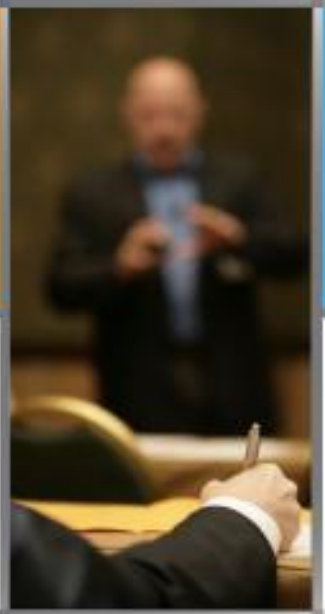
@CSOevents
#CSO50

CSO50 CONFERENCE+AWARDS

Aligning Proactive Security with Modern Threats



May 1-3, 2017

The Scottsdale Resort
Scottsdale, Arizona

PRODUCED BY
CSO
FROM IDG

CSO 50 CONFERENCE +AWARDS

Improving Security in the Third-Party Vendor Supply Chain

Brenda Callaway
Divisional VP, Information Security & IT GRC
Health Care Service Corporation

Craig Eidelman
Modern Workplace Security Specialist
Microsoft

HITRUST at a Glance

Organizational Background and Structure

- Founded 2007
- HITRUST Alliance, Inc. – Not for Profit, responsible for frameworks, standards, methodologies
- HITRUST Services Corp – For Profit, responsible for training and tools

Best Known for

- Developing HITRUST CSF – in 8th (soon to be 9th) major release
- Operating health industry's Information Sharing and Analysis Organization (ISAO)

Adoption of HITRUST CSF

- By 81% of hospitals and by 80% of health plans
- 8,000 vendors to healthcare industry

Adoption of CSF Assurance

- Over 44,000 CSF assessments in last three (3) years (over 18,500 in 2016)
- Most widely utilized approach by healthcare organizations and vendors to healthcare organizations for risk assessments

Supporting Cyber Risk Management, Threat Intelligence Sharing and Incident Preparedness and Response

- Operates Cyber Threat XChange (CTX) as industry cyber threat early warning system and to automate indicator of compromise distribution
- Developed, in coordination with HPH SCC and GCC, guidance for implementing the NIST Cybersecurity Framework

Information Protection Education and Training

- Over 4,500 professionals have obtained Certified Common Security Framework Practitioner (CCSFP) designation

Bringing Controls Together

The HITRUST CSF adds measurable value by integrating and enhancing multiple U.S. and international standards and regulations in a scalable, risk-based, industry agnostic and certifiable framework

Legislative, Regulatory, and 'Best Practice" Standards and Frameworks include, but are not limited to:

ISO/IEC 27001:2005 2013, 27002:2005, 2013, 27799:2008
CFR Part 11
COBIT 4.1
NIST SP 800-53 Revision 4
NIST Cybersecurity Framework (CsF)
DHS Cyber Resilience Review (in CSF v9)

NIST SP 800-66 Revision 1
PCI DSS version 3
FTC Red Flags Rule
FFIEC IT InfoSec Examination (in CSF v9)
201 CMR 17.00 (State of Mass.)
NRS 603A (State of Nev.)

CSA Cloud Controls Matrix version 3.1
CIS CSC version 6 (SANS Top 20)
CMS IS ARS version 2
MARS-E version 2
IRS Pub 1075 v2014
FedRAMP (in CSF v9)

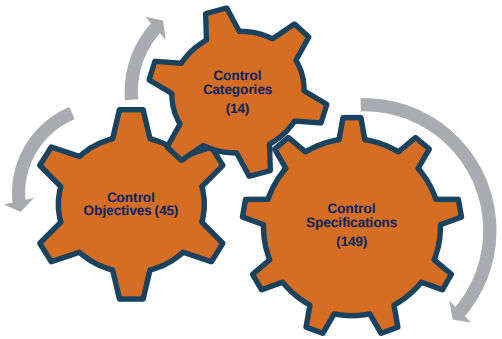
Analyzed, Rationalized & Consolidated

Scoping Factors

Regulatory
- Federal, state and domain specific compliance requirements

Organization
- Geographic factors
- Number of records processed or held

System
- Data stores
- External connections
- Number of users/transactions



Control Categories

0. Information Security Management Program
1. Access Control
2. Human Resources Security
3. Risk Management
4. Security Policy
5. Organization of Information Security
6. Compliance
7. Asset Management
8. Physical and Environmental Security
9. Communications and Operations Management
10. Information Systems Acquisition, Development & Maintenance
11. Information Security Incident Management
12. Business Continuity Management
13. Privacy Practices

HITRUST Benefits

Standardizing on a higher level of security builds greater trust in the electronic flow of information through the healthcare system

HITRUST CSF also provides greater risk protection by

- **Reducing risk:** Reducing risk, cost and confusion by incorporating best practices
- **Increasing confidence:** Increase confidence in the industry's ability to address information security, and streamline interactions with consumers, regulators and legislators
- **Measuring costs:** Establish a single benchmark for organizations to facilitate internal and external measurement
- **Reducing complexity:** Reduce the number, complexity, and degree of variation in security audits or reviews that organizations impose upon their trading partners; in effect establishing trust through certification

CSO 50 CONFERENCE +AWARDS

Applying HITRUST to Improving Security in the Third-Party Vendor Supply Chain

The Challenge

Healthcare Organizations Need to Manage Third-Party Compliance

- **Organizations rely on legions of third-party vendors**
  - From logistics to human resources, software development, financial record keeping, physical security and cybersecurity
- **Vendors have access to the organization's network and sensitive data**
  - Represent an opportunity to improve services and efficiencies and lower costs
  - Represent a potential risk to security, privacy and compliance
- **Organizations need to maintain appropriate general computing and security controls that support industry standards, regulatory and customer-specific requirements**
  - Many industry organizations reserve the right to audit, and may require suppliers to provide periodic evidence of general computing and security controls
  - Organizations have implemented assessment processes to gauge each supplier's overall adherence to these security requirements

Addressing new HIPAA/HITECH legislation extending the responsibilities of security and compliance to third-party vendor suppliers

The Challenge

Third-Party Vendors Need to Respond to Audits

- **Inefficiencies associated with responding to proprietary customer-specific questionnaires**
  - Expensive and time-intensive on site audits by customers
  - Costly and time-intensive data collection, assessment and reporting processes
- **Broad range and inconsistent expectations**
  - Tracking to varied expectations around corrective action plans
- **Inability to consistently and effectively report security posture**

50% of Business Associate vendors (BAs) surveyed completed 100 to 1,000+ third-party assessments annually, spending more than 10,000 hours per year

The Approach

The HITRUST Business Associate Council

Initially 5 of the largest U.S. health plans notified industry of updates to their business associate and partner agreement specifically using the HITRUST CSF Assurance Program

- HITRUST CSF Certification or SOC 2® leveraging HITRUST CSF Controls is required
- 2-year implementation schedule
- Created the momentum to move the industry and vendor community

Roy R. Mellinger
Vice President,
IT Security & Chief
Information Security Officer
Anthem, Inc.

Jon Moore
Vice President & Chief
Information Security Officer
Humana, Inc.

Ray Biondo
Divisional Senior Vice
President & Chief
Information Security Officer
Health Care Service Corporation

Robert E. Booker
Vice President & Chief
Information Security Officer
UnitedHealth Group

Omar Khawaja
Vice President & Chief
Information Security Officer
Highmark, Inc.

The Approach

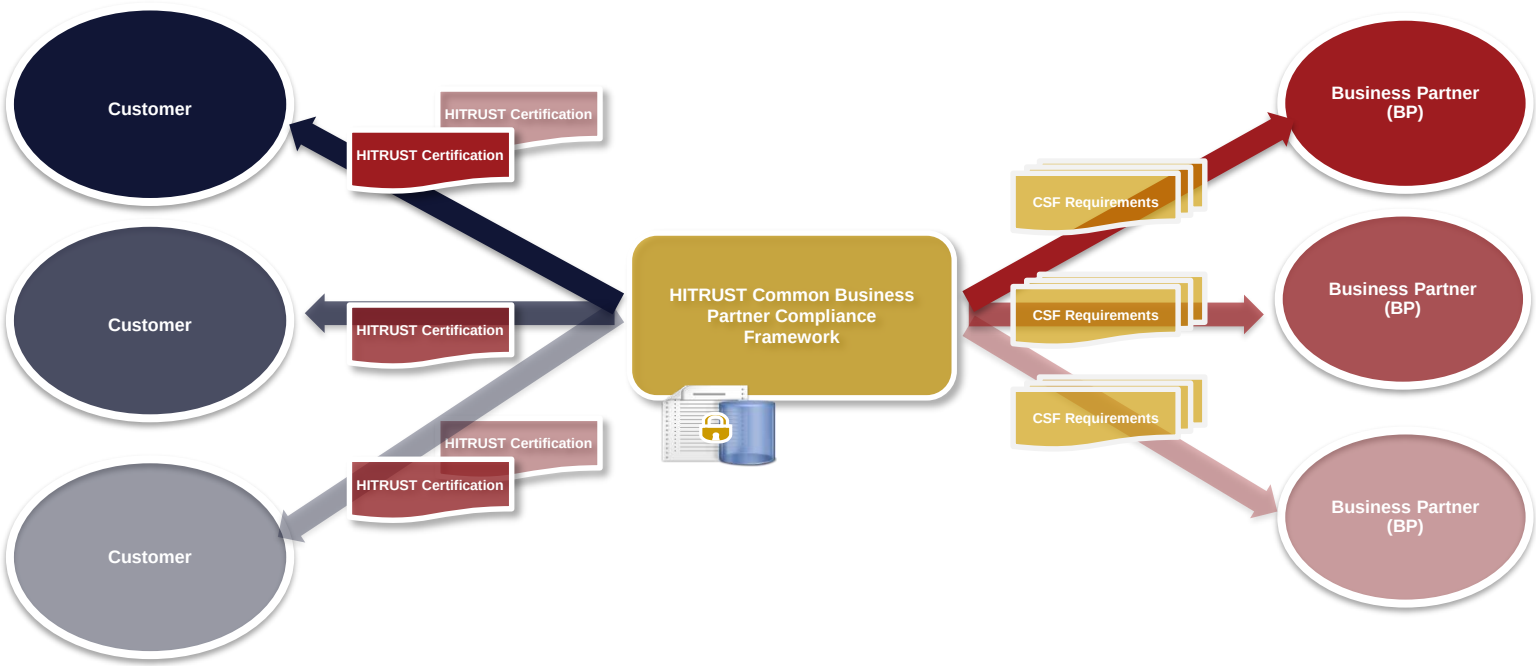
The HITRUST Business Associate Council

Collaborating with 17 vendors serving the healthcare industry representing thousands of Business Associates (BAs)

- **Establishes a uniform set of expectations for communicating information privacy and security posture**
  - Reduce the time and cost of obtaining and maintaining compliance
  - Ensure there is consistent security framework across the business associate and partner network
- **Three-part program to overcome adoption issues and improve industry-wide understanding of new regulations**
  - Get Buy-in and Commitment from Business Associates
  - Develop and Execute an Awareness Campaign
  - Get Buy-in from C-Suite

The Approach

Leveraging the HITRUST CSF Assurance Program:
HITRUST CSF, CSF Assurance and CSF Assessors



The Results

Healthcare Organizations

Mission to instill confidence, manage risk, gain efficiencies and inspire excellence in healthcare IT by driving innovation throughout the third-party vendor supply chain

- Reduces time and expense on redundant audits, assessments and onsite reviews
- Reduces time and expense of procurement managing various assessment processes
- Facilitates a specific level of assurance around implemented controls

Being trusted and being able to trust business partners relating to information security

The Results

Third-Party Vendors

Helping thousands of BAs gain certifications and participate in programs that demonstrate they are safeguarding critical information for individuals and the nation at large: near 100% participation from BAs far exceeded goals

- **Improving customer satisfaction**
  - Customers asking for a single framework
  - Apply on top of existing compliance and audit cycle
- **Marketing differentiator**
  - Increase customer confidence (both existing and potential customers)
  - Demonstrating managing risk not only to customers but also to insurers
- **Reduction in costs and complexity**
  - Reduction in questionnaires, costs, etc.

Assess Once, Report Many

A Model for Other Industries

- **Beyond healthcare**
  - HITRUST CSF not just healthcare regulations and standards, supports many industries
- **Market-driven**
  - Industry benchmarks rather than company- or government- specific
  - Aligned with industry compliance requirements
- **Enhanced business partner communications**
  - Timely and coordinated breach response processes
  - Proactive alert of increased business partner risk
- **Shared resources**

CSO 50 CONFERENCE +AWARDS

HITRUST 10 YEARS
2007-2017
INNOVATION.
PROTECTION.

Visit www.HITRUSTAlliance.net for more information.

To view our latest documents, visit the Content Spotlight.