ISACA®
Trust in, and value from, information systems
San Francisco Chapter

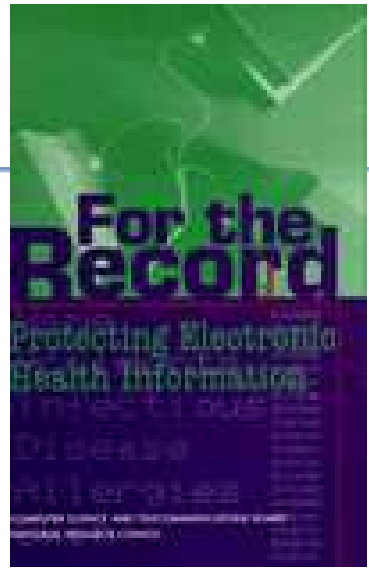
G23- **Lessons Learned: Hard Data from 300 Breaches**

Ann Geyer
Chief Privacy and Security Officer
University of California, Berkeley
ageyer@berkeley.edu

Topics

- Enforcement Trends in Privacy, Security, and Breach Notifications
- Lessons Learned from the Ten Years of HIPAA Breach Cases

1996 Institute of Medicine Study



- Impetus for HIPAA privacy & security standards
- Argued that industry practices were insecure
- Intervention required to 'gauge the vulnerability of electronic health information'
- Called for funding an organization and mechanism to share information about the types of attacks and breaches of health information security

Health Data Breach Report Requirements

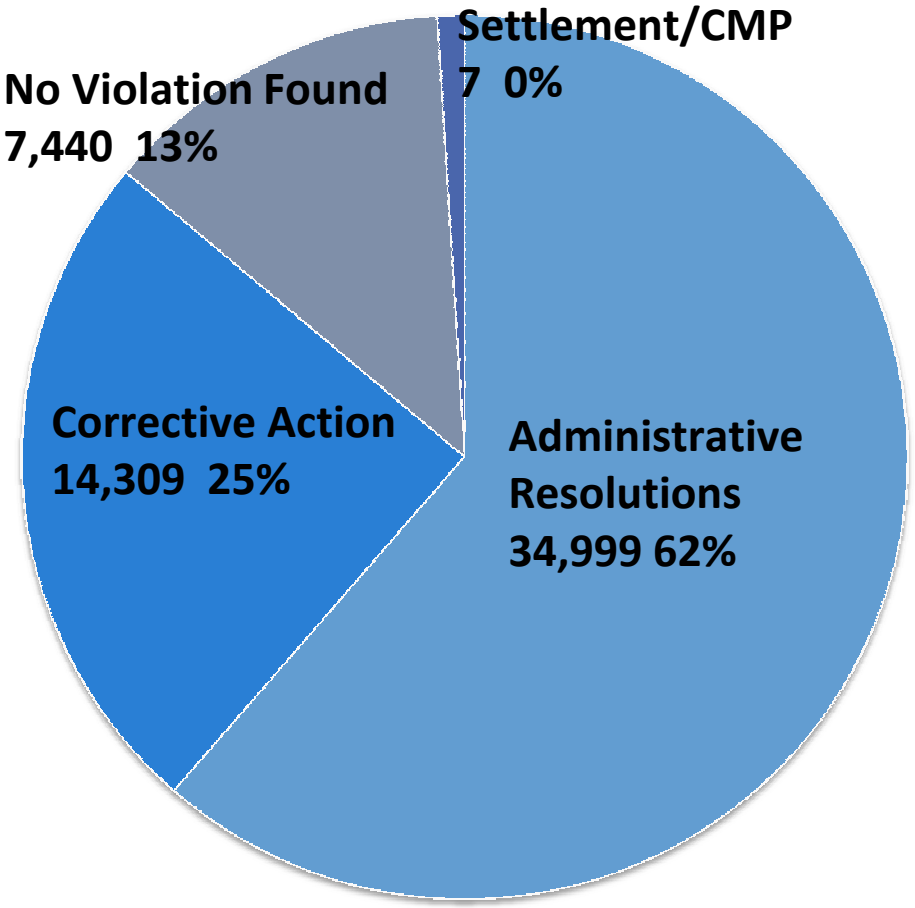
- HITECH -- Health Information Technology for Clinical & Economic Health Act of 2009
  - Mandates that breaches of health information involving more than 500 persons be reported
  - Something less than the incident database recommended by the IOM report
  - Limited data required in the standard report
- CA Breach Notification Law (SB1386)
  - Any breach of electronic data that includes Name, SSN, CC#, CDL, Financial account access data or Medical data

Penalties are Rising; Expectations Strict

- Healthcare Regulations
  - Pre-HITECH:
    - Maximum $100 per violation
    - $25,000 for identical continuing violations
  - Post-HITECH:
    - Minimum $100; Maximum $50,000 or more per violation
    - $1.5 million for identical continuing violations
  - Annual caps are per type of violation
    - Frequently multiple violations
    - 42 Security Rule standards and implementation specifications - $63 million per year
- FTC complaints of unfair practices
- State Attorneys General

Privacy Rule Resolutions

April 2003 to August 2011



Complaints Received:
63,443

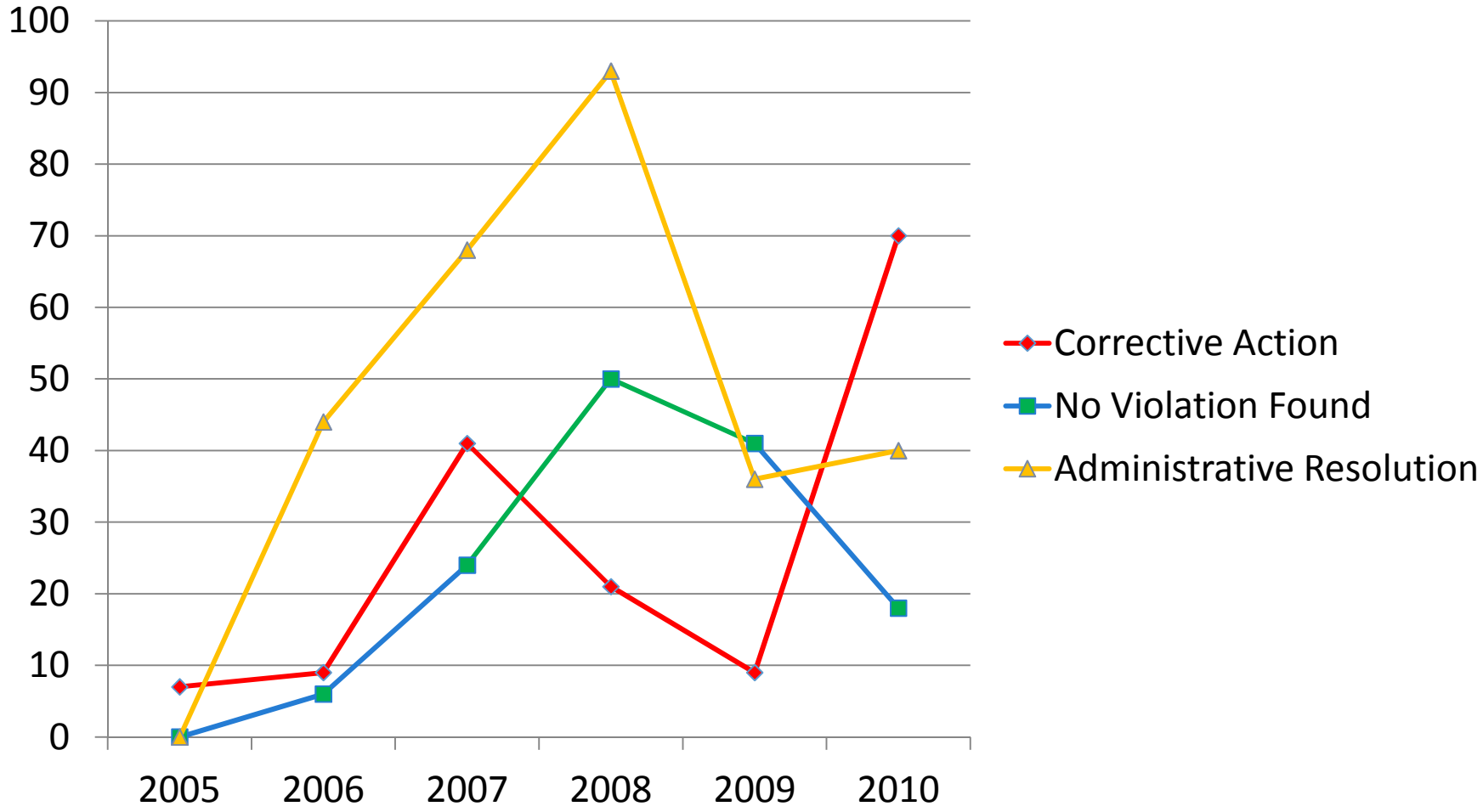
Complaints Resolved:
57,748 (91%)

Top Findings

1. Impermissible uses and disclosures
2. Lack of safeguards
3. Failure to provide access to individual
4. Use or disclosure of more than minimum necessary
5. Failure to provide notice of privacy practices

Security Rule Resolutions

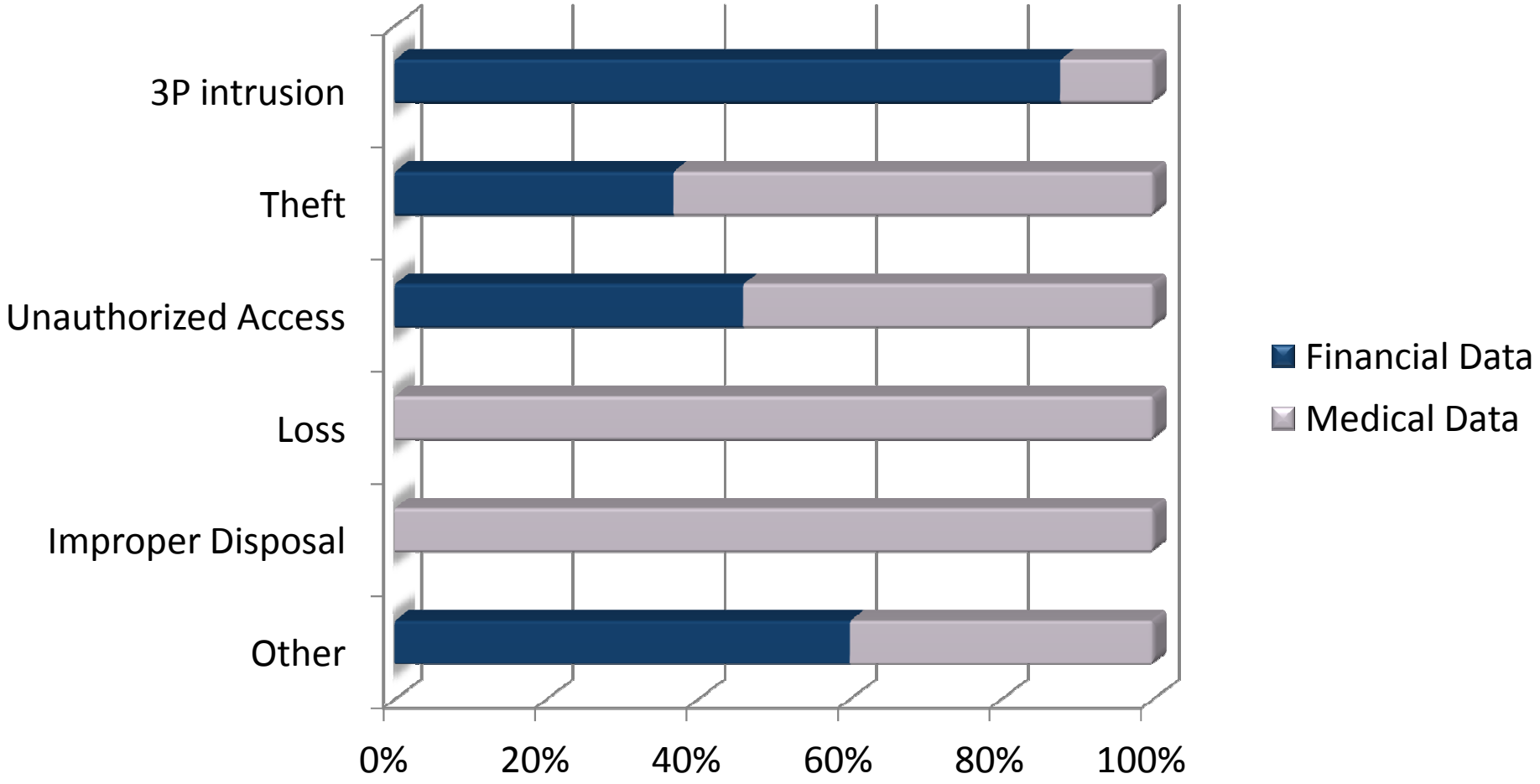
April 2005 to December 2010



Top Security Findings

1. Lack of security incident procedures
2. Lack of security awareness and training
3. Lack of access controls
4. Lack of information access management
5. Lack of workstation security

Financial vs Medical Breaches



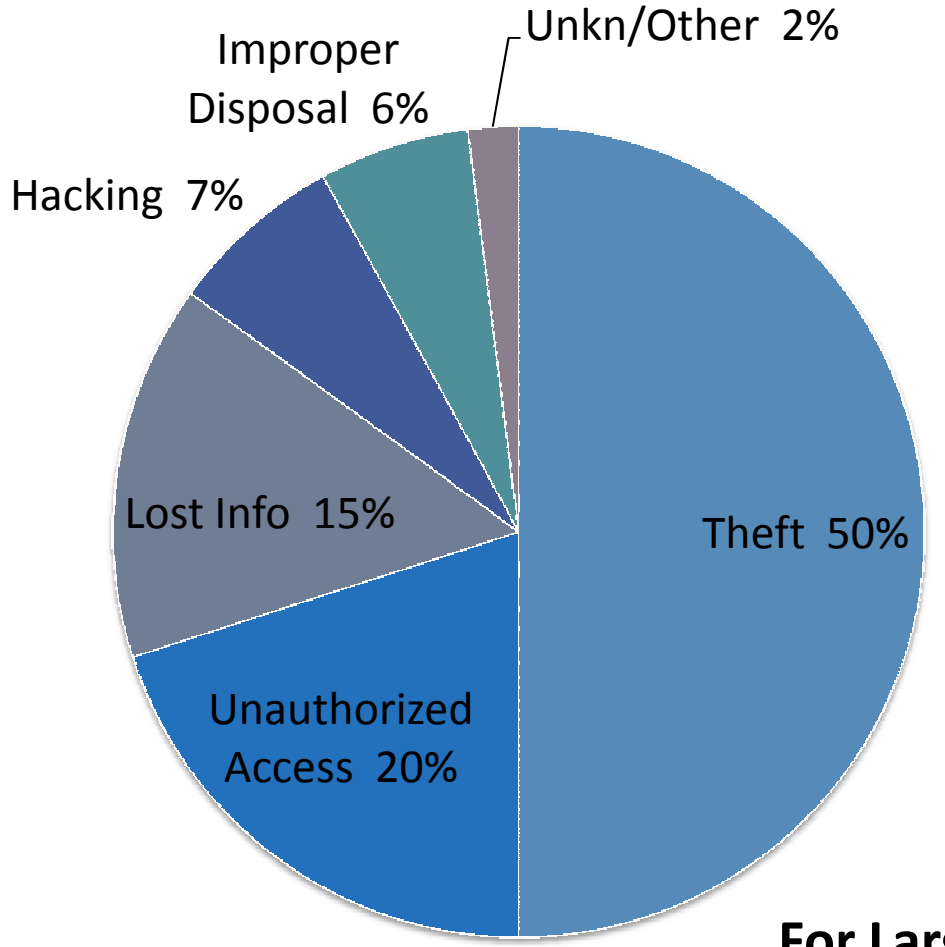
ISACA
Trust in, and value from, information systems
San Francisco Chapter

Back to Business

2011 Verizon Data Breach Report
2010 OCR Report to Congress

Breach Reports by Root Cause

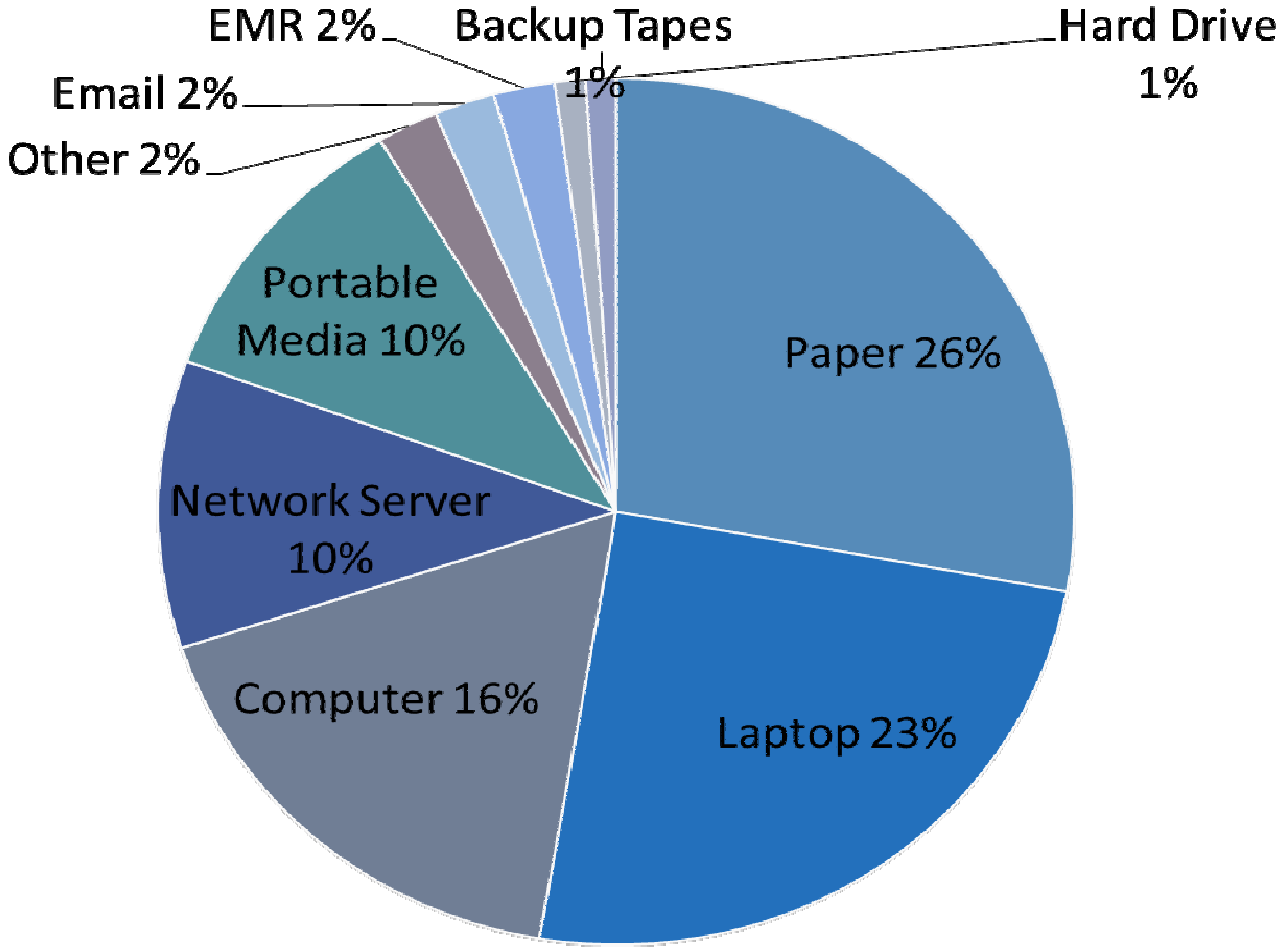
Sep 2009 to Sep 2011



For Large Breaches (>500)

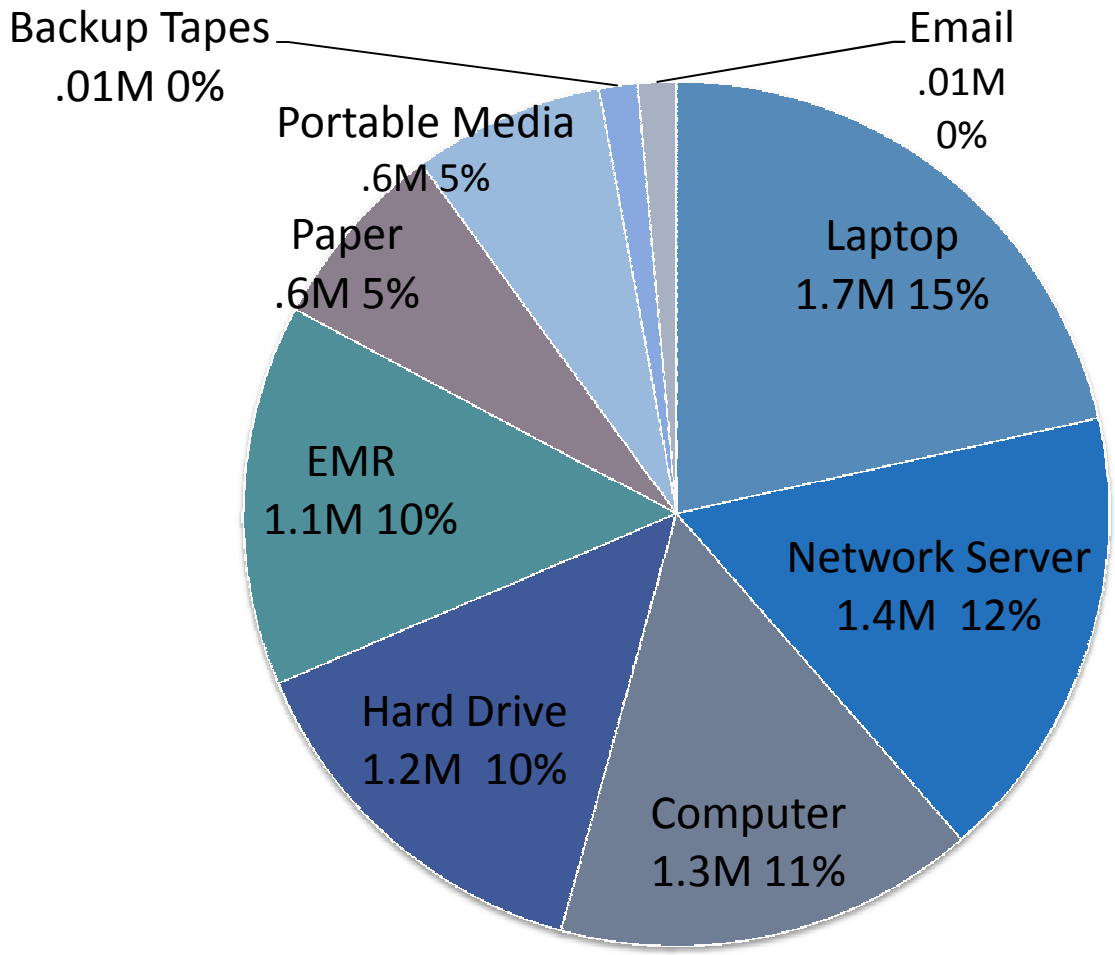
Breach Reports by Media Type

Sep 2009 to Sep 2011

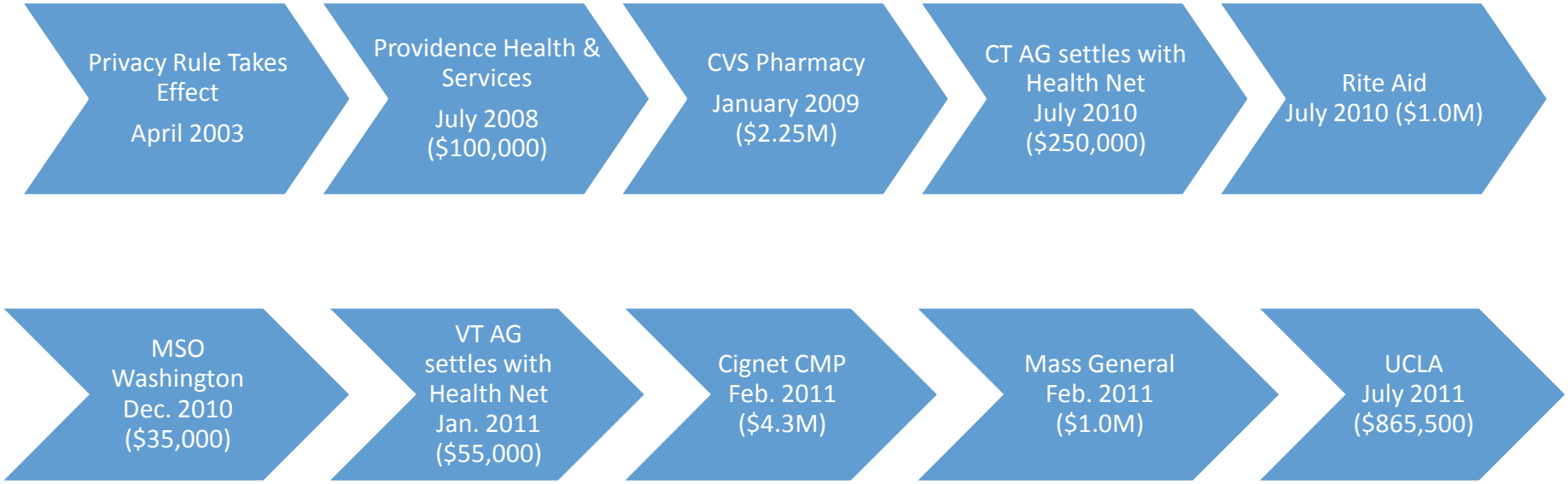


Breach Reports by Number of Individuals

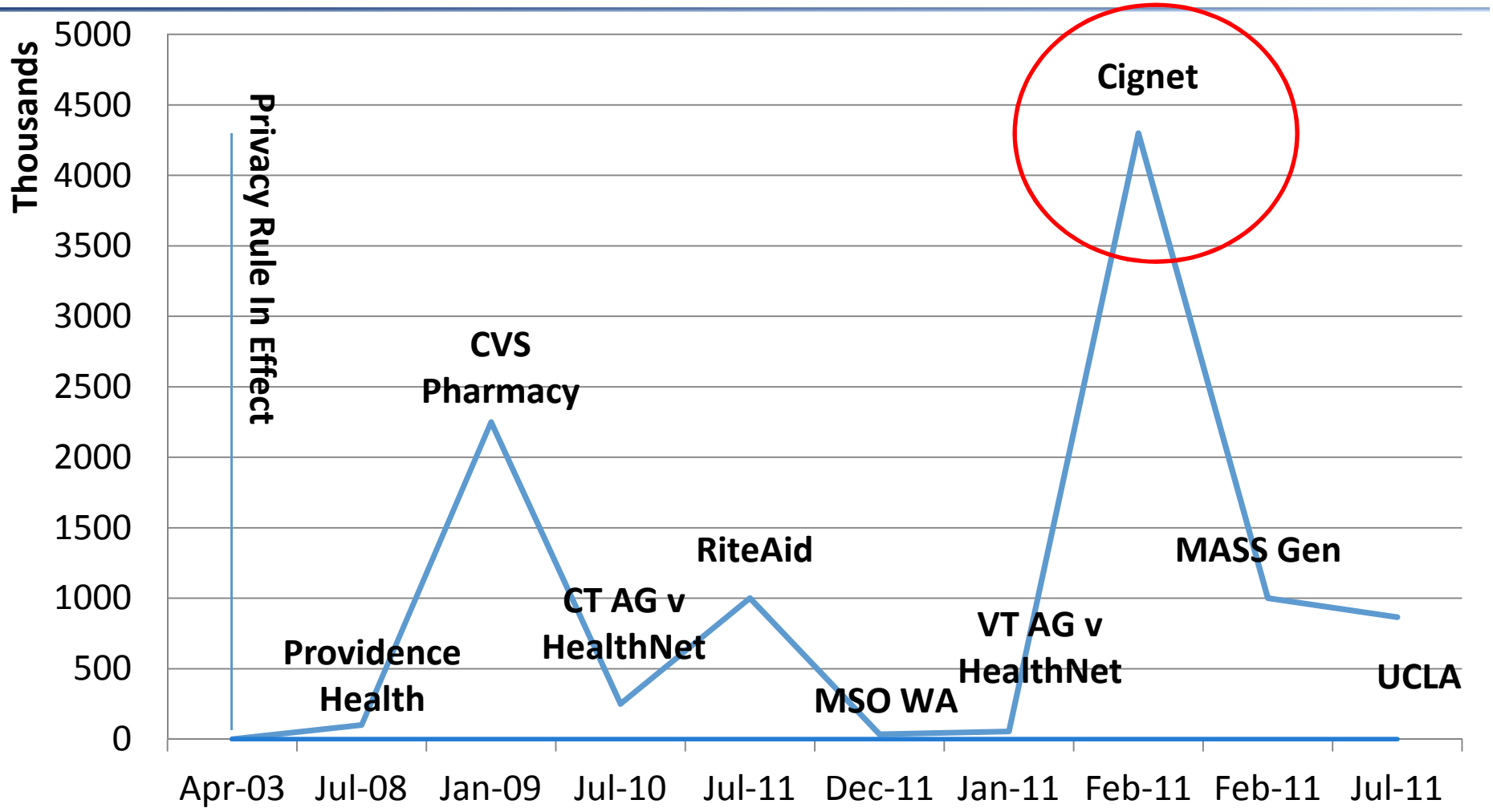
Sep 2009 to Sep 2011



Increase in Settlements/CMPs



Increase in Settlements/CMPs



Issues leading to Settlements/CMPs

- Providence ($100,000, 3-year CAP, int. monitoring)
  - Loss of backup tapes/laptops (over 350,000 affected)
  - Backup tapes/laptops left unattended/unsecured
  - Significant news story
  - OCR/CMS settlement

- CVS/Rite Aid ($2.25 million/$1 million, ext. monitoring)
  - Improper disposal of prescriptions/pill bottle labels
  - Policy on proper disposal was not working
  - Several TV news stories
  - OCR/FTC settlement

Issues leading to Settlements/CMPs

- Management Services Organization of Washington ($35,000, 2-year CAP, int. monitoring)
  - Improper disclosure to affiliate for marketing
  - Small provider
  - Part of a false claims action
  - Joint DOJ/OIG/OCR settlement

- Cignet Health ($4.3 million CMP)
  - Failure to provide patients with records and
  - Failure to cooperate with OCR investigation

Issues leading to Settlements/CMPs

- Health Net
  - Portable hard drive lost with 1.5M patient records
  - Six-month delay in notifying individuals (pre-HIPAA breach rule)
  - Significant news story
  - Connecticut & Vermont AGs settled

- Massachusetts General ($1 million, 3-year CAP, int. monitoring)
  - Loss of 192 paper records
  - Included HIV information
  - Alleged overall issues with policies on transport of records offsite
  - Significant news coverage

Issues leading to Settlements/CMPs

- UCLA ($865,500, 3-year CAP, ext. monitoring)
  - Impermissible viewing of PHI
  - Involved celebrity records
  - Significant news story
  - Also led to criminal convictions

California Department of Public Health

- CMP for quality of care
  - *Failure to comply with state licensing requirements caused, or was likely to cause, serious injury or death to patients.*
  - Penalties
    - Class B $ 100 — 1,000
    - Class A $ 2,000 — 20,000
    - Class AA $25,000 — 100,000
- CMP for data breach
  - *Breach of medical data*
  - Penalties
    - Administrative $25,000 for a single breach (individual)
    - Additive $17,500 for subsequent breaches

Sub-standard Care	Penalty
Medication error	$50k
Medication error	$50k
Patient fell and was injured	$50k
Error led to second surgery	$50k | $75k
Error lead to hospital admission	$50k
Error led to extended hospital stay	$100k
Error lead to patient death	$75K
Error led to patient death	$80k - $100k

Data Breach Penalty	# Records	# Empl/ # Occasion
$5k	1	2/3
$25k	1	1
$60k	1	1/3
$42.5k	1	1/2
$75k	3	1
$100k	33	17
$125k	5	1
$130k	1	7
$225k	9	1
$250k	204	1
$250k	596 (theft)	

Issues Leading to Data Breach Penalties

- Failure to set policy
- Failure to follow policy
- Failure to detect a violation or take immediate preventative action
- Repeated violations

Breach Notifications lead to regulatory investigations and penalties

- Federal triggers:
  - Large repositories of records
  - Sensitive records (including VIPs)
  - Potential for employees to create large repositories of records
- State triggers:
  - Any unauthorized use or disclosure

Lessons

- Stay off the front page
  - Breach reporting makes this impossible
- Errors occur
  - Not an acceptable excuse
  - Policies are not enough, they need to work
  - Increase preventative methods or implement aggressive monitoring
  - Weed out systemic problems
- Go after a culture of privacy