Post-Breach Notification

A Practical Exercise

State Laws on Notification

State Laws

- Located in state
- Doing business in state
- Data of resident of state part of breach
Industry Laws on Notification

Industry Laws

- Federal Information Security Management Act
- Federal Trade Commission Act
- Fair Credit Reporting Act
- Gramm-Leach-Bliley
- HIPAA/HITECH
- Regulation 1075

Global Laws on Notification

GDPR

- Doing business in EU
- Controlling or Processing EU Resident Info
**Goal**

- Provide scenario for data breach
- Analyze requirements for post-breach notifications
- Document steps taken
- Discuss notification requirements as part Incident Response Plan

**Background**

Your firm is located in Alandia, a recently created fictitious State midway between Illinois and Texas

The firm just landed BMW as a major new client and has opened a new office in Munich, Germany with one attorney and one legal assistant to better serve them

Your law firm practice areas include: Corporate law, International law, and Securities work
Scenario

It is 3:30pm on a Thursday afternoon
User in Alandia office calls you (the firm administrator) stating they have a strange popup on their computer
Initial inspection indicates malware is on the computer
Further inspection by your outsourced Managed Security Provider indicates data has been sent out from your network to a 3rd party server

Relevant Laws

Alandia Revised Code
- Applies to firm because you’re in Alandia and the data breach affected residents of Alandia
- 1349.19 – Disclosure Requirements following Data Breach
- 1354.01 – Safe harbor effective November 2

GDPR
- Because firm has an office in EU Member country, assume subject to GDPR
- For the purposes of this exercise, assume that your firm is considered a “Controller” as defined by GDPR
Exercise Objectives

Objective 1 – Discuss and document at a general level the steps that should be taken in response to the threat.

Objective 2 – List the parties that should be involved in the response process and what roles they fulfill.

Objective 3 – List the notification requirements applicable to your firm. List who needs to be notified and within what timeframe. Also list who should be notified even if not required by law.

Objective 4 – Draft an example "Notification Requirements" section that could be included in an overall Incident Response Plan.