

## RECORD AND DOCUMENT SECURITY

An important element of the overall services provided by companies that store records and/or destroy documents are securing the records throughout their storage and the documents prior to their being destroyed. If any records or documents are compromised or stolen, the reputation of the company within the information management industry would be in jeopardy, as would the company's longevity. In fact, most clients expect or demand some level of security for their records and documents. The question then is: what are the most effective methods of securing these documents, both from an industry best practices and cost benefit point of view? In essence, what security measures should be included in the company's security program?

The type and complexity of security measures that a company will implement depends on the needs of their clients based on the security classifications of records and documents that are being stored or destroyed. Sensitive financial records may require a more stringent and complex security strategy than some other type of document. Some degree of security measures will certainly be necessary; otherwise the records would not need secure storage or the documents would not need to be destroyed in the first place. Client demands based on record classification along with industry best practices and reasonable budget constraints will define the type, functionality and size used of the security measures described herein.

Securing these records and documents is accomplished by securing the facility that holds them and controlling the entrance and exit of them to and from the facility. Securing the facility that holds these records and documents is a matter of controlling access, both to the facility itself and to the specific areas within the facility where the records are stored or the documents are destroyed. Controlling the entrance and exit of the records and documents to and from the facility is a matter of proper inventory tracking and visual identification and verification. Both facets of record and document security are best accomplished by a combination of physical security, policies and procedures and personnel. No security program is complete or effective without some combination of these three security elements.

Physical security is used to restrict access to a facility in different manners depending on whose access is being restricted and when. In order to disallow unwanted access to a facility from outside intruders after business hours, locks and lighting are the first steps in that process, and very important steps. Other physical security measures in place become far less effective and in some cases completely worthless if the locks and exterior lighting to a facility are inadequate. Most companies are conscious of these measures and have them implemented. In terms of electronic physical security measures, a burglar alarm system is most common and is for the most part effective and inexpensive. In general and non-comprehensive terms, magnetic sensors are installed on exterior (or interior in some cases) doors and windows, motion detectors or glass break detectors are installed in specific areas of the facility such as where records are stored or documents are destroyed, and keypads are installed in order to arm and disarm the system. If a door or window is

opened or a motion detector or glass break detector is activated when the system is armed, a siren is activated within the facility and in most cases a central dispatch station is notified in order to notify the local police department or facility personnel. A burglar alarm system should almost always be a part of a company's physical security program. However, a burglar alarm's function is limited in that it does little to nothing to secure the facility during business hours, including from otherwise authorized employees.

While this limitation makes a burglar alarm system no less important to an overall physical security program, an electronic access control system is an important addition to that program to help combat that limitation. An electronic access control system can restrict access to both the exterior of the facility and any interior areas of the facility during all hours of the day and night. In general and non-comprehensive terms, access readers are installed along with some type of electronic door hardware on doors, either interior or exterior, where restricted access is required. A company employee uses a credential, usually a card or key tag, to activate the reader and open the door. Depending on the system design, there is either free exit or another credential check to exit the door. These systems are usually PC based and simple programming will allow or deny access by door, time, or user credential (card reader, key tag, number, etc). What this accomplishes is a further restriction of access to specific areas of the facility where records are stored or documents are destroyed, even to otherwise valid company employees. In addition, the system provides an audit trail of who entered or attempted to enter what area of the facility at what time. If any records or documents are compromised, this audit trail is invaluable. These systems are very effective and are moderately expensive, roughly \$2,000 per door.

Controlling the entrance and exit of documents from a facility is more a function of policies and procedures and personnel rather than physical security. There must be specific and verified policies and procedures as to how documents enter and exit the facility and how they are accounted for. There also must be proper supervision to verify the policies and procedures are being followed by the personnel. While proper inventory tracking is accomplished mostly by policies and procedures and personnel security measures, there are physical security measures to help with this effort. RFID systems exist that can track individual packages or boxes of documents within a facility. A 'tag' is placed on the package and through the use of radio signals the location of the package is tracked on a real time basis. If a package goes from an authorized to an unauthorized area of the facility, any number of alert devices can be activated. There is also the option of tracking the packages using GPS technology. These systems are very effective, but also very expensive. Generally they would only be used for records and documents with a very high security need.

Visual identification and verification is accomplished through the use of a Closed Circuit Television (CCTV) system. In general and non-comprehensive terms, cameras are placed in specific locations throughout the exterior and interior of the facility and are recorded on a digital video recorder. A video monitor is installed so facility personnel can either view the camera images live or review recorder images at a later time. The camera images can be stored for as much time as the company desires within the specific

design criteria of the system. These cameras can be used to identify and verify the movement and location of records and documents throughout the facility, including their entrance and exit to and from the facility. The adage 'a picture is worth a thousand words' is in fact true and cameras are an extremely effective physical security measure to both deter record and document compromise and determine what happened should any compromise take place. Unless personnel are watching the camera images live all the time, which is unlikely due to costs and in most cases unnecessary, CCTV systems are not used to track inventory in real time. These systems are moderately expensive depending on the number of cameras required but are a very effective deterrent and incident management tool.

All of these effective physical security measures cannot be used in a vacuum. They require interaction with both policies and procedures and personnel. This interaction can be very simple like making sure someone checks to verify if the doors are locked and the lights are turned on. With a burglar alarm system, someone has to arm and disarm the system at a pre-set specific time or action event such as 'last person out'. If the system is monitored by a central dispatch station, not only do the personnel have to exist to perform the monitoring but there must be policies and procedures in place to determine exactly what should happen should an alarm be generated by the system. This interaction is more complicated for an electronic access control system. These systems require a degree of administration by personnel in order to add or delete credentials as well as monitor the activity on the system to determine if any usage issues exist. There also must be policies and procedures in place so that personnel knows exactly what to do if there are repeated attempts into unauthorized areas, there are doors being propped open, etc. CCTV systems also require a larger degree of interaction. Personnel must at some point review camera images and in some cases view live images in real time for more specific security risks. Policies and procedures must be in place to determine when and for how long this live or after the fact viewing will take place and what to do should an incident be seen.

If there is not a conscious interaction and integration of policies and procedures and personnel with these physical security measures, the measure will ultimately be useless and a waste of resources. It is important to note that while the adoption of policies and procedures is a very inexpensive security measure, personnel will always be the most expensive security measure. The cost of personnel can be mitigated by the addition of effective electronic physical security measures and by utilizing existing personnel for additional security functions. However, personnel costs cannot be completely eliminated and are a necessary component of a proper security program.

Policies and procedures should be in written form and not just verbal or 'understood'. The effectiveness of the written policies and procedures should be evaluated on a regular basis to help insure the security of records and documents. Personnel are clearly a major part of this security plan as people are required to carry out the policies and procedures and operate the physical security measures. Additional personnel are usually not required to perform this security function, thankfully not adding major cost, it is more a matter of training existing personnel to carry out the policies and procedures and system operation. Supervision of the personnel regarding these security measures is critical and some

amount of time for supervising personnel should be dedicated to verifying security measures.

If companies that store records and/or destroy documents implement an integrated security plan that included physical, policies and procedures, and personnel security measures, there is a far less chance of compromise to any records and documents. This in turn lessens the overall risk to the company and creates added value to the clients.

Brian Gouin, PSP, CSC is a security consultant specializing in risk assessment, system design and project management. He can be reached at [BDG@Strategicdesignservices.com](mailto:BDG@Strategicdesignservices.com).