

Who's Knockin' at Your Door? Identifying and Tackling Your Data Security Risks



*Teresa Julkowski, Privacy and Data Security Officer
Lori Oleson, Compliance Director*

Overview

- I. Setting the stage.
- II. Year of Data Security raises employee awareness and achieves specific security measures.
- III. Data Security Risk Management Committee reviews and prioritizes security initiatives.
- IV. Balanced internal and external resources helps ensure effective risk management.



I. Setting the stage

Collaborative internal risk assessment by Information Systems and Corporate Compliance identified opportunities within current data security risk management.

Ratcheted accountabilities due to HITECH Act

2 unrelated departments

Ill-defined roles

Informal analysis and prioritization of security risks.

Interest in better pulse on data security risks

Separate tracking mechanisms for privacy versus data security incidents

Known and unknown data security risks



II. Year of Data Security

Internal security risk assessment prompted IS and Corporate Compliance to develop "Year of Data Security"



- Year-long plan targeted raising employee awareness and achieving specific data security measures.
 - Ensure policies and procedures align with data security best practices.
 - Solicit senior management approval on specific proposals.
 - Develop and launch data security training.
 - Hire vendor to conduct comprehensive vulnerability assessment with penetration testing.



II. Year of Data Security: Communication

Introduced at 1st quarter all-employee meeting:

- Outlined HITECH Act data security protection and reporting implications for average worker.
- Reviewed results from internal risk assessment.
- Introduced new role of Privacy and Data Security Officer within Corporate Compliance.
- Previewed initiatives: enhanced policies and procedures, data security training, external vendor assessment.

Updates provided to targeted groups throughout the year.



II. Year of Data Security: Oversight

New combined Privacy and Data Security officer role.

- Increased efficiency and consistency of breach reporting accountabilities of HITECH Act.
- Fostered strong collaboration between Corporate Compliance and Information Systems.
- Aligned risk management across all aspects of privacy and data security.
- Allowed Information Systems to focus on day-to-day operations and strategic planning while Privacy and Data Security Officer handled risk management.



II. Year of Data Security: Enhanced Practices

Initiatives focused on enhanced data security practices.

- Explored additional protection for data transmissions (e.g., expanded use of encryption, secure websites, secure file transfer exchanges).
- Implemented new removable media policy with forced encryption.
- Launched single sign-on with strong password and automatic logout.
- Strengthened process for managing and monitoring external user access to data.



II. Year of Data Security: Staff Awareness

Compliance Week activities focused on data security.

- HIPAA building check report cards issued to each director; directors followed up with any deficiencies.
- Impromptu questions asked of employees about data security practices; correct answers rewarded with trinkets, including Year of Data Security pin.
- Voluntary compliance quiz; respondents entered into a drawing.
- Compliance Question of the Day: employees whose submitted questions were chosen received trinket.



II. Year of Data Security: Training

A new web-based computer use and data security training module highlighted key principles.

- Complements existing HIPAA privacy and general compliance trainings.
- Employees, contractors and temporaries are required to take the training upon hiring and annually thereafter.
- Scenarios based on real-life examples and updated annually with incidents and employee questions tracked since last training.
- Heightened awareness of individual and organization's responsibilities related to HITECH Act.
- Assessment requires 90% competency to pass.



III. Data Security Risk Management Committee

Committee created as a result of vulnerability assessment recommendations.

- Executive sponsors are General Counsel and Chief Financial Officer.
- Members include Chief Information Officer, Privacy and Data Security Officer, Compliance Director, Network Manager, Security Engineer and Human Resources Director.
- Privacy and Data Security Officer sets agenda and chairs monthly meetings.
- Committee reports to Senior Management.



III. Data Security Risk Management Committee

Committee assists in determining mechanisms to assess data security risk.

- Determines frequency and scope of external vulnerability assessments.
- Examines potential risks as they become known.
- Considers tools and applications to address and mitigate particular risks.
- Oversees data security risk assessments and/or audits.
- Evaluates results to prioritize and recommend corrective action.
- Monitors implementation of corrective action plans.



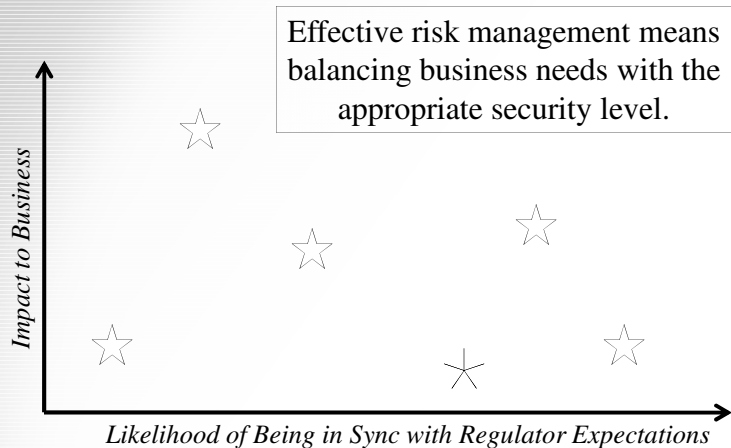
III. Data Security Risk Management Committee

Committee helps ensure strategic approach to data security risk management.

- Initiates and lays foundation for policy making.
- Considers best practices from benchmarking activity (e.g. a health security professionals interest group).
- Recommends and prioritizes resources to address data security matters.
- Identifies potential risk areas for monitoring.
- Advises and assists with data security initiatives and education programs.
- Assists in long range planning related to data security management.



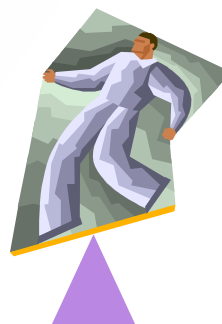
IV. Balancing Resources



Care

IV. Balancing Resources

- Internal Resources
 - People
 - Time
 - Budget
 - Risk assessment tools
 - Incident reports
 - Software
 - Monitoring tools
- External Resources
 - Contractors
 - Industry training/conferences
 - Vendor audits
 - Roundtable discussions



Care

What's Next

- Continue to strengthen collaboration between Compliance and Information Systems.
- New Security Engineer position reports to IS Network Manager and works closely with Privacy and Data Security Officer.
- Continue to implement remainder of data security initiatives sanctioned by the Data Security Risk Management Committee.
- Under the direction of the Data Security Risk Management Committee, develop the long range plan for data security.

