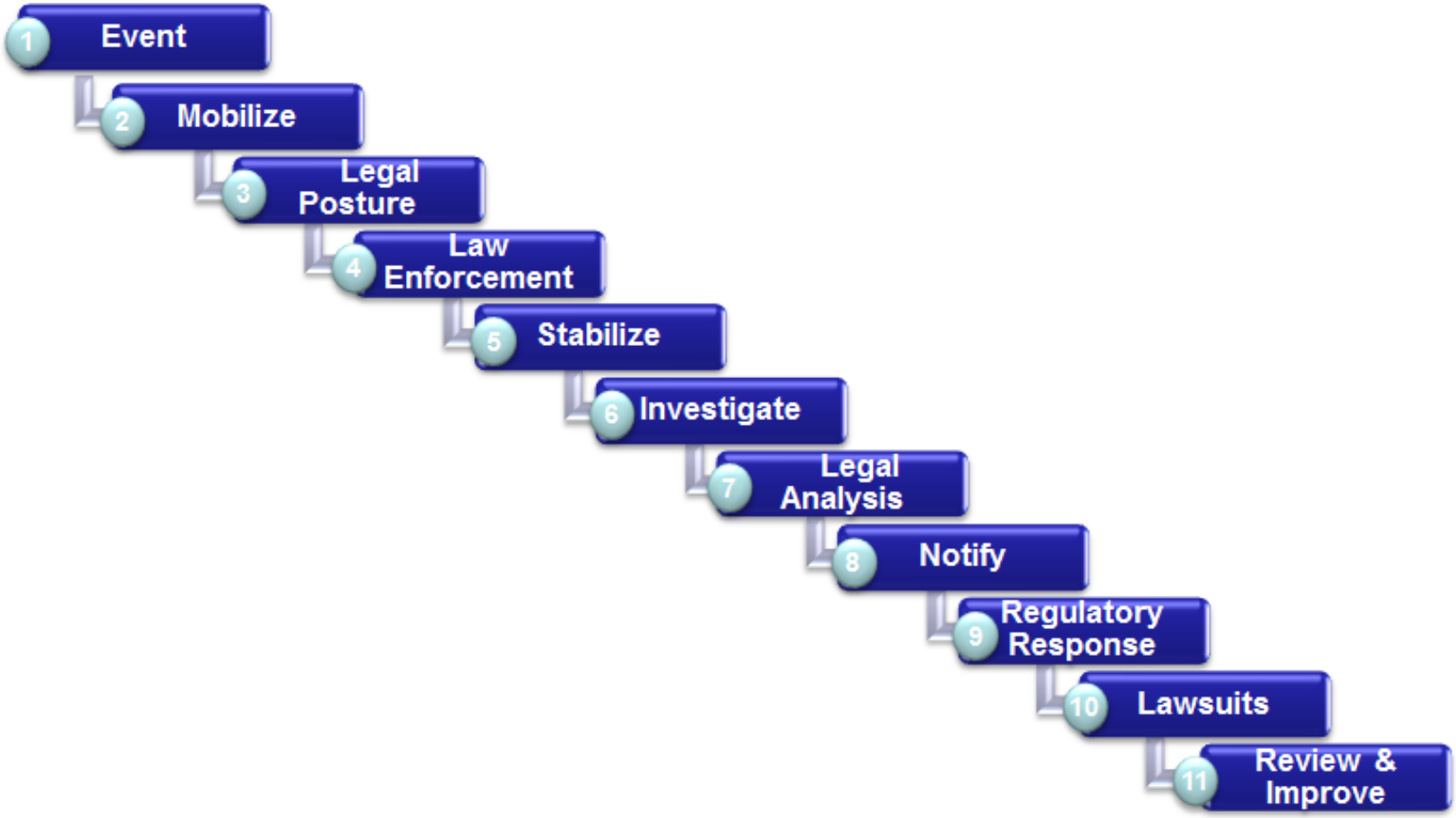
HUNTON& WILLIAMS

Lawline
Managing a Cyber Incident: A How-To Guide

Lisa J. Sotto
Hunton & Williams LLP
(212) 309-1223
lsotto@hunton.com
www.huntonprivacyblog.com

August 24, 2016

Data Breach Response Timeline



Cyber Attack: First Steps

- **Identify event; mobilize response team; protect legal posture**
- Pay attention to threat notifications from law enforcement or reporters
- Identify aberrant behavior
- Mobilize incident response team
- Protect legal posture
  - Preserve privilege when retaining experts
  - Legal hold
  - Insurance

Coordinate with Law Enforcement

- **Information sharing**
- Law enforcement often has a broader view into cyber threats
- Establish an early line of communication
- Determine the most appropriate agency
  - Depends on the nature of the compromise
  - Local, federal and international law enforcement may be necessary

Conduct an Investigation

- **Stabilize affected systems and investigate scope**
- Contain the attack
- Forensic imaging
- Restore the integrity of the system
- Retain third-party forensic experts?
- Understand:
  - Nature of the compromise
  - Data and systems at issue
  - Whether communications systems are secure
  - Whether insiders are involved

