HOSPITALITYLAWYER.COM PRESENTS

2013 THE HOSPITALITY LAW CONFERENCE

FOCUSING ON LEGAL, SAFETY & SECURITY SOLUTIONS

FEBRUARY 11–13, 2013 • HOUSTON , TEXAS

DO NOT DISTURB: DATA PRIVACY & SECURITY ISSUES IN THE HOSPITALITY INDUSTRY

HospitalityLawyer.com

worldwide legal, safety, and security solutions

PRESENTERS

Linn Foster Freedman

- Nixon Peabody LLP
- Partner
- Leader Privacy & Data Protection Group
- Chair, HIPAA Compliance Team
- Recognized as national Leader in the field of Privacy by Chambers

Mark E. Schreiber

- Partner
- Edwards Wildman Palmer LLP
- Chair, Privacy and Data Protection Group
- Chair, Privacy Matters, World Law Group
- Handled numerous national and international breaches

J. Michael Gibbons, Managing Director

- Provides Information Protection Services including Incident Response, Digital Investigation & Data Protection for Alvarez and Marsal
- Former Chief of Cyber Crime Investigations for the F.B.I.
- Garnered 3 Espionage Convictions in Germany for theft of data from Pentagon Systems

OUTLINE OF DISCUSSION

- Breach Scenario
- Discussion of triage of breach and tasks to be completed
- Technical support and issues that may be presented
- Pre-breach planning
- Best practices and practical solutions for this rapidly changing area of the law

BREACH SCENARIO

- Notified by website hosting provider that the personal information of your customers and employees has been "hacked" and malicious code placed on the data server
- All customer and employee information, including name, address, date of birth, credit card information, payroll information, email addresses, medical insurance cards and claims information, social security numbers and drivers' license information has been sent to an unidentifiable gmail account
- What do you do?

BREACH SCENARIO CONT.

- Additional facts:
  - Your website hosting provider subcontracted with another provider to store your data in the cloud
  - It was the subcontractor's server that was "hacked"
  - The server was located in India
  - The website hosting provider that was your subcontractor did not have a written contract with the cloud services provider and is not giving your subcontractor any information about the incident or your investigation

What do you do?

BREACH SCENARIO CONT.

- Notification obligations for customer information
  - State law requirements
- Notification obligations for employee information
  - State law requirements
  - Self-insured health plan
    - HIPAA/HITECH

PRE-BREACH PLANNING

- Data Mapping
- Risk Assessment
- Implement a Privacy and Security Plan
- Assemble a Data Breach Response Team
- Implement privacy and security policies and procedures and breach notification plan
- Train, Train, Train employees
- Research insurance products
- Review contracts with vendors who have access to personal information
  - Require insurance and indemnification
  - Require the ability to audit privacy and security measures in place

LESSONS LEARNED FROM INCIDENTS

- Logging is often overlooked or not managed making it difficult to quickly determine the point of origin of an attack and how far it has spread. IT staff hates logs as it just represents work and cost with little perceived value to the business.
- Users with minimal access can wreak havoc by introducing hostile code attached to web sites and email messages, so end point security and training are as important as network and application security controls.
- Actually stemming the spread of hostile code requires specialized tools that model network behavior and capture real time memory states.
- Information protection requires new thinking about why sensitive data is collected, who it is shared with and when to dispose of it. It also needs proper controls at ***each point*** in its life cycle.

CARD BREACH DEVELOPMENTS - NEW VISA ASSESSMENT PROGRAM

- New higher Visa recovery amounts likely for larger breaches
  - passed through to merchants via merchant agreements with processors/banks
- Global Compromise Account Recovery (GCAR) program
  - announced in October, 2012 Visa regs.
  - retroactive to breaches subject to CAM Alerts noticed May 14, 2012 or later
  - former program Account Data Compromise Recovery (ADCR)

CARD BREACH DEVELOPMENTS - NEW VISA ASSESSMENT PROGRAM CONT.

- New triggers/thresholds:
  - 15,000 exposed Visa card nos.
    - previously 10,000
  - $150,000 or more total expended by all issuers
    - previously $100,000
  - but figure now includes <u>both</u> fraud recovery and operating expense recovery
    - previously only fraud recovery
  - Operating expense now $2.50/card
    - previously $1/card
- Other brands have recovery programs. Will they follow suit to increase amounts?

RECENT LEGAL REQUIREMENTS

- Stay abreast of changes in federal and state laws applicable
  - Rapidly changing
- Children's Online Privacy Protection Act (COPPA)
- CalOPPA
- Massachusetts Data Security Regulations
- HIPAA/HITECH
- CA mobile technology and zipcode laws
- Texas HB 300
- European Union privacy laws
- Canadian privacy laws