Performing a Comprehensive Security Risk Assessment

Kate Borten, CISSP
President, The Marblehead Group

Agenda

- Definitions
- Two Methodologies
- Self-Assessment
- Comprehensive Risk Assessment
- Practical Pointers

Definitions

- Information security is assurance of
  - confidentiality,
  - integrity, and
  - availability of information
- Fair Information Practices require security to assure privacy

Definitions

- Risk assessment: "assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence" (BS 7799)

Definitions

- Risk management: "process of identifying, controlling and minimizing or eliminating security risks ..., for an acceptable cost" (BS 7799)
- Note that there is always risk
- Risk is on a continuum. Where do we want to be on that continuum? That's a business decision. Don't build a $5,000 fence around a $2,000 horse.

Methodologies: "Traditional"

"Traditional" - formal *measurement* of risk

- Problems: attempting to quantify the theoretical (lure of the equation); placing dollar value on privacy
- Reality: healthcare assessments are qualitative, subjective
- Conclusion: Must always weigh risks and compare to cost of remediation, but there's a more practical and effective way --->

Methodologies: "Modern"

"Modern" - compare your environment to standards and best practice (Donn Parker)

- HIPAA security rule describes scope of infosec program and sets minimum standards
- BS 7799 (now ISO 17799): framework for comprehensive infosec program (bsonline.techindex.co.uk)
- Can map security rule requirem'ts to BS 7799
- Both reflect formal infosec body of knowledge

- Weighing risk is still basic to this approach

Methodologies: "Modern"

HIPAA security rule - a comprehensive, formal infosec program:

- Administrative procedures
  - Policies
  - Procedures
  - Workforce education
  - "Assigned responsibility"
- Physical safeguards
- Technical controls

Methodologies: "Modern"

BS 7799

- Part 1: Code of practice for information security management
- Part 2: Specification for information security management systems

Methodologies: "Modern"

- Advantages of "modern" approach of comparison to standards, best practice, and security framework:
  - Practical
  - Easier to comprehend, intuitive
  - Greater assurance of covering all the bases when referencing, e.g., BS 7799
  - Easier to document risk and compliance

Self-Assessment

- Sometimes called a “HIPAA gap analysis”
- A common first step for organizations
- Simple, free or inexpensive checklists rephrasing the security (and sometimes privacy) rule, e.g.:
  - HIPAA Security Summit guidelines
  - HCPro’s HIPAA Self Assessment and Planning
  - NCHICA’s HIPAA EarlyView

Self-Assessment

- Benefits
  - Initial analysis to get senior management attention and support for budget, next steps (ISO, comprehensive assessment)
  - "Low hanging fruit" - Identify obvious work
- Limitations
  - Superficial, short on depth and insight
  - Staff usually lacking in infosec expertise, so decisions about which risks to address and how may or may not be appropriate

Comprehensive Assessment

- Real first step to a comprehensive infosec program
- Requires in-depth knowledge and expertise - both in infosec and in healthcare
- Hence, usually outsourced to experts, not a self-assessment

What's Meant by "Comprehensive"?

- Includes review of policies, procedures, organizational roles, workforce education, physical controls, and technical controls
- *Not just technical controls!*
- This initial, baseline assessment will guide your infosec work for the next year or more

Risk Assessment Report

- Report should identify risks to the confidentiality, integrity, and availability of protected info assets - including specific HIPAA requirements that aren't met
- Report should weigh (H/M/L) each risk to help organization prioritize actions
- Report should recommend steps to reduce each risk

Practical Pointers - 1

- "Comprehensive" assessment but
  - Not every computer system (just highest risk ones)
  - Not every site (just representative ones and ones known to be problematic)
- Extrapolate from these systems and sites

Practical Pointers - 2

- Get information security officer on board (or draft from within and train) so this person has/develops credentials and takes ownership of the report and subsequent actions (preferably should oversee the assessment)
- Else decisions may be made which aren't consistent with the overall long-range goals of the infosec program (e.g., focus on questionable priorities, not choosing optimal remedy)

Practical Pointers - 3

- Once the infosec officer (or stand-in) has an action plan, be sure the corporate officers, board, agency commissioners, etc., are informed and agree to accept unmitigated risks
- They risk fines and prison!

Practical Pointers - 4

- Risk assessment is iterative
- This is just the first assessment of many
- Repeating comprehensive assessments provides for
  - comparison with baseline to show progress
  - identification of new risks, vulnerabilities
- Focused assessments will drill down, especially in technical areas, e.g., specific host vulnerabilities

Practical Pointers - 5

- Resist the temptation to buy technology as an immediate priority and a “silver bullet”!
- First, plan! Turn the risk assessment report into project plans with timelines and priorities, and develop budgets.
- Administrative issues usually need to be addressed first. Technical solutions should be driven by policy, not the reverse.
- Technology, while often necessary, is the most expensive solution. So choose wisely.

Questions??

Kate Borten, CISSP
President, **The Marblehead Group**
One Martin Terrace
Marblehead, MA 01945
Tel: 781 639-0532
Fax: 781 639-0562
kborten@marbleheadgroup.com