XXVII Bank Security Conference

CELAES 2012

"MITIGATING RISKS AND CONVERTING THEM INTO BUSINESS OPPORTUNITIES"

FIBA

Organized by:

FELABAN

FEDERACION LATINOAMERICANA DE BANCOS

Data Security Law and the Cloud

Al Saikali, Esq., CIPP/US
Shook, Hardy & Bacon, LLP

WHY SHOULD YOU CARE?

Why Should You Care?

- It **will** happen to you
- It **will** be expensive
- There will be **investigations/lawsuits**
- There will be **brand** damage
- You can **limit** the risk

It Will Happen To You

- Not **if** . . . But **when**
- **90%** suffered a data breach
- **59%** experienced 2 or more
- **107,655** incidents reported

It Will Be Expensive

- Average Cost =
  - **$7.2 million** or $318 per record

Investigations/Lawsuits

- Lawsuits by private citizens
- Lawsuits between companies who share data
- Investigations by FTC and Attorneys General
- Investigations by card brands

Example #1

- *Zappos.com (Amazon)*
  - 1 cyber attack
  - 24 million records
  - Unspecified millions in damages

Example #2

- *Heartland Payment Systems*
  - 1 cyber attack
  - 130 million records
  - $140 million

Example #3

- *Global Payment Systems*
  - 1 cyber attack
  - 1.5 to 7 million cardholders
  - Cost = ??

Brand Damage

- **Most valuable** asset is at risk
  - **79%** have lost trust
  - **74%** would not shop where info at risk

Limit the Risk

- **92%** are avoidable
- Take **proactive** steps
  - **Administrative** safeguards
  - **Technical** safeguards
  - **Physical** safeguards

WHAT ARE THE ISSUES?

The Issues Are . . .

- What is a **data breach**?
- What **info** is protected?
- Is **notice** required?
- Must you be **proactive**

What is a data breach?

- "When sensitive personal information gets into the wrong hands"

What Info is Protected?

- Personally Identifiable Information
  - Includes financial account information
- Protected Health Information

Is Notice Required?

- Notice to whom?
  - Individual? Card brands? Attorneys General? FTC?
- Authority
  - State laws, Federal laws, International law, contracts, and industry standards

Must You Be Proactive?

- Security standards imposed by law or contract **before** a data breach

Legal Concerns Specific To Cloud Computing

- Jurisdiction – where is the breach?
- Liability – who is responsible?
- Damages – what is a recoverable injury?

HOW CAN YOU MINIMIZE RISK?

Initial Assessment

- Assess systems
- Assess policies
- Audit both

Administrative Safeguards

- Information Security Policy
- Service provider security requirements
- Service provider indemnification
- Data breach response plan

Technical Safeguards

- Email monitoring for third-party code, phishing, and
- Encryption
- Limiting file access
- Password management
- Approved browsers

Physical Safeguards

- Where is the data kept?
- How is it backed up?
- Who has access to it?

Important Safeguards For Cloud Computing

- Contractual obligations/relief
- Dedicated servers?
- File access?
- Encryption

For Further Information:

Al Saikali
Shook, Hardy & Bacon, LLP
asaikali@shb.com

http://www.datasecuritylawjournal.com