The Biometrics Age Is Here

Considerations When Implementing Biometrics Into Your Identity Management Strategy

October 2015
Using biometrics to confirm identities was once confined to James Bond films, but consumer products by Samsung and Apple have brought the convenience of biometrics into the mainstream. Consumers appreciate biometrics for their added convenience since they don’t have to memorize or carry anything, such as a key fob, to access goods and services. And organizations like biometrics because they are harder to replicate and share than passwords or tokens.

Fingerprint has been the first modality to find a strong foothold (and is still one of only two markers the FBI currently recognizes as “true biometrics”), but this method will likely be joined by a wealth of additional modalities in the near future. Voice biometric systems, iris scanners, facial recognition software and other modalities are already on the market, and researchers continue to explore all the ways our individual traits might be used to confirm our identities.

To be sure, biometrics is a valuable tool to help organizations quickly confirm customers’ identities and pass through valid transactions. But they don’t work in a vacuum. The effective integration of biometrics, like that of any other identity management tool, takes planning and an understanding of both your organizations’ and customers’ needs. Here are a few key things to consider as you add biometric solutions to your identity management strategy.

Address Internal and External Concerns to Ensure Biometrics Acceptance

Consumers accept biometrics if it allows faster transactions or greater convenience. A recent Deloitte survey found that 72 percent of respondents would willingly use biometric identification to enable a mobile device for financial transactions.1 Similarly, an Accenture survey showed that 89 percent of respondents across the U.S., U.K., France, Germany, Japan and Australia would share biometric information with government agencies to improve their travel experience.2 Statistics like these make it quite clear that consumer sentiment around biometrics has changed, and sharing this kind of market data can help make the case for biometrics when addressing naysayers in your organization.

To get your internal team on board with biometrics:

- **Identify and engage stakeholders early** – Changes to identity management processes and technologies don’t just affect your security and fraud teams. Make sure you engage the right people from across your organization—both those directly involved as well as employees in ancillary groups such as customer service, operations, IT and others—who may be impacted by the choices you make. This will not only allow you to garner early support, but will also help ensure that the solution you design actually works for your organization as a whole.

- **Create a roadmap for implementation** – Work with your planning committee and key stakeholders to understand your priorities, operating environment and future plans for the business.

- **Communicate match rate and other measurements** – Set benchmarks, in quantifiable terms, for how you expect the solution to perform.

- **Conduct internal beta tests before going live** – Consider recruiting a select set of your employee base to act as your users in order to fully explore the pros and cons of your set-up and to optimize your processes prior to going live with an external customer set.

72% would appreciate the use of biometrics to enable mobile financial transactions.1
Once you achieve internal buy-in, you must persuade customers that the value of using biometrics offsets typical privacy concerns, such as whether one’s fingerprint will be shared with law enforcement. To encourage this acceptance:

- **Communicate privacy policies around usage and storage** – Be upfront and proactive in your communications when rolling out your biometric solution. Send out notices via email, mail or other applicable customer communication channels. Make sure your policies are clearly displayed on your website, mobile apps, terminal interfaces and any other interaction points where customers may be asked to supply their biometric print.

- **Stress security and convenience to increase adoption** – Going back to the Deloitte and Accenture surveys, consumers are largely receptive to the idea of biometrics as long as they see the value in their participation. When promoting your biometrics enrollment program, draw a clear line to the value the customer will receive, whether in the form of reduced wait times, reduced password resets or other benefits.

- **Implement in stages** – Just as you want to test on internal employees before taking your biometric solution external, you may want to pilot the solution with a select set of customers before rolling it out to your entire customer base. This beta group may be defined by a specific product type, customer tier or geographic area.

- **Provide incentive for early adopters** – As part of the “value” equation, consider providing your enrolled customers streamlined, self-service access to transactions that would otherwise require human intervention or a more involved security process (i.e. allow them to unlock certain functionality or transactions only if they enroll in your biometric program).

**Voice Biometrics: Passive or Active Enrollment?**

Voice biometrics recently has been expanding into call centers in health care, financial services, government, retail and other sectors as organizations seek to reduce transaction times, increase self-service capabilities and increase security. As more organizations look to implement voice biometric solutions, one of the first questions to address is: Passive or active?

While passive enrollment is ideal for fraud detection, active enrollment is better suited for authentication purposes. Passive voice biometrics run behind the scenes, looking for patterns that map to known fraudsters. The biometric capture and screening is not apparent to the user, making it less likely that the fraudster can prepare workarounds to thwart the system. It can also be more loosely defined because your organization is not stopping an interaction based on matchability. However, passive biometrics requires multiple interactions to gather a user’s information and build a voiceprint, so it’s harder to achieve in a low-touch environment. It also typically requires other information to correlate the identity, such as phone reputation or verification, historical voice recordings and transactional data analytics.

4-5x

It typically takes four to five interactions to build a print when using passive voice biometrics.
Active enrollment is better for authentication because a would-be fraudster who knows he’s being proofed will avoid enrolling. Conversely, this transparency makes honest customers trust an organization more—customers are told upfront that their voice print is being captured for identity management purposes and they are able to choose to enroll or not. Active voice biometrics also offers 1:1 and 1:N matching, meaning that your organization can confirm not only that the print belongs to the enrollee but also that the print is not associated with other identities in your system. Voice biometrics also supports a self-service model for greater customer convenience. A customer enrolled in an active voice biometrics program, for example, can be given the option to authenticate himself via voice to automatically reset a password, versus having to answer multiple security questions for a customer service rep prior to a manual reset.

To be effective, though, authenticated enrollment is a critical first step in active voice biometric deployment. Authenticated enrollment is the process of proofing the user’s identity before creating her secure biometric credential. In other words, you want to ensure that the person on the other end of the phone is really Sue Smith before you bind the voice print to her identity.

Even with authenticated enrollment, active voice biometrics should still be used as only one part of a multi-layered approach to authentication, integrated with other factors such as device level information, pattern/behavioral data or geo-based information.

**Deployment: On-Device or In-Cloud?**

Now that your organization has decided to move ahead with biometrics, how should the solution be deployed? There is no single “right” answer to this; In-cloud vs. on-device storage decisions ultimately come down to your organizational infrastructure and policies.

Some organizations believe on-device deployment is more secure and have implemented infrastructure and security protocols that are too restrictive to allow for cloud-based deployment. Cloud-based biometric storage and analysis, however, offers the ability to proof the identity before one captures the biometric, which binds the biometric more strongly to the identity. Localized biometrics stored on the device only provide 1-to-1 authentication at the device level; they do not account for the biometric being enrolled on multiple devices or support the ability to compare biometrics across a population for fraud prevention. In contrast, cloud-based storage helps identify this type of fraud by supporting biometric evaluation across devices and locations.

LexisNexis offers secure, hosted biometric solutions that give our customers the ability to flag known fraudulent voices that have previously enrolled in our biometric systems. This allows organizations to share “known bads” since criminals rarely stick to one organization or industry. Organizations would be more likely to implement biometrics if they could rely upon such a resource.
The Biometrics Age Is Here

Biometric Fusion and the Importance of Multi-factor Authentication

No matter what biometric form you choose (fingerprint, voice, facial recognition or other), there will always be biometrics exceptions—instances where biometric capture cannot be adequately obtained, either due to customer constraints (such as calluses, cataracts, or other physical impediments) or environmental factors (such as noisy, crowded areas and low-light settings). The ability to switch from one modality to another to handle these biometric exceptions can contribute to a better overall customer experience and is sometimes lumped into the category of “biometric fusion.”

However, this is not truly multi-factor authentication. Biometric fusion constitutes layering biometrics for greater levels of assurance. While this is an attractive proposition on the surface, it does not adequately address the multi-factor authentication imperative. That is, combining several methods of a single factor does not sufficiently overcome the inherent variability and uncertainty (“biometric entropy”) in biometric samples to meet most security requirements.

To achieve a true biometric–driven multi-factor authentication (MFA) system that accurately identifies and verifies individuals, it is critical to layer biometric verification—‘something you are’—with at least one other factor that addresses knowledge—‘something you know’—or possession—‘something you have’. These sources may include biographical content from government-issued identity documents, identity resolution and verification using authoritative data sources, geo-location/mapping, dynamic knowledge-based authentication, device fingerprinting and risk scores, among others.

Conclusion

This paper outlines some of the initial issues with which organizations grapple, but there are a number of additional factors you may need to consider in deciding which biometric modalities to incorporate and how to best design your solution. Successful implementation requires detailed upfront planning and a solid 360˚ view of your needs and objectives, taking into consideration security goals, service goals, sales goals, customer needs and the like. But the process doesn’t have to be complicated. Seek a vendor that understands identity and authentication workflow and can provide a holistic solution that addresses enrollment, infrastructure and integration needs along with the technical aspects of the solution.

Sources

Have additional questions about biometrics?
We’re happy to help. LexisNexis has the data, technology, partnerships and expertise needed to enhance your IdM efforts, and we provide MFA solutions that are an essential component of any security strategy using biometrics.

For more information
Call 866.887.8343, visit lexisnexis.com/risk/identity

About LexisNexis® Risk Solutions
LexisNexis® Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group plc, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.