CHALLENGES AND CONSTRAINTS TO THE Diffusion of Biometrics IN INFORMATION SYSTEMS

Biometrics are a promising technology for improving security, if they can overcome technical and social challenges.

Computer security incidents have grown exponentially since 1997, and about 90% of all major organizations are affected by them each year [3]. Such incidents can have cascading and devastating effects on an economy, particularly when coordinated. The massive power outage on August 14, 2003 that simultaneously affected the U.S. and Canada demonstrates the vulnerability of an interconnected economy. Terrorists can exploit such vulnerability, with dramatic consequences. An attack on a network can cascade across organizations in many industries and locations, resulting in significant downstream liability issues.

The nature of downstream liability is aptly illustrated through the case of a hypothetical power company, DLI, Inc. An intern gains access to DLI's network and orchestrates a denial of service attack on the company's IS. From a micro perspective, this incident affects only the company's network. But from a macro perspective, it could affect DLI's ability to manage its power grid, with collateral

By Akhilesh Chandra *and* Thomas Calderon

damage extending well beyond its boundaries. It is conceivable that as a result of this act, airplanes might not land or take off, hospitals might not function, ports might not provide loading and unloading services, and gas stations might not operate. Cumulatively, such events could temporarily shut down an entire economy. DLI's user authentication process and access controls were weak, but the other affected organizations did not necessarily have security lapses. With more effective access controls, DLI could have avoided much of the downstream collateral damage.

DLI's case illustrates how a seemingly routine breach of security can affect critical business processes of other entities in widely separated locations. The domino effect comes alive largely because of an increasingly interconnected world economy. The very connectivity that enhances global business increases vulnerability and exposure associated with attacks on computer systems. A primary concern is that many attacks involve surreptitious access to information resources, and organizations are often unaware of unauthorized access to their IS [3]. Given that cyberspace is huge and constantly changing, organizations must act proactively to protect their information infrastructure.

Protection of information resources must involve a process that unambiguously identifies and authenticates users [8]. Biometrics (measurements of the physiological characteristics and behavioral traits of humans) are touted as powerful tools in meeting this ambitious goal. This technology is expected to solve identification and authentication issues in IS and other applications, including customs and immigration, computer access controls, and physical security. (Identification is a one-to-many matching process that ascertains the existence of an individual in a database. Authentication is a one-to-one matching process that verifies the identity of that individual.)

As organizations upgrade information security with biometrics, and security providers seek to meet demand, it is imperative to consider the technology's inherent challenges and constraints in order to reduce control risk—the likelihood that a biometric authentication system will fail to prevent unauthorized access to an organization's information resources. Based on the diffusion-of-innovation literature and recent empirical studies in the IT domain [10, 11], we provide essential caveats in the form of challenges, constraints, and limitations of biometric technology organizations should consider as they evaluate the technology. Figure 1 presents six broad caveats—business, operational, system, technical, legal and regulatory, and people—pertinent to biometric technology. The severity of each caveat can be better understood by examining the process model (see Figure 2) of a biometric authentication system (BAS). Each step in this model is annotated with possible challenges derived from a risk assessment of the BAS.

Business Issues

Biometrics by itself is insufficient as an information security mechanism. Ultimately, the overall security system must be effective in order to ensure confidentiality, availability, integrity, authentication, and nonrepudiation. When biometrics are a component of the internal control system, the challenge is to strategically link and integrate it with other controls to protect business systems. (Examples of these other controls are segregation of duties; supervision and authorization; approval, reconciliation, and verification of transactions and events; control environment; risk assessment; information and communication; and efficient control procedures.) Organizational dynamics and current global instability create a need for a strong and integrated approach to information security and control. Integration becomes more challenging when companies have trading relations in politically unstable regions.

Further, increasing security by using biometrics creates conflicting issues of higher costs and reduced ease of use—vital in the diffusion of innovation [11]. The direct costs of implementing BAS are immediate, tangible, and measurable; the benefits are qualitative, longer term, and difficult to estimate monetarily. This disparity confounds value assessment and financial feasibility analysis, increasing the challenge of communicating the technology's relative advantage and slowing its diffusion [11].

Closely related is the lack of sufficient independent and unbiased performance data on specific biometric devices, hampering credibility. This increases the ambiguity of the benefits associated with the technology and, thus, the likelihood that an innovator will have difficulty defending the efficacy of a BAS in litigation. Such problems can be significant in banking and financial services if customer accounts are erroneously accessed or bona fide users are denied access.

Most biometric applications rely on an assessment of similarity between stored templates created at enrollment and biometric samples taken during user authentication. The matching process suffers from imprecise standards (such as the rigidity of thresholds to define performance precision) for the measurement of similarity. Stricter (or more relaxed) matching requirements result in higher rates of false rejections (or false acceptances).

Further, there is no guarantee that all organizations would benefit uniformly from the use of biometrics.

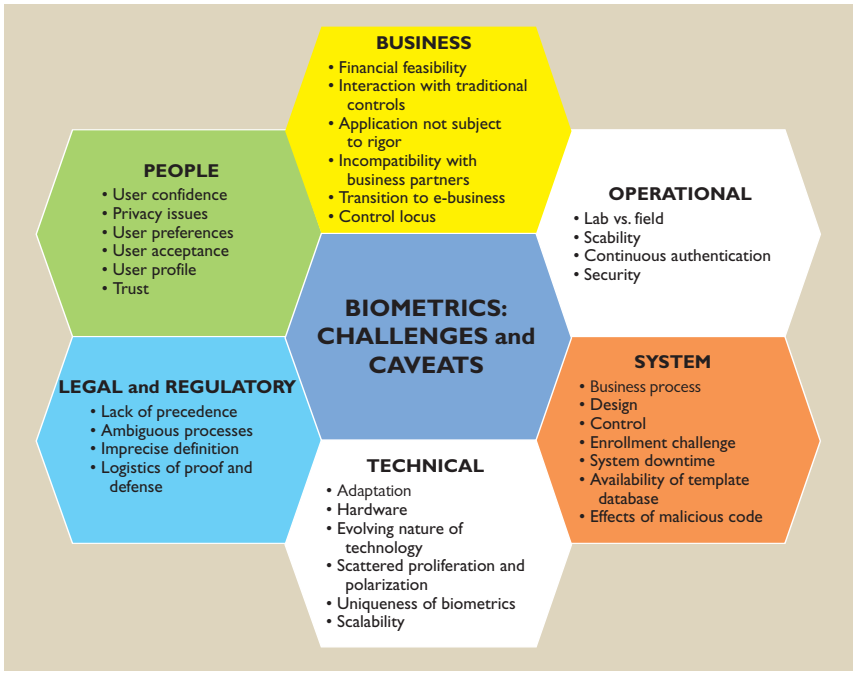

Figure 1. Biometric challenges.

The onus is on supporters of biometrics to build a sound business case driven by an organization's needs and context. The extent of IT deployment in business processes, its strategic importance in the value chain, and the potential for loss due to poor or weak control systems are context-specific factors that influence the potential effectiveness of BAS.

Applied to the DLI case, the company must address both financial and non-financial issues in making a business case for implementing a BAS. The discussion of financial issues could focus on establishing the existence of a positive ROI for biometrics. Equally important, non-financial issues are largely intangibles that include managing relationships with internal and external business partners. Since each entity along the supply chain has to make its own business case for BAS investments, a biometric-enabled IS for DLI does not necessarily ensure the adoption of biometrics by the company's business partners. In the presence of technological asymmetry and IS connectivity, the company would be left exposed to the same security vulnerabilities as its business partners.

DLI would have to selectively identify key components of its IS that needed tight security and access controls. However, the rigidity of such controls could adversely interact with ease of access by bona fide internal and external users of its IS, interfering with normal, smooth business transactions.

Operational Issues

Operational challenges emerge during enrollment, authentication, and storage processes in BAS. The

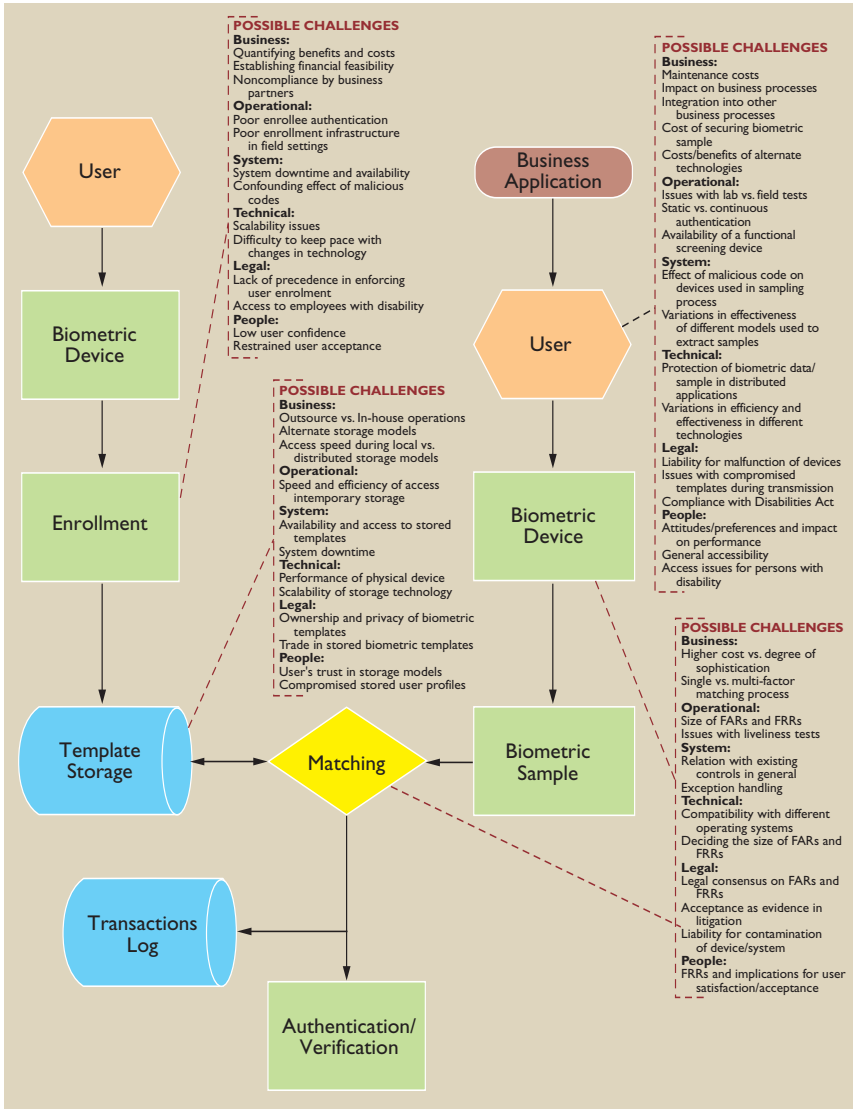

Figure 2. Biometric control process and associated challenges.

security afforded by a biometric device is a function of controls embedded in the enrollment process. A poorly secured enrollment process does little to enhance the effectiveness of the security system or the trustworthiness of a BAS. The promise of biometrics is meaningless if an enrollee is able to construct a false digital persona to access a protected system.

Challenges during storage pertain to access privileges, storage models, outsourced versus in-house storage operations, access speed, and system downtime. For example, storage models can interfere with user acceptance and trust of BAS. The performance of BAS during high-use periods and its ability to keep pace with technological advancements can affect its long-term viability.

While commercial applications are beginning to emerge, the technology is still in its infancy, raising concerns about scalability. Field performances of certain biometrics, especially in large-scale public applications, have not been promising. For example, a facial recognition device at Fresno Airport performed poorly in a U.S. Army test [2]. And finger-scanning devices installed in a large consortium of German banks had a 10% failure rate [1].

No industry-specific guidelines exist to address errors in BAS. For example, certain cosmetics affect the quality and accuracy of fingerprint samples, thereby denying access to users. In such situations, users are typically asked to alter their behavioral patterns in order to facilitate the technology or organizations respond by creating overrides, which can compromise the effectiveness of biometric mechanisms.

Even in situations where biometrics work with fewer compromises, conflicts can arise between authentication in a particular session and in continuous authentication. A user might successfully authenticate at the start of a session, but a different person could take over that session. BASs are used only to verify users' identities when they initiate a session. Once initial access is granted, an imposter can spoof the system in the absence of any real-time continuous authentication [9]. Slow technical progress, lack of standards, and concerns about BAS viability constrain migration toward automated continuous BAS. The distributed nature of contemporary corporate networks exacerbates such issues and concerns.

In the DLI case, if the company chooses to install a BAS, it may not be able to protect the authenticated session on a continuous basis. The standards are primitive and non-rigorous for handling exceptions in case of emergencies and for dealing with business partners that may not adopt the technology. Enrollment and re-enrollment of all potential users in various operating conditions at disparate locations present logistic challenges. Finally, DLI would need to identify and mitigate possible threats at each stage of the BAS (see Figure 2).

The limited number of large-scale business applications, as well as the proprietary and confidential nature of a company's information security, constrain opportunities for developing reliable case studies about biometrics. Yet such case studies can represent a valuable knowledge base for learning about operational conditions leading to successful implementations. Similar arguments hold for biometric devices. Concerns persist about the consistency and reliability of their operation in various field conditions.

THE onus is on supporters of biometrics to build a sound business case driven by an organization's needs and context.

People Issues

A serious challenge in implementing biometrics is building public confidence. Civil libertarians, including the ACLU, stigmatize biometrics as being intrusive by nature, a potential tool for mass profiling, and a harbinger of the erosion of individual privacy. Unlike conventional identifiers (such as passwords and tokens), biometrics are inextricably linked to a specific person and cannot be changed, replaced, or modified.

Other potentially sensitive issues include user distrust of the privacy and confidentiality in BAS, the security of biometric databases, and function creep (use for applications beyond their original purpose). While the post-9/11 public is seen as more willing to trade some privacy for more security [4, 7], the long-term maintenance of this trend is debatable. Many organizations lack systematic incident response schemes for compromised biometrics. Ultimately, organizations must address these contentious issues lest an otherwise promising technology fail the important user acceptance criterion for effective diffusion of innovations [11].

In view of user distrust, independent third parties should provide assurance of the trustworthiness of bio-

metric systems. These services could include verification of the privacy of biometric data and the security and integrity of biometric databases, as well as protection of transmitted biometric templates and samples, particularly over distributed networks.

In the DLI case, requiring certain users to authenticate through a BAS is difficult to justify, particularly if the users are part of the organizational extranet. Such users could represent significant weak links in DLI's security process. DLI vendors and customers without strong user authentication systems could jeopardize the company's information security. As was learned during Y2K incident response planning, the information security threats faced by business partners are ultimately potent threats to an organization's information infrastructure.

Legal/Regulatory Issues

The lag between advances in technology and the law is especially troubling with respect to biometric technology. There are three major concerns:

First, in order to substantiate the use of BAS data as evidence in a court of law, the reliability of the data needs to be established [5]. There is little independent verification of the performance of many of the available devices. This could have implications for the admissibility of BAS data as evidence in litigation. The specific biometric device, as well as the enrollment and sampling processes, should pass the verification and reliability test.

Second, it is unclear whether the user or the organization that uses biometrics owns the samples and templates. A proposed bill in New Jersey is seeking to address this issue by specifying the types of uses that can be made of biometric data and requiring users' approval for any use other than those originally specified [12].

Third, not everyone in an organization has the prerequisite physiological or behavioral traits for using BAS technology. A large international corporation found that certain users do not have sufficient minutiae on their fingerprints for accurate measurement and storage by a biometric device. A more severe case could be a situation where a class of users does not have the underlying biometric (for example, eyes and fingers). It seems likely that the Americans with Disabilities Act would require companies to accommodate those users, potentially increasing the cost of implementing biometrics.

In the absence of standards, defined measures, and precedents, the legal complexity of establishing user identity through distributed or remote BASs is fraught with uncertainty. Perhaps the principal question has to do with the absence of a trustworthy distributed enrollment infrastructure. Equally contentious is the issue of legal jurisdiction in multi-state and cross-border e-business authentications.

The foregoing legal constraints could inhibit the diffusion of this technology as a security mechanism [11]. Lack of legal clarity and concerns about ownership and jurisdiction imply there is room for valid evidence to be set aside on technical grounds. In order to reduce the vagueness surrounding legal interpretation, refinements are needed to establish and independently verify the efficacy of biometric data and processes for automated authentication of IT users. Such issues are particularly germane because most applications use a mathematical representation of a biometric rather than the actual biometric.

Applied in the context of DLI, tracing and fixing responsibility for the first event triggering the domino effect is fraught with ambiguity and legal complications. If the parties at the end of the cascading dominos are involved in a legal dispute as a result of infiltration of DLI's IS, the failure to identify the cause could result in a miscarriage of justice. Fairness in the administration of justice would require clarity in definitions, causal relations, and legal precedence.

Technical Issues

An intriguing technical issue, which could confound perceptions of the technology's relative advantage [11], relates to the extent of biometric distinction across the population of potential users [6]. The literature defines biometrics as distinguishable (rather than unique) physiological and behavioral traits that may be used for identification and authentication [8]. Similarly, a match between a biometric sample and a stored template is classified as probable instead of certain. The issue of uniqueness is most relevant when the technology is used for both identification and authentication in large-scale public applications.

It has been suggested that biometric devices can be spoofed by using various schemes (such as a finger mold). While limited solutions exist to control spoofing, such enhancements exacerbate the trade-off between low error rates and BAS efficiency.

Further, natural aging and unanticipated changes in physiological characteristics (for example, as a result of accidents or surgery) can constrain BAS implementation. Certain cases may necessitate re-enrollment, which could increase costs and reduce the appeal of biometric security. Thus, it is important for organizations to monitor their BAS technology to ensure appropriate responses to systematic temporal degradations in performance.

Storage of templates and the transmission of biometric data complicate security logistics. Storage on a server carries the risk of interception during transmission and

EVEN in situations where biometrics work with fewer compromises, conflicts can arise between authentication in a particular session and in continuous authentication.

of unauthorized access to the database. The legal ambiguity between ownership of the physical record and ownership of the underlying information is exacerbated when biometric data is stored on a server rather than on smart cards. Storage of biometrics on a local device or smart card alleviates some of those issues.

Assuming DLI implements a BAS, we could expect a reduction in control risks. This implies that the probability of unauthorized user access would be reduced. However, authorized users could still orchestrate a denial of service attack in the same way that DLI's intern could. Thus, in addition to biometrics, DLI should employ other robust information security initiatives to minimize both direct and collateral damage.

System Issues

System-related challenges include the effect of technology on business processes, systems design and performance, and data modeling and architecture. The need to secure the stored biometric template and the log of authentication sessions, as well as limits on the potential for complete re-engineering of ISs, are critical issues. There is a paucity of tested system design and data storage/processing models that illustrate the integration of biometrics with conventional controls.

The effects of malicious cyber attacks, downtime, and major disasters are unclear. Existing models of data storage and data transmission do not fully address the security and privacy issues, as many of the potential threats are still emerging. Inherent in this debate is the conflict between centralized administration and decentralized, easy-to-use systems.

The suitability of controls in each business process must align with the desired degree of security, ease of use, and normal business transactions. In the case of DLI, the system challenges translate into deciding how to transmit electricity over power lines to remote geographical locations and how to secure critical assets from pilferage, sabotage, and terrorism. Any biometric authentication solution the company adopts must facilitate security and performance in the context of those system challenges.

Conclusion

This discussion of the challenges to and constraints on the diffusion of biometrics in IS applications offers a pragmatic model researchers can use in future empirical or model development work related to the diffusion of biometrics in information security applications. Vendors and user companies planning to implement BAS technology should reflect on and seek solutions to these challenges and constraints in order to accelerate the diffusion of the technology and strengthen their biometrics innovations.

Challenges in implementing the technology need a holistic solution that satisfies users' concerns and blends well with the traditional internal control model. Until the technology matures, legal issues are clarified, and user trust is at acceptable levels, organizations should strive to meet these challenges on a case-by-case basis, duly weighing security needs, mission-critical nature of business processes, and potential user resistance. C

References

1. CardTechnology.com. German savings banks reject biometrics at ATMs. *Card Technology Magazine,* 2000; www.cardtechnology.com (accessed Sept. 19, 2002).
2. Claburn, T. Man vs. machine. *Smart Business 15,* 4 (2002), 34.
3. CSI. 2003 CSI/FBI Computer Crime Survey, 2003; i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf (accessed July 28, 2003).
4. Furnell, S.M., Dowland, P.S., Illingworth, H.M., and Reynolds, P.L. Authentication and supervision: A survey of user attitudes. *Comput. Sec. 19* (2000), 529–539.
5. Harvard Law Review. Evidence—fingerprint experts—Seventh Circuit upholds reliability of expert testimony regarding the source of latent fingerprint—United States v. Harvard, 260 F.3d 597. *Harvard Law Rev. 115,* 8 (2002), 2349–2356.
6. Jain, A.K., Prabhakar, S., and Pankanti, S. On the similarity of identical twin fingerprints. *Pattern Recog. 35* (2002), 2653–2663.
7. Lavonne, K. Grocer seeks loyalty boosts through biometrics. *Amer. Banker 167,* 87 (2002), 13.
8. Matyas, S.M., and Stapleton, J. A biometric standard for information management and security. *Comput. Sec. 19* (2000), 428–441.
9. Monrose, F. and Rubin, A.D. Keystroke dynamics as a biometric for authentication. *Future Gener. Comput. Syst. 16* (2000), 351–359.
10. Mustonen-Ollila, E. and Lyytinen, K. Why organizations adopt information system process innovations: A longitudinal study using diffusion of innovation theory. *Inf. Syst. J. 13,* 3 (2003), 275–297.
11. Rogers, E.M. *Diffusion of Innovations.* Free Press, 2003.
12. State of New Jersey. Biometric Identifier Privacy Act. Assembly No. 2448. State of New Jersey. 210th Legislature. Introduced June 13, 2002 by Joan M. Quigley.

Akhilesh Chandra (ac10@uakron.edu) is an associate professor of accounting and associate director of the Center for Research and Training in Information Security and Assurance (CReTISA) at the University of Akron, Akron, OH.

Thomas Calderon (tcalder@uakron.edu) is chair and professor in the George W. Daverio School of Accountancy and director of CReTISA at The University of Akron, Akron, OH.