An alternative view in the development of healthcare security metrics

Anthony Luizzo, PhD, CFE, CST, PI (ret. NYPD) and Bernard J. Scaglione, CPP, CHPA, CHSP

The use of security metrics, according to the authors, is a much better way of improving the acceptance of security awareness programming. However, they report, healthcare security budgets continue to be based largely on the intuition of company management. In this article, they present a number of metrics that speak the language of clinical and administrative personnel and give security professionals more effective ways to validate the business of security to the C-Suite.

In an October 15, 2013 article by Scott Greaux featured in PhishMe.Com, “Use Metrics to Measure and Improve Security Awareness,” while discussing the overall importance of using metrics to improve security awareness, the author states that most security awareness programming fails to gather and/or use metrics as part of its protection mosaic. Greaux goes on to discuss the importance of gathering as much information as possible about an institution’s services so that appropriate metrics can be developed and applied to properly meet today’s and tomorrow’s challenges.

In “Persuading Senior Management with Effective, Evaluated Security Metrics” published by the ASIS Foundation in 2014, the report summarizes the need for effective metrics as follows: “Security metrics support the value
proposition of an organization’s security operation. Without compelling metrics, security professionals and their budgets continue largely on the intuition of company leadership. With metrics, the security function grounds itself on measurable results that correlate with investment, and the security professional can speak to leadership in a familiar business language. Security metrics are vital, but in the field and in the literature one finds few tested metrics and little guidance on using metrics effectively to inform and persuade senior management.”

**DERIVING MOST BENEFIT FROM USING METRICS**

Metrics is a management tool that provides a measure of performance for a given project or entity. Business Dictionary.Com defines metrics as a standard of measurement by which efficiency, performance, progress, or quality of a plan, or process, or product can be assessed. To derive the most benefit from using metrics, it’s important that security administrators understand the benefits of using metrics in their daily endeavors, and make them part of their managerial toolkits. The use of metrics to evaluate the effectiveness of healthcare security services and staff has been widely debated. Several security organizations, including the International Association of Hospital Security and Safety (IAHSS) have conducted surveys and studies to determine which metrics work best in order to evaluate a given service. To date however, no real consensus has been obtained on what works best. On the contrary, many different ideas have been brought forth and many different types of metrics are used by healthcare organizations.

Oftentimes, most security executives rely on individual security expertise when developing metrics. These metrics are understood by the security professional but have not gained ground outside of the healthcare security field. Consultants and senior executives alike have not seen real value in security metrics, and in general dismiss them as being ineffective or demonstrating no real value to the evaluation process. In “Persuading Senior Management with Effective, Evaluated Security Metrics” the authors discuss the criteria for evaluating an effective...
security metric. They state that a security metric should be reliable, have validity and have generalizability. They should operationally demonstrate cost, timeliness and be manipulative. They should be strategic demonstrating return on investment, organizational relevance and be easily communicated.

IDEAS THAT DESERVE CONSIDERATION

PRODUCTIVITY INDICATORS:

Clinical Length of Stay/Discharge Rate. On the surface, it appears that there is no real value in the use of length of stay or discharge rate when evaluating security services; and in general, that is true. Alone, this metric holds no real value in the determination of service relative to the security of patients, visitors and staff. But, when we compare these rates with the long term evaluation of incident rates or calls for service, we can compare the effectiveness of monthly or quarterly service by monitoring its highs and lows. This metric works because when length of stay is low, and discharge rate is high, the number of patients and visitors within the hospital is greater. In theory, the number of incidents and calls for service should be accordingly higher as well. When compared over time, the security department can demonstrate value by showing a decrease in the incident rate when more people are using the hospital. Comparing security-related incident rates or calls for service with length of stay or discharge rates illustrates the effectiveness of security services as compared over time and to other hospital departments that utilize the length of stay metric in evaluating service.

Square Footage. Although it is clear that square footage alone is not a valuable metric in the evaluation of security services, it is a statistic that many consultants rely upon in evaluating healthcare support services. For security services, the amount of square feet does not wholly determine the amount of staff necessary in order to provide a safe and secure environment. Still and all, this statistic can be useful in demonstrating the effectiveness of services. The value of using square footage as a metric is its acceptance with consultants and the C-Suite alike. This metric demonstrates its value...
when compared to security data over time, or with other facilities of similar square footage. If the call for service rate is higher in comparison to other facilities, or increases over time, the metric demonstrates an increase in the level of service and suggests the need for more staff. If the incident rate is lower over time, or lower than other similar institutions, the security service is efficient in its delivery.

**WORKLOAD/CALLS FOR SERVICE**

“Touches.” Generally, security departments report the number of incidents that occur, the number of patrols conducted, or the number of visitor passes dispensed. These statistics, no matter how they are presented, demonstrate the amount of work that the security department produces in a given time period. It does *not* show the value of the service provided. However, if the data collected shows how many times the security department interacts with patients, visitors and staff, coupled with the type of interaction furnished, then the security department can demonstrate its value and effectiveness based upon the patients, visitors and staff served. So, what metric is important in the evaluation of calls for service? *Ergo, then “Touches” is the metric that should be used!* Touches are not the number of patrols conducted, or the hours that an officer held a post, it is the interaction with the customer and the results of that interaction. Reporting the number of times security accompanied and/or assisted staff to their designation, provided directions or escorted them to their vehicle, is a more definitive evaluation of the service as compared to the number of patrols conducted or the hours an officer stands post. Many times security departments will document and report the number of doors they unlocked or the number of doors that were found unlocked and/or opened. With respect to these types of assignments, opening a door for a staff member is a touch. In this case, a staff touch can be both a positive and negative metric. Having a high number of touches to assist staff in a non-patient related way may not be seen as a positive metric when it is compared to patient and visitor touches. Comparing the number
of staff touches with patient and visitor touches can demonstrate the need to reduce staff interaction or increase patient and visitor interaction, translating to less door openings and more facility patrols.

**Near Misses.** The term, “Near Miss” is used in the healthcare setting to indicate the intervention or discovery of an incident or event that *could have been adverse*, but was averted. This concept can be used in healthcare security since it is more readily identifiable than a door found open, a behavioral health patient that tried to leave the hospital and was stopped, or the continued denial of an access card being presented to a storeroom or high security door. In lieu of reporting the number of doors found open, reporting a near miss related to a purse left unattended or a computer that could have stolen is a better, more understandable, metric. Not reporting the patient who almost left the hospital or the employee who is continually trying to access a door that they have no access to, negates the effectiveness of the security services provided to the institution. A near miss is an evaluation tool to which risk management, nursing and administration can relate.

**Interventions.** An intervention is a term that is used in the healthcare profession generally in the behavioral health arena. An intervention is a planned or unplanned interaction with a patient or client because of negative or potentially negative behavior. A patient restraint is an intervention; a patient watch is an intervention, a disruptive patient or visitor is an intervention. An intervention is a metric that can describe aspects of the execution of the security operative’s job that is not demonstrated by reporting basic workplace violence. Using interventions as a metric demonstrates actions taken to improve a declining or detrimental situation, and can be used to categorize the workload conducted by security staff in the prevention of violence within the hospital. This phraseology helps behavioral health administrators better understand the use of this metric by security and can provide a more defined application of security services.

**Staff Configuration/Work Force Management.** Staff configuration and/or work force man-
agement is the evaluation of staffing requirements and the costs associated with labor and other expenses, and are another metric that can be used to evaluate the effectiveness of security services. Generally, the security professional sees work force metrics as the cost by officer post or hours worked, two metrics that provide little insight into the financial value of security services as seen by the fiduciary administrator. In finance, the value of service is determined by the expense or the cost compared to patient care data or industry known metrics.

As such, in order to show value within financial metric circles, expenses should be compared by square foot or discharge rate. Comparing labor expenses or overall security expenses with square footage or discharge rates alone has no real value in determining the effectiveness of security services; but when compared over time or with like facilities, these metrics can demonstrate the value of security services over time. These metric measurements speak the language of the fiduciary aficionado. Experience demonstrates that the best metrics to use in fiduciary-related situations varies from entity to entity. Besides labor or expenses compared to square footage or discharges, financial data should be determined based on exceptions. In finance, exception reporting paints a true picture as to the state of expenses and overages that plague budgets. So, items like overtime, sick time, injury time off, accidents or breakdowns in vehicles and extra training are all examples of exceptions that influence budgets.

**Other Metrics.** From a programmatic perspective, the best metrics for security executives in the healthcare environment to employ are those metrics that hospital administrators know and understand. These may include: demographics related to employment/background checks, equipment outages, emergency responses, and policy and/or procedural violations. Finding the appropriate metric to exploit is limited only by the security administrator’s imagination.

**CONCLUSION**

Metrics are an effective way to validate the business of security to the C-Suite. By speaking the
language of clinical and administrative personnel, metric use and evaluation can better position the security department in the evaluation of services and its value to the organization. Beyond simply using metrics, it’s imperative that a dashboard be developed to appropriately monitor and evaluate whether programmatic standards and metric applications are within acceptable, defined compliance standards. A dashboard consists of a series of graphs or data points presented on a single sheet of parchment, or on a computer screen that furnishes a clear picture of the task at hand. Applying effective mathematical metric measurements gives the security professional the capability of deciphering adverse incidents before they have an opportunity to adversely impact the intuitional setting.

**Selected Bibliography**