Published on *Security Management* (http://www.securitymanagement.com)

The Biometric Devil's in the Details

By Ben Rothke CISSP, QSA, and Benjamin Tomhave, MS, CISSP
December 2008

After numerous false starts, it seems that biometric controls are everywhere. Once the province of sci-fi TV shows and movies, biometric solutions are increasingly being deployed at border crossings, in airports, and in the work place. Yet, despite their increasing prevalence, the reality remains: far more deployments fail than succeed. The situation has been so bad at times that many organizations wonder why they should even bother considering biometrics in the face of so many possible failed cases. There are, however, many advantages to using biometric controls, which can be deployed successfully when a detailed, strategic approach is used.

Before examining why biometrics are alluring, often fail, but nevertheless can succeed, companies interested in deploying biometrics must know precisely what these technologies do and how authentication differs from identification.

Biometric controls use technologies that confirm a person's identity by comparing patterns in their physical characteristics against enrolled computer records of those patterns. Biometric controls may include scans of the iris or retina, measurements of hand geometry, or any other measurement of the physical person that represents a reasonable unique attribute. These measurements are then compared against previously registered measurements to effectively authenticate an individual.

It is important to note that biometric controls are only used as a form of authentication, not identification. The difference is that identification is a one-to-many match, most often used by law enforcement to identify criminals or to identify qualified recipients for benefit programs. Authentication, on the other hand, is a one-to-one match. The user presents a live body attribute and it is compared to a stored sample previously given by that individual during enrollment. The match is then confirmed or rejected.

Biometrics: Why Bother?

With a long and distinguished history of project failures, why should anyone attempt to deploy biometric controls?

One of the main benefits of biometric controls is the ability to avoid the need for user created passwords. Good passwords are hard to create and users, often oblivious to what makes a good password, have historically chosen ineffective, easy to crack passwords. Biometric controls, on the other hand, offer a reasonably secure solution to insecure passwords in a form that is harder to lose or forget.

In the past, the most successful biometric deployments have been those that are for small-scale, closed-loop applications. These are often niche areas where biometric controls provide a unique solution to an unwieldy or unsolvable problem. The most significant biometric success stories have been with those organizations that had a specific security issue to solve, such as identifying bank employees in vaults or for customer access to safe deposit boxes, security guard stations, and sensitive payroll systems.

Yet with the myriad benefits biometrics offer, it's challenging to deploy an enterprise-wide biometric solution. Even after a successful biometric pilot test, the decision to not deploy the solution is often made because of cost, acceptance and adoption issues, or complexity.

The cost of deployment and maintenance is perhaps the biggest issue for many companies. Unlike passwords, which rely

on software and the user, biometric controls also require specialized hardware devices. Depending on the application, this could require a biometric device per user if biometric solutions are located at each workstation or work location.

Cost can also become problematic from a technical support standpoint. Historically, biometric controls have had difficulties with accuracy and consistency, to the point that many solutions, like hand geometry, have had their tolerance levels opened wide in order to reduce false negatives and to lower the overall support costs. Enrollment itself can be a costly process, requiring physical presence from both an authority conducting the enrollment and from the person being enrolled.

Another common negative factor is acceptance of biometrics by employees. Many people see any sort of device that records their physical attributes for the benefit of their employer as an invasion of privacy. Concerns have even been raised in the past decade regarding how employers might use biometric data collected to authenticate users. Other times, certain legacy biometric solutions were simply uncomfortable to use, such as forcing the eye open while it's scanned.

Finally, biometric security systems are complex. This challenge is made worse by the lack of standardization between vendors. Few enterprises enjoy vendor lock-in and the relative lack of alternatives—due in large part to inadequate interoperability—can make the decision to move to biometrics even more difficult.

Biometric Failures

Biometric control projects fail for a variety of reasons, but many of those reasons aren't fully understood and appreciated. Given the significant number of failures, it is, perhaps, instructive to look at some cases in which biometric deployments failed to see what lessons can be learned.

No Pilot Testing. Pilot testing is a way to simulate the live operation of a new technology within an organization. In a case of rushing to delivery, historically, it is not uncommon for biometric control projects to attempt an enterprise-wide roll out without first performing a pilot on an adequate sample size of users. Failing to pilot a solution will reduce the overall acceptance by end-users, often because of an increased level of anxiety over the seemingly intrusive nature of the technology.

No Documentation, Processes, or Procedures. Policy defines the aims and goals of the biometric solution. A comprehensive biometric security policy is required to map abstract security concepts to the real world biometric implementation. As part of a risk resilient organization, all technical solutions must be supported by a complete set of supporting documentation, including well-defined processes and procedures. Everything from enrollment to disaster recovery must be accounted for to ensure a successful deployment. If a major network component upon which your biometric solution is dependent fails, how do you get into the server room protected by the biometric solution? The fastest way to kill a deployment is to have it cost the company money by hindering the normal operation of the business thanks to poor planning and documentation.

Ineffective Training. Deploying a technical solution is far more than installing hardware and software. Users and administrators must be provided proper training on use and maintenance of these solutions. Never is this more evident than in biometric solutions. If the solution is not optimized to meet the needs of the business, and users aren't trained in the proper and efficient use of the interface, then nobody should be surprised when the solution develops a negative reputation that eventually leads to its demise.

Inadequate Server Provisioning. One of the most common deployment failures is in planning adequately for server utilization and performance. Without adequately scaled infrastructure, processing times may be excessive, introducing additional costs to the deployment that were not previously expected. Performance and scalability must be included attributes during the design phase.

Lack of Legacy Support. For all the security benefits of biometric controls, they can only be realized if the solution can be integrated with existing technology. Case in point, if an enterprise relies on legacy mainframe programs and does not plan to recode these applications in support of a biometric solution, then the overall benefits of the solution may decrease substantially. These issues should be identified during the design phase and addressed during the positioning phase.

Oversized Initial Roll-out. Similar to the first failure listed above, if the initial deployment of a biometric solution is oversized, then users and administrators may become overwhelmed. This fail case usually plays out in one of a couple ways. Either the enrollment process bogs down because of inadequate staffing to integrate the test users, or the support

team becomes overwhelmed by support calls when the roll-out experiences challenges user acceptance and usability. This fail case is often amplified by an ineffective training program.

BR/DRP Not Included in Design. As already noted previously, it is imperative that there be thorough, functional, and effective documentation in place ahead of a deployment. Perhaps the most important set of documentation pertains to business recovery and disaster recovery procedures (BR/DRP). If a biometric system goes down and there is no alternative way to authenticate, then companies will often stop using biometrics. This fail case is more than just a matter of throwing the baby out with the bath water. If a technical solution cripples a business, the result will be lost revenue and increased overhead expenses. Both of these impacts can be effectively mitigated through proper planning during the design phase.

Inadequate Project Management. A skilled project manager will address many of the above fail cases. As is true of all major IT deployments, biometric controls must be deployed through a formalized project management process. Given that biometric solutions are used for authentication, it is thus imperative that such a project be well managed. This is especially true when the deployment gets to the point of enrolling users. Proper project management should expect chaos and develop a plan for controlling it as best as possible. An efficient and painless enrollment process and an effective training program will maximize user acceptance as well.

No "One Size Fits All" Technologies. Not every technology is suitable to every individual. For example it has been found with fingerprint-based solutions that many people cannot be fingerprinted due to factors such as thin skin as a result of prescription drugs or genetic make-up; extensive use of cleaning chemicals; finger injuries, including minor cuts and scrapes; fingers with limited movement (as they sometimes cannot be scanned properly); and the difficulty of enrolling elderly and construction workers due to injury or disease or both.

Succeeding with a Strategic Approach

One of the most common mistakes made by companies when rolling out a biometric solution is thinking that biometric controls are a plug-and-play technology. The reality is that biometric solutions are 10% technology and 90% policy and management.

An effective biometric solution rollout must be deployed in the context of an effective methodology. Project planning and requirement definition is imperative to success.

The quality that separates an effective rollout project plan from an ineffective one is attention to detail.

For biometric security controls to work, they must be deployed in a strict, methodical fashion. There are many attributes that need to be taken into consideration. Everything from budget to politics and culture to staff training and support will be affected by the decision to implement biometric controls.

Toward this goal, a successful biometric controls project should employ a strategic approach comprised of three broad phases: design, positioning, and deployment.

The Design Phase. The purpose of this initial phase is to fully define the business drivers for the biometric rollout, enumerate relevant regulatory requirements, and perform a pilot test. A significant portion of project time should be invested within the design phase to ensure the success of the project. During design, the attributes mentioned above should be identified and detailed, with an action plan drafted accordingly.

The design phase may also include performing solution identification and evaluation. In the case that a solution is identified, a pilot must be performed to test the efficacy and adequacy of the solution. During the pilot, key stakeholders should be given an opportunity for hands-on testing to ensure that pre-identified concerns are addressed and to determine if other concerns may exist that were not previously identified.

This phase of work should not only focus on the technical aspects of the given biometrics suite but should also include an evaluation of cultural and social issues relevant within a given environment. A training and awareness program should be chartered to support future phases of the project. The objective of this phase is to thoroughly define the problem space and contributing factors, identify and test a solution, and develop the base framework for training and awareness.

The Positioning Phase. During the positioning phase, legacy systems will need to be updated or bypassed, overall

project risks determined, and a training and awareness program should be launched. All decisions should be supported by the risk management process, such as identifying key risks and performing a trade-off analysis to help ensure that the proper degree of risk resiliency will be achieved (or maintained) by deploying the chosen solution.

The primary objective of the positioning phase is to initiate and to complete intermediate changes required supporting the pending full deployment of the solution. This phase provides another opportunity to pull the emergency brake on the project should it be determined that the solution does not meet the needs of the business, or that it makes the organization less risk-resilient.

By the end of this phase, all stakeholders should be comfortable with the solution and the deployment plan. The deployment plan should be evaluated independently to minimize related risks, and the results of the pilot should be integrated into the plan as part of lessons learned.

The Deployment Phase. During the deployment phase, hardware and software are implemented, end-user training and awareness are mainstreamed, and steps are taken to ensure continuing process improvement. Biometric controls should be fully functional by the end of this phase, and the overall risk posture of the enterprise changed favorably. The enterprise should be more resilient to risk than at the onset of the project.

Deployment Requirements. Generally speaking, for a biometric controls' deployment to be successful, it must fulfill the following seven requirements.

- Universality – Every person must have this characteristic. Don’t take it for granted that all of your users will have this physical characteristic. If you are working in a factory and thinking of a hand scanner, realize that there are plenty of people without 5 digits on their hand.
- Uniqueness – Make sure two people will unlikely share this characteristic. Height, weight, hair, and eye color are clearly not unique. The iris, retina, and fingerprint are perfect examples of biometrics that are highly unique.
- Permanence – The characteristic must be available over the long term. If your users are working with chemicals or sanding agents, fingerprint readers may not be the best option.
- Collection – The biometric must be easy and unobtrusive to obtain. If your users perceive an iris scan as "being shot in the eye by a laser,” perhaps you need to think of a different biometric.
- Performance – The biometric technology must be accurate, fast, and robust. A biometric that works quickly in the test lab may fail when thousands of users are logging in during the morning rush.
- Non-circumvention – No one should be able to bypass the biometric. Once you deploy a security technology, you will often find out how resourceful users can circumvent it.
- User acceptance –End users must accept the technology. See the following section regarding how the least technical requirement can be the one that can undermine everything.

Planning For, and Dealing with, Resistance

End-user resistance represents one area where organizations generally underestimate the amount of planning required in support of a biometric deployment. In fact, one of the most successful biometric initiatives undertaken never saw the light of day for this very reason.

In 2006, the Piggly Wiggly grocery store chain actively tested fingerprint-based biometric solutions. While there was significant consumer interest at the beginning of the rollout, Rachel Bolt, assistant director of information systems for the $700 million grocery chain, stated in an interview in *e-Week* that this interest evaporated due to negative publicity.

Bolt said she didn’t appreciate how emotionally intense some of the opposition was until she visited a store and saw a 70-year-old woman literally throw a Bible at an employee trying to enroll people in the program. The customer was reacting to the concern of some in the religious community that RFID (radio-frequency identification) and biometric controls were the embodiment of the Biblical “mark of the beast” from the Book of Revelations.

“She told him that God was going to rain hellfire on him and that he was promoting the devil’s work," Bolt said, adding that she took that to mean the customer was not interested in enrolling. “We piloted it in four stores and it worked out extremely well,” Bolt said. “The rollout to the entire chain, however, did not go nearly as well as we expected.”

The complaints that Piggly Wiggly encountered are not unique. Most user complaints are concerns over the unknown.

Issues such as privacy, hygiene, employee groups resisting change, and more can undermine even the best-conceived biometric controls' projects. Biometrics concerns have stemmed primarily from an incomplete understanding of the technology on the part of the end-user and a mistrust of the entities that want to implement the technology.

Until biometric controls are more mainstream and generally accepted, the only way to deal with this challenge is an effective end-user awareness and education program in advance of the roll-out of biometric controls. Biometric deployments will be most effective and flow most smoothly when users are educated ahead of deployment.

From a security and privacy perspective, it is imperative to let users know that their biometric images will not be stored. Most biometric applications, with the notable exception of law enforcement, do not store the actual biometric image (fingerprint, retina scan, etc.). Instead, they generate a composite of biometric data from a number of individual data points (minutiae).

This composite data is often mathematically hashed, and the hash is then stored, just as is typically done with passwords today. It is important to educate users that there is no way to recover a full biometric reading from the minutiae scanned.

Making users aware of the actual implementation details can go a long way in defraying their concerns and subsequent resistance. Many users incorrectly believe that their biometric data can be stolen and used against them, but this is not true of modern biometric security systems. (Note that this is not saying biometric controls cannot be tricked, but that the data itself is innocuous.) Though users will still ultimately have to trust that the system is performing as described, it is vital that they understand that this data cannot be used to reconstruct actual user biometric images.

Making Biometrics Work

According to Forrester Research, the most successful applications of biometric controls to date – in terms of scale, efficiency, usability, and public acceptance – have been facilitated by government agencies, intergovernmental agencies, and companies like airlines that cooperate closely with government. However, private companies do have success stories to tell, primarily in the financial services sector, such as in areas like payments and ATM transactions.

The ultimate challenge is taking the potential security benefits that biometric controls offer and making them into a viable solution. Most of the challenges associated with biometric solutions will be business rather than technical in nature. Since biometric controls are for the most part stable and reasonably mature, the focus should be on core business issues, such as:

- Making biometrics meet business requirements
- Integrating biometrics into applications
- Producing documentation to deliver trust
- Management and reliability
- Planning and deployment
- Managing migration and scalability

Before going down the path of using biometrics, it is important to know what the specific security problem is and how a biometric solution can solve it. If this fundamental question can't be easily answered, odds are that the biometric initiative will fail. In essence, it is of the utmost importance to properly define a problem before attempting to apply a solution.

Another key factor in successfully deploying biometric controls is to start with a small-scale rollout. It is good to gain small technical victories and then expand the program. It is often a mistake to attempt a huge enterprise roll-out right away when a pilot program can more easily demonstrate the utility and effectiveness of the solution. Use these scaled-down successes to build the case for a broader deployment.

Given that metrics are a crucial area within information security, it is vital to include them as a gauge of the efficacy of a biometric deployment. Some useful metrics and other ways to determine the efficacy of your biometric solution may include:

- Does the solution deliver real business benefits?
- Is it deployed in a timely and cost-effective manner?
- Is it secure and does it provide trust?
- Is it reliable and easy to use?

- Can it be managed?
- Can it evolve and scale?
- Was it cost effective?
- Does it support regulatory efforts?

In addition to these metrics, the report Biometrics: Beginning to Fulfill Its Promise from Forrester Research highlights two success factors. First, end users understand the system and trust the provider. Public fears of biometrics technology stem primarily from two sources: a lack of knowledge of the technology and mistrust of organizations that would deploy and manage biometric applications. Second, the system should be simple. When the public perceives direct benefits from using biometrics technology, there is a much higher degree of acceptance. Anyone planning to incorporate biometric technology into any business process needs to clearly define these benefits.

Not Silver Bullets

The efficacy of biometric controls is tied to how effectively the solution is deployed. It is important to understand that biometric solutions are not a security silver bullet. While these controls may solve some security problems, they won't solve all problems. They may, however, unintentionally introduce new challenges.

Nevertheless, by using a strategic approach that includes appropriate requirements definition and project management, most biometrics projects can succeed.

This approach advocates ensuring that an appropriate amount of time, staff, and budget is expended. By following this advice and focusing on small-scale, closed-loop problems within an organization, the likelihood of achieving a successful biometric deployment will increase significantly.

Ben Rothke CISSP, QSA (ben.rothke@bt.com [2]) is a Senior Security Consultant with BT Professional Services and the author of Computer Security: 20 Things Every Employee Should Know. Benjamin Tomhave, MS, CISSP, (benjamin.tomhave@bt.com [3]) is a Senior Security Consultant with BT Professional Services.

Security Management is the award-winning publication of ASIS International, the preeminent international organization for security professionals, with more than 35,000 members worldwide.

ASIS International, Inc. Worldwide Headquarters USA, 1625 Prince Street, Alexandria, Virginia 22314-2818
703-519-6200 | fax 703-519-6299 | www.asisonline.org

Links:
[1] http://www.securitymanagement.com/magazine/2008/12
[2] mailto:ben.rothke@bt.com
[3] mailto:benjamin.tomhave@bt.com