



Security Risk Assessment

HL7 Security Working Group
DRAFT OUTLINE



Introduction



Healthcare today has some of the most diverse needs with regard to sharing of data and the need to securely move patient information among systems.

This level of data sharing requires an awareness of security in order to protect our patients.



Objectives

This cookbook covers only the risk assessment of security awareness. The focus of this briefing is primarily on healthcare information technology and the use of risk management in developing and implementing technology strategies.





The Value of Defining Security Risks

Identifying Security Risks will address:

- The Success of new technology or architecture
- Data Integrity
- Privacy Concerns
- Compliance with HIPAA
- Decreased introduction of unauthorized use
- Decision making processes

Security *must be* proactive to be effective!





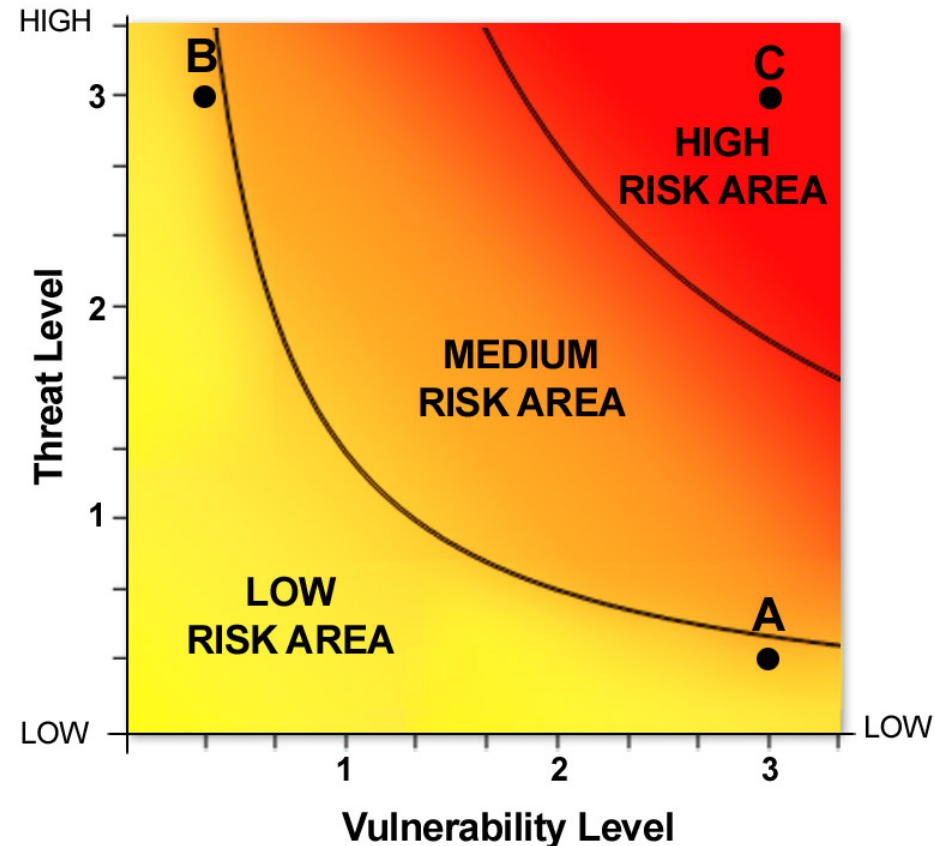
What is a Security Risk?

Risk is “The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.”
(ISO/IEC PDTR 13335-1)

To quantify risk, experts use the calculation of level of threat (probability of event) to the level of vulnerability, often stated as:

Threat x Vulnerability = Risk.

- Point A: A significant vulnerability with little or no threat = low to medium risk.
- Point B: A high threat with little or no vulnerabilities tied to the threat = Low to medium risk.
- Point C: A high threat with a credible vulnerability = high risk.

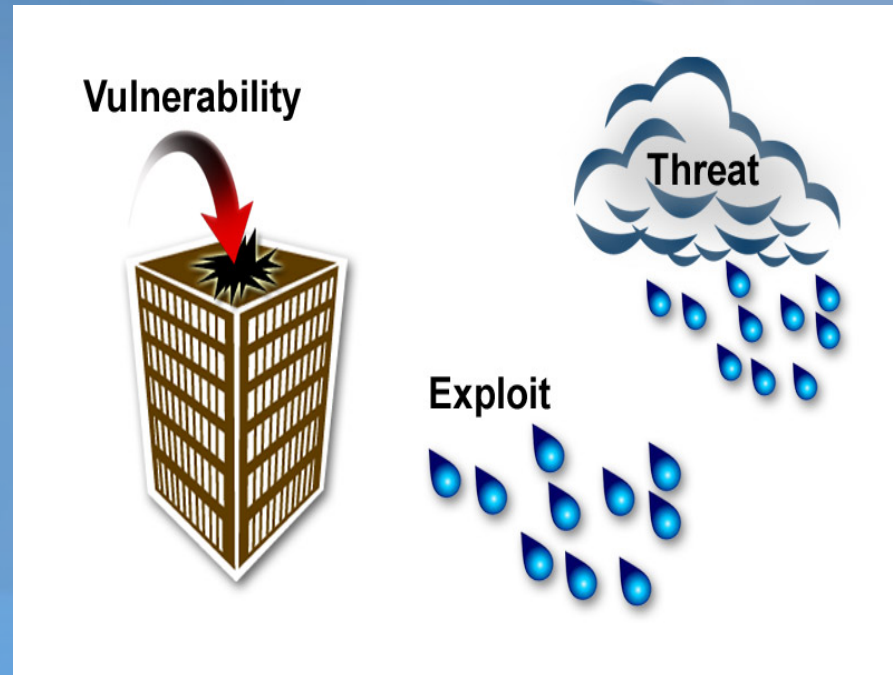


What is a Security Risk?



In this scenario:

- Vulnerability is the hole in the roof
- Threat is the rain cloud
- Rain could exploit the vulnerability



The risk is that the building and equipment in the building could be damaged as long as the vulnerability exists.

Risk Management



Effective risk management enables senior management, middle management, and technical and operational staff to:

- Improve business performance through improved decision making and planning,
- Promote innovation where taking calculated risks in pursuit of opportunities is encouraged,
- Provide a basis for integrated risk management and internal controls as components of good corporate governance,
- Assist in meeting healthcare requirements and objectives,
- Facilitate partnerships with other healthcare organizations to address the issues inherent in interoperable systems and data sharing, and
- Benefit patients who are often shared among unrelated healthcare providers in both the handling of their information as well as improving the safety of healthcare services.



Risk Management - Recognize, Identify



What are the data assets that we are trying to protect?

- What are the possible threats and threat scenarios to those assets?
- What are the vulnerabilities of the systems in place around these assets?
- What are the risks resulting from these vulnerabilities?





Risk Management – Analyze

Once a comprehensive list of risks has been prepared, assign a value to each based on quantitative business impact. i.e.,

- Likelihood of occurrence (based on the threat level and vulnerability level): Very High, High, Medium, Low, Very Low
- Consequence*: Catastrophic, Major, Considerable, Significant, Minor

*See Table 2, Source ISO/TS 25238



Risk Management – Prioritize



1. Scheduling and availability of radiation systems
2. Medication to medication conflict
3. Patient location tracking and transferrals
4. Spelling of patient name and other identifying information
5. Coding of medication order

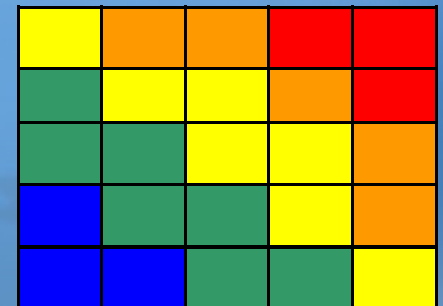
Impact / Consequence	Very High		5			1
	High					
	Medium		4			2
	Low					
	Very Low	Tolerance level				3
		Very Low	Low	Medium	High	Very High
		Likelihood				





Risk Management – Planning (Strategize)

Once the security risks have been identified and prioritized, those risks with an overall rate of 3-5 (yellow, orange or red zones on the risk map) should be documented in a risk register. This will guide the assignment, tracking and mitigation action and ownership.



Risk Management— Execute, Address



Weigh the costs of the risk versus the cost of mitigating it. To each of the prioritized risks execute one of the following tactics:

- **Accept the Risk** — Sometimes it is more prudent and effective to create a disaster recovery plan than to try to stop the inevitable.
- **Transfer the Risk** — Leverage contractual documentation to transfer the cost or recovery from a risk away from the organization.
- **Mitigate the Risk** — Initiate or Propose an activity that will reduce (not eliminate) the risk level such that it becomes tolerable enough that the focus of efforts can move to other priority risks.



Risk Management – Monitor, Review



- Monitor, Review
 - Risk register should be reviewed on a regular basis
 - Re-analyze existing risks and update status and mitigation status



Risk Management – Document



The risk register, risk map and risk summaries serve both as an audit record of due diligence as well as a valuable lesson for future risk analysis.

Keep this information for posterity!



Escalate Issues to Security WG



Issues are escalated to the Security Working Group for review by the Issue Response Team.

Issue Response Team consists of:

- Issue Response Manager
- Communications Coordinator
- Security WG Issue Consultant



Risk Issue Process



The Issue Response Team will perform a risk assessment and assist in assigning a value of low, medium or high.



Risk Issue Process



An appropriate Security WG Consultant will be assigned to create an action plan that may include documentation, a time line and a proposed solution back to your working group.



Risk Issue Process




An Issue Review Database will be created by the Security WG which will be used for:

- Tracking purposes
- Documenting and managing similar issues



Conclusion



Risk management can assist organizations in planning and implementing healthcare technology.

A properly maintained risk management program will add value to decision making and business processes but it will require an initial investment of time and resources.

