

Lessons Learned: Hard Data from 300 Breaches

Ann Geyer

Chief Privacy and Security Officer, University of California Berkeley



HIPAA/HITECH – G23

Session Abstract

Information security risk managers are often frustrated by the lack of 'hard data' when estimating expected losses. A new source of data derives from the HITECH mandates for transparency of breaches of PHI privacy and security. When a breach impacts more than 500 individuals, details of the breach must be reported to HHS. HHS publishes these details online. This is the beginning of a database that allows for an empirical threat profiling of health care organizations.

The talk will provide practical recommendation on how to use this data in HIPAA mandated risk assessments as well as discuss some surprising findings.

Target Audience

Privacy, security and compliance officers.

COBIT Objectives

Speaker Bio

Ann Geyer is the Chief Privacy and Security Officer at UC Berkeley. She is responsible for information policy and practices affecting over 100,000 students, faculty, staff, as well as the patients of the University's several HIPAA components. Prior to her University appointment, Ann was a consultant at Tunitas Group where she managed HIPAA privacy and security projects for over 50 healthcare clients.

Ann is a practicing attorney with professional certifications in privacy (CIPP), security (CISSP, CISM), and healthcare risk management (CPHRM). She has written extensively on the topics of identity and access management, electronic signatures, policy driven data protections, and IT governance. She is an instructor in the SF ISACA Chapter's CGEIT Exam Prep course and is a frequent speaker at local and national conferences.