# *Beyond PCI DSS: State and Federal Data Regulation*

*Dr. Heather Mark, PhD, CPISM, CISSP, CIPP*
*Exec. Dir. Society of Payment Security Professionals*



Society of Payment Security Professionals

# Agenda

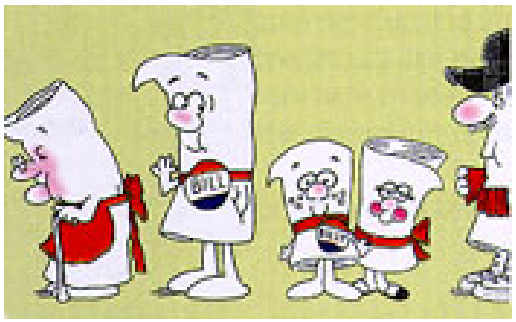
- Brief Overview of the Policy Process
  - *Why does Government Get Involved*
- Current Environment
  - *Breaches, Identity Theft and Public Perception*
- Limitations of PCI DSS
  - *Limited Focus, Static Standard*
- State & Federal Regulations
  - *Protected Data, Protections Required*
- Addressing Regulation through IT Governance




Society of Payment Security Professionals

# Policy Process

- Three Relevant Theories of Public Policy at Play
  - *Issue Attention Cycles - the more the public pays attention, the more likely legislators are to pay attention*
  - *Incrementalism - nothing new in public policy; legislation by baby step*
  - *Punctuated Equilibrium - crisis leads to rapid legislation containing significant changes*



Listen to those Congressmen arguing! Is all that discussion and debate about you?
-Schoolhouse Rock, "I'm Just a Bill."

http://www.school-house-rock.com/Bill.html




Society of Payment Security Professionals

# Theories in Practice

- In applying the Theory:
- Issue Attention Cycle
  - *We are squarely in the "Alarmed Discovery Stage"*
- Incrementalism
  - *Have used this theory in creating a sectoral, piecemeal privacy lattice*
  - *Privacy and security regulation leaves serious gaps in some areas and overlaps in others*
  - *Government has tried to extrapolate existing legislation rather than creating new policy*
    - *Federal Trade Commission Act §5a*
- Punctuated Equilibrium
  - *Knee-jerk reactions at the state level include breach notification laws, among others*




Society of Payment Security Professionals

# Government Involvement in Privacy

- **“ The right to be let alone...”** **-Samuel Warren and Louis Brandies**
- Definition has shaped public policy towards privacy since the early 20th century
- Public Policy was not *(still is not)* equipped to deal with “the connected” world in which data serves as currency
- Public policy typically deals with traditional privacy issues
  - *telephone conversations*
  - *photographs*
- Result is a sectoral approach to data privacy




Society of Payment Security Professionals

# *Why Does Government Care?*

- Consumer Privacy
  - *government does not care if websites are vandalized, but if customer privacy is compromised*
- Consumer Confidence
  - *uncertain consumers become infrequent consumers - witness current economic situation*
- Unfair and Deceptive Trade Practices
- Privacy of Children

# *Current Data Environment*

- Recent reports indicate that data breaches have increased almost 50% over the previous year
- Organized criminal enterprises targeting repositories of personal information
  - *Payment card information AND personally identifiable information are equally vulnerable and equally targeted*
- Identity theft and financial fraud are growing concerns
  - *media has put forth the idea that payment card fraud is equivalent to identity theft*
- Focus on standards instead of addressing risk




Society of Payment Security Professionals

# *Limitations of PCI DSS*

- PCI DSS is a catalyst for what should be the larger discussion surrounding the protection of consumer data, but not the mechanism for complete protection
- Focus is solely on payment card information
  - *Failure to look beyond payment card information increases risk of exposure of personal information*
- Static Standard in a Dynamic Environment
  - *Any static, prescriptive standard is necessarily limiting*
  - *infrequent updates mean compliance does not always address risk*
- Compliance with PCI DSS may not mean compliance with laws




Society of Payment Security Professionals

# State & Federal Legislation

- State Breach Notification Laws
- Minnesota Plastic Card Security Act
- Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth
- Nevada Encryption Law
- Proposed State Laws and Amendments
- Federal Trade Commission Act

# State Breach Notification Laws

- More than 45 states now have breach notification laws
  - *many important definitions vary from state to state*
    - ***"trigger," "notification," "breach"***
- Require notification of affected individuals in the event of a compromise (or suspected compromise) of Personally Identifiable Information (PII)
- Common definition of PII includes:
  - *First name or initial and last name in conjunction with*
    - ***social security number***
    - ***driver's license number or state ID number***
    - ***financial account number, credit or debit card number and password or PINs that will allow someone to access the account***
- It is possible to have an Account Data Compromise under PCI DSS that does not invoke state breach notification requirements and vice versa




Society of Payment Security Professionals

# *Minnesota Plastic Card Security Act*

- Codifies card brand prohibition on storage of sensitive authentication data
- Impacts anyone “doing business in the state of Minnesota”
- Those found in violation of the law can be held accountable according to the following
  - *processing more than 20,000 transactions annually - can be held responsible for re-issuance costs, notification costs, damages paid to affected consumers and private right of action*
  - *processing fewer than 20,000 transactions annually - can be held accountable to private right of action*
- Holds merchants accountable for compliance of their service providers




Society of Payment Security Professionals

# *MA Data Protection Law*

- Recent Accompaniment to the MA data breach law
  - *note that MA defines compromise as an exposure of data that includes first name (or initial) and last name in conjunction with ssn, driver's license numbers or account numbers. It does not require the exposure of passwords or account access codes.*
- Effective date recently extended from Jan 1, 2009 until May 1, 2009 (same date as Red Flag clause extension)
- Most prescriptive state level data protection requirements to date
- Applies to any company storing data on any MA Resident




Society of Payment Security Professionals

# MA Security Requirements

| Security Program Requirements | System Security Requirements |
|---|---|
| Data Inventory | Encrypt personal information stored on laptops and portable devices, transmitted wirelessly or over public networks |
| Limits on Data Retention | Secure user authentication protocols, access control measures, and unique user ids |
| Restrict Access to Need to Know | Monitor systems for unauthorized access or use of personal information |
| Contractually Obligate Service Providers | Anti-virus and patching must be “reasonably up-to-date” |
| Develop, Document, Implement Security Policies - impose penalties for violations | Firewall must be “reasonably up-to-date” |
| Document Response to Security Incidents | Employee Training |

# Nevada Encryption Law

- Nevada passed law last year, became effective October, 2008
- Requires **ALL TRANSMISSIONS** of personal data outside the "secure systems of the business" to be encrypted
- Personal Data is defined as "first name or initial and last name in conjunction with financial, credit or debit card account and password or other security code that would allow access to those accounts."
- NV Definition of Encryption
  - *"any protective or disruptive measure including but not limited to cryptography, enciphering, encoding, or a computer contaminant to (1)prevent, impede, delay or disrupt access to any data...(2)cause or make any data, information, image, program, signal or sound unintelligible or unusable or (3)prevent, impede, delay or disrupt, the normal operation or use of any component, device, equipment, system or network."*

# *Proposed Laws & Amendments*

- PCI DSS-related Laws
  - *Florida, Michigan, Indiana, Washington, Texas and others proposing legislation that would codify parts of PCI DSS*
- California Proposed Amendment to Breach Law
  - *breaches affecting more than 500 individuals to be reported to state AG*
    - ***reports indicate that less than 10% of breaches are being reported***
  - *specify what must be included in breach notification to individuals*
  - *Recently amended to include health care information*




Society of Payment Security Professionals

# Federal Legislation - FTC

- Federal Trade Commission §5A
  - "The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations...*from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."* – 15USC§45(a)(1)
- *How is it used in the context of a data breach?*
  - *Posting a privacy policy and failing to adhere to that policy is a deceptive practice*
  - *"information practices that cause substantial harm to the consumer" are unfair practices*
- FTC can require a number of actions in the wake of a data compromise
  - *injunction on business practices*
  - *penalties, customer redress*
  - *government oversight of information security and privacy programs for up to 20 years*




Society of Payment Security Professionals

# Compliance First or Security First?

- Managing compliance with state, federal and industry regulation is like fighting the hydra
  - *Chasing compliance is a haphazard, inconsistent approach to data protection*
- Prioritized Approach? - Start with protecting the data
  - *protect from the inside out*
  - *address security through a strong IT governance program that addresses all classes of regulated data*
    - *Risk analysis - design and implement controls commensurate with the risk in your environment*
    - *Regularly test and monitor for new vulnerabilities and respond to new potential exploits*
      - *ex - we know that malware is capturing data in transit over internal networks, so encrypt traffic on the internal network*
- **Compliance alone is NOT enough to protect data**

Image "Hydra" created on 08 June 1997; last modified on 05 December 1999. http://www.pantheon.org/areas/gallery/mythology/europe/greek_people/hydra.html © MCMXCV - MMVI Encyclopedia Mythica™. All rights reserved.




Society of Payment Security Professionals

# *IT Governance and Compliance*

- Security is Compliance, but compliance is not always secure
  - *any given, prescriptive standard is static and therefore somewhat lacking in proactive controls and processes*
- Compliance alone does not account for the objectives and needs of the business
- IT Governance
  - *Supports Business Objectives (financial, compliance, etc)*
  - *Involves Cross-Functional teams of executives, managers, etc*
  - *Controls Risks*
  - *Enhances Performance/Operations*




Society of Payment Security Professionals

# Conclusions

- Rate of new regulation makes chasing compliance detrimental to security, IT operations and business objectives
- Compliance alone is not enough to protect data from exposure or your company from liability
- Regulation is a fact of life and it's better to be proactive than reactive
- Robust IT Governance can help achieve
  - *Security*
  - *Compliance*
  - *IT Risk Management*




Society of Payment Security Professionals