CSO PERSPECTIVES

What to Do – and Not Do – When Attacked: A Moderated Workshop

Michael R. Overly, Esq., CISA, CISSP, CIPP, ISSMP, CRISC

Agenda

- Overview
- Building a team
- Manage your experts
- Internal team
- First 24 hours
- Assessing the Incident
- Vendor Relationships
- Case Studies/Discussion

Overview

- The importance of establishing diligence
- Understanding quantum mechanics
- An ounce of prevention . . . .

Preparation is critical

"*Healthcare organizations are entering a new frontier. Reported incidents will rise and regulations will force teams to reevaluate data management procedures or face heady fines. Preparation is not just nice to have, it is a must.*"

– 2014 Data Breach Industry Forecast, Experian

Building a Team

- Internal incident response team
- External experts
  - Forensics
  - Legal
  - PR

Manage External Experts

- Finding the right expert
- Ensuring availability
- What's it going to cost/project management
- Attorney/client privilege & Work Product
- Mitigate expert risk
  - Data protection
  - Where is my data?

Internal Incident Team

- Members
- Training
- Policies and procedures
- Media contact
- Regulatory contact
- Manage internal communications

Vendor Relationships

- Insider threat: Vendors having access to or possession of your data
- Cloud and other hosting engagements
- Offshoring
- Diligence, incident response, notification, prevention should be part of all relevant vendor agreements

First 24 Hours are Critical

- Failure to act quickly can result in continued data loss, misappropriation of data, lost evidence.
- Acting quickly can mitigate, and sometimes even avoid, breach notification obligations, data loss.

First 24 Hours are Critical

- Reputational damage can be minimized with quick action – exacerbated with unreasonable delay.
- Demonstrates reasonable conduct and diligence in responding to incident

Assessing The Incident

- Nature and extent of data impacted.
- Was the data encrypted.
- Was data actually accessed or acquired.
- Who had custody of the data at the time of the incident?

Case Study #1

Your organization is setting up its first incident response program. As part of that program, you must identify what, if any, relationships to establish with third party experts. Your company is a large technology company and believes its own personnel are sufficiently expert to conduct the investigation and forensics.

Case Study #1, cont'd

- Should your company use its own personnel? Are there any issues that should be considered?
- What other experts should be used?
- How do you identify and vet experts?
- What qualifications are most important?

Case Study #2

Your organization is setting up its first incident response program. As part of that program, you are tasked with developing your internal breach notification policy(ies) and creating a training program for your personnel.

Case Study #2, cont'd

- Which stakeholders in the company should be involved in policy and training development?
- What key elements should be included in the policy?
- How and when should employee training be conducted?
- How should the policy and training be updated?

Case Study #3

You represent a consumer e-commerce company. A reporter calls asking if you would care to comment on a rumor that thousands of your customers' credit card numbers and other personal information have been posted to a known hacking site.

Case Study #3, cont'd

- What is your response to the reporter?
- Do you ask any questions of the reporter?
- What are your first steps?
- Should you develop a draft press release? If so, what should it say?

Contact Information

Michael R. Overly, Esq. CISA, CISSP, CIPP, ISSMP, CRISC
Information Technology & Outsourcing
Foley & Lardner LLP
Tel: 213-972-4533
moverly@foley.com