MARSH

LEADERSHIP, KNOWLEDGE, SOLUTIONS...WORLDWIDE.

INFORMATION SECURITY – RESPONDING TO A DATA BREACH

California Grocers Association
July 31, 2013

Susan Beresford
Marsh, San Francisco

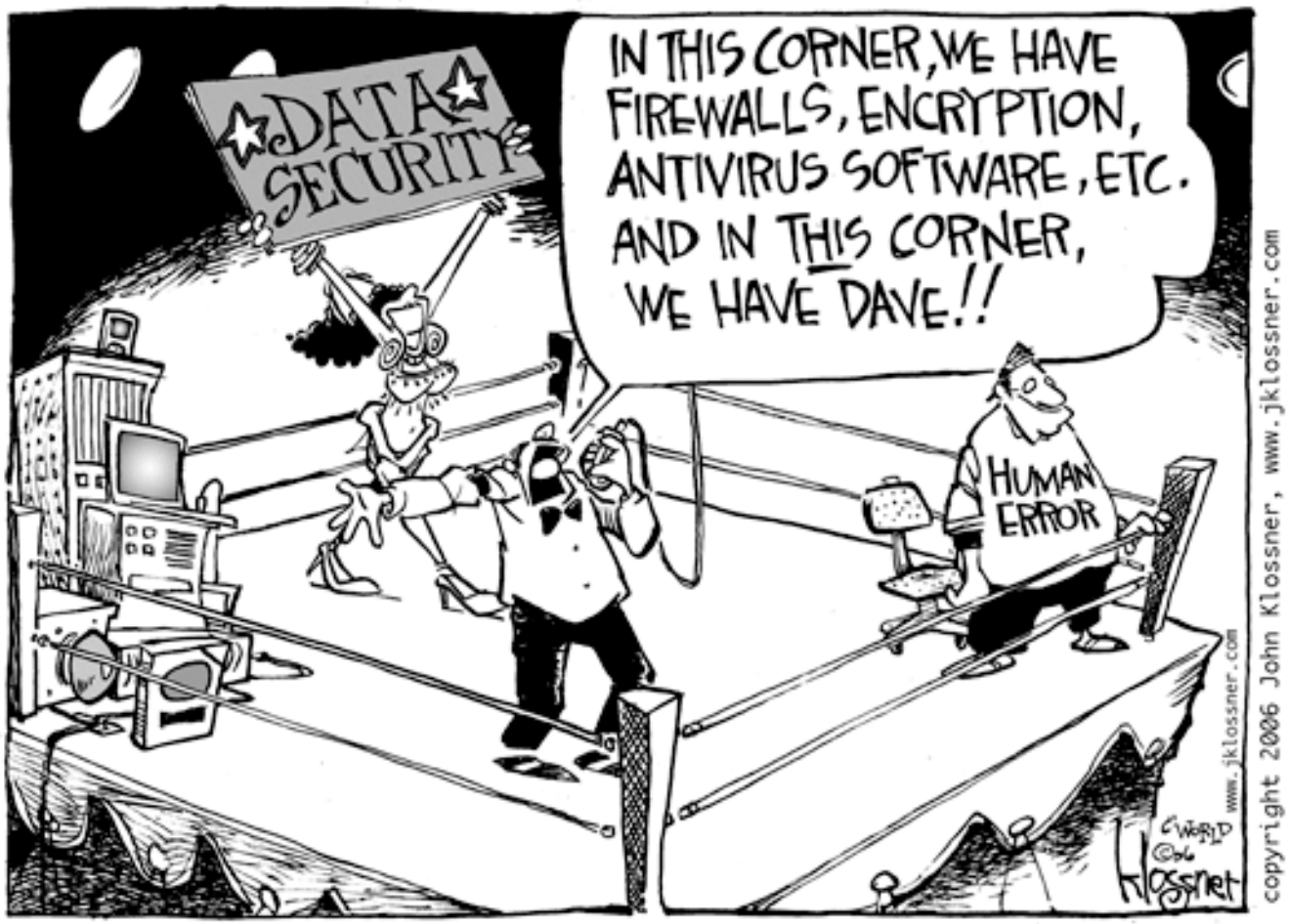
MARSH & McLENNAN COMPANIES

Agenda

- What are Information Security/Cyber Risks?
- Cost of a Data Breach
- You've Just Experienced a Data Breach…Now What?!
- Appendix:
  - Crisis Management Before, During & After a Breach
  - Threat Environment – summary findings from Verizon Security Consultants 2013 Data Breach Investigations Report

What are Information Security/Cyber Risks?

This is the reality……



What are Information Security/Cyber Risks?

- Legal liability to others for computer security breaches
- Legal liability to others for privacy breaches of confidential information
- Costs to investigate and notify others of a breach
- Regulatory actions, fines and scrutiny
- Cyber-extortion
- Cyber-terrorism
- Electronic content
- Loss or damage to data / information
- Loss of revenue due to a computer attack
- Extra expense to recover / respond to a computer attack
- Loss or damage to reputation

Costs of a Data Breach

Cost of a Data Breach

Number of Records Compromised	100,000	500,000	1,000,000
Number of Credit Card Numbers Compromised	100,000	500,000	1,000,000
Forensics, Legal & Advisory Costs	$100,000	$100,000	$250,000
Notification Costs	$200,000	$1,000,000	$1,000,000
Call Center Costs	$100,000	$500,000	$1,000,000
Credit Monitoring Costs	$450,000	$1,500,000	$2,250,000
Identity Theft Repair Costs	$375,000	$1,875,000	$3,750,000
Estimated First Party Costs	**$1,225,000**	**$4,975,000**	**$8,250,000**
Credit Card Reissuance Costs	$600,000	$3,000,000	$6,000,000
Consumer Redress Fund & Fines	$600,000	$3,000,000	$6,000,000
Other Liability	$500,000	$2,500,000	$5,000,000
Defense Costs	$100,000	$500,000	$1,000,000
Estimated Third Party Liability	**$1,800,000**	**$9,000,000**	**$18,000,000**
Estimated Privacy Event Insurable Cost	**$3,025,000**	**$13,975,000**	**$26,250,000**
Assumptions			
Per record notification cost	$2.00	$2.00	$1.00
Call center participation rate	20%	20%	20%
Per call cost	$5.00	$5.00	$5.00
Credit monitoring participation rate	15%	15%	15%
Credit monitoring per record cost	$20.00	$20.00	$15.00
Identity theft rate of occurrence (of those monitored)	5%	5%	5%
Identity theft per record cost	$500.00	$500.00	$500.00
Credit card reissuance cost per card	$6.00	$6.00	$6.00
Consumer Redress & Fines per record	$6.00	$6.00	$6.00
Other liability experience rate	1%	1%	1%
Other liability cost per record	$500.00	$500.00	$500.00

Regulatory Actions usually precedes the civil action, substantial expense-legal and forensic can be incurred even for events where no one is actually harmed or even at risk of harm

You’ve Just Experienced a Data Breach…Now What?!

Simplified Data Breach Timeline

Discovery

Actual or alleged theft, loss, or unauthorized collection/disclosure of confidential information that is in the care, custody or control of the Insured, or a 3rd for whom the Insured is legally liable.

Discovery can come about several ways:

- Self discovery: usually the best case
- Customer inquiry or vendor discovery
- Call from regulator or law enforcement

First Response

Forensic Investigation and Legal Review

- Forensic tells you what happened
- Legal sets out options/obligations

External Issues

- Public Relations
- Notification
- Remedial Service Offering

Long-Term Consequences

- Income Loss
- Damage to Brand or Reputation
- Regulatory Fines, Penalties, and Consumer Redress
- Civil Litigation

Now What?!?!

- **Response Steps**
  1. Receive initial report
  2. Assemble breach response team
  3. Initial internal communications (who needs to know?)
  4. Engage external counsel
  5. Investigate
  6. Validate nature and extent of the incident
  7. Containment, control and correction
  8. Notifications: who, when, where, how and what
  9. Conclude investigation and prepare incident report
  10. Retain report

Investigate & Validate

WHO

- Who are the affected parties?
  - First party coverage is for Data Asset Protection and Business Interruption.
  - Third party coverage is for breaches of privacy involving data entrusted to the Insured by another party.

WHAT

- What data has been compromised?
  - First party losses involve damaged or “locked-out” data, along with loss of network effectiveness.
  - Third party losses include Personally Identifiable Information and “Corporate Confidential.”

WHERE

- Is the data that was compromised in the hands of a Business Process Outsourcer?
  - If so, it is still treated as a loss for the Insured, but there may be indemnification available through the B.P.O.
  - Most policies are written on a duty to defend basis, so the insurer will pay covered losses and then have option to subrogate.

WHEN

- Notice to insurer should be provided as soon as practicable.
- Operative date is typically date of discovery, not the date of the breach (these may be different, particularly if a B.P.O is involved).
- Check post-policy reporting provisions for deadlines.
- For Personally Identifiable Info, Federal and state statutes define time frames for notification to affected parties and law enforcement agencies.

WHY

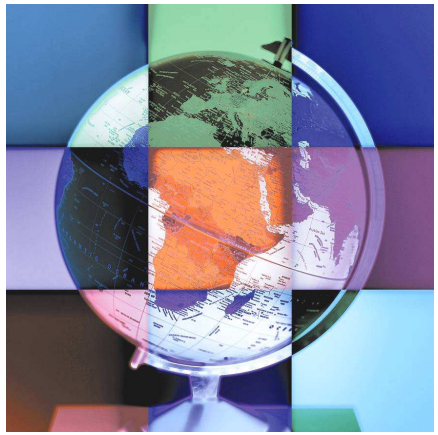
- Motivation could be for:
  - sport (hackers)
  - to commit ID theft (phishing)
  - political (hack-twist)
  - competitors seeking trade secrets
  - organized crime/cyber extortion
  - rogue employees/careless staff
- Data asset protection may be excluded if the perpetrator is an officer of the company.

HOW

- Statutory requirements apply to (and coverage is triggered by) breaches of Personally Identifiable Information, regardless of how the data was compromised.
- On the other hand, there is no coverage for first party losses resulting from poor planning for network traffic, or unforeseen customer demand. There must be a failure of security.

Initial investigation…

- **What was the cause of the event?**
  - Hacking / extortion
  - Rogue employee, internal fraud
  - Email sent to wrong address
  - FTP file transfer
  - Failure of controls / preventative measures
  - Failure of hardware or software
  - Wrongdoing or failure of a vendor or other related third-party entity

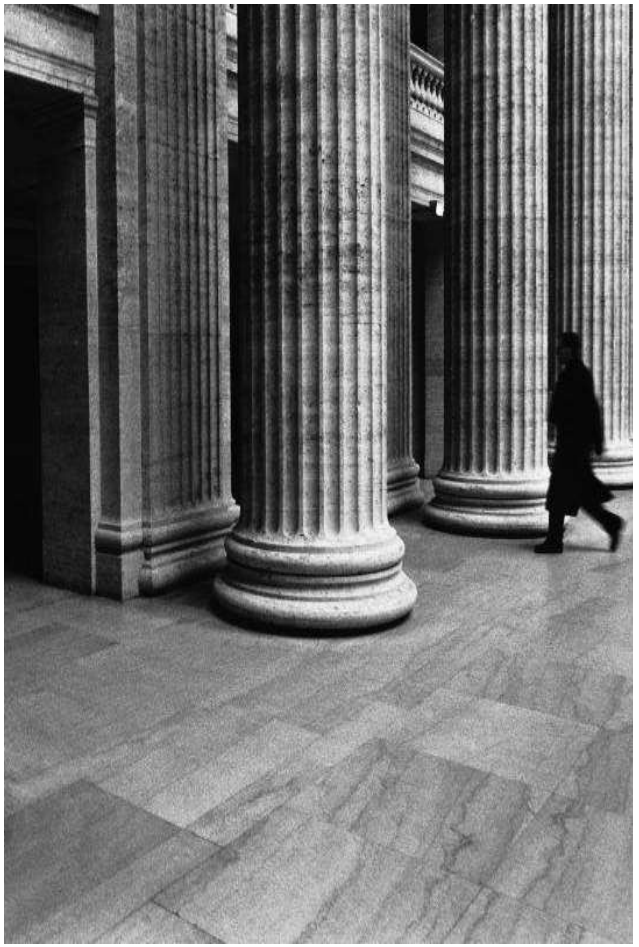


What was lost/compromised?

- **What type of data was involved?**
  - Corporate confidential information
  - Personal Health Information (PHI)
  - Credit Card Data (PCI/DSS)
  - Personally Identifiable Information (PII):
    - First name or initial combined with a social security number
    - Driver's license number
    - State ID number
    - Account number with access code or password

Managing the Event

- **How do you notify victims of the event?**
  - Mail
  - E-Mail (E-Sign act)
  - Mass Media (TV, Newspaper, etc.)
- **What is your deliverable to the victims?**
  - *"We breached your data and here is a list of things you can do to protect yourself"*
  - To monitor or not to monitor? That is the question!
- **Notify correctly vs. quickly**
- **Call center (questions and answers)**
- **ID Theft Insurance vs. ID Theft Recovery**



Best Practices for Breach Preparedness and Prevention

- **Assess your exposure**
  - Marsh Self-Assessment Tool
  - Marsh's Damage Analysis Model
- **Provide "Certification" through e-Learning**
- **Develop an Incident Response Plan**
  - Internal Staff
  - External Counsel
  - Forensics Provider
  - Reputational Risk Advisor
  - Breach Service Provider
- **Hold a cross functional "Privacy Summit" to identify vulnerabilities**
  - Include Risk, Privacy, HR, Legal, IT C-Suite, Facilities, etc.
- **Keep current to federal, state and foreign legislation**

Carriers' approach to Privacy Event Response Costs

- **Currently there are two approaches to privacy coverage in the market**:
  - Providing a dollar sublimit
    - Pro's:
      - Insured maintains control of the process
      - Insured knows exactly how much money they have available for an "event"
      - Can be outside the limit of liability
    - Con's:
      - Insurer may not agree to all costs incurred
      - Insurer may not approve insured's selected vendors
      - Dollar sublimit may not be sufficient to respond to all costs associated with an "event"
  - Providing a per person/record sublimit.
    - Pro's:
      - Typically outside the aggregate limit of liability
      - Insured selects response firm from a panel counsel list
      - the response is handled by the insurer
    - Con's:
      - The Insured hands over the response to the insurer

- **For larger clients, the per person sublimit removes control which they expect to maintain.**
- **For smaller less sophisticated clients, the per person option provides a turn key product necessary to satisfy statutory regulations**.

Appendix

- Crisis Management Before, During & After a Breach
- Threat Environment – summary findings from Verizon Security Consultants 2013 Data Breach Investigations Report

Principles of Crisis Management – Before

1. Establish clear team leadership and defined responsibilities
   - Data security is responsibility of IT; data loss requires a broader corporate response
   - Crisis management will coordinate and manage responses of management, IT, GC, HR, marketing, communications and IR, security, etc.
2. Define activation criteria for crisis management
   - Size? Level of confidence? External enquiry?
   - What is process for forensic investigation?
   - Are there clear reporting and communications channels?
3. Understand your legal and regulatory obligations
   - Existing state requirements on notification – when, how?
   - Federal requirements are in place? CMS, HIPAA, etc.

Principles of Crisis Management – Before

4. Develop procedures and policies in advance – response needs to be executed, not created
   - Do you extend your data security policies to your suppliers? Vendors? Does that change how you respond?
   - Beyond meeting minimum legal notification requirements, what level of protection are you prepared to offer?
   - When and what do you communicate to non-impacted employees or customers, your board, business partners, etc.?
5. Make sure your process is understood by those who will have to implement it
   - Exercise, exercise, exercise
   - Even the best plan won't help if executives don't know what to do
   - Only consistent factor in success

Principles of Crisis Management – During

1. Understand the scope
   - Forensic analysis
   - What kind of data has been lost? Financial, personal, strategic? Confidential business information?
2. A crisis must be managed (not simply responded to)
   - Activate CMT to coordinate decisions across the enterprise
3. Crises do not happen in a vacuum
   - Understand the potential for spillover into unrelated areas
   - What else is going on? New leadership? Budget negotiations? Major events/deals?
4. Demonstrate concern, commitment, and control

Principles of Crisis Management – After

1. Conduct a post-incident review immediately to understand:
   - Damage to stakeholder opinion
   - Effectiveness of response
   - Effectiveness of established procedures
2. Learn from your mistakes and successes
   - Assess IT security program, gaps, internal educational efforts, etc.
   - Revise/update CM program and contingency plans
3. Assess reputational impact
   - It takes approximately three-and-a-half years for an organization to recover from a reputational failure

Threat Environment- Targets of Opportunity

Verizon Security Consultants 2013 Data Breach Investigations Report

A sample of 47,000 reported incidents with 621 confirmed breaches. Some key findings:

- 78% were not highly difficult involving little to no resources or customization of software.
- 75% were not targeted at a specific individual or company
- 76% of network intrusions exploited weak or stolen credentials
- 29% of attacks utilized social tactics (email, phone calls, or social network information)
- 14% of attacks involved insiders; 50% of those were former employees using old credentials
- 2/3^{rds} of breaches involved data at rest (databases and file servers). The remaining amount was compromised at the time processed.
- 66% of breaches took months (62%) or years (4%) to discover
- 69% of breaches were discovered by an external party (9% by customers)

Industries groups represented by percent of breaches (total exceeds 100% due to rounding):

- 37% from Finance and Insurance
- 24% from Retailers
- 20% from Manufacturers, transportation and utility
- 20% Information and professional service firms

Marsh


MARSH