-29

October 30, 2013

“Third Party Relationships” Bulletin

Title Insurance and Settlement Company "Best Practices"

- **Mission Statement**
  - ALTA seeks to guide its membership on best practices **to protect consumers, promote quality service, provide for ongoing employee training, and meet legal and market requirements.**
  - These practices are designed to ensure a positive and compliant real estate settlement experience.
  - ALTA is publishing these best practices as a benchmark for the mortgage lending and real estate settlement industry.

ALTA's Seven "Best Practices" (cont'd.)

1. Establish and maintain current license(s) as required to conduct the business of title insurance and settlement services.
2. Adopt and maintain appropriate written procedures and controls for Escrow Trust Accounts allowing for electronic verification of reconciliation.
3. **Adopt and maintain a written privacy and information security program to protect Non-public Personal Information as required by local, state and federal law.**
4. Adopt standard real estate settlement procedures and policies that ensure compliance with Federal and State Consumer Financial Laws as applicable.

ALTA's Seven "Best Practices" (cont'd.)

5. Adopt and maintain written procedures related to title policy production, delivery, reporting and premium remittance.
6. Maintain appropriate professional liability insurance and fidelity coverage.
7. Adopt and maintain procedures for resolving consumer complaints.

ALTA – Seventeen Assessment Procedures

- ✓ Written Plan
- ✓ Trained Employees
- ✓ Risk Assessment
- ✓ Independent Testing of Key Controls
- ✓ Acceptable Use Acknowledgements
- ✓ Access Controls for NPPI
- ✓ Network Access Controls w/Background Checks
- ✓ Removable Media Controls
- ✓ NPPI encryption in motion and at rest
- ✓ Monitor, detect & respond to attacks
- ✓ Physical controls to protect premises & NPPI
- ✓ Change/Modification & Back-up controls
- ✓ Privacy Disclosures
- ✓ Records Retention & Destruction

Wells Fargo Title and Settlement Newsletter March 6, 2014

- Wells supports customer choice provided such third-party provider "**consistently meets all applicable requirements**"
- Wells is **expanding and enhancing third-party oversight**…in order to monitor and measure performance
- Prepare for "**Top Performer**" status
- Wells "**supports" ALTA Best Practices**, which should already be in place for "businesses providing title and closing services"
- Wells recognizes some may need "**transition time**"
- If not currently following ALTA Best Practices, **do you have a plan in place for adoption**?
- Can you **document and demonstrate** inspection processes to **validate your adoption of ALTA's Best Practices**?

Beginning the Compliance Process

Practical Steps to Take:

- ☑ Develop all required privacy and data security policies, procedures and plans
  - ☑ Information Security Plan
  - ☑ Incident Response Plan
  - ☑ Disaster Recovery Plan
  - ☑ Secure Password Policy
  - ☑ Electronic Communications and Internet Use Policy
- ☑ Assess your company's risk profile
- ☑ Educate and train your work force
- ☑ Secure your work flows
- ☑ Ensure compliance of all service providers
- ☑ Implement a sound document destruction policy

Critical Security Controls

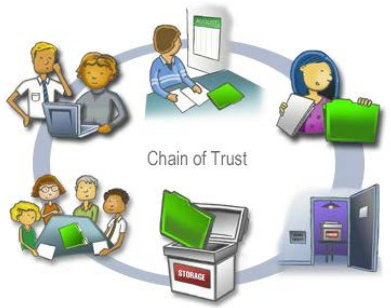
A. Administrative

B. Physical

C. Network

A) Administrative Security Critical Controls

1. Staff Training
2. Manual of Policies and Procedures
3. Privacy Notice
4. Shred-All Policy
5. Vendor Non-Disclosure Agreements (NDA's)
6. Background checks on employees handling NPPI
7. Clean Desk, Office and Screen Policy
8. Authorized Devices



A) Administrative Security Critical Controls

Staff Training

1. Training is an essential element of creating and maintaining a Privacy Smart culture and environment and is essential to regulators.
2. “The most effective data security plans deal with four key elements: physical security, electronic security, employee training, and the security practices of contractors and service providers.” (*Federal Trade Commission, Protecting Personal Information: A Guide for Business*)
3. An effective information security plan requires, “training employees to take basic steps to maintain the security, confidentiality and integrity of customer information,” (April 2006: FTC, *Complying with the Safeguards Rule*).

A) Administrative Security Critical Controls

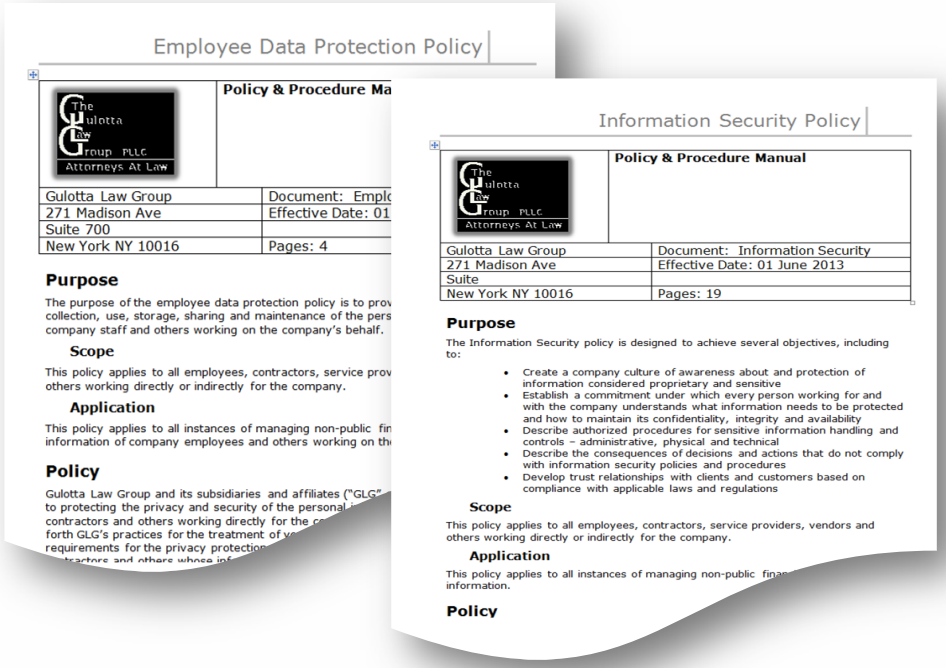
Staff Training (cont'd.)

4. The CFPB "Supervisory Highlights" Bulletin states that companies "must provide for an effective training and compliance management program for all employees and service providers."
5. 39% of all data breaches are caused by employee or contractor negligence (Ponemon Institute, "2011 Cost of Data Breach Study").
6. Beware of Malicious Insiders and former employees.

A) Administrative Security Critical Controls

Manual of Policies and Procedures

1. ALTA, the CFPB and the FTC require clearly defined written policies and procedures to be in place.



Employee Data Protection Policy

Policy & Procedure Ma

Gulotta Law Group	Document: Emplo
271 Madison Ave	Effective Date: 01
Suite 700	
New York NY 10016	Pages: 4

Purpose

The purpose of the employee data protection policy is to prov
collection, use, storage, sharing and maintenance of the pers
company staff and others working on the company's behalf.

Scope

This policy applies to all employees, contractors, service prov
others working directly or indirectly for the company.

Application

This policy applies to all instances of managing non-public fin
information of company employees and others working on th

Policy

Gulotta Law Group and its subsidiaries and affiliates ("GLG"
to protecting the privacy and security of the personal i
contractors and others working directly for the co
forth GLG's practices for the treatment of y
requirements for the privacy protection

Information Security Policy

Policy & Procedure Manual

Gulotta Law Group	Document: Information Security
271 Madison Ave	Effective Date: 01 June 2013
Suite	
New York NY 10016	Pages: 19

Purpose

The Information Security policy is designed to achieve several objectives, including to:

- Create a company culture of awareness about and protection of information considered proprietary and sensitive
- Establish a commitment under which every person working for and with the company understands what information needs to be protected and how to maintain its confidentiality, integrity and availability
- Describe authorized procedures for sensitive information handling and controls – administrative, physical and technical
- Describe the consequences of decisions and actions that do not comply with information security policies and procedures
- Develop trust relationships with clients and customers based on compliance with applicable laws and regulations

Scope

This policy applies to all employees, contractors, service providers, vendors and others working directly or indirectly for the company.

Application

This policy applies to all instances of managing non-public fina
information.

Policy

A) Administrative Security Critical Controls

Privacy Notice

1. FTC Privacy Rule States that financial institutions are required to provide “a clear and conspicuous notice” (*i.e.*, a “Privacy Notice”) to customers and consumers that accurately states the Institution’s privacy policies and practices.
2. Client
    1. Initially and annually
3. Consumer
    1. Initially and at closing

A) Administrative Security Critical Controls

Shred-All Policy

1. Have a Shred-All Policy for your office. This eliminates employee discretion and concern that a document with NPPI could be discarded improperly.
2. These should include, all paper and digital media (USB, disks, hard drives, etc.)

A) Administrative Security Critical Controls

Vendor Non-Disclosure Agreements (NDAs)

1. Just as lenders are responsible for our actions, title and settlement Third-Party Service Providers are also responsible for our sub-vendors.
2. To protect your company, your third-party vendors should be made to sign an NDA to demonstrate that they too comply with State and Federal privacy laws.
3. This can include, for example: IT consultants, search companies, storage facilities, accountant, etc.

A) Administrative Security Critical Controls

Background Checks on Employees Handling NPPI

1. "Checking references or doing background checks before hiring employees who will have access to customer information." (April 2006: FTC, *Complying with the Safeguards Rule*)
2. Be sure to comply with State and Federal Laws relating to how to use and handle any "adverse" information in these searches.

A) Administrative Security Critical Controls

Clean Desk, Screen and Office Policy

1. All employees should keep files off of their desk except for the file they are currently working on so onlookers don't see information they shouldn't.
2. Staff's desk should be cleared of all work and files at days end.
3. When stepping away or even when at their desk, staff shouldn't keep unnecessary sensitive information up on their screen unless they are currently using said information.
4. Common areas that outside closers, etc. use should be "clean" as well.

A) Administrative Security Critical Controls

Authorized Devices

1. You need to keep track of what devices are connected to the office network.
    1. This list needs to be kept up-to-date and old devices should be restricted immediately upon removal.
    2. This includes smart phones, tablets, computers, etc.
2. Companies need to also keep track of unauthorized devices. Letting staff know if they aren't allowed to use personal devices for work.
    1. This also includes that work devices should only be used for official work use.

B) Physical Security Critical Controls

1. Entryway Security & Sign-in Log
2. Clean Desk Policy
3. Clean Office
4. Locked Filing Cabinets
5. Security Cameras
6. Privacy Screens
7. Locked Offices
8. Shredding of Paper and Digital Media
9. Locks on Computers

B) Physical Security Critical Controls

Entryway Security

1. Invest in a good entryway lock system.
    1. **Consider having an FOB access system setup so that staff access can be monitored and regulated.**
2. Invest in a good security system.
3. Have a secondary door that separates your main entry area from the main office.
4. Have sign-in logs for all visitors

B) Physical Security Critical Controls

Clean Desk and Office Policy

1. When stepping away or even when at their desk, staff shouldn't keep sensitive information on their desk or up on their screen unless they are currently using the information.
2. NPPI should not be left lying around the office for any unauthorized person to take or see.
3. At night all desks and office space should be void of files or documents containing NPPI.

B) Physical Security Critical Controls

Locked Filing Cabinets and Offices

1. All files should be secured at the end of the day in locked filing cabinets to prevent access by unauthorized personnel.
2. Senior staff's offices should be individually locked to prevent access by unauthorized personnel.
3. This includes but is not limited to server rooms, executive and manager offices.

B) Physical Security Critical Controls

Security Camera System

1. Having security cameras is useful to see who accessed your office and when. In case of a breach both law enforcement and forensic investigators will need and want to access these records.
    1. Remember if you wish to record during office hours, then staff and visitors need to be notified by way of posted notice. After hours is allowed without notice.
    2. All video recordings should be stored for at least 3-6 months.

B) Physical Security Critical Controls

Privacy Screens

1. Privacy Screens prevent unauthorized people from viewing a monitor unless they are seated at that desk.
2. Especially critical for staff near windows, in common space and for those dealing with banking or other highly sensitive information.

B) Physical Security Critical Controls

Server Room Security

1. Should be locked at all times.
2. Only a few authorized personnel should have access.
3. Server should be on a raised rack not sitting on the floor.
4. The rack itself needs to be securely fastened (*i.e.*, bolted to the floor and/or ceiling)
5. Room should be air conditioned to prevent over heating.
6. Should have a battery backup for all equipment on server rack.

B) Physical Security Critical Controls

Shredding of Paper and Digital Media

1. Have numerous shredding bins stationed around the office so it is easy and convenient for staff to destroy/shred all documents.
2. These bins should be provided by your shredding service and be locked at all times.
3. Collect weekly receipts of each shredding visit.
4. When disposing of digital media (floppy, CD/DVD, Hard Drive, USB sticks, etc…) get receipts confirming destruction.

B) Physical Security Critical Controls

Locks on Computers

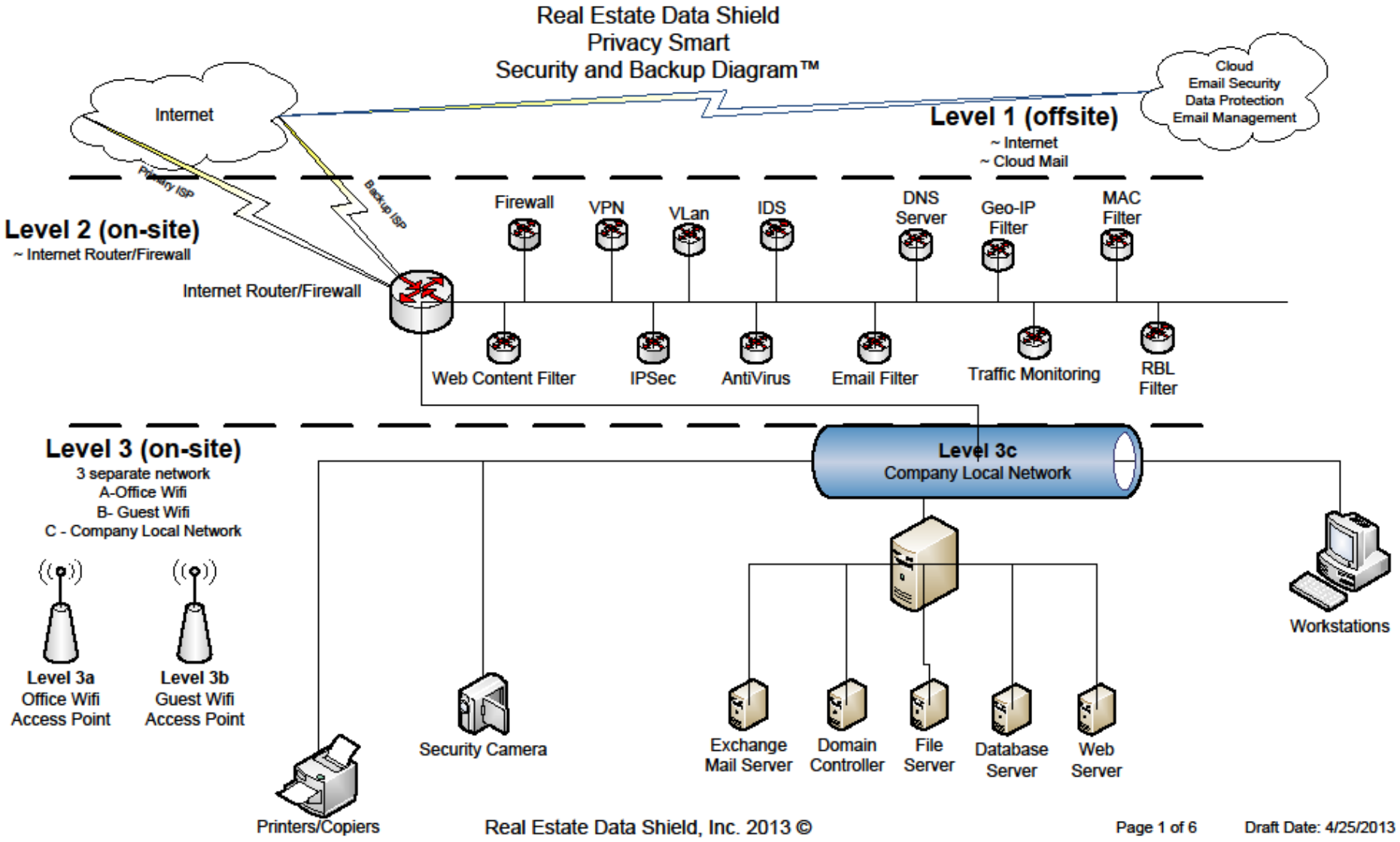
1. Keep computers physically locked in place so a thief cannot easily remove the CPU from the office.

Secure off-site storage, protected from destruction or damage by a secure, certified facility.

C) Network Security Critical Controls

1. Password Protection
2. Computer Screen Timed Lockout
3. Using Various Brands of Firewalls (Defensive Depth)
4. Port Lockdown
5. Network Printers/Scanners
6. Restrictive Access to Programs, files etc.
7. Updates and Patches
8. Email Encryption

C) Network Security Critical Controls



C) Network Security Critical Controls

Password Protection

1. All computers, servers and databases should be password protected.
2. Passwords should be 9 or more characters in length and should include a number, a symbol and an uppercase letter.
3. Passwords should change at a minimum of every 90 days.
4. Default Admin passwords, on any device or system should be changed to something unique.

C) Network Security Critical Controls

Computer Screen Timed Lockout

1. Computers screens should lockout or go to sleep mode after a certain amount of inactivity as to prevent snooping by unauthorized personnel.
2. Once awakened the computers should require a password to prevent access by unauthorized personnel.

C) Network Security Critical Controls

Using Various Brands of Firewalls

1. Multiple firewalls provide multiple levels of security.
2. Having different providers is good because if they are all the same company a hacker can use the same protocols to defeat the same type of security coding. Defense in depth is essential.

C) Network Security Critical Controls

Port Lockdown

1. Direct data port (DVD, USB, etc.) access can bypass your network security and infect individual computers directly. Also, depending on how your network is set up can provide a less secure backdoor into the rest of your network.
2. By locking down and preventing access to USB, CD and other data ports another attack vector is eliminated.
3. Employee negligence can lead to a major breach. By locking down these ports you can reduce their chances of bringing a virus into the system.

C) Network Security Critical Controls

Network Printer/Scanner

1. Copiers/printers have hard drives which should be wiped weekly if not daily to ensure a data thief can not steal more than 1 day's worth of NPPI by removing the hard drive.
2. Admin passwords should be changed from the default passwords.
3. Limit remote access to service vendors.

C) Network Security Critical Controls

Restrictive Access

1. Principle of Least Privilege

   Staff should only have access to files, folders or programs on the network that they require to perform their intended work responsibilities.

2. Maintain and review network access logs for suspicious activity.

C) Network Security Critical Controls

Updates and Patches

1. Most software companies release updates and patches to plug vulnerabilities and glitches that hackers exploit.
2. All programs should be systematically kept up-to-date and be monitored with diligence.
    1. **Anti-virus or anti-malware software is useless if it isn't current.**
    2. **Breaches often result from vulnerabilities to programs that have patches available but are not yet installed. Often breaches occur in the time period between the patch being distributed by the software company and the user actually installing it.**

C) Network Security Critical Controls

Email Encryption

1. Emails containing NPPI in their text or an attachment, should only be sent if the email is encrypted.
2. Make sure everyone is trained on email encryption to understand how to use it and when to use it.
3. Consider implementing a security filter (such as DataMotion's 'Gateway' product) that scans outgoing emails and attachments for potential NPPI and "forces" encryption.

Disclaimer

- This presentation, supporting materials and the information contained therein does not constitute legal advice nor an attorney client relationship and is provided for information purposes only. Because laws, rules and regulations change frequently and because local laws may apply, you should consult an attorney for any specific compliance or related inquiries.

SCA

SECURITY COMPLIANCE ASSOCIATES

Matthew Froning

Chief Information Officer

Assessment Process

- **Phase 1 – Initial Call**
- **Phase 2 – Pre-Assessment Due Diligence**
- **Phase 3 – External Assessment**
- **Phase 4 – Internal Assessment**
- **Phase 5 – Post-Assessment Report**
- **Phase 6 – Remediation**

SCA
SECURITY COMPLIANCE ASSOCIATES

Phase 1 – Initial Call

- Provide the client with expectations on the process
- List of some of the items the engineer will need, such as:
  - Information Security Policy
  - Acceptable Use Policy
  - Business Continuity/Disaster Recovery Plan
- Explain the personnel interview process & who will be interviewed
- Answer any other questions the client may have about the on-site assessment

SCA
SECURITY COMPLIANCE ASSOCIATES

Phase 2 – Pre-Assessment Due Diligence

Prior to the engineer coming on-site, you should:

- Review policies & procedures
  - Up-to-date & Contain necessary information
- Review network topology
  - Security devices configured to be effective
- Antivirus Updates
- Check Web Content Filtering
- Server configurations
  - Ensure Firewalls & IDS/IPS properly configured
- User management
  - Remove old user accounts
  - Rename default administrative account names

SCA
SECURITY COMPLIANCE ASSOCIATES

Phase 3 – External Assessment

- External Vulnerability Assessment/Penetration Testing:
  - Test IDS/IPS vendor response
  - Test target IP addresses for vulnerabilities and create Proof Of Concepts (POC) for vulnerabilities found

- Social Engineering to test employee awareness and IS training effectiveness:
  - Spear Phishing emails
  - Phishing email containing a forged link
  - Pre-text calling – similar to phishing, the intention is to obtain sensitive information via telephone

SCA
SECURITY COMPLIANCE ASSOCIATES

Phase 4 – On-Site Assessment

Once we arrive on-site, we will begin the assessment process by:

- Conducting an external physical assessment of the site
- Internal physical assessment
- Conducting an internal network vulnerability scan
- Conduct interviews with management & IT staff
- Review in-place policies & procedures
- Workstation reviews
- Server configuration reviews

SCA
SECURITY COMPLIANCE ASSOCIATES

Phase 5 – Post Assessment Report

The post audit reports includes, but is not limited to:

- Detailed findings of all parts of the assessment
- List of vulnerabilities discovered and the associated hosts
- Recommendations for:
  - Vulnerability remediation
  - Policy recommendations
  - Acceptable use recommendations
  - Implementation of Business Continuity/Disaster Recovery Plan

SCA
SECURITY COMPLIANCE ASSOCIATES

Phase 5 – Post Assessment Report

ALTA Best Practice Pillar No. 3

Internal Information Security

(Ctrl)

Corresponding Assessment Procedure	60	Criteria	Question Response		Comments
			Yes	No	
3.07e	43	Do wireless controls require user authentication to obtain network access via a wireless device?	X		
3.12a	44	Does the Company test the technology prior to implementing new technology and updates to determine its ability to meet business needs?		X	Patch management, testing & updating are handled by Continuum
3.12a	45	Are system modifications (hardware and software) consistent with the approved security program?	X		
3.12a	46	Are system modifications documented, tested and approved in accordance with previously outlined business strategies and procedures?		X	Patch management, testing & updating are handled by Continuum
3.07d	47	Is access to Personal Information limited to ensure that individuals with a legitimate business purpose obtain only the minimum access necessary to perform specific job functions?	X		
3.07d	48	Are periodic reviews conducted of Personal Information user-access rights, with more frequent reviews occurring for those with privileged access rights?	X		
3.07d	49	Has the Company created procedures to prevent unauthorized access to operating systems, data and services?	X		
3.07c	50	Is "Separation of Duties" enforced in systems containing Personal Information so that users with the ability to add, modify and remove user access are not assigned to perform business transactions within the system?	X		

SCA
SECURITY COMPLIANCE ASSOCIATES

Phase 5 – Post Assessment Report

Change Management – Internal Assessment

Risk Level: Medium

Description: An appropriate change management program should be implemented in order to track and monitor all changes. Effective communication of planned changes and the ability to test and restore changes before deployment to production is very critical to the success of the security program.

Results: CLIENT does not have a formal change management program that addresses software and hardware upgrades/patches, vendor releases, installation of new clients and servers, establishing new networks and subnets, migrating and installing new operating systems, and authorization.

The IT support staff has privileges to make system and software changes. The IT staff handles the installs of all software. However, general users do possess the ability to download and run executable files. No compatibility or security testing is conducted on any new software prior to deployment onto operational system/network.

Recommendation: SCA recommends that CLIENT implement a formal change management program. As part of this program, it is recommended that all new proposed software changes be tested outside of operational environment to ensure the integrity of the operational network and services. Also, SCA recommends that CLIENT restrict the privileges of users so that general users do not have the privileges to download and run executable files on workstations and/or the CLIENT network.

In order to effectively manage the licensing of vendor software, SCA recommends that CLIENT acquire or develop a program that tracks the licensing information of all licensed software used by CLIENT and informs the appropriate personnel when licenses are set to expire and need to be renewed.

Phase 6 – Remediation

- Review findings, then:
  - Determine ability to remediate shortfalls & vulnerabilities
  - Work with IT support on remediation steps for technical vulnerabilities
  - Remediate non-technical shortfalls/vulnerabilities
  - Document remediation steps performed
- Use ISO on-demand availability to answer questions you may have and provide guidance
  - It's a resource for you – Take advantage of it!

SCA
SECURITY COMPLIANCE ASSOCIATES

Common Mistakes / Weaknesses

- Antivirus
  - Disabling antivirus active scan due to speed issues
  - No antivirus on the server because it is not accessed
- No firewall
- Not monitoring firewalls, IPS/IDS, and event logs
- Allowing anyone to access files on file servers (Not using permissions)
- Allowing anyone on the internal network through the wireless access point
- Employees providing username/password
- No backup plan or Disaster Recovery Policy

SCA
SECURITY COMPLIANCE ASSOCIATES

QUESTIONS

Dama Brown, Regional Director, Southwest Regional Office, Federal Trade Commission
Matthew Froning, Chief Information Officer, Security Compliance Associates
Christopher Gulotta, Founder and Chief Executive Officer, Real Estate Data Shield, Inc.