WOLF
& COMPANY, P.C.

HITRUST Common Security Framework - Are you prepared?

Michael Kanarellis, HITRUST CCSFP
May 17, 2017

© 2017 Wolf & Company, P.C.

Before we get started…

- Today's presentation slides can be downloaded at www.wolfandco.com/webinars/2017.
- The session will last about 45 minutes, and we'll then have time for Q & A.
- Our audience will be muted during the session.
- Please send your questions in using the "Questions Box" located on the webinar's control panel.

About Wolf & Company, P.C.

- Established in 1911
- Offers Audit, Tax, and Risk Management Services
- Offices located in:
  - Boston, Massachusetts
  - Springfield, Massachusetts
  - Albany, New York
  - Livingston, New Jersey
- Over 250 professionals

As a leading regional firm founded in 1911, we provide our clients with specialized industry expertise and responsive service.

Meet Today's Presenter

Michael Kanarellis, HITRUST CCSFP
IT Assurance Senior Manager
Wolf & Company, P.C.
617-428-5408

mkanarellis@wolfandco.com
www.wolfandco.com

IT Assurance Services

- HIPAA and Regulatory Audits
- HITRUST
- NIST/ISO/PCI/COBIT Reviews
- Information Privacy Review
- Application Security Review
- Vulnerability Assessments
- Social Engineering Assessment
- Risk Assessments
- PCI DSS
- Business Continuity Planning (BCP)
- Incident Response Planning (IRP)
- Penetration Testing
- SSAE16 & SOC 2 Assurance

Objectives

- Why HITRUST?
- Affect of Office of Civil Rights (OCR) Enforcement
- HITRUST lessons learned and problem areas
- SOC 2 Plus HITRUST Overview
- HITRUST Roadmap

Why HITRUST?

- Need for HITRUST Common Security Framework
  - Healthcare under attack
  - Increasing cost of Breaches (Both Providers and Business Associates
  - Office of Civil Rights (OCR) increased regulatory scrutiny
  - Increased concern from customers and vendors
  - The need to “talk the same language”
  - Lack of standardized certification (No HIPAA stamp)

WOLF & COMPANY, P.C.

OCR Enforcement Fines

Violation Category	Each Violation	All Identical Violations per Calendar Year
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect – corrected in 30 days	$10,000 - $50,000	$1,500,000
Willful Neglect – not corrected	$50,000	$1,500,000

OCR Enforcement

- Actions focused on covered entities
  - Massachusetts Eye & Ear Infirmary (3/12, $1.3 million)
    - Laptops lost and NOT encrypted
  - Oregon Health & Science University (7/16, $2.7 million)
    - Breach involved Google cloud-based document storage; no BAA
  - U of Washington Medical (12/15, $650,000)
    - No Risk Assessments for Affiliated Entities
  - Care New England Health System (9/16, $400,000)
    - BAA had not been updated since 2005
  - Catholic Health Care Services of Archdiocese of Phila. (6/16, $650,000)
    - Theft of unencrypted IPhone; no mobile policy

Memorial Healthcare

- 4.5 Million Dollar Fine (2/17)

- From January 2011 to June 2012, MHS failed to implement procedures to regularly review audit logs, access reports and security incident tracking reports, and the system further failed to oversee access authorization policies that establish, document, review and modify user rights of access, OCR charged.

- Electronic protected health information must be provided only to authorized users, and “Organizations must implement audit controls and review audit logs regularly,” said Robinsue Frohboese, acting director for OCR, in a statement announcing the sanctions.

HITRUST Overview

- Assessment Reports
  - Self Assessment
  - Validated Assessment
  - SOC 2 Plus HITRUST
  - SOC 2 Plus HITRUST Plus HITRUST Certification

HITRUST Business Drivers

- Blue-Print to build out the security program
- HITRUST is an aggregate of ISO, NIST, PCI, HIPAA and state and local regulations combined into an aggregate standard
- HITRUST is prescriptive as opposed to descriptive requirements from other regulatory standards which are hard to interpret

HITRUST Overview

- HITRUST Common Security Framework (CSF)
  - Certifiable framework for the healthcare industry
  - 14 of the 19 HITRUST Domains based on ISO 27001
  - Incorporates aspects of HIPAA, HITECH, NIST 800-53, PCI DSS, FTC, COBIT and State Laws (Texas and Massachussetts)
  - Tailorable based on the organization

HITRUST Overview

- Common Security Framework (CSF) Components
  - 19 Domains
  - 46 control objectives
  - 149 implementation requirements (135 Security / 14 Privacy)
    - **66 required for certification**

HITRUST Overview

- Three implementation requirements
  - Level 1 is the base level requirement
  - Level 2 and 3 build on each other based on YOUR risk factors
    - Organizational factors (type and size of organization, records held)
    - System factors (number of systems in scope, accessible from the internet, accessible from the internet, mobile devices)
    - Regulatory factors (PCI, FISMA, State Laws)

HITRUST Overview

- Maturity Implementation Scoring
  - Policy (25%)
  - Process (25%)
  - Implementation (25%)
  - Measured (15%)
  - Managed (10%)

- Need to a score of 3 or higher to gain certification(roughly 70%)

Lessons Learned

- Organizational buy in
- Scoping, Scoping, Scoping
- Prepare for success
- Common gaps seen

Organizational Buy In

- You need it!
- Include people from all business lines
- HITRUST working group

Scoping Issues

- What's considered in scope?
  - It's up to you!
  - Don't bite off more than you can chew! Only scope what is necessary
  - Don't fail to accurately define business drivers
- Risk factors (Organizational, System, Regulatory)
  - Don't choose everything
  - Choose based on your need
- Number of records processed per year
  - Only count unique records

Prepare for Success

- Spend your time where it counts!
  - Policy
  - Process
  - Implemented

- 75%!!!!
- Have a project manager or dedicated team internally

Prepare for Success

- Be comfortable with your assessor
- Perform a readiness assessment
  - Be honest!
- MyCSF tool Training
  - HITRUST onsite training
  - Working with your assessor firm
- Policy writing
  - Common gap

Problem Areas

- Access Control
- Vendor Management
- Incident Response Planning
- DR/BCP
- Security Awareness Training!!!!!!

What is a SOC 2 Report?

- Service Organization Control (SOC) Report
- Offers independent third party attestation over controls in place at a service provider
- Not the same as a SAS 70 or SSAE 16 Report

SOC 2 + HITRUST CSF

- Partnership between AICPA and HITRUST
- Can issue the report based upon the 66 controls required for certification
- Includes: Security, Availability, Confidentiality, and HITRUST CSF mapping
- Requires that the auditor is both a licensed CPA and a HITRUST CSF assessor

Benefits for Combined Report

- Identify overlap in controls to improve efficiency
- Consolidate audit evidence
- Consolidate audit firms
- Save time and money
- Reduce audit fatigue

HITRUST Roadmap 2017

- HITRUST CSF V9
  - Update 21 CFR Part 11 (FDA –electronic signatures)
  - Add FFIEC, FedRAMP, DHS Critical Resilience Review
  - Review OCR Audit Protocol and adjust HITRUST controls
  - NIST Cybersecurity Framework Scorecard
  - NIST Cybersecurity Framework Certification

Thank You & Questions!

Michael Kanarellis, HITRUST CCSFP
IT Assurance Senior Manager
Wolf & Company, P.C.
617-428-5408

mkanarellis@wolfandco.com
www.wolfandco.com