Implementing Technical Security is Not Enough to Adequately Protect PHI

A Focus on Risk Management

Gerard Scheitlin | RISQ Consultant
Product and Organizational Risk Solutions
Healthcare and Health Information Technology

* Quality, Information Security, Clinical Safety, Compliance, Privacy

Agenda

- Organizing for Risk
- Risk Structure
- Risk and Management
- How to Measure Risk
- Building an ERM
- Maturity Model
- Questions/Discussion

Organizing for Risk

What is Risk?

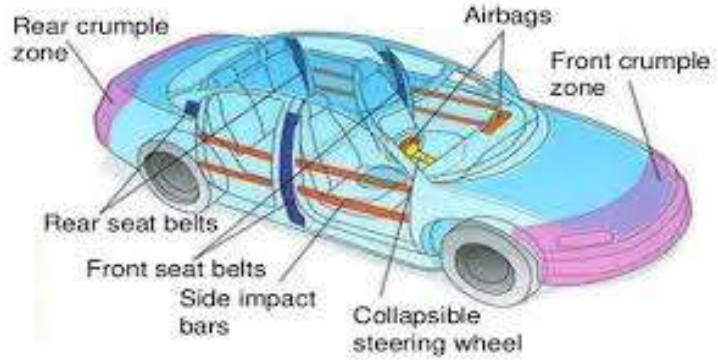
- **An event or condition that, if it materializes, could have a positive or negative effect on business objectives.**

Risk is not

- **What occurs after a risk materializes**

Scope your risks

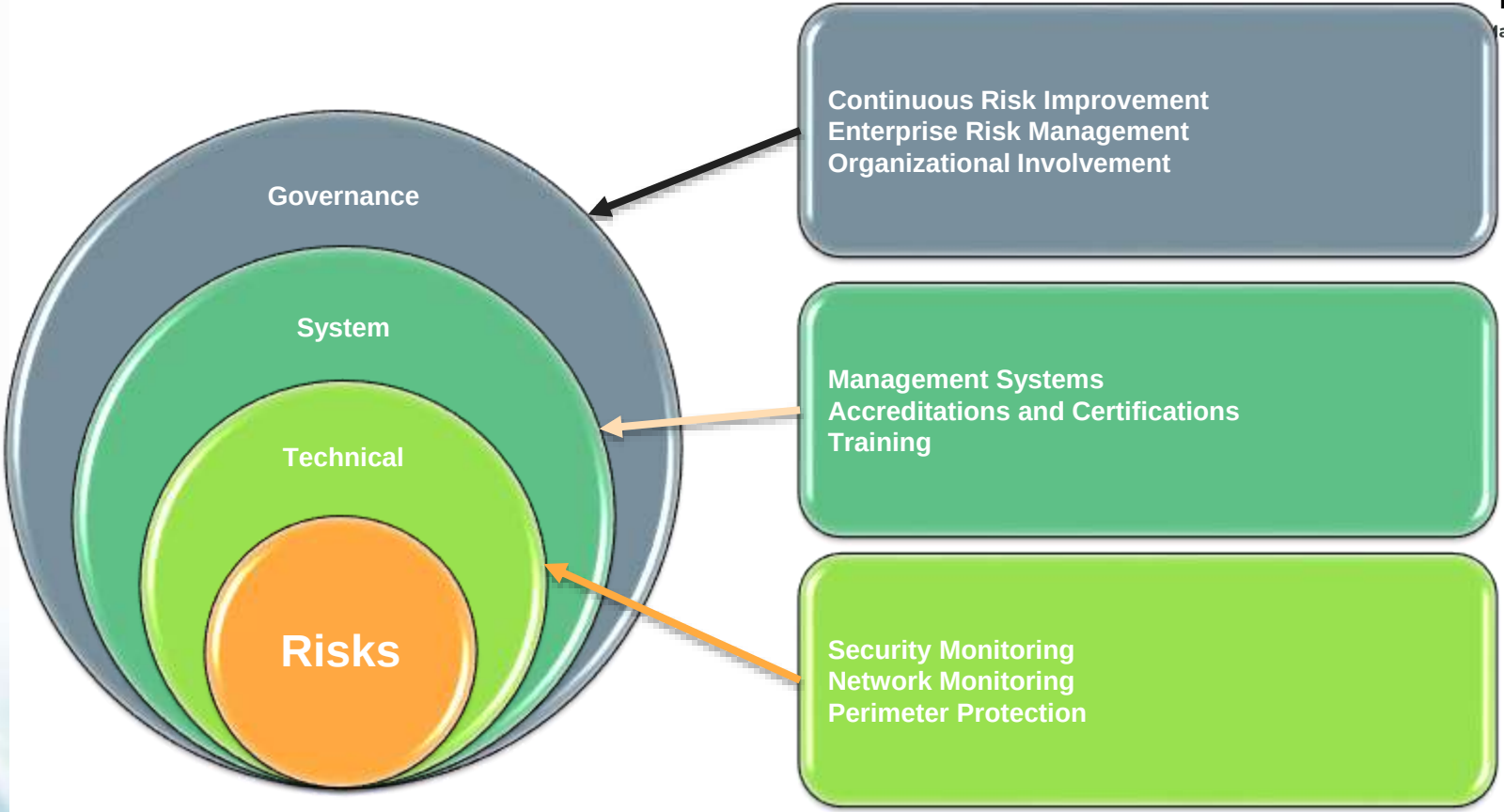
- **Risks are everywhere in your organization**



Organize to Manage

- **Risk Management must encompass the entire organization**

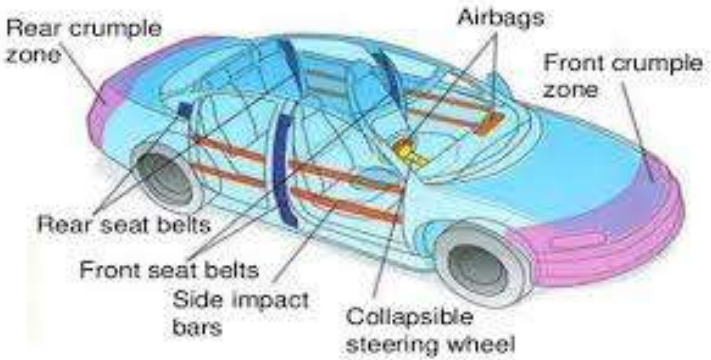
Tiered Approach to Risk Assurance



Risk Structure

What Can you do with Risk?

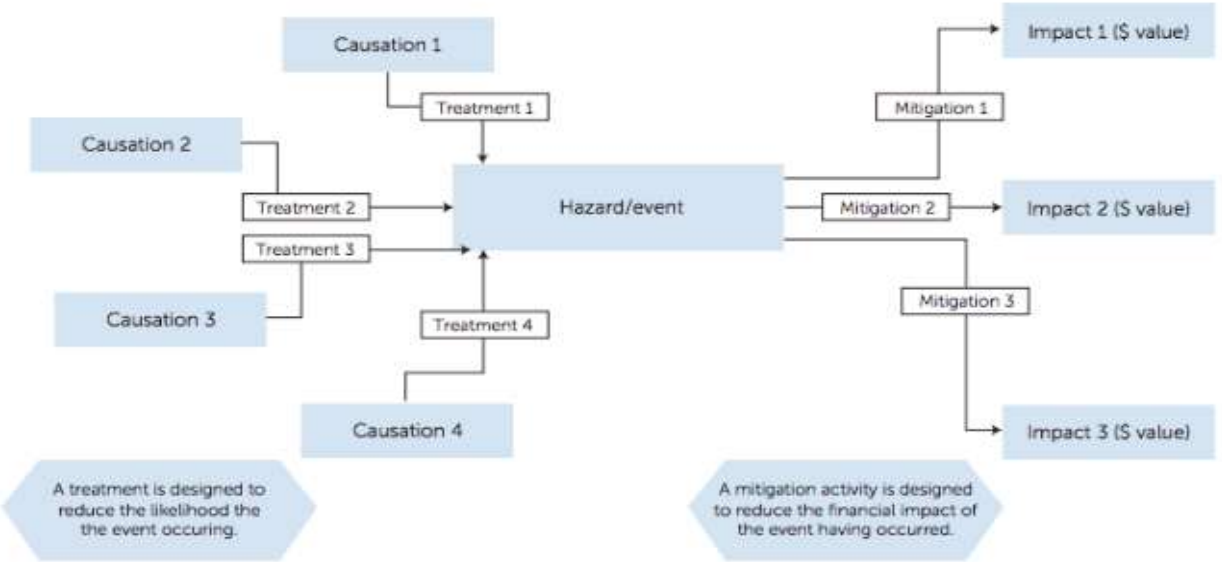
- **Accept**
- **Mitigate**
- **Transfer**
- **Avoid**



What Defines a Risk

- **Cause**
- **Treatment**
- **Mitigation**
- **Impact**

Risk Mapping - Bowtie Model



Risk Analysis

- **Likelihood**
  - The probability that a risk will materialize
  - Reduced by treatments
- **Severity/Impact**
  - The effect that would be felt if the event did occur
  - Reduced by Mitigations
- **Velocity**
  - How fast a materialized risk will affect an organization
  - Slowed down by mitigations
- **Materialization**
  - (Severity +Velocity)/2
  - Reduced by mitigations





Velocity Defined - the time to impact.

- **Low velocity provides more time to respond to the risks.**
  - Time to develop a contingency plan

- **High velocity threats strike quickly.**
  - More likely to create an impact, potentially costing more time and money.

Risk Materialization

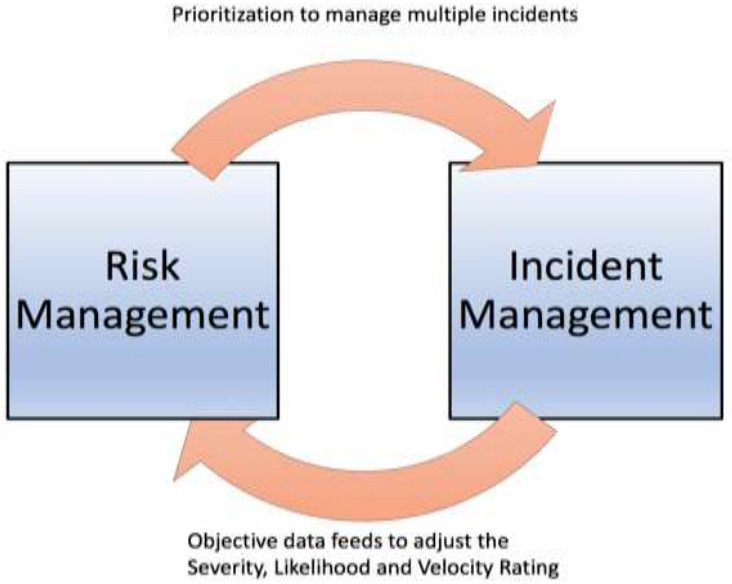
- **Materialization**
  - A measure of the impact capability of a materialized risk
  - (Severity + Velocity)/2
    - Both Severity and Velocity can be reduced my mitigations, prevented by treatments

- **Examples**
  - Risk of Rust
    - Severity – 5
    - Velocity - 1
    - Materialization – 3
  - Risk of Brake Failure
    - Severity - 5
    - Velocity – 5
    - Materialization - 5

Risk and Incident Management

Risk and Incident Management Interaction

- **Incident management should interact with the risk management system, creating an overall system of risk and incident management**



Risk based on incidents

- Inexperience
- Teenage passengers
- Distraction while driving, including from using cell phones and texting
- Driving at excessive speeds, close following, and other risky driving
- Drinking and driving. While drinking and driving is not very high among novices, it causes a disproportionate number of fatal crashes. In the later teen years and young adulthood, drinking and driving increases greatly.

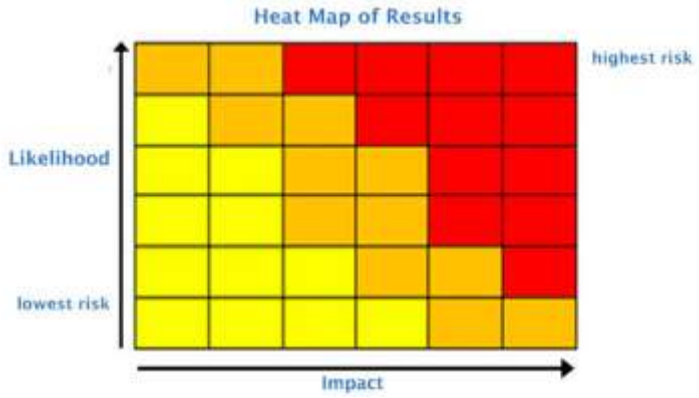
Why would business not do the same type of analysis using internal incidents?

How to measure risk

How to measure risk

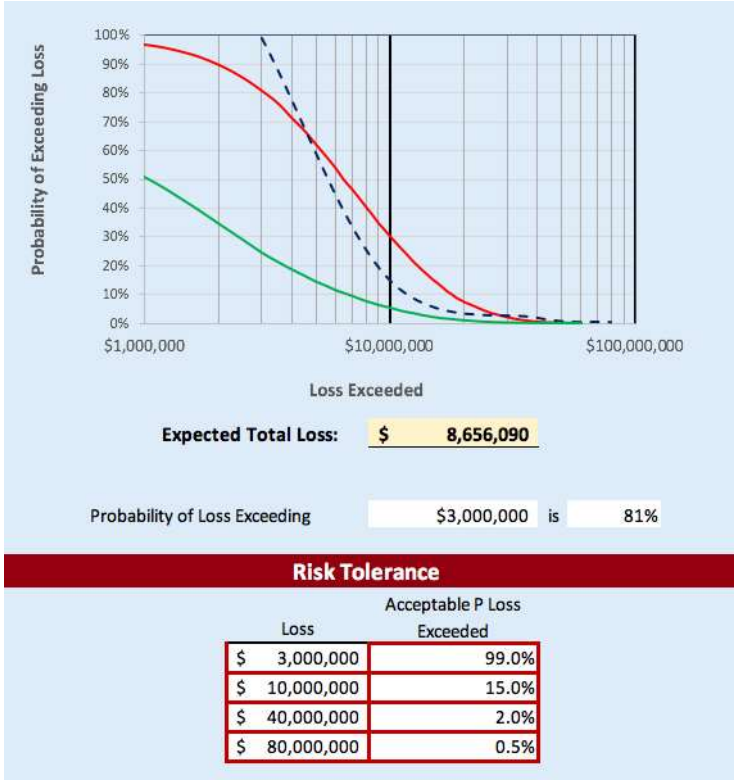
Risk Measurement

- **Standard Heat Map**
  - A way of representing the resulting qualitative and quantitative evaluations of the probability and severity of risk occurrences
  - For consistency, establish a ***risk appetite*** that is well communicated and followed



Probabilistic Risk Measurement*

- **Aims at a more quantitative approach to Risk Measurement**
  - Estimation of likelihood in probability
  - Establishment of severity in $ Range
  - Establishment of Velocity in weeks to impact
- **Can display inherent and residual risk simultaneously**



* How to measure anything in cybersecurity risk; Douglas W. Hubbard, Richard Seiersen, 2016

Building an ERM

What is an ERM?

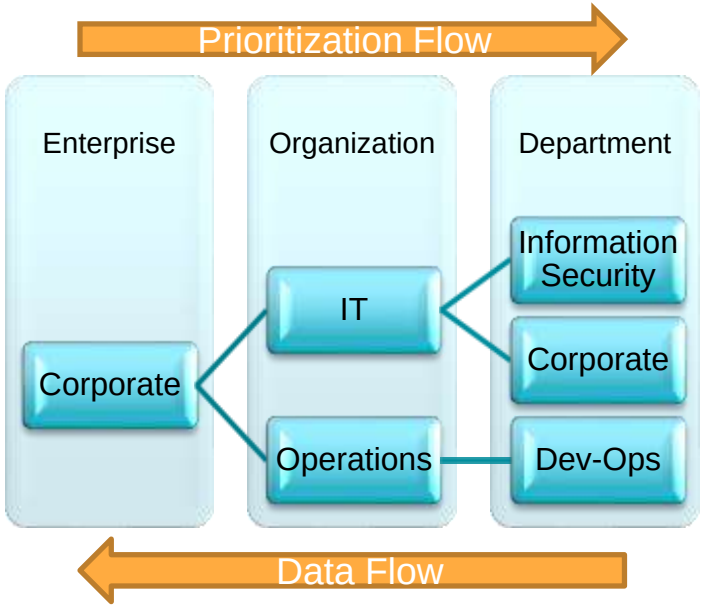
“a process, effected by an entity’s board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.” *

- **A process, ongoing and flowing**
- **Effected by employees at every level of the organization**
- **Applied across the entire enterprise, at every level and department, and includes taking an entity-level portfolio view of risk**
- **Designed to identify potential events affecting the entity and manage risk within its risk appetite**
- **Able to provide reasonable assurance to an entity’s management and Board**
- **“A means to an end, not an end in itself.”**

* The Committee of Sponsoring Organizations (“COSO”)

ERM Hierarchy

- **Risk management systems have the same structure, regardless of the size or scope of the organization or department**
  - Start small, but plan for scalability



Board and Executive Involvement

- **Start with what is relevant – A review of the key industry risks**
  - Clinical
  - Cyber Security
  - Privacy
  - etc.
- **Align industry risks with internal incidents**
  - Odds are great there is significant alignment to help create risks
- **Risk Appetite/Risk Tolerance Curve – The Board must decide**
  - Have them help develop – It is a key to focus and education opportunity

Items to watch for

- **Don’t combine Risk and Incident Management**
- **Standardize Risk Appetite or Probabilistic Risk**
  - There are proven methods to improve the estimation capabilities of the subject matter experts
- **Risk Trend Plots can be misleading**
  - Risk going down may not be caused by treatment and mitigation, but by lack of identification
- **Risk CYA**
  -

Maturity Model

How do I know I am improving?

RISQ Management Maturity Model

Reactive State

Risk Control

Organizations are focused on issues that have already occurred and are working to prevent a client impact.

Control Phases

Unknown Incident
Incident Management
Problem Solving

Proactive State

Risk Assurance

Organizations are working to prevent issues, rather than addressing the issue after occurrence.

Control Phases

Prevention
Continuous RISQ Improvement

Questions

Contact Information

Gerard Scheitlin
Phone: 615.260.4455
email: gerard@managerisq.com
web: www.managerisq.com

Gerard Scheitlin is the owner and founder of RISQ Management, a company specializing in product and organizational risk solutions. Before devoting his work fulltime to RISQ Management, Gerard was an executive leader with a thirty-year extensive background in multiple industries including Health Care, Information Technology, Automotive, Electronics, and Distribution.

Gerard is actively involved in focusing organizations on RISQ Management and Business Transformation to achieve sustainable growth and cost reduction. Gerard currently has nineteen publications ranging across multiple media platforms, and covering a broad range of topics focusing on his RISQ Model. Gerard has been a guest speaker and a panelist at a number of nationally accredited symposiums, as well as individual company summits. Gerard has been a guest lecturer at Arizona State University in the School of Biomedical Informatics.

Gerard is passionate about RISQ remediation and process improvement with a 'client-centered' approach that focuses on prevention, rather than reaction. Gerard is a Lean Six Sigma Master Black Belt with Engineering degrees from Purdue University and The University of Alabama.

RISQ Management

615.260.4455
gerard@managerisq.com
www.managerisq.com