Dashboards as an Effective Tool for HIPAA Security and Privacy Compliance

Bikram Bakshi
President & CEO

©QSSI 2011-12
Objectives

• The problem
  • Key causes for data breaches
  • Comparing these causes with CMS findings on HIPAA Security Compliance

• The Solution
  • Monitoring compliance
  • Data visualization – “Dashboards as a solution”
  • Automation of compliance monitoring - Solution design

• Practice
  • Compliance monitoring – Business case
The problem

?
Key causes for privacy breaches

Analyses of recent breach events

• Inadequate
  – Monitoring of how business process is managing privacy controls
  – Monitoring and Alerts on any security events or incidences
  – Periodical assessment of policies and procedures
  – Employee education

• Significant role of an insider - undetected

CMS Compliance review findings

• Inadequate
  – Risk assessment and risk management
  – Policies and procedures
  – Training
  – Monitoring of:
    • Policies and procedures followed by employees
    • Security procedures

*2009 HIPAA Compliance Review Analysis And Summary of Results – Published by CMS and OESS September 2009
The problem

- Monitoring privacy and security compliance, as in IT as well as business practices
- Identifying incidences proactively
- Making timely decisions to eliminate the risks

The solution.....
Solution!
Monitoring compliance

– Monitoring the operations against Policies and procedures
– Identifying and Monitoring incidences which may be potential causes of breach
– Implementing automation tools for identifying potential “risk incidences” and provide alerts
– Managing the alerts life cycle and making timely decisions

Can Monitoring compliance using data visualization be the solution?
Data Visualization - Dashboard

• Visual device
  • Data visualization for communicating progress and performance, in a simple and impactful way.

• Using Business intelligence
  • The thinking that goes behind dashboards is often complex but their value is in how simple they are.

• Presenting data with clarity
  • They can cut through the noise and information overload so many employees suffer from today.
How HIPAA Compliance can be monitored using dashboards?

A 30,000 ft level architectural explanation of information flow and business analytics and visual representation of compliance posture.
Conceptual design of Compliance Monitoring Automation

- Security Incidences and events data
- Business operations data
- Regulations database
- Policies and procedures

Business Intelligence
Analyze the data

Dashboard Project
Compliance level
Alert on key incidences
Provide management capabilities for events and alerts

03/10/2011
HIPAA Summit East 2011
©QSSI 2011-12
Key elements of Automation

• Well defined incidence identification
  • Based on patterns
  • Classified as critical, high, medium or low
  • Able to recognize false positives

• Well designed operational activities capture
  • Role based, timely capture of activities
  • Not increasing the burden of the staff

• Business intelligence to connect the regulations, policies and procedures as well as events and activities

• Excellent reporting tool
  • From high level to system level
Is it only visibility on a dashboard is a solution?

Behind the scenes.....

Business intelligence

Various data sources and business processes, policies and procedures and rules/Fed and State
Business case for Continuous monitoring

Convincing the CFO
Business case for continuous monitoring

- Reduce the risk – reduce risk of penalties and other financial damages
  - Know your compliance level at any time
  - Identify any potential incidences proactively, preventing serious incidences from happening
- Be ready for audits – save on time and cost of supporting audits
  - Easy access to the data required for audits any time
- Make timely decisions – Being proactive saves you time, prevents damages as well as cost effective
  - Manage alerts
  - Timely investigations and corrective actions, not waiting for any incidence to happen
- Reduce insider threats – Added incentive!
  - Deter insider threats by advertising the monitoring
- Reduce cost of security and privacy monitoring
  - Automated monitoring is cost effective
  - Reduces burden on the security and privacy personnel
ROI

Cost of compliance monitoring
Cost of breach – millions of dollars!

Cost of Automation – few thousands!

Any CFO here has any questions?
About us

Monitoring compliance, automation, dashboards, visibility and ...... more!
Discussion on “is automation possible?”