SNIA

Education

Data Breaches and the Encryption Safe Harbor

Eric A. Hibbard, CISSP, CISA
Hitachi Data Systems

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.
  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Abstract

Data Breaches and the Encryption Safe Harbor

As data breaches continue to plague organizations and the impacts to individuals increase, the statutory and regulatory responses become more severe. Nearly all states in the U.S. have passed data breach laws, which include costly breach notification requirements. The international community has adopted stringent privacy laws and some countries are now considering adding breach notification requirements as a further deterrent for organizations that haven't taken the requirements seriously.

This session explores the complexities and ambiguities associated with these breach laws, especially when encryption can serve as a safe harbor. Recent massive breaches and lawsuits will be used as case studies.

Encryption & Key Management Overview

A Few Definitions

- **Plaintext** – Original information (intelligible) that is used as input to an encryption algorithm (cipher).
- **Ciphertext** – The encrypted (unintelligible) output from an encryption algorithm.
- **Encryption** – The conversion of plaintext to encrypted text (ciphertext) with the intent that it only be accessible to authorized users who have the appropriate decryption key.
- **Cipher** – A mathematical algorithm for performing encryption (and the reverse, *decryption*).
- **Key** – A piece of auxiliary information used by a cipher during the encryption operation.

Encryption Introduction

- Goals of Encryption
  - Make data unintelligible to unauthorized readers
  - Make it extremely difficult to decipher data when attacked
- Factors to consider:
  - Strength of encryption (algorithm, key size)
  - Quality of encryption (sufficiently reviewed by experts; implementations subjected to accreditation)
  - Speed of encryption
  - Management of the persistent encryption keys
  - Randomness (use of random number generator)

Encryption Algorithms
(General Categories)

- **Symmetric-key Ciphers** (Secret-key Cryptography)
  - Uses the same key to encrypt and decrypt the data
  - Two types: block ciphers & stream ciphers
  - Block ciphers commonly used for storage
  - Generally much less computationally intensive than asymmetric-key ciphers
- **Asymmetric-key Ciphers** (Public Key Cryptography)
  - Use a pair of keys with a mathematical association that allows any data encrypted by one key to be decrypted only by the other.
  - Often used for authentication & digital signatures rather than encrypting data
- **Hashing Algorithms**
  - Does not encrypt data, but provides a one-way (non-reversible) transformation used to store data securely as well as to verify data integrity
  - Does not require the use of keys
  - The size of the value output by the hashing process is fixed

Key Management Introduction

- **Definition:** The *activities* involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction.

  -NIST SP 800-57 Part 1

- Appropriate and successful key management is critical to the secure use of *every* crypto system without exception.
- Considered the ***most difficult aspect of cryptography*** because of the human element (involves system policy, user training, organizational and departmental interactions, coordination between end users, etc.)

Major Key Management Operations

- **Generation** – Creation of fully random keys
- **Distribution** – Keys have to be adequately protected (encrypted) when they are transmitted over networks
- **Storage** – Keys are encrypted wherever they are stored on some form of media; decryption of one key should not expose others in the process
- **Recovery** – Ability to restore (e.g., from backup or escrow service) a key that has been lost or corrupted
- **Destruction** – Ability to permanently destroy an encryption key, rendering the encrypted data unusable

Key Management Guidance (1)

- A cryptographic key should be used for only one purpose.
- Use appropriate key wrapping (encryption of symmetric keys) when keys are transmitted and/or stored.
- Limit the amount of time a key is in plaintext form and prevent humans from viewing plaintext keys.
- Use a cryptographic integrity check on the keys.
- Use a minimum of 112 bits of security strength (no necessarily key size) for symmetric keys

Key Management Guidance (2)

- A symmetric data encryption key should be used no more than 2 years to protect (encrypt) data
- When data are retained as ciphertext for extended periods and/or the key may have been compromised, the data should be re-keyed (decrypted and then encrypted, using a new key)
- Have a compromise recovery plan in the event of a key compromise.
- Destroy keys, rather than expire, as soon as they are no longer needed.

Remember…

- Determining the primary driver for encryption is critical
- Classification of the organizational data can significantly improve the effectiveness of most encryption solutions
- Know (or be able to discover) where the data resides
- The "need" for encryption, combined with insufficient budget, often results in impacts to business processing
- Key management complexities are almost always overlooked, but they are critical success factors for the encryption solution
- Interoperability is not guaranteed, so attention to detail is important
- For all that encryption offers, it does not come for free
- If you can't prove encryption is operational, why bother

Data Breaches

What is a Data Breach?

- A ***breach*** is
  (1) the unauthorized acquisition, access, use, or disclosure of protected health information,
  (2) which compromises the security or privacy of such information.
  – U.S. HITECH Act

- A ***personal data breach*** "means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community".
  – EU ePrivacy Directive (EC Proposal)

- A ***data breach*** (a.k.a., *unintentional information disclosure*, *data leak* and also *data spill*) is the intentional or unintentional release of secure information to an untrusted environment.
  – Wikipedia

Data Breach Consequences

- Direct costs for notifications, customer service support, credit monitoring, customer incentives, restitution, card replacement, etc.
- Damage to the firm's reputation and brand
- Regulators impose fines and penalties, including jail time.
- Consumers flood the courts with class action lawsuits over breaches.
- Business partners may sue to recover the costs of responding to a breach.
- Investors may sue over stock losses.

Where Do Data Breaches Come From?
(2012 Verizon Data Breach Investigation Report)

Education SNIA

WHO IS BEHIND DATA BREACHES?

- **98%** stemmed from external agents (+6%)
- **4%** implicated internal employees (-13%)
- **<1%** committed by business partners (<>)
- **58%** of all data theft tied to activist groups

HOW DO BREACHES OCCUR?

- **81%** utilized some form of hacking (+31%)
- **69%** incorporated malware (+20%)
- **10%** involved physical attacks (-19%)
- **7%** employed social tactics (-4%)
- **5%** resulted from privilege misuse (-12%)

WHAT COMMONALITIES EXIST?

- **79%** of victims were targets of opportunity (-4%)
- **96%** of attacks were not highly difficult (+4%)
- **94%** of all data compromised involved servers (+18%)
- **85%** of breaches took weeks or more to discover (+6%)
- **92%** of incidents were discovered by a third party (+6%)
- **97%** of breaches were avoidable through simple or intermediate controls (+1%)
- **96%** of victims subject to PCI DSS had not achieved compliance (+7%)

Largest opportunities to reduce exposure to loss:

- Keyloggers and the use of stolen credentials
- Backdoors and command control
- Tampering
- Pretexting
- Phishing
- Brute force
- SQL injection

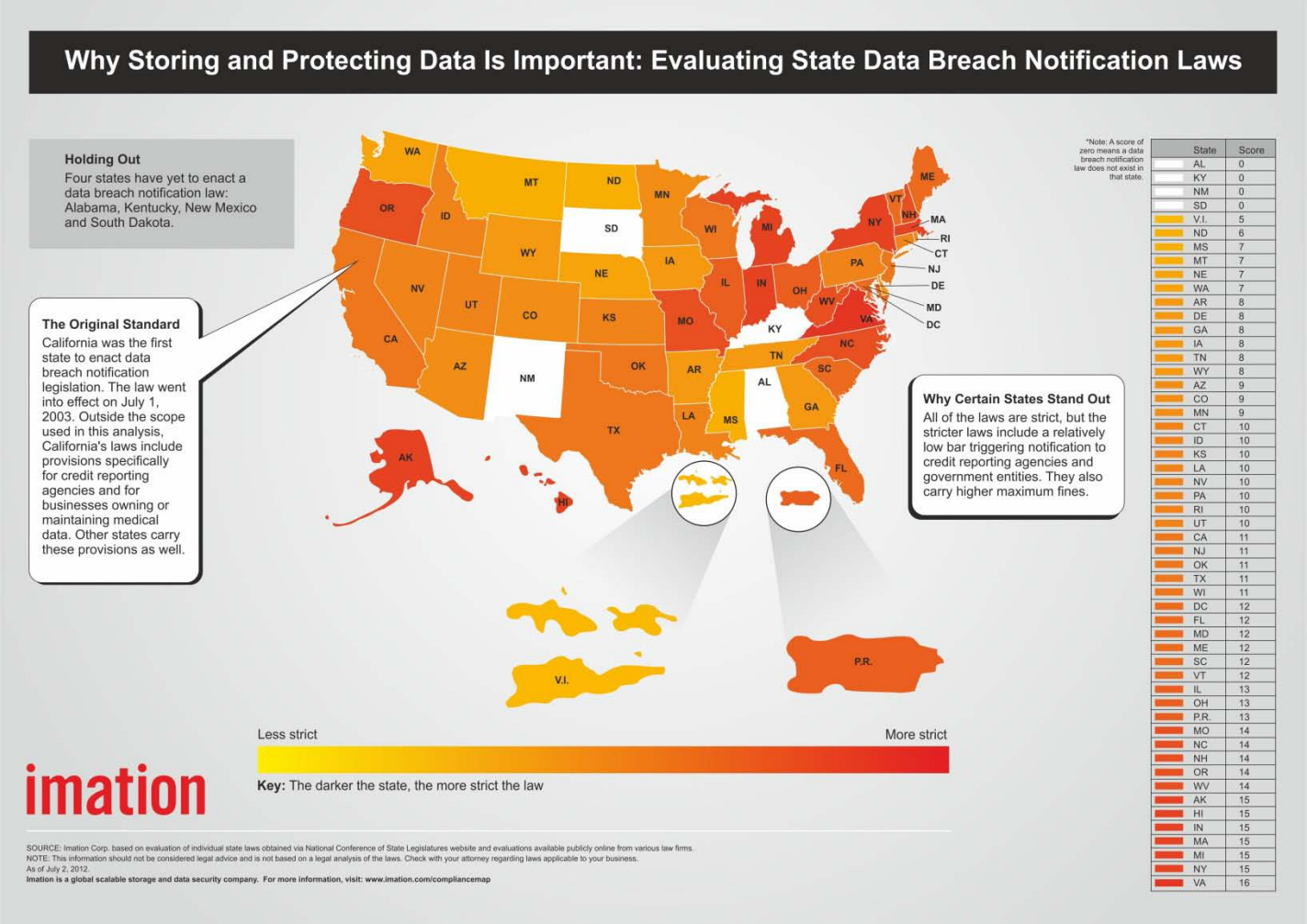
SOURCE: *2012 Data Breach Investigation Report,* Verizon Risk Team, June 2012, http://www.verizonbusiness.com/about/events/2012dbir/

Data Breach Notification
(U.S. Legal Requirements)

- Data breach laws cover sensitive information likely to be used for identity theft or fraud
- Triggering Event
  - Any breach of security (some states)
  - Breach with reasonable likelihood of harm (other states)
- Obligations on Breach
  - Notify persons whose information was compromised
  - Notify state enforcement agencies (some states)
  - Notify credit agencies (some states)
- Intended to incentivize proper security

SOURCE: RSA Conference 2012, Session: LAW-203, *Data Breach Laws: Will They Save or Sink You in a Massive Attack?,* February 2012

State Data Breach Notification Laws



SOURCE: *Imation Compliance Heat Map,* July 2012, http://www.imation.com/compliancemap

Data Breach Notifications
(Obligation Outside the U.S.)

- Statutes
- Official guidance
- Contract commitments
- Registration of a database
- Obligations to protect data
- Proactive steps may minimize harm
- Obligations to disclose sharing with third parties
- Commercial considerations

EU Commission Proposal (1)
(New Data Protection Regulation)

- Intended to replace the existing Data Protection Directive 95/46/EC
- A single set of rules that would apply across the 27 EU Member States
- Regulation instead of directive; individual countries cannot tailor it in any way
- Goals:
  - Update and modernize the existing EU data protection rules
  - Address the protection of personal data processed by law enforcement and judicial authorities
  - Give individuals more control over their personal data and facilitate access to and transfer of such data
  - Harmonize data protection rules across the EU

EU Commission Proposal (2)
(New Data Protection Regulation)

- Provisions of the proposed Regulation that are likely to have a significant impact:
  - Expansion of Definition of "Personal Data"
  - Express Consent Requirement to *Process* Personal Data
  - Breach Notification Requirement
  - Requirement to Adopt Policies and Implement Measures to Ensure and Demonstrate Compliance with the Regulation
  - Binding Corporate Rules (BCRs)
  - Data Security Obligations
  - Data Protection Impact Assessment Requirement
  - Requirement to Appoint Data Protection Officer
  - Significant Penalties
  - Transfers of Personal Data to Third Countries

Safe Harbor

What is Safe Harbor?

- A provision of a *statute* or a *regulation* that reduces or eliminates a party's liability under the law, on the condition that the party performed its actions in good faith or in compliance with defined standards.

  – Wikipedia

- For data protection regulations, safe harbor clauses are often used to entice organizations to do the right thing (i.e., actually protect the data).
  - Offer relief from costly notifications
  - Avoid characterizing a security incident as an actual data breach

International Safe Harbor Privacy Principles

- Streamlined process for US companies to comply with the EU Directive 95/46/EC on the protection of personal data.
- Designed to prevent accidental information disclosure or loss.
- US companies can opt into the program as long as they adhere to the following 7 principles:
  - **Notice** - Individuals must be informed that their data is being collected and about how it will be used
  - **Choice** - Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties
  - **Onward Transfer** - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles
  - **Security** - Reasonable efforts must be made to prevent loss of collected information
  - **Data Integrity** - Data must be relevant and reliable for the purpose it was collected for
  - **Access** - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate
  - **Enforcement** - There must be effective means of enforcing these rules
- After opting in, an organization must re-certify every 12 months.

Encryption – A Safe Harbor?
(Part 1)

- In the U.S., a significant number of the data protection laws include language about encryption
  - Almost 50% of the breach notification statutes provide no definition of encryption whatsoever
  - The other 50% use varying definitions of encryption
    - An algorithmic process that renders the data unreadable or unusable
    - An algorithmic process that results in a low probability of assigning meaning to the data
    - A 128 bit or greater algorithmic process that results in a low probability of assigning meaning to the data
    - Another method that renders data unreadable or unusable
    - A method specified by a regulator

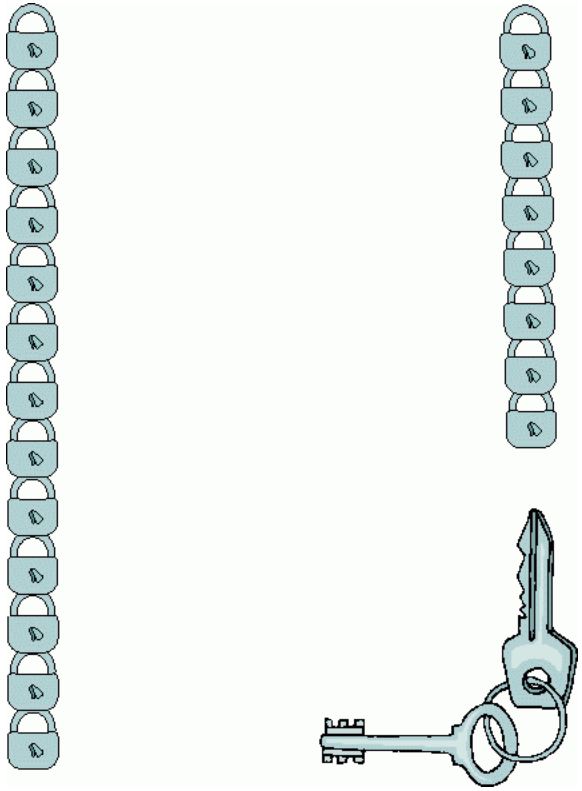
SOURCE: RSA Conference 2012, Session: LAW-203, *Data Breach Laws: Will They Save or Sink You in a Massive Attack?,* February 2012

Encryption – A Safe Harbor?
(Part 2)

- Many data breach laws define "breach" to exclude data that is encrypted according to the definitions in the particular law
- In a possible breach situation (incident), one has to determine:
  - what data are affected
  - whether the data are protected under the breach law
  - whether the individuals whose data were affected by the incident need to be notified in a breach
  - how the breach occurred
  - whether the affected data was actually encrypted
  - whether the encryption is in accordance with the applicable definitions of "breach" and "encryption"
- If the data are covered by an applicable data breach notification law, and the organization that was breached can prove the data were encrypted in accordance with the definition of "breach" in the law, then the safe harbor applies and notification is not required

Consult appropriate legal counsel!

When is Encryption Not a Safe Harbor?



- Encryption Keys
  - Inadequate/inappropriate key management can result in data breaches and/or loss of data
  - If the encryption key is compromised the protection is lost
- Security Lapses
  - Encryption must be implemented properly
  - When information is encrypted, notification is not required; but all data must be protected

SOURCE: RSA Conference 2012, Session: LAW-203, *Data Breach Laws: Will They Save or Sink You in a Massive Attack?,* February 2012

Final Thoughts

Action Plan to Prevent Data Breaches

- Conduct a risk assessment – security controls must address all risks in the risk assessment
- Develop a comprehensive information security plan specifically designed to prevent data breaches
- Develop a data retention and destruction plan so personal data is not at risk – sanitize regularly
- When information is encrypted, notification is not required; but all data must be protected (e.g. TJX, Heartland)
- Match the encryption solution to the risk
  - Strength of security (DES versus AES; ECB versus XTS)
  - Approach of encryption solution (self-encrypting drives, file-level encryption, etc.)
  - Pedigree/certification of encryption (Common Criteria, FIPS 140)
- Data classification (even rudimentary) will help guard against over-protection (cafeteria menu) or under- protection
- Compliance-driven encryption necessitates proof-of-encryption capabilities
- Inadequate/inappropriate key management can result in data breaches and/or loss of data

SOURCE: *Data Breach and Encryption Handbook*, Lucy Thomson, February 2011, American Bar Association, ISBN: 978-1-60442-989-3

Summary

- Data protection regulations (with data breach clauses) are prevalent throughout the world
- As data breaches continue, countries try to find ways to ***incentivize*** better security controls and practices
- Many countries are beginning to follow the U.S. lead in adopting breach notification provisions
- Encryption and key management are important tools to help guard against data breaches, and may be a safe harbor in the case of a data incident
- **Always** consult appropriate legal experts to ensure compliance with data protection regulations

SNIA Security Organizations

- SNIA Security Technical Work Group (TWG)
  - Focus: Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
  - http://www.snia.org/tech_activities/workgroups/security/
- Storage Security Industry Forum (SSIF)
  - Focus: Educational materials, customer needs, whitepapers, and best practices for storage security.
  - http://www.snia.org/ssif

Attribution & Feedback

The SNIA Education Committee would like to thank the following individuals for their contributions to this Tutorial.

Authorship History

Eric A. Hibbard – September 2012

Updates:
N/A

Additional Contributors

SNIA Security TWG

Lucy Thomson, Esq.
Tom Smedinghoff, Esq.
Dr. Robert Thibadeau
Dr. Michael Willet
Greg Farris

Please send any questions or comments regarding this SNIA Tutorial to
tracktutorials@snia.org