

Legal Corporate
Cyber Security →



Itinerary

Cyber Security
Data Breaches
To Cloud / Not to Cloud
Best Practices

Legal / Statues / Laws
Stored Communications Act
Gramm-Leach-Bailey

Questions?

November 20, 2014

Brad Moody, Shareholder, *Baker Donelson*
Andy Mozingo, CHFI, ACE, *Global CFI, LLC*

Get Out of My Cloud! ... and Other Suggested Responses to Avoid Becoming a Hacking Victim



Cyber Security

- 2012 – 267 Million Records Compromised
- 2013 – 822 Million Records Compromised

Targets

- Electricity
- Oil & Gas
- Information Technology
- Transportation




To Date: 2014

**400 BILLION
Cyber Crimes
Globally**


“A computer lets you make more mistakes faster than any invention in human history - with the possible exceptions of handguns and tequila.”

Mitch Ratcliffe – Technology & Software Design Consultant

Cyber Security



CNIC
Naval Air Station Pensacola



us-cert.gov

**** NEW **** US-CERT (U.S. Computer Emergency Readiness Team)

- > 2nd Facility to be built (1st in Virginia)
- > 150 Cyber-Analyst to be hired
- > Malware facility
 - tracking every node of U.S. Government network



Alerts
Bulletins
Tips



Cloud Hacking

Duration: 1:17

Credit Card Breach

--estimated 6 Millions cards compromised
from The Home Depot Network

Duration: 0:45

*JP Morgan Chase
Apple iPhone Malware
Fire @ O'hare*

Hacking Techniques

#1 – Phishing / Spear Phishing (target executive)

- > Spoofing Email Accounts
(receive email from bmood@bakerdonelson.com)
- > USB Drives (infected with virus)
- > Leaving Laptops in Cars
- > SQL Injections (exploit code)
- > Magnetic Reader (hacked)
- > IT – Punching Holes in Firewall



EMAIL ATTACHMENTS

Greetings Andrew, you are due for a refill, please take the time to visit our fresh, new, redesigned website to refill your order. Thank you for your past order on our network. Please read this email carefully and keep a copy for your records.

Your next refill is as follows:

Date and Time: 2013-11-13 19:31:41

Ship to Address: po box 1482

Patient Status: Subsequent Filling

[Please go to our refill site to fulfill this transaction now.](#)

[Refill Here](#)

Thanks again.
Sincerely,
Customer Care.

You received this email because you are a patient with the refill network.

BAKER DONELSON

Hacking / Security Breaches



T
H
E

R
U
B

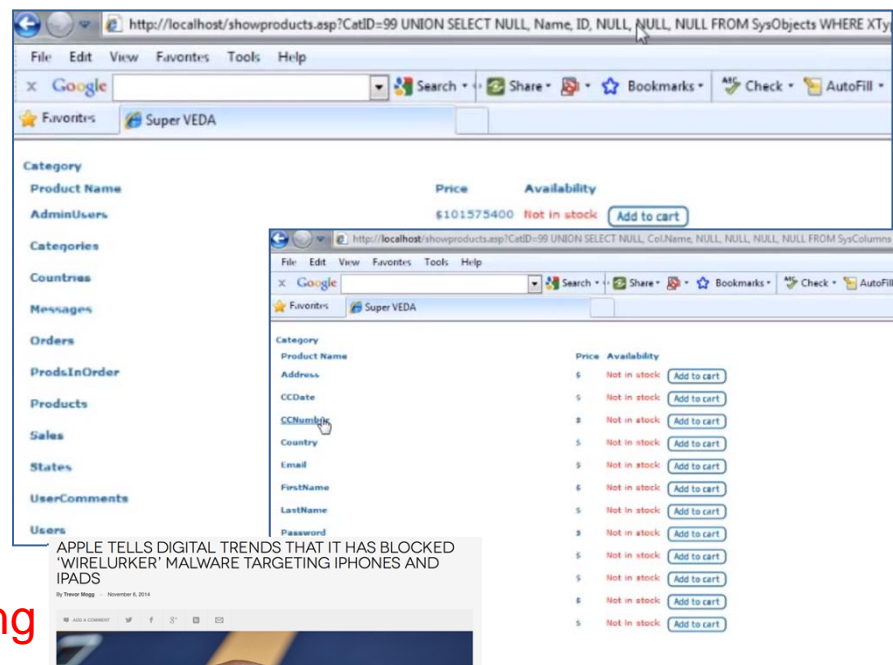


WIFI "FREE" Programs

..download **SPYWARE** / Phishing

SQL Website Injections

Objective: Steal Usernames & Passwords



APPLE TELLS DIGITAL TRENDS THAT IT HAS BLOCKED 'WIRELURKER' MALWARE TARGETING IPHONES AND IPADS



To Cloud or Not to Cloudthat is the question

- Advantages
 - Provides off-site storage & backup
 - Encrypts across networks
 - Eliminates local Information Technology server management

- Disadvantages
 - Where is your data stored?
 - Network administrator has security
 - Open to “hackers”
 - Creates challenges for Computer Forensic Investigators

Defend your Password

...Username TOO!!

- Change on regular basis
- Use Numbers, Letter, Symbols
 - Spell out Phrase
 - *1 L0v3 th3 B@nk!ng*

Defend your Email

- #1 Issue -- Attachments !!
-

Passwords / Email Phishing

Types of Password Attacks

Dictionary
Brute Force

Preventing Attacks

- Implement good Anti-Virus Protection (*Symantec, AVG, Malware Bytes, Kaspersky, etc.*)
- User Training (*don't click just anything*) → *Don't download just anything*
 - > *STRONG*: Usernames and Passwords
 - > Watch out for => Spoofing Email Accounts
 - (receive email from bmoody@bakerdonelson.com ← call me on this)
 - > Email Attachments
 - > USB Drives (infected with virus)
 - > Don't leave laptop, external drives, etc. just anywhere
 - > Briefcase approach
 - > Switches, Computers (*malware on chip from factory*)

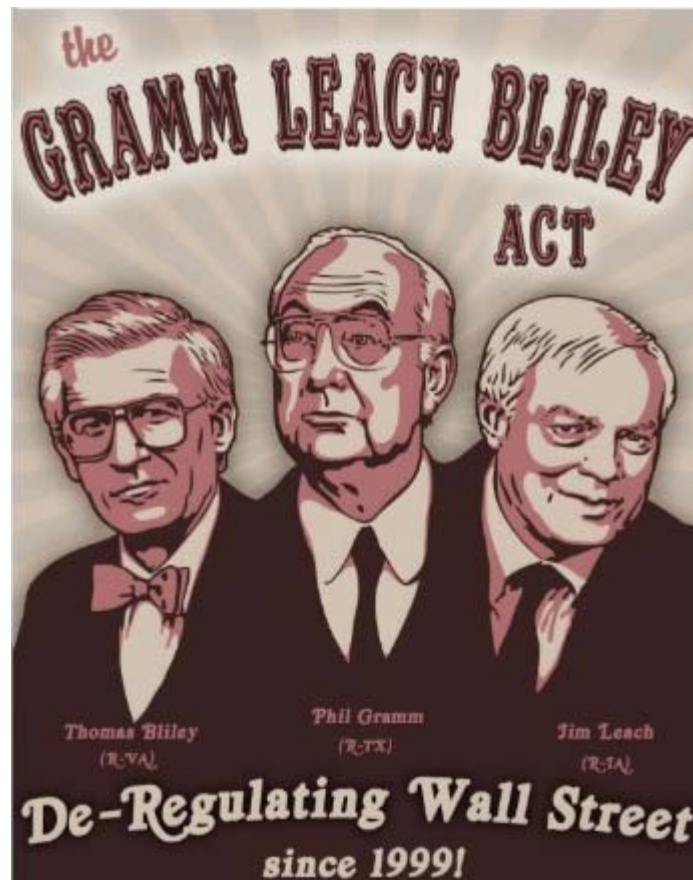
The Law



Hodgepodge of Laws

- **Gramm–Leach–Bliley Act (15 U.S. Code § 6801)**
- **HIPAA & HITECH Act**
- **Stored Communications Act**
- **State Laws**
- **European Union Laws**

Gramm-Leach-Bliley Act



Gramm-Leach-Bliley Act

- ▶ **Financial Privacy Rule (15 U.S.C. § 6801(a))**

- ▶ **Safeguards Rule (§ 6801(b))**
 - ✓ Screen prospective employees
 - ✓ Use passwords
 - ✓ Secure and limit access to servers
 - ✓ Encrypt customer information

- ▶ **Pre-Texting Provisions (§ 6821)**

Gramm-Leach-Bliley Act

Penalties:

- ▶ **A financial institution faces fines up to \$100,000 for each violation**

- ▶ **The officers and directors of the financial institution can be fined up to \$10,000 for each violation**
 - Ex. Franklin Toyota in Georgia – accidental P2P filesharing of customer data by employee

 - Paid steep fines and is subject to audits for years

HIPAA & HITECH ACT

- ▶ Protects Private Health Information (“PHI”)
- ▶ Imposes duties on providers to safeguard PHI
- ▶ Requires use of Business Associate Agreements
- ▶ Imposes stiff penalties for violations
 - Blue Cross & Blue Shield fined \$1.5 million in 2009 for theft of unencrypted PHI.

Stored Communications Act

- ▶ 18 U.S.C. § 2701(a):
Violation for anyone who “intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains ... access to a wire or electronic communication while it is in electronic storage in such system.”

Stored Communications Act

Examples

- ▶ No violation: *Shefts v. Petrakis*, 758 F. Supp. 2d 620 (C.D. Ill., 2010) (implied consent found where employee handbook informed plaintiff text messages would be logged)
- ▶ Violation: *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748 (N.D. Ohio 2013) (no implied consent where 48,000 personal emails were read by executive after plaintiff turned in her company-issued PDA)

Mississippi Laws

Miss. Code Ann. § 75-24-29

- ❑ Breach of security: unauthorized access of unencrypted “Personal Information” of Mississippi resident
- ❑ Protected Personal Information:
 - Social Security Number
 - Driver’s License Number (or state ID)
 - Account number or credit or debit card number with access information
- ❑ Notice Requirements: Must notify after reasonable period of time to investigate UNLESS investigation leads to conclusion that breach likely won’t lead to harm
- ❑ Enforcement by Attorney General as unfair trade practice; no private cause of action

Laws in Surrounding States

Alabama: None

Fla. Stat. 501.171: Mandatory notice to state; exception for consumer notice like in Miss.

Ga. Code Ann. 10-1-911 *et. seq.*: Applicable to “information brokers”; mandatory notice to affected residents; no penalty

La. Stat. 51:3071 *et. seq.*: Mandatory notice to affected residents unless harm is unlikely; private cause of action for untimely notice

Tenn. Code Ann. 47-18-2107: Mandatory notice to affected residents; private cause of action and civil penalties

Tex. Bus. & Com. Code § § 521.002 *et. seq.*: Duty to protect Personal Information; mandatory notice to affected consumers; civil penalties paid to the state

New & Proposed Laws



New & Proposed Laws

California: Expanded scope of security laws to include businesses that “maintain” data of residents

Kentucky: Added new protections to student data stored in the “Cloud”

Minnesota: Proposed new legislation to require Minnesota businesses to contact any person whose information was affected

European Union: EU Parliament seeks to create uniform privacy laws; provide “right to be forgotten” on the internet; impose fines of up to 100 million euros (\$140 million)

Questions



**Brad Moody, Shareholder
Baker Donelson**

bmoody@bakerdonelson.com

Meadowbrook Office Park
4268 I-55 North
Jackson, Mississippi 39211
www.bakerdonelson.com

**Andrew P. Mozingo, CHFI, ACE
Global CFI, LLC**

amozingo@globalcfi.com

120 Shelby Speights
Purvis, Mississippi 39475
www.globalcfi.com