Improving security program effectiveness through data-driven decisionmaking

Katherine Eyestone and Shon Agard, MS, CHPA

Following this step-by-step guide to collecting data can help you to maximize your security resources and explain your decisions to administrators.

(Katherine Eyestone is the Chief Transformation Officer, and Shon Agard, MS, CHPA, is a Business Analytics Manager, at HSS, based in Denver, CO. Both are members of IAHSS.)

Most healthcare security leaders today are under pressure to figure out how to maintain or improve the quality of their programs while at the same time manage shrinking budgets. The challenge of how to optimize security services can be made harder when it is difficult to quantify the impact of a security program or when the preferences of hospital administrators dictate the design of security. An important tool that can help healthcare security leaders navigate this challenging terrain is utilizing data to objectively inform resourcing decisions. While not a substitute for security experience and expertise, utilizing data can create more of a balance in terms of how expertise and evidence work together to inform security program design, as shown schematically in Figure 1.

Figure 1. The Balance of Security Expertise and Evidence

Data such as benchmarks can help security leaders answer questions such as the following:

- How do I optimize my budget for security?
- What is my justification for increasing my budget?
- How do I know if my security program is effective?
- How does my security program benefit my organization?

It can be challenging to figure out how to utilize data to make security program decisions when this information is not yet widely available in the industry. However, many security leaders, particularly those in multihospital systems, likely have enough data available to get started. In this article, we

- explain why it is important to consider Security's ability to impact security incidents when designing security programs,
- provide data and tools that will help leaders understand how to compare various healthcare facilities based on risk, and
- explain some simple ways that security program leaders can begin to leverage data for decisionmaking.

EXPANDING THE DEFINITION OF HEALTHCARE SECURITY *QUALITY*

When tackling the question of how to optimize security resources, you would be wise to expand your definition of the *quality* of a healthcare security program. Traditionally, the quality of a healthcare security program has been defined largely in terms of *process* and *structure*. Examples of quality *processes* are adhering to well-written post orders, monitoring of rounding, and following protocols for documentation of security incidents and activities. Examples of *structural* quality indicators are training requirements

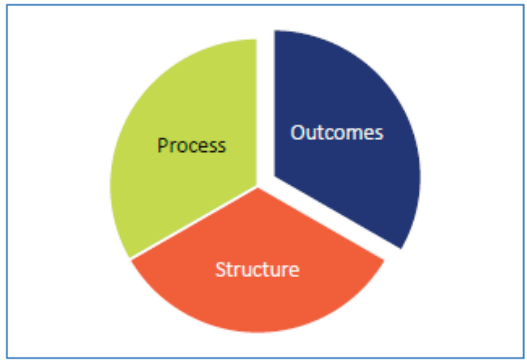
for officers, staffing schedules, and leadership-to-staff ratios. Process- and structure-focused quality indicators are types of "performance measures."

A new element of quality that we recommend you incorporate into your planning is the impact of your program on *outcomes*—which is to say, security incidents. (See Figure 2.) Because workplace violence is a predominant security concern in healthcare, a good place to start is by looking at the number and severity of assaults that are occurring across the locations for which you are responsible. In addition to tracking assaults documented as security incidents, you might also ask your organization for workers' compensation data for claims related to violence. Assessing security program quality in terms of its ability to impact security incidents produces "effectiveness measures."

The notion of expanding the definition of healthcare security quality to include impact on incidents, or outcomes, parallels what has happened in the field of healthcare delivery over the last roughly two decades. Healthcare quality used to be defined primarily in terms of processes (such as accurately following care protocols) and structure (which relates to things like the proper training and education of care providers) or by the ratio of care providers within a clinical area. Today, the emphasis is on outcomes. Did the patient have to be readmitted? How well did the patient recover from surgery?

Moving into this space of impacting outcomes is important for enabling a security program to demonstrate its full value. Think

Figure 2. The Three Dimensions of Security Program Quality



about it: If you can measure and reduce the cost of assaults over time, you can quantify the value of that achievement to your organization (an amount well above the direct spend on security).

HSS's early efforts to analyze healthcare security data focused on identifying the key drivers of security incidents. By utilizing multivariate regression analysis, HSS analyzed data from the more than 100 healthcare facilities we secure to determine the factors that are statistically significant drivers of security incidents. (HSS's statistical modeling explained 76% of variance in "crimes against people" and 71% of variance in "crimes against property.") Of the many kinds of data studied, the types shown in Figure 3 were found to have a statistically significant impact on security outcomes, particularly crimes against people.

Understanding the statistically significant factors that impact security incidents will be useful as you consider how to best organize your security program. Below are several initial steps a security program director can take to inform data-driven decisions about security program design.

STEP 1: BUILD A DATA SET

The first step toward data-driven decisionmaking is to collect and organize available and relevant data. The spreadsheet in Figure 4 illustrates the kinds of data that may be useful, including:

• **Risk Characteristics.** Overall national crime forecast/index

Figure 3. Statistically Significant Drivers of Security Incidents

Type of Variable	Statistically Significant Variable
Hospital Community Demographics	• Overall National Crime Forecast/Index Score (See note.)
Hospital Size/Volume Characteristics	• Annual Emergency Department (ED) Visits
Security Program Characteristics	• Security Officer Tenure • Presence of TASERs • Presence of Magnetometers

Note. HSS utilized Crimecast by CAP Index score data for the referenced statistical modeling.

score and annual ED visits are important to document because they are known statistically significant drivers of security incidents. Give some consideration to additional characteristics of the hospitals you secure that may increase risk. If there are other important considerations, such as the presence of a behavioral health unit, document that information in a simple spreadsheet by facility, as shown in Figure 4.

• **Security Program Characteristics.** Document basic information about the structure of the security program in place at each location. Unlike the risk characteristics of the hospital, security program characteristics are factors that you can control, and that you might change based on the results of your analysis. You might think of them as levers to be adjusted to improve security program effectiveness. Information such as the number of security officer hours worked per week, management hours worked per week, presence of TASERs or magnetometers, and tenure of the security officers should be documented.

Note that HSS's statistical analysis showed that security officer tenure is a statistical driver of security incidents. This measure is of the tenure of the team of officers in place at a location. As the team tenure increases, security incidents decline. This finding would suggest that officers with more healthcare security experience are able to more proactively manage and de-escalate situations before they become security incidents. This may not be information you have readily available but, because it has been shown to be statistically impactful, it is information worth calculating and documenting.

Figure 4. Building a Data Set

	Risk Characteristics			Security Program Characteristics					Security Outcomes		
	Crime Index	Ann ED	BH Unit	# SO Hrs/Wk	# Mgmt Hrs/Wk	TASERs	Magnet	SO Tenure	Assaults	Threats	WC Claims - Assaults
Hosp 1											
Hosp 2											
Hosp 3											
Hosp 4											
Hosp 5											
Hosp 6											

HSS's statistical modeling also revealed that the presence of conducted electrical control devices (TASERs) and magnetometers can reduce the number of security incidents by statistically significant amounts. In our data set, we typically found TASERs and magnetometers in hospitals serving communities with an overall national crime index score of 280 or higher; if TASERS and/or magnetometers were added to the security program in a community with a lower crime index score, they would be unlikely to statistically reduce the number of security incidents.

• **Security Outcomes.** Figure 4 illustrates several types of security-related outcomes data, all of which relate to workplace violence. It is likely that your program collects the number of assaults that occur per location, and that you may be able to obtain data on workers compensation claims due to assaults per facility. You might also collect data on threats of assault. You can begin to quantify security's impact in terms of dollars as a reduction in workers' compensation claims. The point is to utilize available security incident or related data. If thefts or other types of crimes against property or people are a concern within your organization, expand your data collection effort to include that information.

STEP 2: RISK-STRATIFY HOSPITALS

Utilizing a risk-stratification model will enable you to objectively identify the relative risk of each hospital you secure. As noted, in HSS's statistical modeling, we found two characteristics of hospitals to have a statistically significant impact on security incidents: overall national crime index score and annual ED visits. These are the only non-security program characteristics with statistical impact identified to date in our statistical modeling and, as such, they are an initial basis for delineating the relative risk of each hospital covered by your security program.

These two factors can be used to construct a simple risk-stratification model, as shown in Figure 5. If you know the range of annual ED visit volume across the hospitals in the organization that you secure, and you determine the range of crime index scores they represent, you can construct and populate this simple model. From

your specific data set, delineate what sub-range is a "small" number of annual ED visits, versus medium and large. Similarly, determine from across your hospitals what the low end of the crime index score range is, versus medium and high. Facilities that fall into the darkly shaded boxes in the lower left represent relatively lower risk. Facilities that fit into the top left to lower right boxes (light-colored boxes) are medium risk, and the darkly shaded boxes in the upper right indicate the facilities of highest risk based on crime index score and ED visit volume.

Plot your facilities into the 9-box to see which fall into the low, medium, and high-risk categories. It is important to note that there may be other considerations, such as the presence of a behavioral health unit at one of the hospitals, that increases the risk of that facility compared to the others. In our statistical modeling, we did not specifically test to determine whether the presence of a behavioral health unit within a hospital has a statistically significant impact on security incidents. When your experience and intuition tell you that there are additional important hospital characteristics like this to consider, use your judgment and adjust the plotting of the facilities as appropriate. For example, assign the hospital with the behavioral health unit a "higher" risk if your experience

Figure 5. 9-Box Risk-Stratification Model

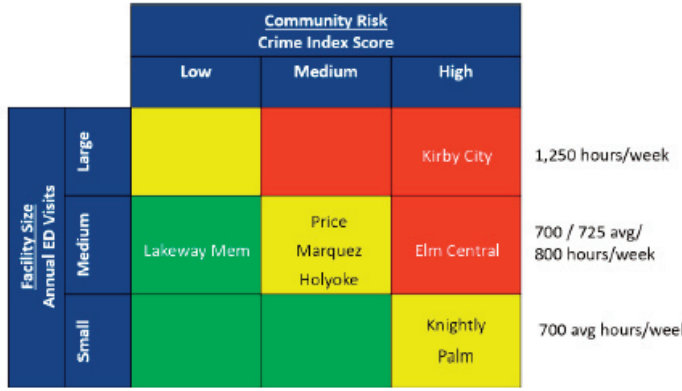
tells you that this assignment would be a more accurate categorization. For most facilities, we expect that the risk stratification based on ED visits and crime index score will produce a fair representation of the relative security risk.

STEP 3: CALCULATE BENCHMARKS

Benchmarks are simple points of comparison. After you have plotted your facilities into the 9-box risk-stratification model, look for boxes with more than one facility in them, and create benchmarks by averaging the data of the facilities in each box. Figure 6 provides an illustration of this process. Note that the names of these facilities were selected at random and do not represent an actual hospital system.

One type of data that can be averaged to create benchmarks is security program data. Let's use security officer hours worked per week as an example. By averaging security officer hours worked per week, you can begin to see approximations of "community standard" security program design for facilities with a given level of risk. This information begins to reveal which facilities at a given level of risk have relatively high or low levels of staffing relative to facilities with a comparable level of risk. As you consider the number of hours

Figure 6. Populated Risk-Stratification Model with Benchmarks



worked to the relative risk present at each location, this information may begin to reveal opportunities to invest or reduce investment in the security program at a given site.

This same technique can be useful for developing simple benchmarks for other security program elements, such as security officer team tenure.

Another type of data that can be averaged to create simple benchmarks is security outcomes data. Again, working with data from hospitals within a particular box of the 9-box, average the number of security incidents by type—assaults, for example (see Figure 7). Remember that the hospitals have been stratified by risk level. It is reasonable to expect a similar number of assaults to occur in hospitals with similar risk. Where variation in the number of assaults is present among facilities of similar risk—particularly when those trends have persisted for numerous reporting periods—it is worth digging deeper to understand what differences in security programs or other factors might be contributing to these varied results.

Use this comparative information to identify potential best practices to improve your security program. In the example shown

Figure 7. Variation in Security Outcomes

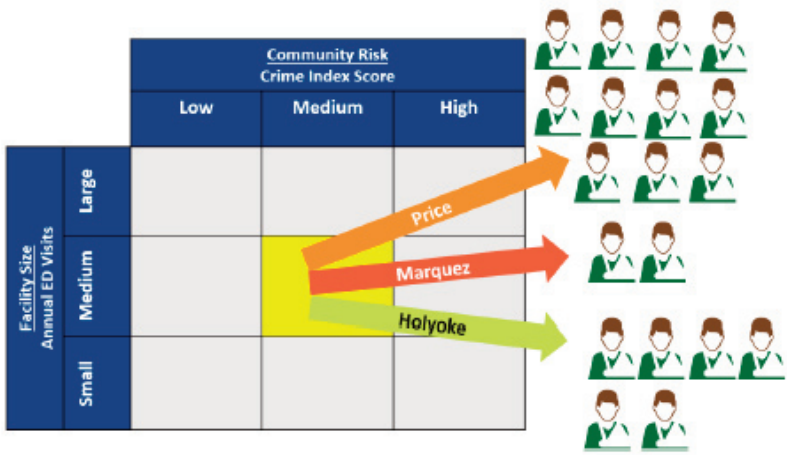


Figure 8. Data-Driven Security Program Adjustments

	Lakeway	Price	Marquez	Holyoke	Kirby City	Elm Central	Knightly	Palm
Risk Stratification	Low	Med	Med	Med	High	High	Med	Med
Current Security Officer (SO) Hours	700	750	750	675	1,250	800	900	500
SO Hours Benchmark	700	725	725	725	1,250	800	700	700
Additional Risk Factors		Behavioral Health						
Assaults	1	10	2	6	15	12	8	12
TASERs	-	-	-	-	-	-	-	-
Magnetometer	-	-	-	-	√	-	-	-
SO Tenure	Low	Low	High	High	Low	High	Low	Low
ACTION		Bump to 800 hrs; Add TASER, Add more experienced officers	Drop to 725 hours	Bump to 725 hours		Add TASER	Drop to 700 hours	Bump to 700 hours

in Figure 8, Price, Marquez and Holyoke Hospitals have similar crime index scores and ED visit volume, yet Marquez has notably fewer assaults than the other two facilities. Price not only has the highest number of assaults but also the additional risk factor of a behavioral health unit. A security director could bolster Price's security program by placing and/or attracting more tenured officers there (since improved officer tenure contributes to reductions in assaults) and could also redistribute security hours from Marquez to Price and Holyoke, as indicated in Figure 8. In this way, statistical data and benchmarks are informing decisions to improve, if not optimize, security program effectiveness across the hospital system.

OVERVIEW

Taking these simple steps to utilize data in decisionmaking will, over time, result in more objective decisions that will help counter preference-based security program design. As your database grows, you will have an improved ability to trend security incidents over multiple study periods, which will lead to greater understanding of the impact your security programs sustain over time. If you lack the data to create the benchmarks described in this article, consider the following:

- Create benchmarks by pooling and averaging data for all the

hospitals in each risk tier. For example, lump the low-risk hospitals together and average their results to create benchmarks.

• Build a network of peers at hospitals with crime index scores and annual ED visit volume roughly equivalent to your facility. Sharing basic data such as shown in Figure 8 will enable you to calculate benchmarks or community standards to which you can compare the structure and effectiveness of your facility.

• Participate in industry-wide efforts to gather data for purposes of developing community standards, such as IAHSS's benchmarking data project.

• Consider utilizing the services of a third-party healthcare security consulting firm that incorporates community standard benchmarking into its risk assessment methodology.

Most importantly, recognize that utilizing data to drive healthcare security program decisions is a journey. Like other fields that preceded healthcare security, early stages often rely on imperfect and incomplete data, which improves over time. The key is to gain experience and confidence in using data to drive decisions and use those early wins to demonstrate how data can enhance the decisionmaking process.