Reducing Manpower Intensive Tasks through Automation of Security Technologies

Ronald T. Carback
United States Department of Defense
National Security Agency

ABSTRACT

Security in today's government and commercial environments is changing. The willingness to provide manpower against security threats is diminishing Risk management is preferred to risk avoidance. In order for management to ensure that the appropriate security is provided while downsizing or right sizing protective services and other security personnel, automation of security technologies is a necessity. Several manpower intensive tasks and processes are: facilities access control, issuance of staff and visitor badges, provision of information for visitors, access control to interior facilities, and the issuance of office keys. Reduction of the required manning for these processes is enabled though the automation and integration of various security technologies including biometric identification systems. This paper provides a background on manpower intensive tasks and processes, security technologies that may be employed within them, resource reduction capabilities, and a customer's experience with the use of the technologies within a large Government environment.

Enterprise Rightsizing

In today's changing economic climate, security is facing a continual trend toward down or rightsizing in order for Government and large commercial entities to reduce the security costs generally considered to exceed requirements. The corporate search continues for the ever elusive profit and takes the inward approach of minimizing or reducing the cost of producing the end product. For government entities, mandates for downsizing are forcing security management to do more with less. In years past, when a security problem arose in industry and more commonly in government, the typical solution was to throw money and people against the problem. Today, the people and the money are not available.

Risk Management versus Risk Avoidance

It is imperative when defining security solutions to today's complex security problems that the organization's business be understood and the threat to the security of the core business processes be defined and measured. The threat must be defined and accepted at every level of the organization and reviewed annually. It must not just be an accepted or perceived threat by a few members of the organization. The security and corporate managers must be able to discriminate among the requirements and threats in order to define the security posture for the entity.

In years past, the lack of complete definition of the real threat to the organization's security and the abundant availability of resources resulted in applying a risk avoidance philosophy to security problems.

Risk (risk) noun. 1. the chance of injury, damage, or loss; dangerous chance; hazard 2. a) the chance of loss b) the probability of loss.

Avoidance (-'ns) noun. 1. the act of avoiding, or shunning something. 2. the act of making void; annulment.

Thus, risk avoidance, as practiced, has become an institution where the security posture is to ensure that all threats are protected against with security technology, money, and manpower. This practice is cost and manpower intensive and will not meet the resource restraints applied today. The alternative is to practice risk management.

Management (man'ijment) noun. 1. the act, art, or manner of managing, or handling, controlling, directing, etc. 2. skillful managing; careful, tactful treatment. 3. skill in managing; executive ability.

Risk management is the art of skillfully controlling and directing measured security countermeasures against the defined threat. To meet the growing demands of corporate executives to minimize support and more specifically, to reduce direct security costs, security principals must understand and practice the philosophy of risk management when applying any and all security countermeasures within their organization. This practice applies to funds for security technologies and staffing manning resources. Practical management of the risk requires the use of security technologies tied together through automation to provide the requisite security functions, yet reduce manpower and resource requirements.

Manpower Intensive Tasks

In large organizations, the security function consists of multiple personnel that are directed to ensure that the physical and personnel security philosophies are practiced. Functions which are inherently manpower intensive and therefore resource thinning include: Facilities Access Control, Badging and Visitor Processing, Intrusion Detection and Monitoring, and Office Control. Their intensity grow in proportion to (1) the size of the organization's campus, (2) the number of personnel employed, and (3) the number of customers, clients, or other personnel expected to visit the facilities.

Facilities Access Control

Facilities access control structures vary in size depending upon the organization's size and assets that are protected. Typical of very large organizations are the requirement for a dedicated protective force composed of staff security officers or a contract guard force. These persons are responsible for executing the security posture of the organization which includes visual verification for access to facilities by staff personnel and visitors. Also typical of large organizations are automated access control systems which automate the access discrimination process. Even though basic automated systems are acquired to reduce the manning required to provide facilities access control, most organizations rarely decrease their security staff upon installation or implementation, since the processes and the technologies employed require oversight. Often these systems are used for interior access control (doors or laboratory areas where limited staff require access). On large campuses, the implementation of interior access control tends to minimize due to the cost per door of the devices.

Intrusion Detection and Monitoring

The intrusion detection process which uses motion detectors, alarm systems, and closed circuit television (CCTV) are fairly expensive to install due to communications requirements. Security personnel often believe that the processes require minimal resources due to their low maintenance. However, what most organizations and security personnel neglect is that at the end of the CCTV, motion detector, and alarm device's fiber optic cable is a monitor that is watched 24 hours a day to monitor access and to provide a focal point when an incident occurs. The use of a protective services force to oversee this function is commonly accepted as a fixed annual cost.

Often, large campus based organizations employ geographically distributed communication centers due to the large number of alarm and CCTV points. Thus, a corporation with several manufacturing plants may have multiple communication centers providing 24 hour monitoring of numerous alarms, access control, intrusion detection, and CCTV, resulting in exorbitant protective force costs.

Most protective forces provide monitoring of access control and intrusion detection 24 hours a day, 7 days a week. The costs to provide such are defined in Table 1. A typical 8 hour a day, 5 day a week security post has a post manning factor (PMF) equivalent to 1.0. The estimated annual fully burdened cost (salary plus benefits) for a single security officer is $43,618[1]. For other manned posts such as 16 or 24 hour posts, Table 1 provides the required post manning factor and average annual costs for the aggregate officers to provide the manning function.

Table 1. Security Officer Cost[1]

Post	PMF	Estimated Annual Cost Per Post
8 Hour, 5 Day	1.00	$43,618
16 Hour, 5 Day	2.60	$113,407
24 Hour, 7 Day	5.46	$238,154

Identification Badging for Staff and Visitors

Security at its essence provides authentication and verification for access. Control of the identification of staff and visitors requires significant manning. Authentication and verification of the person's identity are crucial in the identification process. Biometric technologies are often used to ensure identity and verify credentials when the assets protected are of high value or sensitivity.

Large commercial and government organizations use an identification badge to segregate their population from the rest of the world. Providing an identification badge enables an organization's staff to know who belongs and who doesn't, an increasing requirement as competition stiffens in virtually every market and especially with the increase of violence in the work place. Most organizations use some type of badge development system whether it is a simple cut and pastes with films and laminates or an electronic identification workstation. Although the manual laminate processes still exist, they require more resources than the digital capture stations.

For organizations with a large corporate base or a large number of visitors, the visitor processing function often takes the form of a visitor center or office, commonly staffed by many persons who fill staff requirements for new or replacement badges and also funnel staff requests for visitor access and badges. This process not only requires significant manpower, it is paper intensive and time consuming. In today's age of providing consummate quality and efficient customer service, requiring a visitor to wait greater than five minutes for a badge and requiring paperwork to be completed is intolerable. If the process is too time consuming, it may result in impeding the visitor from getting to meetings on time and may cause the organization to lose the customer. The visitor center staff tend to be least beloved by visitors and other staff.

An additional function the visitor center staff are typically required to provide, but are ill equipped to provide is detailed information such as:

- Phone numbers or room numbers of the person visited,
- Directions to the office location within the campus or building,
- Security policies,
- Information on processing for a staff or visitor badge,
- Accommodation and restaurant information, and
- Directions to the airport.

Office Key Control

Office door key control is a daunting task for security personnel. Employee turnover turns the key control process into a cat and mouse game for security personnel trying to control the keys and locks. As more and more organizations automate access to offices or sensitive areas, they expend their resources on internal access control equipment such as swipe or proximity devices and their associated electric locks. The cost of these equipments can vary from $100 to $4,000 per door (many organizations are even beginning to employ hand geometry biometric devices as a door control mechanism, significantly increasing the cost per door[2]). For those organizations that choose not to employ technology, but allow the offices to be unlocked or allow staff to keep their keys, accountability is not provided and an audit trail is not generated. *Lack of control is no control.*

Enabling Security Technologies and Processes for Resource Reduction

Advanced Card Technologies

Recently, there has been a large corporate roll out of multiple technology badges, such as the Multitech^{TM} Proximity Card developed by Motorola/Indala Corporation. The Multitech^{TM} card is of the standard credit card size and width, has a PVC plastic surface, and has two access control technologies: radio frequency (or proximity) and magnetic stripe. Other corporations are providing similar technologies. The dual technology cards are enabling organizations to migrate to newer technologies, to less invasive technologies, and enable multiple types of technologies to be used in campus environments. This achievement will increase the lifetime of many access control systems and the dual technology devices are a resource reduction enabler.

Access Control Systems

Implementing access control systems may eliminate the visual access process for facilities, but it may not result in the reduction of security costs. Technologies that enable organizations to reduce manning requirements include high security turnstiles, revolving doors, vertical turnstiles, and high security portals (also called access booths). Inherent within each device is the provision of a partial or full physical barrier when deployed. The physical barrier is the key to enabling resource reduction. Without a barrier, officers are required to provide visual access control oversight. With a partial barrier, officer oversight is able to be minimized. With a full barrier: floor to ceiling, wall to wall, security officers are not required.

Specific Access Control Devices

Each device below has varying times for the recovery of the installation investment based upon the application (the number of devices employed and the number of officers reduced). The more officers that can be reduced, the greater the resource savings.

High Security Turnstiles[1]

High security turnstiles provide a partial barrier and are best placed at facility entry control points. The installation must have additional walls or another physical barrier filling the entry space so that unauthorized entry is not allowed without visual observance by the security officer. To accommodate persons transporting packages (or to meet ADA requirements) it is imperative to include either an ADA approved Disabled Persons/HandCart gate turnstile or simple theatre roping. Turnstiles are an efficient means to minimize officer control of large entry areas, but do not enable complete officer removal or oversight. Since turnstiles are the least costly and have the greatest throughput for entry, they should be used in high traffic areas for access discrimination.

High Security Portals

High security portals are devices that are used for anti-tailgating purposes within a facility or at the facility entry point. These devices typically have one or more biometric technologies employed. Use in an access event is begun by presenting the access token and then entering the portal. A biometric such as a hand geometry unit is then used to verify the identity of the person and a second biometric such as a weight or load cell may be used to verify that only one person is within the portal (anti-tailgating). Following authentication and identification, access is granted. Access portals are expensive to acquire and install. Portals are used in lieu of officer oversight as the access control mechanism within is a biometric device (although they are often employed with CCTV and monitored at a central monitoring station). Due to their low throughput capability, portals should be used to control entry areas where low pedestrian traffic is expected (after hours/weekend access or a low occupancy building) or to control inner areas of a significant sensitive nature.

Revolving Door

Automated revolving doors when integrated into an access control system may be installed to provide a complete physical barrier at the entry control point. Some of the newer technologies employed within revolving doors such as those provided by Revolving Door Control, Inc., enable audio sensing of multiple persons within the door, and therefore limit tailgating. The ability to eliminate tailgating and provide a complete physical barrier by installing it in the door entryway enables the organization to remove all officers involved in the process. If the defined threat is to ensure the exact identity of the person requesting access, a biometric should be employed prior to removing officer oversight. Revolving doors are energy efficient as they provide a double door barrier. The only limiting factor in their use is their throughput time. Revolving doors installed in high traffic building entryways may not have the throughput to keep pace.

Vertical turnstiles, similar to revolving doors, provide a capability for reduced oversight of a facility entrance. These devices are normally employed external to the building or within the building and are not a part of the normal entry door to the building. Depending on the access device used, they do not provide anti-tailgating. If anti-tailgating is required, the entry requires officer oversight.

Table 2. Access Control Device Throughput

Device	Entry Throughput Per Person[2]
Turnstile	< 7 seconds
High Security Portal	< 22 seconds
Revolving Door	< 11 seconds
Vertical Turnstile	< 12 seconds

Electronic Identification

Technology for developing identification badges changes daily. Digital capture and storage of identifying images and data at a local desktop or using a distributed client/server architecture are becoming the norm. Use of these technologies such as the Polaroid ID 4000TM, which provides for digital capture of a person's image and then prints the identification badge in a one-step process automates the previously time consuming cut and paste process. The advent of PVC printing technology which incorporates dye-sublimation/resin thermal transfer technology onto the surface of a PVC plastic card is revolutionizing the identification industry. Laminating film based identification badges can cost on the order of $2 per badge for supplies, while the cost of printing with the PVC printing technology costs approximately $0.50 per card (even with a pre-printed silk screen logo or corporate name). In addition to the rapid advances in printing technologies, today's software applications allow industry standard formats such as JPEG to be used and also allows the image or badge format to be presented at the desktop or officer station on a common personal computer. While this advance may not directly reduce resources, it certainly makes the officer's job much easier.

Automated Visitor Processing

The current process employed by organizations to process visitors is a paper or telephone process initiated by the sponsor of the visit and forwarded to the visitor center or security force. At the National Security Agency (NSA), we have employed an automated electronic visitor request process for agency staff to generate and input requirements to the visitor center staff for over 10 years. As part of an effort to reduce the manning that is required in the badging processes at agency facilities, the concept for an ***Automated Badge Issuance and Information Kiosk*** (ABIIK, patent pending) was conceived by the government and developed by Quintron Systems, Inc.

ABIIK

The ABIIK's purpose is to:

1. Issue Staff and Replacement Badges,
2. Issue Visitor Badges,
3. Issue Passes, Permits, and other Formats, and
4. Provide Information via Multimedia.

Table 3. Device Costs

Enabling Device	Cost[3]	Officer Required	Resource Reduction Capability[4]
Turnstile	$5,000 - $15,000	Yes	1
Portal	$40,000 - $100,000	No[5]	3
Revolving Door	$30,000 - $60,000	No[5]	4
Vertical Turnstile	$10,000 - $25,000	Yes	2

The ABIIK, a multimedia kiosk, is able to be configured in stand-alone mode or on a network for remote access to data. In stand-alone mode, visit and enrollment information are entered into the ABIIK via floppy disk or tape. In network mode, the ABIIK can be configured to remotely attach to various databases or other files. The ABIIK is operational 24 hours a day and requires no manned presence other than for occasional replenishment of supplies. In its normal state, it awaits an initialization by a user via the touch screen. Users can request the processing of a badge or obtain agency and security information. Some of the multimedia information made available to the general public on screen and which may be printed include: staff phone numbers, staff room numbers, directions by room location, campus layout, building layout, security policies, information on enrollment, ABIIK information, direction to area airports, accommodation and restaurant information, Agency introduction video, security policy videos, facility videos, and security device use and demonstration videos. The ABIIK will authenticate an expected visitor or staff person and then automatically generate and issue their badge, pass, or permit *without any security personnel involvement.*

If a user requests the processing or issuance of a badge or pass, the ABIIK may search a local or a remote database to retrieve the requirement. For a visitor badge, the ABIIK receives visitor request information in advance of a visit and contains the essential data required such as the person's name, social security number, dates of visit, and organization represented. The device uses a hand geometry unit for bioverification, retrieves the digital image associated with the requested data and then prints the requested badge or pass via the dye-sublimation/resin thermal transfer process using a PVC Printer. The PVC Printer also provides on-line encoding of the requisite data on the badge's magnetic stripe to enable the use of the badge within the agency's access control system. For passes and permits, the PVC card may not be encoded. Depending on the pass or permit, a digital image may not need to be fetched. For issuing badges and permits that contain a person's image, staff and visitor personnel must be pre-enrolled into the system during their first agency visit. The pre-enrollment process incorporates the capture of a digital image and the enrollment of the person's hand geometry template. This process occurs only once and takes approximately two minutes. On follow-on visits, visitors go directly to the ABIIK for their visitor badge.

The ABIIK has been developed to reduce the manpower and paper intensive processing required in visitor processing centers and also provides other security and location information as the quintessential security customer service tool.

Technologies within the ABIIK

The ABIIK is a self contained unit similar to other information kiosks found at malls, shopping centers, and airports. It incorporates a custom multimedia software application, touch screen interface, PVC card printer with on-line encoding, hand geometry biometric, and phone. The touch screen interface provides a simple easy to use interface for the staff or visitors to gain access to information in multiple media forms (display, paper, video) or to have their badge or other permit or pass automatically generated. The PVC printer provides the print technology *and* the magnetic stripe encoding for badges and other identification passes. The hand geometry device is used to provide biometric verification of the person using the ABIIK. The biometric device enables the ABIIK to be installed without officer or visitor staff oversight. A phone is provided with a touch screen dialing capability so that visitors may automatically dial their sponsor or other persons. In case of emergency, the phone has a direct 911 connection. For ease of use for visitors, their point of contact's name, phone, and room are displayed when they request a badge. Visitors are provided one touch dialing to announce their arrival or to mention they are late. Various printing technologies are available (laser, thermal, deskjet, or dot matrix). If security policies accompany the issuance of a badge, they are printed during the badge issue process.

Resource Reduction

Implementing the ABIIK enables the visitor and staff identification processing to consolidate into minimal manning. The use of the ABIIK deletes the requirement for visitor centers with the exception of the need to pre-enroll staff and visitors during their initial employment or visit. In the typical visitor process, the time required to provide a badge can range from 1 to 20 minutes. Using the ABIIK, the issuance of a visitor badge averages 2.5 minutes. The ABIIK comes in various configurations and options and it's cost ranges from $30,000 to $100,000. Employing a single ABIIK in place of one officer or visitor center staff enjoys a return on the acquisition investment in less than one year. The ABIIK can print to dual technology access control cards that contain PVC plastic ensuring its adaptability to advances in access control and electronic identification technologies.

Office Key Control

The first question to ask is not how to control office keys, but what data or assets the organization wants to secure and from what the organization is securing the office from. Often interior access control devices are expensively deployed on office doors that only one person has access to. A simple key may suffice. Automated access control should be used to segregate those areas and offices that have limited access requirements by multiple persons.

Many organizations, to the contrary, provide no key control and give each employee or staff a key to their office. Although this is a common practice, it does not provide control. When an investigation is required, no audit trail is possible to determine who had access.

A key control system that began its life as a key and car loss prevention solution for automobile dealerships, was transposed into an inexpensive office key control system at our facility is the Key Systems, Inc. Automated Key Access Machine (AKAM). The AKAM costs from $15,000-$20,000, can control up to 406 keys per machine, and uses a robotic arm to retrieve and return the user's key. The interface is a touchpad with display. Any access control device or system may be integrated to control key access, including biometric devices. The average time to access a key from the machine is 19 seconds. The machine uses a networkable controller (common PC) which contains a key access database and audit data. The AKAM enables key control to be automated without the need or requirement for any security personnel to be involved in the process of handing out or returning keys. Security personnel install the machine initially and then only need change access lists based on changing requirements for access.

Assuming that one machine is used to replace the function of a single officer, the return on investment is achieved in four months[6]. Additional benefits received by using the AKAM vice officer or security personnel include minimization of human errors due to their elimination from the process, the complete reduction of the burdened cost of the officer providing the function on a yearly basis, the provision of an accurate and timely audit trail, and the ability for the AKAM to operate on a 24 hour basis enabling access by staff after hours and on weekends.

The implementation of a single AKAM may reduce officer costs on an annual basis from between $43,618 to $238,154 depending on whether the distribution of keys is performed during the day shift or if it is a 24 hour operation. For large campus environments where key control is an elaborate process with multiple officers involved in the process, the ability to replace officers with AKAMs enables cost savings to increase proportionally. For organizations that have no key control, the AKAM provides audit trail capability and operates 24 hours a day.

Communication Center Consolidation

When organizations operate in a campus environment, one of the most significant resource reduction methodologies is to consolidate all intrusion detection monitoring centers through process redesign into a signal, central communication center. Today's information and communications technology allow integration of CCTV, Alarms, 911, Computer Automated Dispatching, Loudspeaker, access control monitoring, and incident reporting at the desktop workstation. The communication center location is no longer required to be near the facility protected. Advances in information, communications and networking technology have enabled location transparency.

Consolidating multiple communication centers enables significant reductions in the officers or communications staff required to provide the function. In addition, facilities, space, and communication resources are reduced.

FORTEZZA, a future issue

FORTEZZA is a credit card sized Personal Computer Memory Card International Association (PCMCIA) card. It is designed to provide writer-to-reader network security such as data integrity, access control, authentication, non-repudiation, and confidentiality for the following applications: electronic mail (e-mail), file transfer, remote login, and database management. It is compatible with commercial computing and networking technology and ensures protection against unauthorized disclosure or modification of information while integrating systems at various sensitivity levels.[3]

FORTEZZA is more than just a writer-to-reader computer network security device. It has the capability to become a high end identification badge in the commercial and government sectors. Data will be capable of being stored internally as well as in host computer databases. Discussions with technology vendors to incorporate radio frequency identification (proximity technology) within the PCMCIA package are ongoing. Discussions on adapting infrared technology as an interface, adapting PVC plastic surfaces on one or both sides to allow dye-sublimation/resin thermal transfer for printing identification badges, and the adaptation of a magnetic stripe on a PVC plastic surface continue.

Some of the issues that affect its presence in the marketplace and its implications to security technologies are its high initial cost, the infancy of the global infrastructure required to ensure global use, and commercial and government (such as the National Information Infrastructure (NII) or Information Superhighway) buy-in to the technology and the services provided.

A Customer's Perspective

The National Security Agency is a large government entity comprised of multiple buildings on several campuses containing government owned and leased facilities. Greater than 5 million square feet of office, warehouse, and laboratory space are within the campuses. The risk management philosophy has been in practice for several years. As part of this philosophy, in conjunction with congressional mandates to reduce support costs in light of the agency's mission, security technologies have been employed to provide for the reduction of the number of officers required to support the protective services function. Essential to receiving the investment funds for installing the various devices and processes has been the requirement to generate a detailed cost to benefit analysis describing the overall reduction in manpower staffing and time line for the recovery of investment funds following acquisition. Developing these analyses has provided security investment funds in an era of financial restraint. The provision of funds has enabled a reduction of greater than 100 security officer and visitor staff positions equating to greater than $4.8 Million in annual cost savings alone, not including the intangible benefits of reducing cycle and process time.

The agency has or will employ multiple high security turnstiles, high security portals, and revolving doors within the agency campuses and at agency sites overseas. High security turnstiles have been employed at every facility's entryway. The turnstiles have been designed to aestheticallly match the interiors of the entryways. The high security portals and revolving doors are used within the interior of the buildings to segregate sensitive areas from the general staff population, while eliminating the requirement for a security officer to provide access control. For these sensitive areas, the portals originally employed the EyeDentify 7.5^{TM}retinal scan biometric[4], but due to staff perceptions and difficulty in use by segments of the population, a different biometric is being installed. Implementing these advanced security devices has enabled a reduction of 32 officers from the protective force.

Table 4. Resource Reduction Enablers

Task	Risk Avoidance	Enabling Process for Risk Management	Automation Technologies	Benefit
Visitor Identification	Receptionists, Visitor Centers, Multiple Officers	Electronic Identification Workstation	Digital Image Capture	Reduced Supply Costs, Semi-automate the Process, Image and Data Storage
		Automated Badge Issuance and Information Kiosk (ABIIK)	Biometric, Multimedia, Client/Server, PVC Printing with On-line Encoding	Completely Unmanned Process, Reduces Human Error, 24 Hour Operation, Stand-alone or Network, Reduce Cycle Time, Efficient Process
Facilities Access Control	Multiple Officers	Turnstiles	N/A	Partial Physical Barrier, Minimized Officer Oversight
		Revolving Doors	Biometric,	Physical Barrier, Unmanned, Anti-tailgating
		Access Portals	Biometric	Physical Barrier, Unmanned, Anti-tailgating
Office Key Control	Personal Keys, Officer Key Distribution	Automated Key Access Machine (AKAM)	Robotic Arm, Client/Server	Unmanned, 24 Hour Operation, Audit Log and Trail, Remote/Network Access
Communication Center	Multiple Monitoring Areas, Multiple Equipments	Consolidation of Monitoring Centers	Client/Server, Systems Integration, CCTV on screen, ALARM Graphics on screen	Reduced Manning, Reduced Equipment, Reduced Space, Consolidated Resources

The development of the Automated Badge Issuance and Information Kiosk will enable the reduction of 14 visitor center staff or security officers. Of more importance is the reduction in processing time for replacement staff badges and visitor processing. No longer do visitors have to wait in a visitor lounge for their escort to arrive, their badge to be processed, or for directions. The ABIIK has provided one-stop processing. The information provided is also used by the general agency population, not just visitors.

Migrating the manned key control function of every building within the campuses to a network containing multiple distributed Automated Key Access Machines is enabling the reduction of 34 security officer positions. The capability to provide error free distribution of keys 24 hours a day has significantly increased the level of customer satisfaction. We are assisting in the adaptation of the technology to other federal agencies.

The newest manpower and cost reduction strategy that is under development is for the consolidation of 10 geographically dispersed communication rooms into a central communication center. This effort was conceived while visiting industry, federal agencies, and municipal Police and Fire communication centers to benchmark the quality of service and processes undertaken. The implementation shall enable the reduction of a minimum of 30 security officers currently assigned to the communications function. Should other employees or contracted communications' specialists provide staffing, the number of positions reduced will increase proportionally. In addition to the cost savings, the cycle time for reacting to incidents shall be sharply reduced as CCTV, alarm points, and mobile dispatching are integrated into a desktop workstation.

Table 5. Resource Reduction

Security Technology	Officers Reduced	Annual Savings
Advanced Devices	32	$1.40 Million
ABIIK	14	$0.61 Million
AKAM	34	$1.48 Million
Communication Center Consolidation	30	$1.31 Million

Selection of Biometric

In coordination with an internal research department, we continue to investigate multiple biometric technologies to determine which are appropriate for use in our environment. A summary of our results are presented in Table 6. Our initial implementation of a biometric was based on the requirement to restrict access to sensitive areas and use the device that had the best false acceptance and false rejection ratios at the time. Little regard was given to operator training, user training, or user perceptions. Time has shown that the invasiveness of the device is a function of the user's perception, not actual invasiveness. Our users perceived the facial recognition to be the least invasive and the retinal scanning biometric as the most invasive. In implementing the ABIIK, we required a biometric that was not only non-invasive, but also easy to train the average operator and end-user. Since visitors and other persons would be using the ABIIK on an aperiodic basis, ease of use was the second major requirement. The third requirement is for the template of the biometric to be as small as possible due to the great numbers of visitors that are processed in a single day and therefore the amount of data storage required per visitor (the agency receives greater than 1,000 visitors per day). Our fourth requirement was to employ a biometric that has been a product for several years and therefore was required to have a substantial user base with known weaknesses and strengths. Due to these requirements and the ratios for false acceptance and false rejection were within our implementation standards and constraints, the Recognition Systems, Inc. ID3D HandKey hand geometry biometric has been accepted as the standard agency biometric for agency security implementations. Coincidentally, this same unit has been accepted as the Department of Energy standard biometric technology and device[5].

Lessons Learned

In implementing security resource reducing technologies and processes we have learned many lessons. The following items are in summary:

The implementation of the technology is fairly easy, the training of the average user is much more difficult.

Knowledge of the customer and their desires is required in evaluating the constraints placed by the technologies.

Communication between the customer or end user, the security officers, and management is a daily exercise.

Resource reduction will occur following investment of technology or changing the process.

Make sure the installation is correct and working the first time.

Ensure the installation is aesthetically pleasing and matches the surrounding environment.

No equipment or software are ever "off-the-shelf".

Acquire and install today's technology, not tomorrows.

Security technologies provide greater security than security officers.

Table 6. Biometric Devices

Biometric Technology	Operator Training[7]	User Training[8]	Ease of Use	Invasiveness	Template Size
Hand Geometry	Minimal	Minimal	Easy	Moderate	9 bytes
Retinal Scanning	Moderate	Extensive	Hard	Extensive	< 100 bytes
Speech Processing	Minimal	Moderate	Moderate	Minimal	~ 1,000 bytes
Fingerprint	Minimal	Moderate	Moderate	Moderate	~ 2,000 bytes
Facial Recognition	Moderate	Minimal	Easy	None	~ 2,000 bytes
Weight	Minimal	None	Easy	None	4 bytes

NOTES

1. The definition of high security turnstile does not include optical turnstiles since no physical barrier is provided.
2. Details provided by vendors or as determined from practical application. Only the High Security Portal throughput incorporates a biometric device.
3. Cost per device typically includes system integration, installation, training, and facilities modifications.
4. Resource reduction capability is provided in a range from 1 through 4. 1 equates to the least capability for providing manning or other resource reduction and 4 equates to the highest capability for resource reduction.
5. If distinct identification is required a biometric device must be integrated.
6. Average Cost for an AKAM / Average Cost per Officer = $17,500 / $44,000 = 0.40, therefore the return on investment is recovered in 4.8 months.
7. Operator is assumed to be familiar with access technology and devices.
8. User has no known prior knowledge of devices other than for typical access events.

REFERENCES

[1] R. T. Carback, "A White Paper Proposal for the Integration and Consolidation of the Office of Security Services' Protective Services Division's Various Communication Centers into a Central Communication Center", Internal NSA Document, pp. 1-26, December 1994.

[2] D. C. Bright, "Examining the Reliability of a Hand Geometry Identity Verification Device For Use in Access Control, " Thesis, Naval Postgraduate School, Monterey, CA, AD-A181467, March 1987.

[3] Insight Magazine, DMS Award Issue, 1995.

[4] EyeDentify, Inc., "The EyeDentification System 7.5™ Health Safety and Statistical Performance Review."

[5] E. J. McCallum, "Distribution Memorandum; Subject: Biometric Standardization", Department of Energy, Washington, DC, March 13, 1995.

BIOGRAPHY

Ronald T. Carback, received a B.S.E.E. from the Pennsylvania State University and a M.B.A. with concentration in Information Technology and Strategic Management from the University of Baltimore. He has worked for the NSA since 1992 and was previously employed in private industry. He is also the principal for Carback and Associates, a business/security process reengineering, information technology consulting, and database application development firm. He may be reached at ronc@romulus.ncsc.mil or 301-688-8293 Voice, 301-688-7623 Facsimile.