Business Associate Risk Profiling and Compliance

Gary Glover, SecurityMetrics

securityMETRICS

About Us

- Gary Glover
  - CISSP, CISA, QSA, PA-QSA
  - Director of Security Assessment Team
  - 8 years in Information Security compliance
- SecurityMetrics
  - Regulatory security compliance assessments and consulting
  - Digital forensics & penetration testing
  - Regulatory compliance programs (validation, tracking, training, support)
  - Helped over 1 million small to large entities manage security compliance

securityMETRICS

Why Am I Here?

- Can a CE effectively track compliance for potentially thousands of BA's?
- For the past 8 years, worked in industry that requires annual compliance attestation from entities at all levels, small to large
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Help merchants comply with payment security standards
  - Bank/merchant relationship analogous to CE/BA

Payment Card Industry Perspective

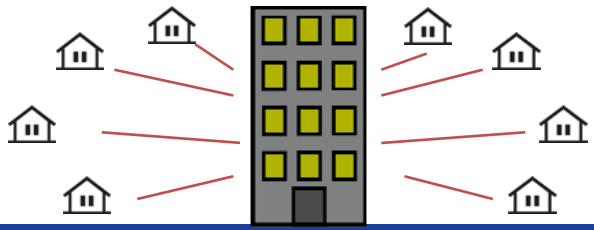
- Large merchant banks have hundreds of thousands of entities doing annual compliance attestation
- Validation levels defined based on risk to card data
- Typically small team at bank tracks compliance
- Merchants bear the cost of compliance validation as a "cost of doing business"

By the Numbers...

- ~400K business associates in U.S.
- 62% of breached records reported to HHS, or 4.4 million, involved a BA
- Data breaches cost U.S. healthcare providers an estimated $7 billion per year

Covered Entity Challenge

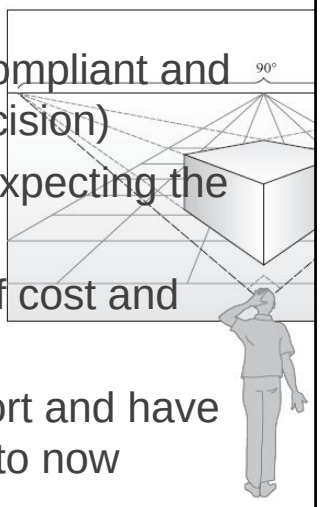
- Covered entities need to work with compliant BA's
- Covered entities at risk if BA looses data
- A single CE can have hundreds or thousands of business associates
  - Which BAs do security right?
  - Which BAs represent highest risk to ePHI?
  - How and where do you start?...Sept 23rd deadline



Perspectives of Health Care Provider

- Hard for small compliance team to manage a thousand BA's (compliance and contracts)
- For our protection we want assurance above a BA's signature on an attestation letter
  - Get compliance validation based on BA risk
- What can we do to feel good about the security of small CE's that have access to our data (doctors, clinics, etc.)

Perspectives of Business Associate



- Large BA's motivated to be compliant and attest to it (good business decision)
- Some have been pro-active expecting the rule changes
- Many have waited because of cost and resource issues
- Small BA's may lack IT support and have not worried about it but need to now

The Goal

- Get BA's moving quickly towards compliance to HIPAA ePHI security requirements
- Limit CE risk by:
  - Categorizing of BA's by their risk level / compliance status
  - Get high risk BA's done first!

Risk Profiling Overview

- Compile list of BAs who handle ePHI
- Profile BAs into risk categories
  - Simple conversation using weighted questions
  - Results in risk score
- CE decides what level of validation to impose on a BA based on overall risk
- Create and execute a plan
  - Mass communication program
  - Risk analysis tools
  - Compliance/Risk assistance (support center)
  - Risk reporting

Sample Risk Profiling Questions

- Profiling Questions:
  - How is PHI data received?
  - How much PHI data is received per month?
  - How/where is PHI data stored?
  - Is PHI data accessed via web applications?
  - Are mobile devices used to access PHI data?
  - Do you have an internal IT department?
  - etc.

- Each question is ranked and an overall risk score is calculated

Attestations of Compliance

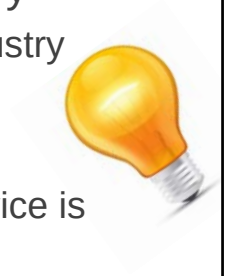
- Apply attestation/validation requirements based on risk, .e.g.- low risk BA needs simpler requirements
- Determine BA risk levels that require additional validation
  - BA's pay for vulnerability scanning, onsite auditing, gap analysis, detailed self assessment questionnaire, etc. (it's a cost of business)
- This is how mass compliance works in the Payment Card Industry

Tracking BA Compliance Status

- CE's need to manage BA's annual compliance status with minimal resources
- Management console tools essential
  - Quick snapshot of all BA data, % attested, etc.

Apply Mass Compliance Lessons

- Model for mass compliance programs exist now for payment card industry
  - Easily adaptable for health care industry
  - Tools exist today
  - Rapid scaling to deadlines possible
  - Compliance cost applied where service is required, and is risk based



Questions?

Gary Glover
Director Security Assessment, QSA, PA-QSA, CISSP, CISA
gglover@securitymetrics.com