A Metrics Based Model for Risk Assessment

Introduction

Conducting a security risk assessment is essential to providing more effective security services. The results of a well conducted security risk assessment provide valuable information that can be incorporated into everyday operations and serves as a road map toward more efficient security services and continuous process improvement. In all aspects of the evaluation, metrics should be used to justify each component of the security program. A metrics based assessment provides a non-biased survey, focusing on identifying avenues to improve the capabilities of security services.

The Metrics Based Risk Assessment

Metrics based assessments utilize data to determine high-risk areas and risk probabilities. Unlike traditional assessments which rely on physically surveying the hospital to pinpoint inadequacies within the current security program, metrics based analysis highlights data to illustrate avenues for improvement. A metrics based assessment provides the security director with a view of his/her immediate and tactical concerns as well as a strategic perspective to help mitigate risk in the future.

A metrics base assessment starts with the determination of high-risk or security sensitive areas. This data is obtained through the analysis of:

- Incident data review
- Benchmarking with like hospitals
- Literature review of organizational publications
- Calls for service data
- Complaint data
- Staff and patient survey data
- Self-reporting survey data
- Industry standards and guidelines

Once analyzed, the data will yield categories to be developed that identify specific areas for improvement. Then those high-risk or security sensitive areas can be surveyed and assessed to determine what methods for improvement will be most effective.

For example, incident and call for service data broken down by incident demographics, i.e. time of day, incident type, day of the week, victim type. Benchmarking data that identifies problems other hospitals may be experiencing. Another source of data important to the assessment includes self-reporting surveys. Surveys should be developed specifically for each high-risk area and administered to staff, patients and visitors. Questions should request general information on the security of the area, like how safe they feel or do they have security concerns? Then more specific questions can be asked that relate to the data collected identifying specific areas of concern.

Once all the data is collected it should be reviewed by an assessment team. This team should be comprised of key stakeholders within the identified areas of risk along with security and senior administrative personnel. The purpose of the team is to review the data and develop recommendations to improve the overall quality of the security program. Important to the metrics based assessment is the implementation of recommended solutions.

Data acts as a baseline in determining the effectiveness of resolutions and proven quality improvement metrics for the security program, which is a language that is better understood by the C-Suite and senior management. Are you more likely to obtain $20,000.00 for a visitor management system for Woman's Health by presenting senior management with an anecdotal statement that your staff feels insecure or by presenting empirical data that includes incident reports, calls to respond and industry guidelines which document the risk of unauthorized visitors entering the Maternity unit? Additionally, monies allocated to the visitor management project can be further justified by trending its long-term effectiveness through lower incident and call rates documented over time.

Conclusion

To conduct a thorough and complete assessment, major resources must be committed to the project over a long period of time. Because of this required commitment, consideration should be given to utilizing a third-party provider/consultant who understands the metrics based assessment process. Working as a team, data collection and analyzed can be conducted by the consultant while recommendations can be developed through the in-house assessment team. Leaving the security director to focus on appropriate resolutions. Recommendations determined by the assessment team can then be documented by the consultant and given to the security department to present to the C-Suite. Follow-up can also be conducted by the consultant providing trended data to the security director that demonstrates quality improvement to the security program over time.