Use Your Head......

theUriahgroup

The Data Breach You Didn’t See Coming

Gordon Meriwether

The Uriah Group

03.08.11

Introduction

- Leadership in Crisis: A review
- The Data Breach
  - Definitions
  - Vulnerabilities & Risks
  - Examples of Current Threats
- Tabletop Exercise
- Hotwash: Lessons Learned

Today

- Ground Rules
  - There are no rules!
  - Cell Phones
  - Interactive
  - Follow up
  - Hot Wash

Our goal today is to keep it simple…….

Simplicity wins in a crisis!

Leadership in Crisis

A Review

Impacts on Leaders in Crisis

- Tension and Stress
  - Psychological, mental, & physical
- Speed
  - Warp or tedious
- Personal
  - Availability of the right people…making due.
- Organizational
  - Rigidity or flexibility

- Stakeholder variance
  - New players and expectations
- Communications
  - New channels
- Media
  - Exponentially more attentive and focused
- Simplicity wins in Crisis
  - More complexity less likely success.

Crisis Leadership Cycle

- **Preventing**
- **Preparing**
- **Responding**
- **Recovering**

How do we React to a Crisis?

Humans will react to a crisis in 4 steps with:

1. Our Instinct
2. Our Emotion
3. Our Head
4. Our Plan

The trick is to get to step 4 as quickly as possible….but be ready to adjust back to step #3.

Lessons in Crisis Leadership

1. ***Quick Response to a crisis is mandatory.*** *(Challenge the Process)*
2. ***Continually build teams around empowered managers.*** *(Enable others to act)*
3. ***Take guidance from your core values.*** *(Model the Way, Inspire a Shared Vision)*
4. ***Maintain your personal balance.*** *(Encourage the Heart)*
5. ***Maintain control over the team, the crisis, and your assets.*** *(Enable others to Act, Encourage the Heart)*

The Data Breach

Definition

- Data Breach
  - A security incident in which sensitive, protected or confidential date is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. (Privacy Rights Clearinghouse)

Crisis Preparation Priorities

- Food contamination resulting in death or illness.
- Catastrophic weather event
- *Data Breach* √
- Active Shooter
- Death and injury on the premises
- Pandemic outbreak
- Robbery
- Labor action

Data Vulnerabilities

- Data Vulnerabilities
- Point of Sale systems (access to debit cards, credit cards)
- Supply Chain (ordering and payment)
- Employee Information (personnel & health records)
- Trade secrets and intellectual property
- Customer loyalty cards (customer information, buying trends)

Lloyd’s 360° Risk Insight

- Managing Digital Risk
  - Digital risk needs to become a ***Board-Level concern***.
  - Digital risks facing companies are ***likely to grow*** and become increasingly complex with advances in technology.
  - The range, frequency and scale of digital attacks on business will grow with ***increasingly sophisticated attackers*** quickly adapting to the rapidly changing digital environment.
  - Risk managers need to develop ***comprehensive digital risk management strategies*** that involve a range of mitigations, as well as risk transfer solutions.
  - There is a need ***for increased communication, co-operation and collaboration*** to tackle digital risk.

Recent Data Breaches*

- 2010: Restaurant: Malware on server obtained passwords for system with customer information.
- 2010: Grocer: Tampered payment card terminals placed in stores
- 2010: Services: Hacker accessed payment system and transferred funds into private account.
- 2010: Restaurant: Hackers accessed online newsletter for customer information including birthdates.
- 2011: Appliance manufacturer: Hacker code discovered on server
- 2011: Restaurant: Skimming device used to copy customer credit card information. Sold to third party.
- 2011: Retail: Overseas hacker obtained access to customer credit and debit cards.

* Privacy Rights Clearinghouse

The Tabletop

Hotwash

Lessons Learned

Responding to a Data Breach

- Develop a preliminary data breach plan as part of your Crisis Management Plan
- On occurrence assess the situation
  - What’s been compromised?
  - How was the data compromised?
  - Can you contain the damage?
- Notification of Federal Agencies
- Notification of Impacted: customers, employees, suppliers,…..
- Update your plan of action
  - What’s been put in place for those impacted?
  - How are you going to mitigate damages?
  - What have you put in place to insure that it doesn’t happen again?
- Execute that plan
- Effectively communicate according to the plan
- Evaluate the results of the plan
  - Did you contain the damage?
  - Conduct a Security Review
- Adjust the plan

Use Your Head......

theUriahgroup

Thank You!