David Mortman

CSO-in-Residence, Echelon One, LLC

How to Navigate Regulations Both in the U.S. and Abroad

Today We'll Talk About

- U.S. state regulations
- The possibility of a federal law
- Overseas initiatives
- Tackle compliance using a multidisciplinary approach
- What's next?

State Legislation

- CA1386 Started It All
- As of 10/15 39 states have similar laws
- AB779 almost passed in California last month
  - Would have legally codified PCI

State Privacy Guides

- Scott and Scott, reference chart

http://www.scottandscottllp.com/resources/state_data_breach_notification_law.pdf

- Perkins, Coie summary of laws

http://www.digestiblelaw.com/files/upload/securitybreach.pdf

- Proskauer Rose, listing of laws

http://privacylaw.proskauer.com/2007/08/articles/security-breach-notification-l/breach-law-data/

Federal Legislation

- Several Disclosure laws have been proposed
  - So far all have stalled or died in committee
- GLBA
- HIPAA
- Patriot Act, FISA, CALEA
- PCI
  - Vendors pushing back on storage requirments

European Legislation

- European Data Directive
  - Google being investigated
  - UK Data Storage Law
- Belgium - not just data, but also video
- Canada
- Japan
- Australia
- Asia-Pacific Economic Cooperator

Making It All Work

- You need to understand the business
  - Where does it operate?
  - How does the money flow?
  - Where does the data go?
  - Leverage compliance efforts
- Partner
  - Legal
  - HR
  - Sales
  - Alliances

www.unifiedcompliance.com

Control Objectives	Sarbanes Oley	PCAOB	SAS 94	Basel II	Gramm Leach Bliley	Append of 12 CFR 30	FFIEC Information Security	FFIEC Development Acquisition	FFIEC Business Continuity Planning	FFIEC Audit	FFIEC Management	FFIEC Operations	HIPAA	CMS CSR
Monitoring and Measurement	§ 104	§ 49		¶ 689	4(e)						Pg. 33			
Establishing overall monitoring and logging operations			§ 319.53				Pg. 82						.308(a)(1)(ii)(D)	
Key concepts							Pg. 78-79							
Measurement		§ 13												
Traceability														
Thoroughness	§ 104(d)	§ 13												
Frequency	§ 104(b)													
Collecting Logs and Monitoring Data			§ 319.54				Pg. 64				Pg. 33	Pg. 22	.312(b)	
Initialization of the audit logs							Pg. 64-5							
Ensure that it is impossible to disable an audit log														
All accesses to personally identifiable data														
All actions taken by any individual with root or administrative privileges														
Access to all audit trails														
Audit logs must contain timestamp which tracks user activity														
Use of identification and authentication mechanisms														
Invalid logical access attempts							Pg. 39							
Review audit logs and IDS reports regularly							Exam Tier II Q C.8						.308(a)(1)(ii)(D)	§ 1.2.1, 1.6.1, 2.1.6, & 4.2.4
Creation and deletion of system level objects														
Assessing Performance		§ 7, 13												
Assessing Customer Satisfaction											Pg. 18	Pg. 39		
Management Reporting and logging	§ 404(b)			¶ 701				Pg. 6			Pg. 24	Pg. 38		

What Next?

- What does the future look like?
- UK pushing for data breach laws
- More US vendor PCI pushback
- Leahy-Specter ID Theft Bill

Q&A

David Mortman

CSO-in-Residence, Echelon One, LLC

How to Navigate Regulations Both in the U.S. and Abroad