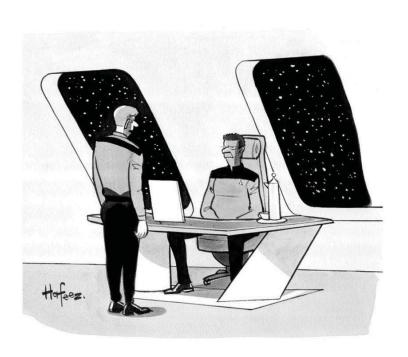
Responding to a Cyber Breach

Art Ehuan, Alvarez & Marsal - Washington, DC Bart Huffman, Locke Lord LLP - Austin, TX

UT Law CLE
Essential Cybersecurity Law
August 16, 2016
Austin, Texas



"Bad news, captain. The ship's computer has been sharing all our personal data with the Romulans."

Cyber Breach Methodology



- The Impact
- Financial lossHarm brand
- and reputationScrutiny from regulators
- · Cyber Attacks are multi-stage, using multiple threat vectors
- Organizations often don't identify that they have been compromised for months after the event¹
 - 206 days on average before detection of compromise
- Over two-thirds of organizations find out from a 3rd party when they have been compromised²
- 3

1 – Ponemon Cost of Breach FY 2015 2 – 2014 mTrends Threat Report

Important Considerations

- Different types of incidents
 - malware
 - inadvertent disclosure
 - portable media loss
 - compromised access credentials
 - denial of service attacks
 - "special" types of data: payment card data, Protected Health Information, Nonpublic Personal Information, personally identifiable information, ...
- Different scenarios
 - unknown loss or damage but known compromise
 - known loss or damage but unknown compromise
 - holding access to or use of data or systems hostage
 - extortion
- Variations in severity level
 - volume and nature of data
 - · criticality to operations
 - potential regulatory or litigation risk
 - potential reputational impact
 - potential exposure to interested third parties

Being Prepared ...

- for loss of data or interrupted systems
- for operational and business continuity issues
- for immediate initiation of investigation(s)
- for preserving evidence
- · for task force / response team leadership and meetings
- for immediate engagement of forensic investigator(s) (including, if applicable, PCI Forensic Investigator), counsel, public relations firm, negotiator, other breach response service providers
- for internal communications
- for communications to third parties
- for responses to the media
- · for notices to regulators, interested third parties
- for reports to shareholders, Board
- for notices to individuals
- · for intelligence sharing

See, e.g., NIST Computer Security Incident Handling Guide, Special Publication 800-61 rev. 2.



Crisis Management

- ❖Organization and Management
- ❖Security v. Operations
- Candor and Prudence
- ❖Skills and Experience
- **❖**Compliance and Ethics
- ❖Good Judgment





Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the <u>UT Law CLE eLibrary (utcle.org/elibrary)</u>

Title search: Responding to a Cyber Breach

Also available as part of the eCourse

<u>Essential Cybersecurity Preparedness and Response: Internal Controls,</u>

Developing an Incident Response Plan and Responding to a Data Breach.

First appeared as part of the conference materials for the 2016 Essential Cybersecurity Law session "Responding to a Data Breach"