Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Security Lessons Learned from HIPAA Enforcement

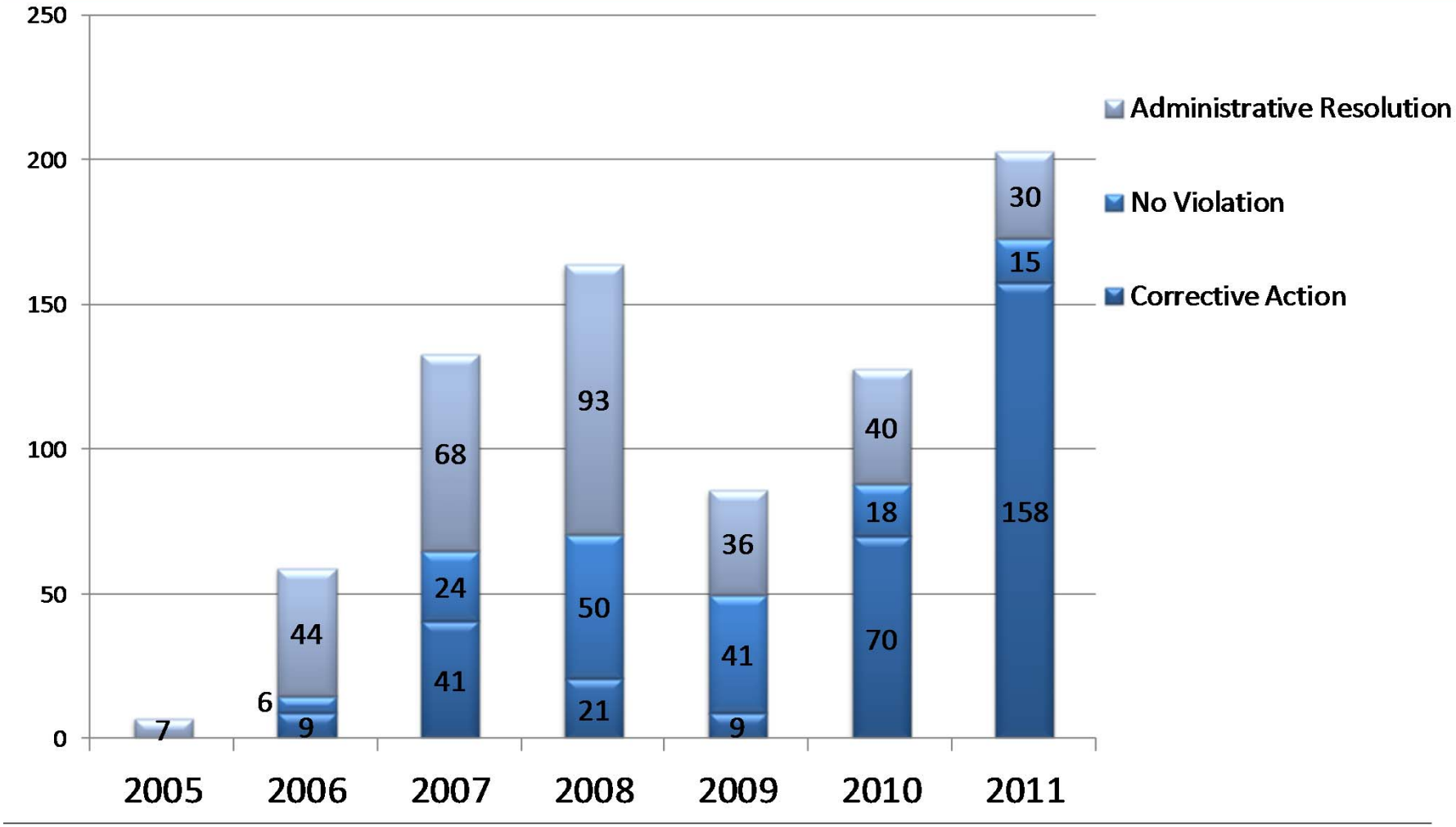
Presentation to HealthSec '12
August 7, 2012

Adam H. Greene, J.D., M.P.H.
Partner, Davis Wright Tremaine

Enforcement of the Security Rule

- HIPAA Security Rule published in 2003 with compliance date of April 2005.
- Initially enforced by HHS Centers for Medicare & Medicaid Services (CMS)
- HHS Office for Civil Rights (OCR) took over enforcement in July 2009

Security Rule Closures
(April 2005 to December 2011)



Davis Wright Tremaine LLP

Top Security Issues
(April 2003 to 2009)

1. Lack of information access management
2. Lack of access controls
3. Lack of security awareness and training
4. Lack of security incident response and reporting
5. Lack of device and media controls

Top Security Issues (2011)

1. Lack of risk analysis
2. Lack of security incident response and reporting
3. Lack of security awareness and training
4. Lack of access controls
5. Failure to address encryption and decryption (data in storage)

Overview of Breach Reports

- 452 large breaches reported between Sept. 2009 and June 2012
- Over 50,000 small breaches reported in same period
- Over 20 million individuals affected by large breaches

Lesson 1:

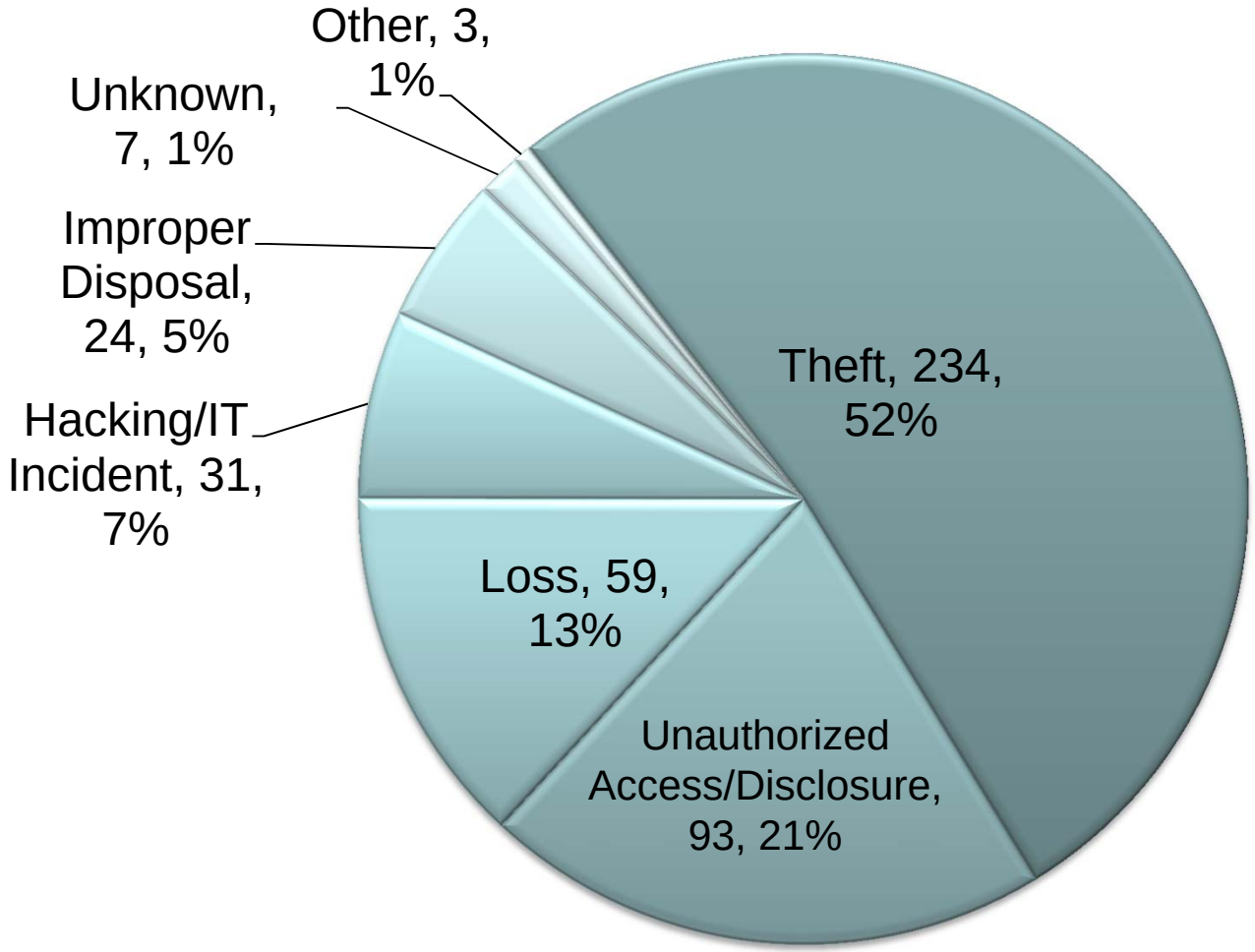
You should be less concerned with:



And more concerned with:

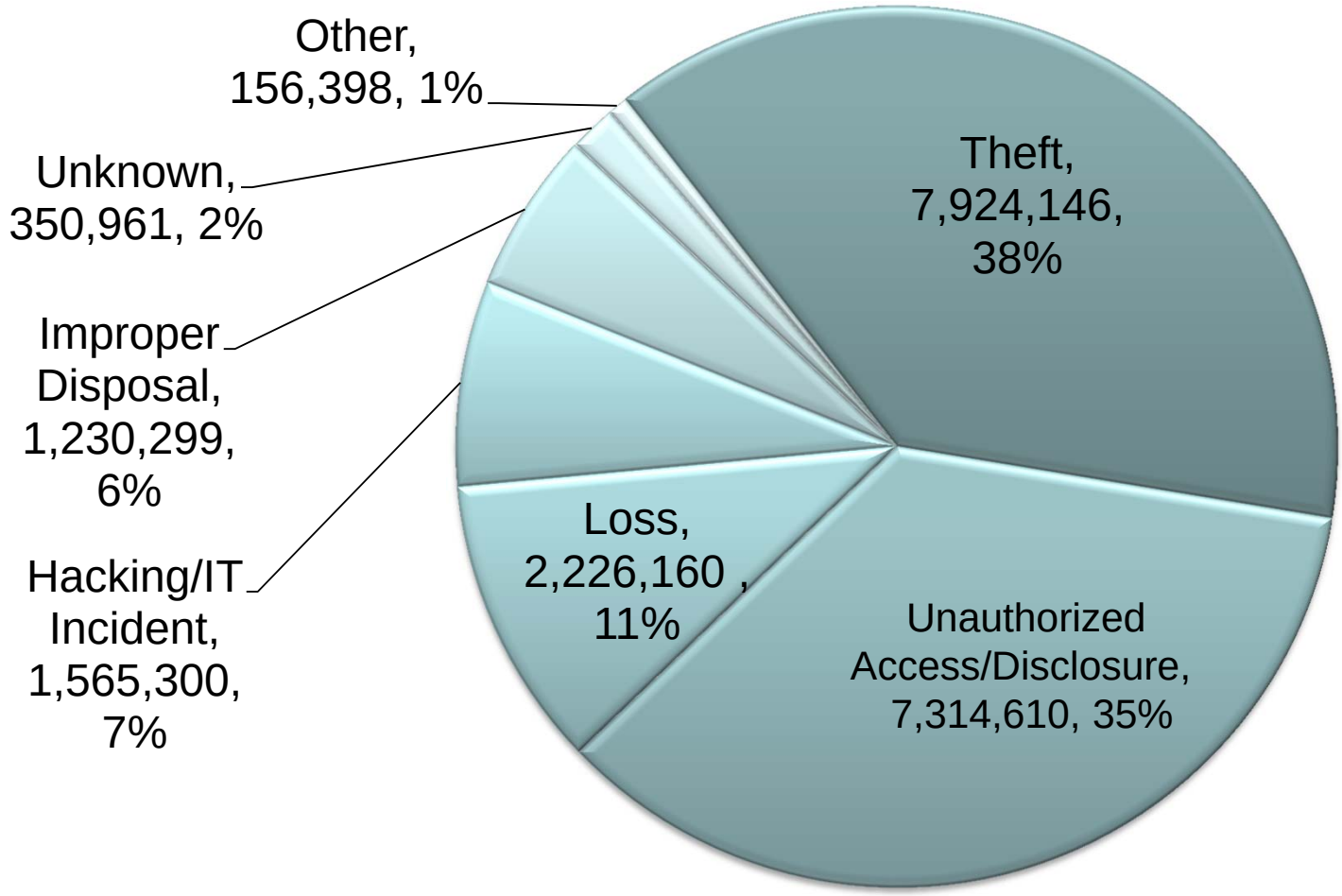


Causes of Large Breaches (by number of breaches) Sept. 2009 to June 2012



Davis Wright Tremaine LLP

Cause of Large Breach (by # of affected individuals) Sept. 2009 to June 2012



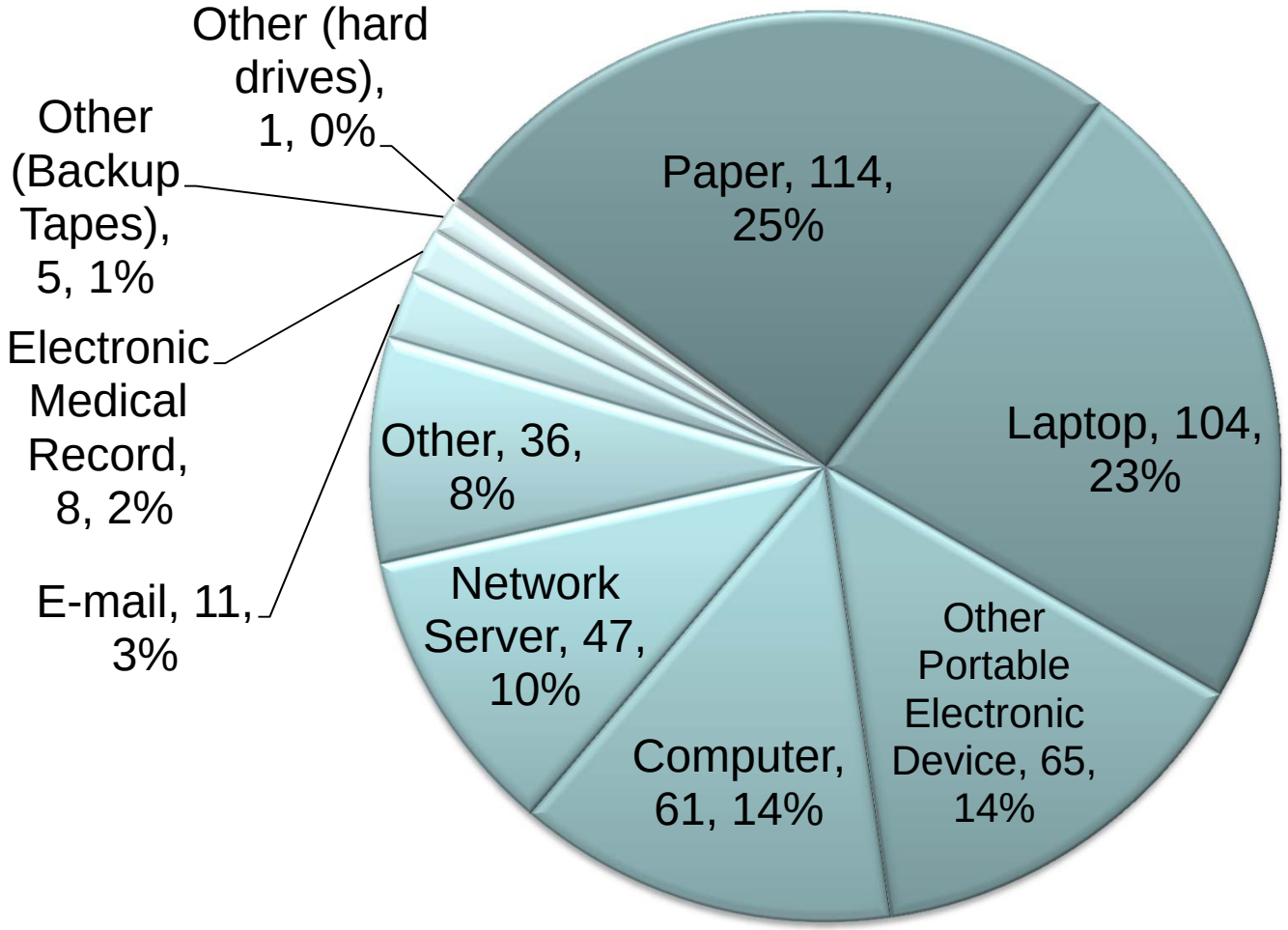
Davis Wright Tremaine LLP

Lesson 2:

The highest number of breaches involve:

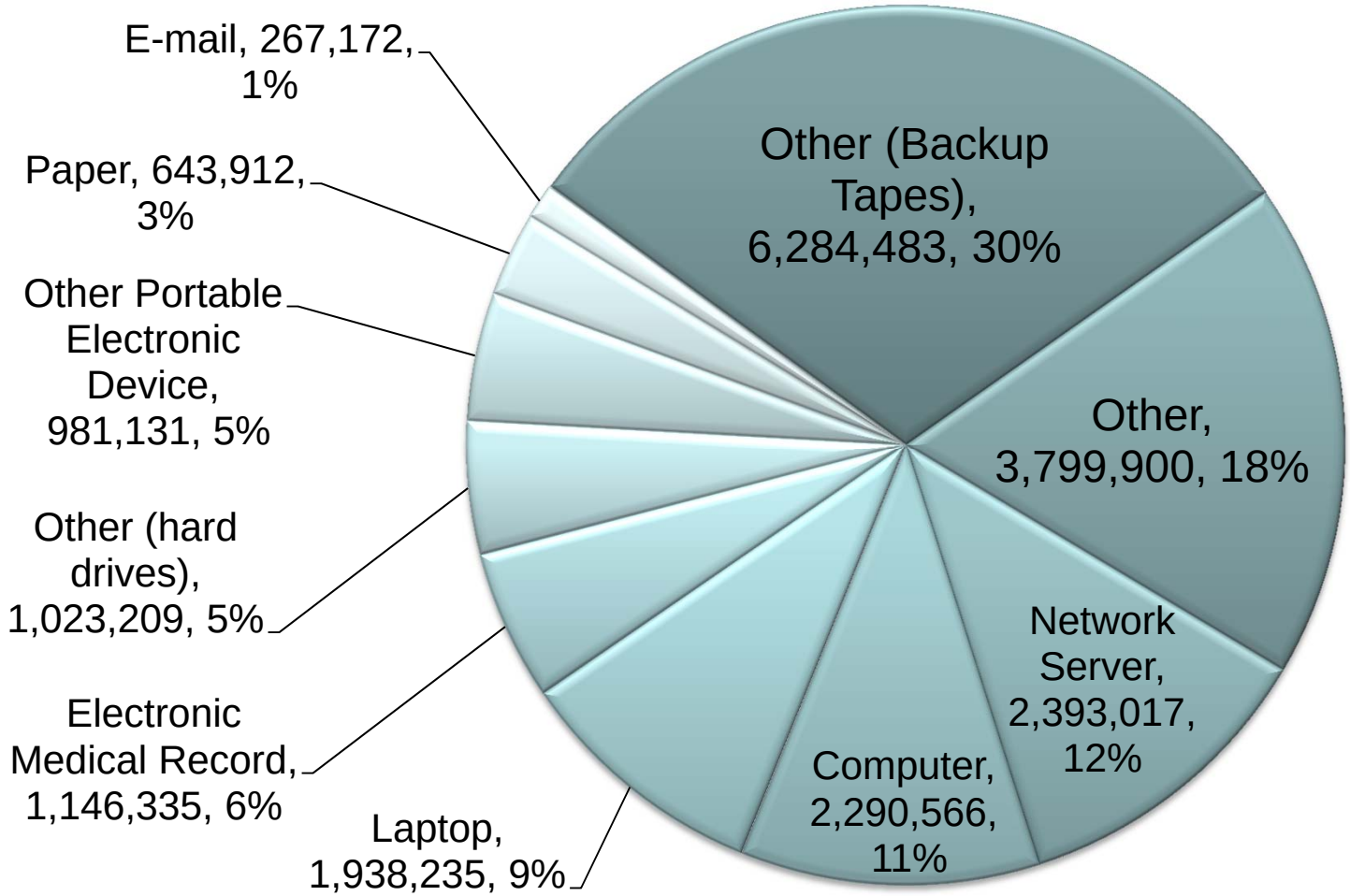
a) Desktops
b) Laptops
c) Other portable devices
d) Paper

Location of Large Breaches (by # of breaches) Sept. 2009 to June 2012



Davis Wright Tremaine LLP

Location of Large Breach (# of individuals affected) Sept. 2009 to June 2012



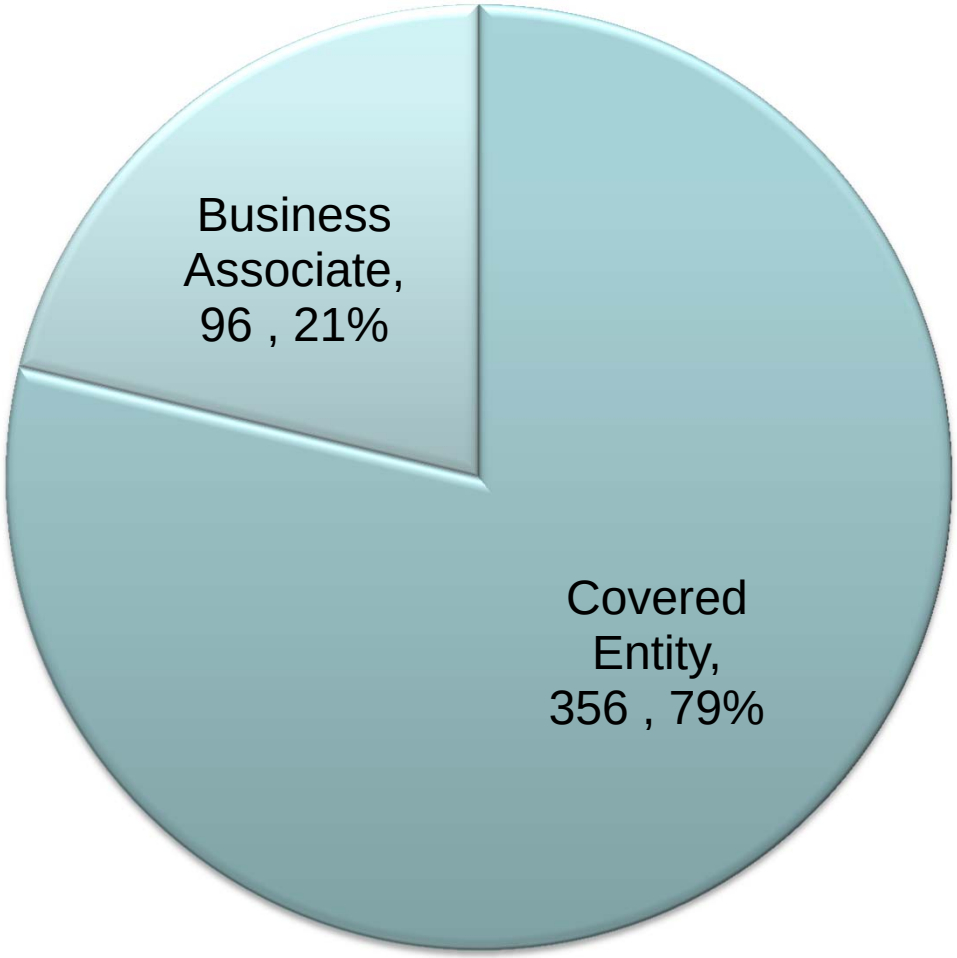
Davis Wright Tremaine LLP

Lesson 3:

It isn't me, it's you …

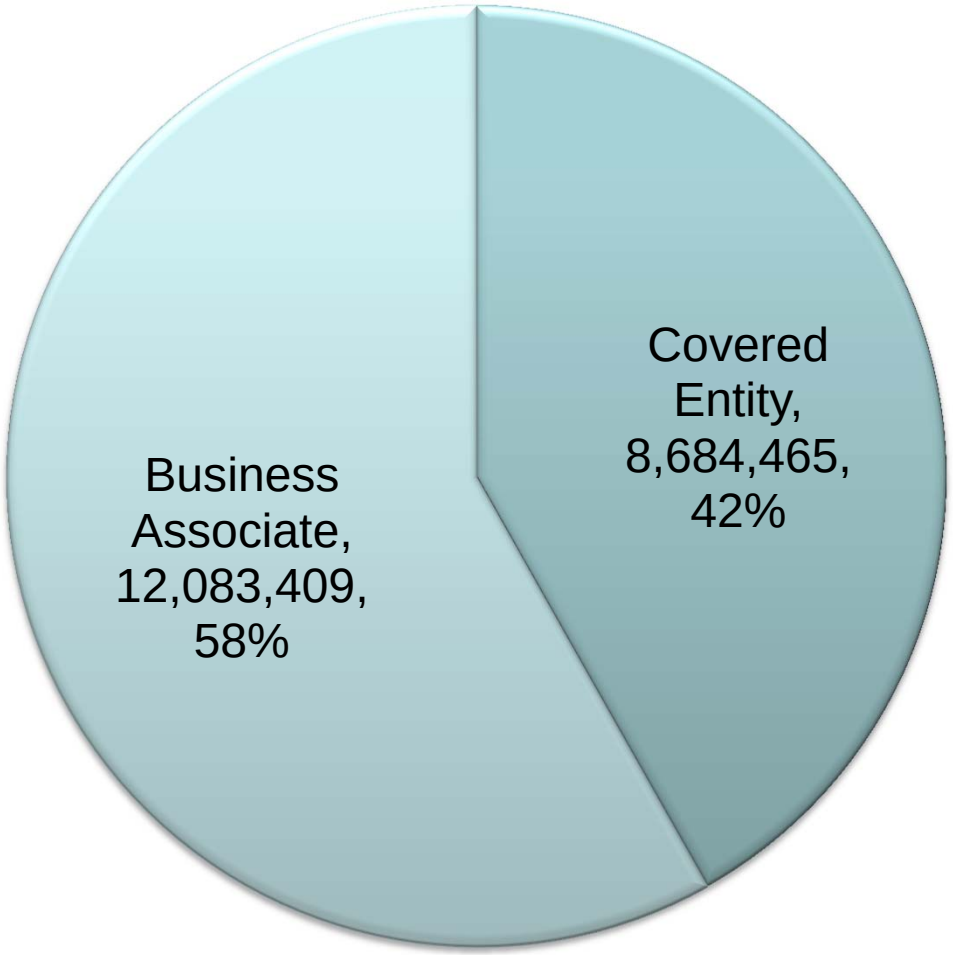
- Many large breaches are caused by business associates, not covered entities

Large Breaches Caused by BAs (by # of breaches) Sept. 2009 to June 2012



Davis Wright Tremaine LLP

Large Breaches (by # of affected individuals) Sept. 2009 to June 2012



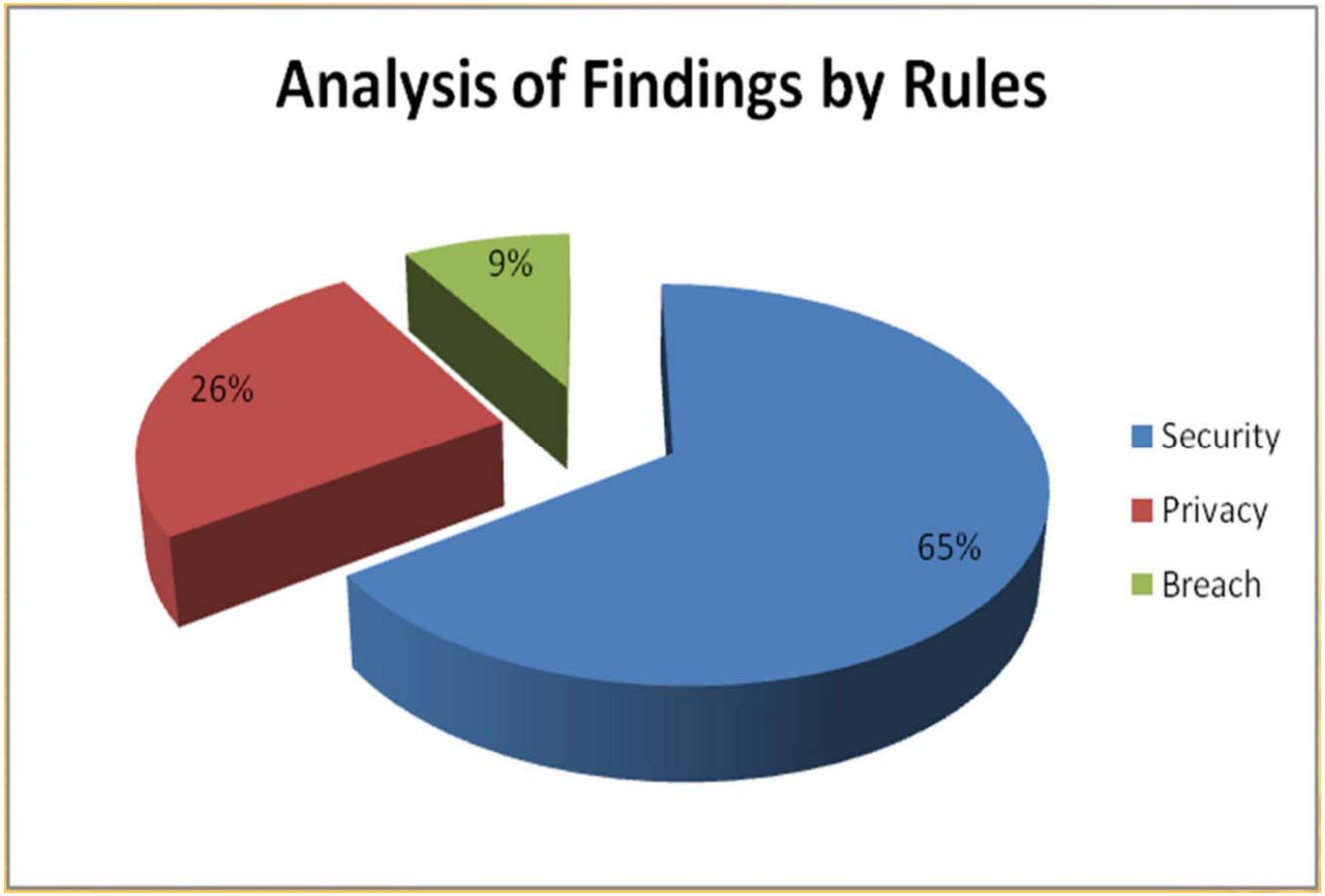
Privacy and Security Audits

- First substantial HIPAA privacy and security audits
- First proactive review (rather than incident driven)
- Audits include site visits and audit reports
- Includes very limited notice (10-15 business days to produce documents)
- Site visits of 3-5 persons for 3-10 days

Who Will Be Audited: First 20 Audits

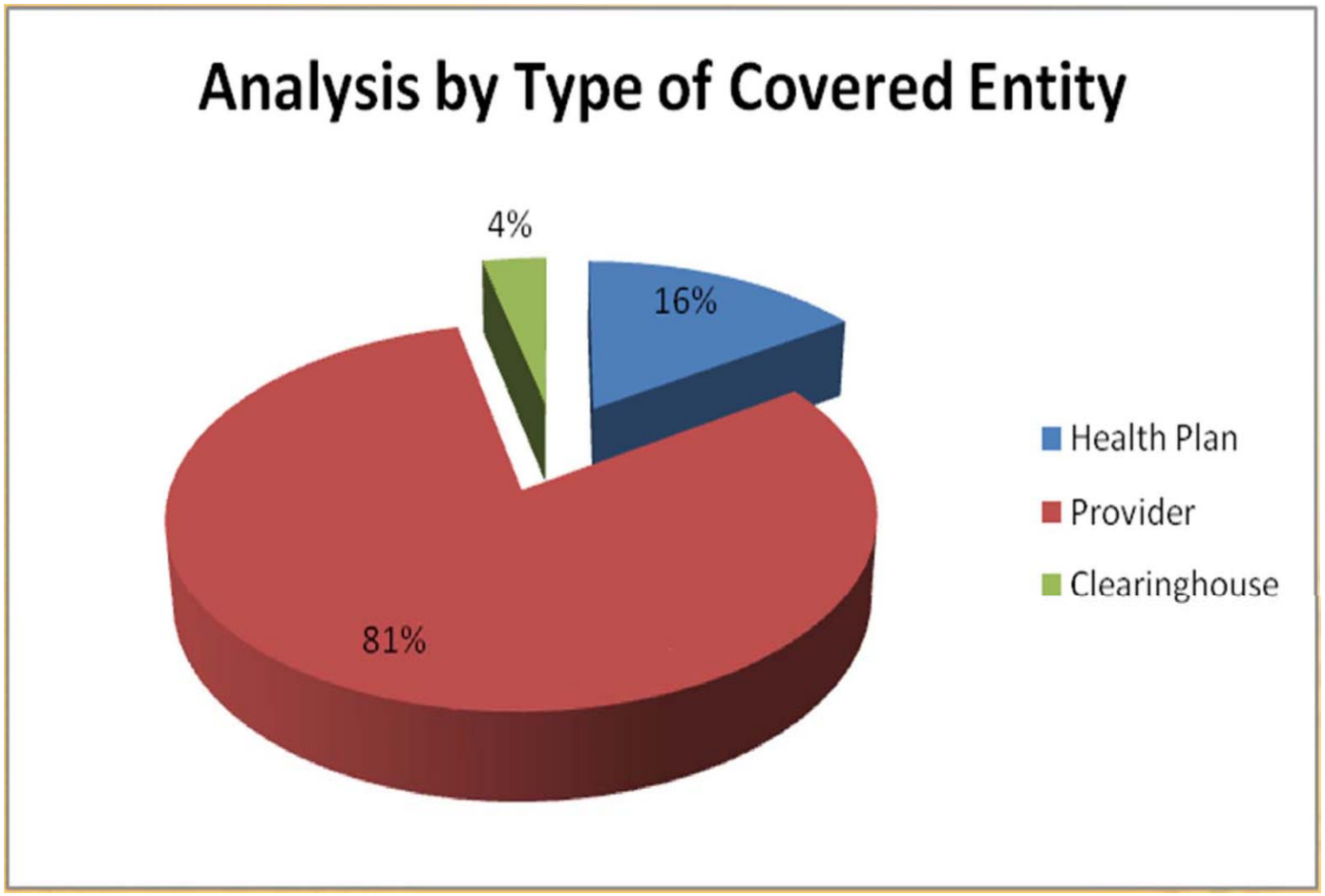
	Level 1 **> $1B**	**Level 2** **$300M - $1B**	**Level 3** **$50M - $300M**	**Level 4** **<$50M**	**Total**
Health Plans	2	3	1	2	8
Health care providers	2	2	2	4	10
Healthcare clearinghouses	1	1	0	0	2
	5	6	3	6	20

Initial Audit Results



Source: "2012 HIPAA Privacy and Security Audits," OCR/NIST Conference, 6/7/12

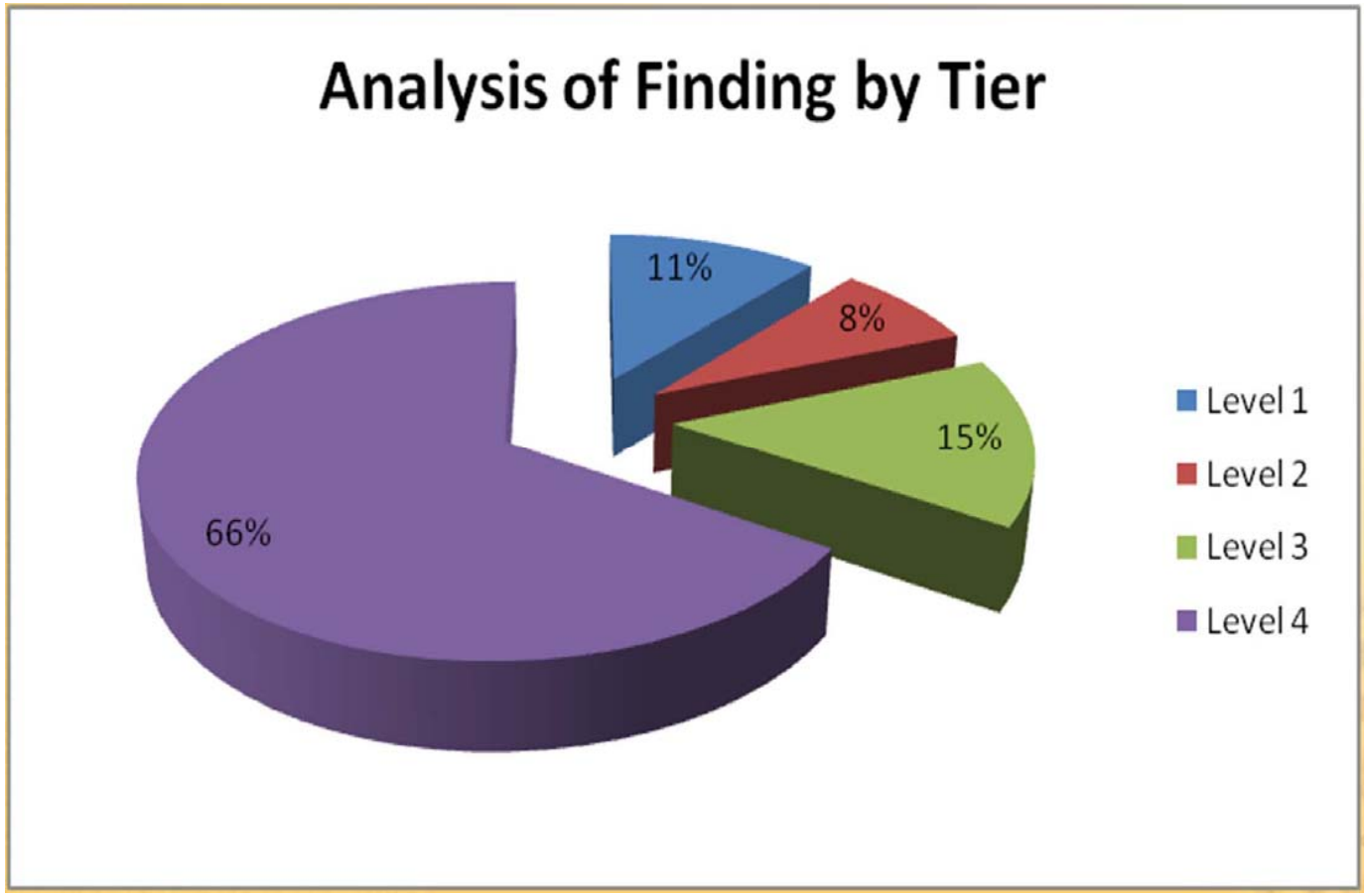
Initial Audit Results



Source: "2012 HIPAA Privacy and Security Audits," OCR/NIST Conference, 6/7/12

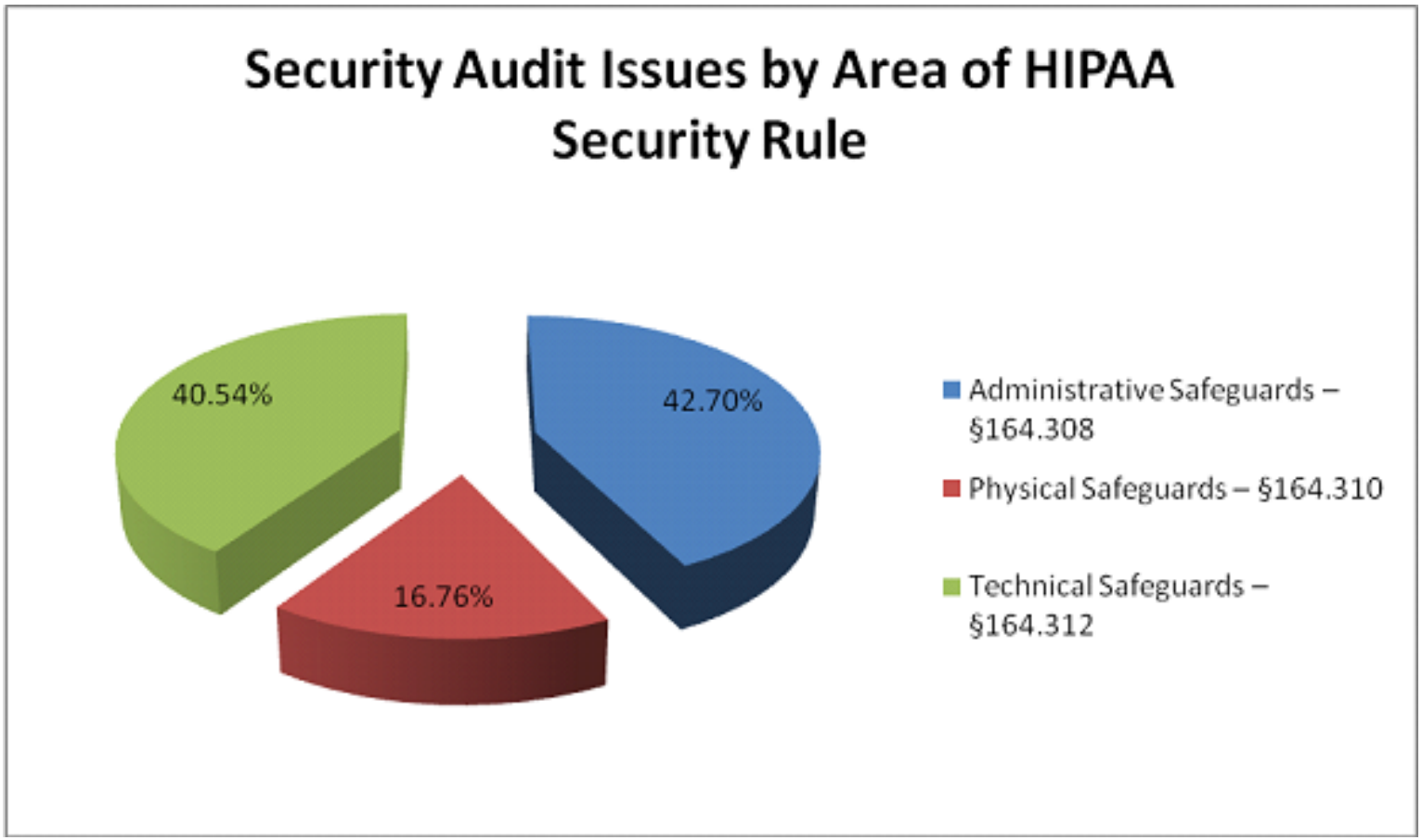
Davis Wright Tremaine LLP

Initial Audit Results



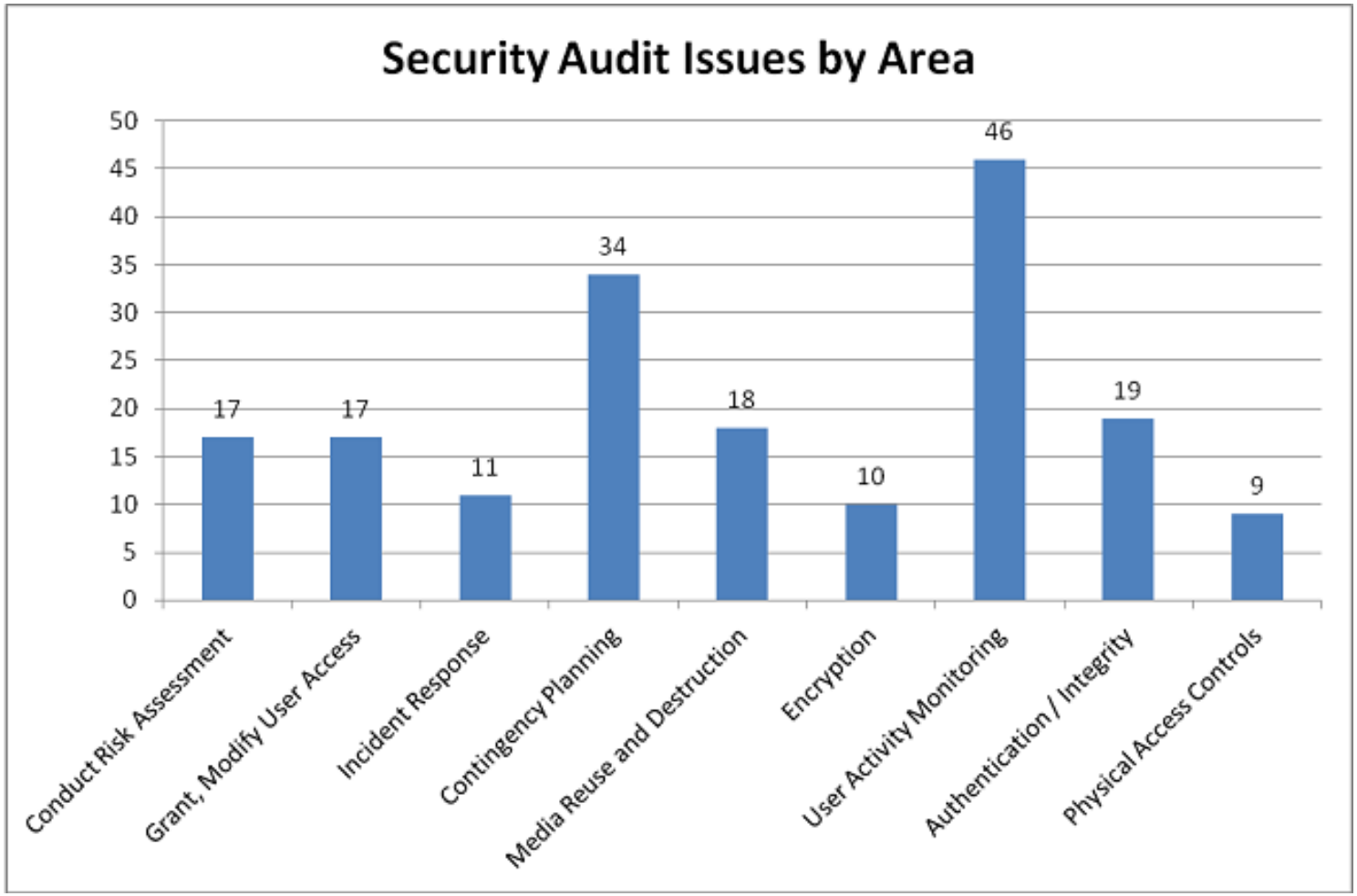
Source: "2012 HIPAA Privacy and Security Audits," OCR/NIST Conference, 6/7/12

Initial Audit Results



Source: "2012 HIPAA Privacy and Security Audits," OCR/NIST Conference, 6/7/12

Initial Audit Results



Source: "2012 HIPAA Privacy and Security Audits," OCR/NIST Conference, 6/7/12

Davis Wright Tremaine LLP

HHS Settlements/Penalties

- Issues that have led to HHS settlements*:
  - Breaches involving over 350,000 (Providence, BCBS of Tennessee)
  - Breaches involving sensitive information, such as HIV or celebrities (Mass General, UCLA)
  - Improper disposal “caught on tape” (CVS, Rite Aid)



* Settlements represent allegations not formal findings

HHS Settlements/Penalties

- Issues that have led to HHS settlements*:
  - Improper disclosure for marketing (discovered through OIG/DOJ false claims investigation) (MSO Washington)
  - Inappropriate use of online calendar/general lack of compliance, lack of BAs (Phoenix Cardiac Surgeons)
- Issue that has led to a penalty
  - Refusal to cooperate with OCR investigation (Cignet)

* Settlements represent allegations not formal findings

State AGs Join the Party

- HITECH Act (2009) provided State attorneys general authority to enforce HIPAA
  - Four suits have been brought (three settled) (CT, VT, MN, and MA)
  - None have coincided with HHS formal action
- Issue that has led to AG actions: Large breaches
  - Large breach can lead to multiple AG settlements and other enforcement
- Average settlement: $260,000

* Settlements represent allegations not formal findings

HIPAA Criminal Cases

- Almost 20 criminal convictions
  - Began mostly with financial fraud cases
  - More recent convictions involve snooping
- Mostly employees
- Penalties range from probation and community service to over a year imprisonment



Lessons Learned

- HHS and State AGs focus enforcement on breaches and headlines
  - Encrypt, encrypt, encrypt
  - Focus on large data sets, including back-up tapes and spreadsheets
  - Pay close attention to VIPs and sensitive information



Lessons Learned

- HHS tends to look for systematic problems
  - Was a breach due to systematic failures?
  - Were there policies? Training? Sanctions? Auditing?
- HHS has a history of voluntary enforcement, but settlements are increasing (a few a year)

For more information



Adam H. Greene, JD, MPH

Davis Wright Tremaine LLP

adamgreene@dwt.com
202.973.4213

Questions

