Technology Intelligence

ALLIEDBARTON® SECURITY SERVICES

Local Response | National Support

Technology Intelligence: Tour Management Data

By David Feeney, IT Director, Integrated Solutions, AlliedBarton Security Services

The last in this three-part series on the value of security data will review Tour Management systems. Many security professionals have had some experience with Tour Compliance systems, often comprised of pipes and buttons and used to simply monitor that a security officer's "rounds" or tours are completed as scheduled. The more advanced systems enable deliberate scheduling of security officer rounds from one checkpoint to the next, increasing the officers' visibility and acting as a force multiplier.

Tour Management systems can be even more future-focused with the utilization of a mobile device, opening the door to automated instructions to the security officers and questions for security officers to answer at each checkpoint in real time. This enables the addition of data collection capabilities to Tour Compliance systems, and thus adds the "data collector" function to the role of the security officer.

The result is two core benefits. The expanded security officer's role, made possible by incorporation of this technology, increases the value and ROI of an organization's security investments. And, the data that officers collect in their expanded roles provides significant value of its own by enabling analysis and program adjustments to mitigate identified risks and improve security strategy.

All checkpoints typically have questions associated with them, and more advanced Tour Management systems allow for different customer-configured question sets at various checkpoint types such as entrances, escalators and emergency callboxes. This data can be easily analyzed through simple reports to identify operational risks. These risks might include policy issues, such as specific doors repeatedly being left unlocked; safety issues, such as recurring hazards at specific escalators; or maintenance needs, such as inoperative callboxes.

A security officer may be tasked with performing daily tours of a facility and checking fire extinguisher inspection dates on a monthly basis. Tour Management systems enable the daily tours to include checkpoints near fire extinguishers that prompt the security officers on a monthly basis to enter the fire extinguisher's inspection date, essentially combining two tasks and providing additional value to the existing security service. To take that a step further, a report can then display fire extinguishers sorted by inspection date. These additional functions increase efficiency, simplify post orders, enhance compliance, and reduce costs.

As an additional example, security officers may also be tasked with monitoring temperature readings in storage containers, in addition to their daily tours. Checkpoints at these assets can be configured to prompt for temperature, and then prompt with instructions and notify key personnel if temperatures are outside of a pre-configured range. Reports can also be created to identify faulty thermostats based on historical data from past rounds.

When used in this capacity, Tour Management systems are automating post orders; initially to ensure completion of assigned tasks, but ultimately producing a pool of data from which trends are identified and concerns rectified. The end result is an optimized security officer force and, in turn, a more efficient security program.

There are many technology solutions available to enhance and support the services provided by security officers. When the solutions are selected to meet the specific needs of a security program, and the intelligence gained is utilized to fuel strategy, the return on security investment is compounded and safer and more secure environments are created.

Technology Intelligence

AlliedBarton® Security Services

Local Response | National Support

Technology Intelligence Fuels Security Strategy

By David Feeney, IT Director, Integrated Solutions, AlliedBarton Security Services

Security technology can be an incredible asset for your daily operations, but the data it generates also brings clarity to future needs. Process improvements, program changes, establishment of metrics, and funding requests become more strategic when built on a foundation of intelligence.

While intelligence is sometimes not the primary goal of implementing technology into a security program, it is often its most valuable result. Among other things, technology captures and stores relevant data, and then presents it in intuitive views. Filtering, sorting, and grouping data leads to measuring, trending, and quantifying – which delivers actionable information. That intelligence supports security strategy and enables optimized security officer deployments, precise post orders, directives for specific threats, and countermeasure deployment to enhance security in areas where it is needed most.

This introductory installment of my three-part series will examine two critical technology features that maximize an organization's ability to create intelligence from data.

Customer-Configurable Forms

Software providers initially configure their software to capture and store the data that they believe important to their customers. While that is a good start, no one knows your requirements better than you. These canned forms would require customization if you request changes or additions. To address this, many software packages add user-defined fields to their forms, which can be configured by customers to capture additional data. But the most advanced systems go beyond user-defined fields and allow customer-configuration of forms and fields. This is the solution that creates a truly tailored experience.

Another important attribute is the ability to capture customer-configured data in the system's reports. Some software reports may be limited to capturing only the canned fields. This leads to the second Ecritical function…

Flexible Reporting

A system's reporting engine is what converts data into intelligence. No matter how much meaningful data is captured, it is only useful if it is accessible and organized in a digestible fashion. For example, consider the difficulty of identifying a mall's high-traffic areas from a list of shoppers in a given month, as opposed to the easy review of a graph of incidents grouped by location for the same period. It is the reporting engine that simplifies "big data" for security personnel and brings the information, and needed changes or enhancements, to life.

Canned reports offer views of system data that the vendor believes will be valuable to their customers. More advanced systems have ad-hoc reporting that allows users to build reports to suit their needs. Some advanced systems also include the ability to save new reports and even publish them to other users.

The next two segments of this series will examine the valuable data within two specific types of systems: Incident Management systems and Tour Management systems for security officers. These and other technology solutions can create efficiencies, target security efforts and give security leaders the power to make informed decisions that deliver even greater return on their security investment.

Technology Intelligence

AlliedBarton Security Services

Local Response | National Support

Technology Intelligence: Incident Management Data

By David Feeney, IT Director, Integrated Solutions, AlliedBarton Security Services

Incidents, though often unfortunate, deliver an incredible opportunity to not just respond to and correct the situation, but to compile and analyze data that can greatly contribute to security strategy. This effort has evolved over time with the adoption of security technology.

Organizations commonly implement incident management systems to address challenges with lost, illegible or incomplete incident reports. The drive for sustainability also plays a part. Beyond the ease of use, efficiencies and mobility gained, forward-looking organizations also understand the automation possibilities of utilizing such a system.

Arguably the most important feature of an incident management system is the reporting engine, which is the primary tool for data analysis. Reporting is what prevents a system from becoming a black hole for data. The more flexible a system's reporting functionality is, the more powerful its data can become. Incident data can help to guide the evolution of an entire security program. It can enable an organization to deploy countermeasures against the specific threats and adjust their deployments as threats evolve.

An incident management system's reporting interface should allow users to easily identify sites, areas within sites, time ranges, days, months and seasons of high or low incident volume based on the historical data in the system. This is most useful in setting staffing levels for security officers. Many organizations are surprised by the degree of opportunity they have to move staff from low-volume to high-volume shifts, areas or sites in order to increase efficiency. This results in safer properties and improved risk mitigation, which in turn reduce costs to the organization.

An incident management system should also enable the rank-ordering of incident types on number of occurrences, costs to the organization, or resource utilization. This is most helpful in prioritizing risks for future mitigation, and using the severity and total cost of an incident type to determine the importance of mitigating it. Also, knowing the potential cost of a type of incident allows the security professional to understand the value of mitigating it, which is a key determinant of the elusive return on security investment (ROSI).

The incident management system's data can then be used to compare total incident cost before and after the implementation of a countermeasure, which is the primary component of ROI for that countermeasure. When done on a repeated basis, the average ROI can serve as a predictor for future implementations. This becomes even more powerful if sites are grouped based on similar risk profiles or assessment results. An organization can then conclude that sites with similar risk profiles will experience similar results from implementation of a given countermeasure, and repeat the cycle by measuring afterwards to determine success.

The results of an incident management system are simple – better information. How each organization utilizes that information is up to them but the knowledge it affords is undeniable.

There are many technology solutions that generate data to support security strategy. The next segment of this series will examine the security data to be gained from tour management systems.