Security Breaches – To Disclose or Not to Disclose

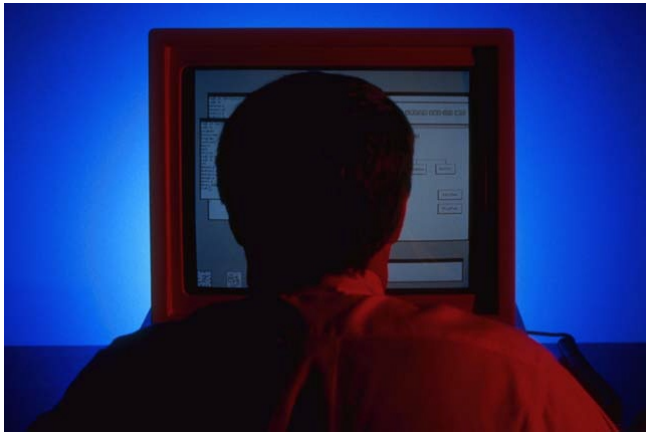
Gib Sorebo, JD, CISSP

June 2008

SAIC
From Science to Solutions

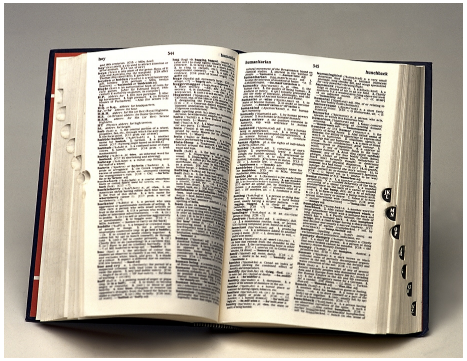
Overview

- **Breaches and Their Evolution**
- **Breach Legislation**
- **Recent Breaches and Lessons Learned**
- **Steps to Take in Response to Breach**



Disclaimer: This presentation should not be construed as providing legal advice or advocating any sort of compliance regime. The state of incident response and breach notification is evolving rapidly. New court opinions, industry practices, and rule making may contradict what is presented today. Individuals and organizations are advised to consult legal counsel before disclosing any breaches or formulating any breach notification policies or practices.

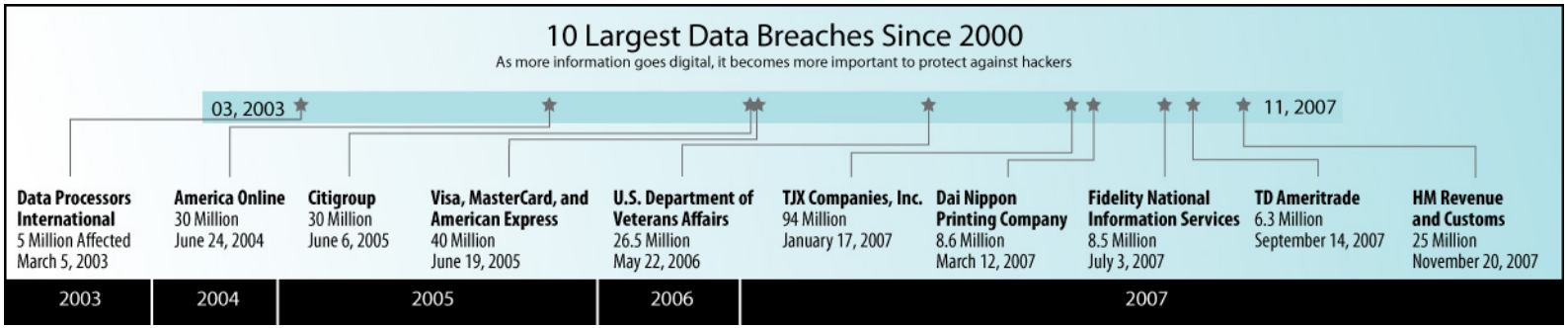
What is a Breach?



- **Breach concept has had several meanings (e.g., Webster's defines breach as *"infraction or violation of a law, obligation, tie, or standard")***
- **It is commonly understood as when an intruder has actually broken into a system**
- **California law [Cal. Civ. Code § 1798.82] and many others define breach as**
  - "[U]nauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."
- **For sensitive data, the view has often been that a breach occurs when the data are viewed or downloaded**
- **Recent cases take a different view**
  - Some hold that breach occurs when vulnerability makes successful attack likely
  - Breach may be sensitive data sent over the Internet in the clear
  - Lost laptop or backup tape may be considered a breach

How Have Breaches Evolved?

- **In early breaches like the Pfizer Prozac mailing list, it was clear that sensitive information (i.e., subscribers) was distributed to strangers**
- **In the ChoicePoint case, data were specifically obtained to commit fraud**
- **In more recent cases, items such as computers were stolen or backup tapes were lost and reported even though no evidence existed to show that data was accessed**
  - In a 2006 Veterans Administration case, after the hard drive was recovered, a debate ensued about whether the hard drive was accessed
- **More recent cases have dealt with vulnerabilities on Internet-facing computer systems**
- **It is still an open question whether data sent in the clear is a breach**
  - ABA Advisory Opinion holds that it is not unethical to send client communications in the clear

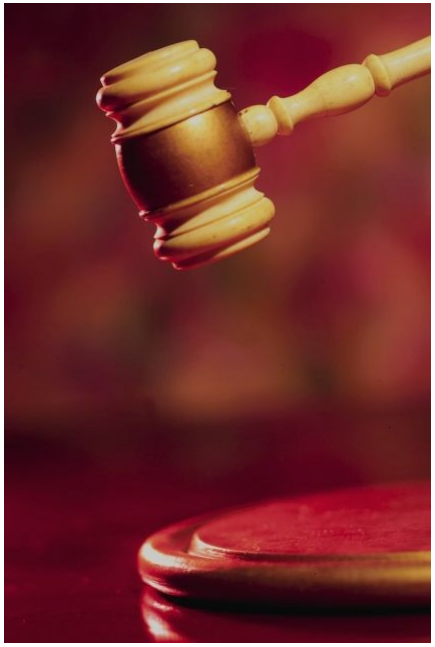


Recent Breaches and Lessons Learned

- **TD/Ameritrade**
  - Late notice; more than a year went by
  - Lawsuit may have forced the disclosure
- **Hannaford**
  - Spending millions on remediation efforts
- **Most breaches still resulted from offline compromises (e.g., laptop thefts, lost tapes)**
- **Successful online attacks seem to be growing or at least are being reported more often**
- **Law enforcement sources point to organized crime as a growing threat in the online world with a greater focus on financially motivated attacks**
- **Average per-incident cost of breach = $6.3 million (PGP/Vontu study)**

Breach Legislation: An Inevitable Outcome?

- California SB-1386 was initially seen as a “feel-good law” that would not accomplish much
- The law had no enforcement provisions
- Instead, the law became perceived as the de facto standard
- 42 other states have followed suit
- Federal laws are under consideration and regulations are in place for regulated industries
- There is little guidance for the award of damages



SAIC From Science to Solutions

International Considerations

- **Legal schemes differ**
  - The United States maintains a sector-based approach that is heavily dependent on regulatory regimes and best practices for that industry
  - European Union countries impose privacy rules with no explicit breach notice requirements, but they often impose implicit requirements
  - Just as states impose different reporting obligations, so do countries
  - In some jurisdictions, failure to report breaches can result in severe sanctions, including criminal penalties (New York Attorney General investigation resulted in $60,000 settlement for costs related to the investigation)
- **General practices to consider**
  - Consider segregating customer data by country if feasible
  - For general principles, reference OECD Privacy Principles
  - Obligations for reporting breaches arise from core privacy principles
- **In preparation for breaches**
  - Ensure in-house or outside counsel is familiar with legal obligations
  - Maintain relationship with local law enforcement
  - Publish breach disclosure practices in all relevant languages
  - Follow consistent practices unless local laws conflict

International Considerations

- **Overview by country**
  - United States
    - Laws vary by state (no national breach law for private sector, yet …)
      - » What data is covered?
      - » When is it a breach requiring notice?
      - » How soon is notification required?
      - » Penalties, if any, for failure to disclose?
      - » Private right of action?
      - » What breaches are exempt (e.g., encrypted data, immaterial)?
  - Canada
    - Breach notification guidance provided by British Columbia and Ontario
    - Some are proposing amendments to Personal Information Protection and Electronic Documents Act (PIPEDA) to include breach notification
  - Europe
    - Some Data Protection Authorities (DPA) have used the EU Data Protection Directive to require breach notification based on its effect on the organization's registration

SAIC From Science to Solutions

International Considerations

- **Overview By Country**
  - Latin America
    - Breaches tend to be handled on a case by case basis
    - There is generally no formal scheme
    - Organizations need to understand local practices and be responsive to customer expectations
  - Asia and Africa
    - Dubai's data privacy law requires notice to data protection commissioner
    - South Africa and India are considering breach laws
    - Southeast Asian countries tend to be more pragmatic about privacy issues generally than their European counterparts
  - Japan
    - Based on the country's privacy law, notifications are imposed by regulation
    - Companies sometimes pay an "apology fine" based on the number of user accounts affected
  - Australia and New Zealand
    - Released guidance based on Canadian approach
    - Further legislation is under consideration

Step One: Pre-Breach Preparation

- Policies and procedures should dictate appropriate responses and reporting guidance
- Technology should be in place to detect activities (e.g., IDS, log correlation, security information management [SIM] platforms)
- Points of contact, including technical, management, and legal need to be documented
- Systems should be implemented with reliable logging and other mechanisms to provide a clear view of what happened
- Incident response teams, either internal or contracted, should be trained and ready to respond immediately

Step Two: Breach Discovery

- Treat suspected breaches as breaches
- Maintain tight but comprehensive communications loop
- Determine scope of event
- Ensure affected system owners are in the loop and are prepared to decide on actions to take
- Maintain detailed documentation of all events detected and any actions taken
- Prepare a list of options
- Attempt to confirm validity of breach and potential damage

Step Three: Breach Response

- **Act to contain problem**
  - Consider the nature of the affected asset
  - Decide whether a legal action will result
  - Determine likelihood of compromise extending to other assets
- **Ensure stakeholders are represented in all decisions**
- **Involve legal counsel and consider contacting law enforcement if serious enough**
- **Preserve all evidence to the extent possible**
  - Use proven computer forensics tools
  - Maintain chain of custody

Step Four: Breach Disclosure Discussion

- **What data are affected?**
  - Is personally identifiable information involved?
  - Is customer information involved?
- **Have sensitive data been accessed or downloaded?**
  - What do the log files say? Are they reliable?
  - Can the level of access be determined (e.g., number of affected customers)?
- **What damage could result?**
  - Will reputations be damaged?
  - Will compromised data harm affected subjects?
- **What is the timing and means of the disclosure?**
  - Are sensitive law enforcement investigations ongoing?
  - Would greater harm result from a disclosure?
  - Can the scope of the disclosure be limited?

Step Five: Breach Disclosure

- **Work with law enforcement (through legal counsel) to ensure timing does not affect investigation**
- **Work with legal counsel and communications on wording of notification**
  - Emphasize remediation that has been done
  - Provide concrete suggestions to affected parties to prevent fraud
  - Offer to compensate credit monitoring and other predictable costs
  - Avoid setting up for a blank check
- **Ensure announcement is made in a manner likely to reach affected parties**

Step Six: Dealing With the Fallout

- **Provide clear and concise explanations (e.g., web site notices, postal mail, e-mail, press releases)**
- **Ensure call centers are available**
- **Prepare for possible litigation**
  - Preserve all notes, data collected, logs, etc. and maintain chain of custody is maintained
  - Consider hiring outside litigation counsel
  - Explore options for offensive litigation
- **Consider long-term remediation programs, including**
  - Increasing investments in incident response and monitoring
  - Deploying automated patching and vulnerability scanning products
  - Providing additional user training on combating phishing and other social engineering attacks
  - Deploying technologies that enable you to segregate customer data and track activities on individual records

Final Considerations on Disclosure

- **Know your customers and their data**
  - Is it the type of data that are easily exploited?
  - Are you likely to lose them by disclosing?
  - Will you keep them if you disclose promptly?
- **Make sure you clearly define what a breach is ahead of time and draft guidance on when to disclose**
- **Ensure management, legal, and technology groups are all briefed on the process**
- **Consider identifying a breach response team in advance**
- **While breach laws are only effective if there are damages, consider whether notification is warranted for other reasons like reputational harm**
- **Consider data leak prevention technology to help identify the movement of sensitive data across the enterprise**

Wrap-Up

- **Questions?**
- **Contact Information**

SAIC
Gib Sorebo, JD, CISSP
AVP/Chief Security Engineer
sorebog@saic.com
tel. 703.676.2605