
10

TEN CRITICAL THINGS YOU NEED TO KNOW ABOUT SECURE IDENTIFICATION

DatacardGroup

SECURE ID AND CARD PERSONALIZATION SOLUTIONS

TEN THINGS YOU NEED TO KNOW — TODAY

WiFi networks. Malicious code. GPS tracking. Industrial espionage. Pervasive computing. Terrorist threats.

These and other factors are reshaping the way we do business. More important, they are changing the definition of security — as it applies to the information, intellectual capital, networks, facilities and other assets in an enterprise. In this rapidly changing world, people need to know more about secure identity and how to maintain it in a complex organization.

As recently as 10 years ago, for example, most people accessed a company by walking through the front door. Today, authorized and unwanted visitors alike can gain access electronically, using any number of public or private channels. In this new reality, the most pressing security question quickly becomes, “How do I confirm the identity of every individual who interacts with my enterprise?”

The same forces are influencing government agencies, colleges, universities, hospitals, hotels, health clubs, casinos and other organizations. The questions are similar: “How do I establish security without hindering productivity? How do I maintain a safe, secure campus? How do I utilize customer information without compromising privacy?”

This document frames 10 critical issues of secure identification. It explores key issues and provides some insight. What it does not do is provide all the answers you need. For detailed answers that speak directly to your industry, please contact a Datacard Group secure identity specialist.

ONE SOLUTIONS PROVIDER YOU NEED TO KNOW

Datacard pioneered digital photo ID systems more than a decade ago. Today, we still lead the industry with bold, innovative solutions for secure identity.

But this single component — the ID card — is far from our only area of expertise. Today, Datacard designs and develops complete, integrated solutions that help organizations of all sizes establish a safe, reliable and easy-to-manage approach to secure visual and virtual identification.

Our latest generation of secure ID solutions incorporates emerging technologies, from smart cards and biometrics to customized holograms and optical variable devices (OVDs). Every day, well-known corporations, government agencies, colleges and universities rely on Datacard® solutions to maintain security in their enterprise. Of course, these solutions are designed to grow with you. No matter how large or small your operation, Datacard Group can deliver a secure ID solution that suits your specific needs.

As you read this document, you will likely have additional questions. How do these ideas apply in my market? What technology is right for my organization? What steps should I take right now? What about the future?

To find the answers, call 1.800.944.4216 ext. 6606. You can also send email to identity@datacard.com or visit www.datacard.com for more details.

10 CRITICAL THINGS

Most users see risk, threats and vulnerabilities all around them but remain confused about which way to turn. Before choosing a technology solution, they labor through about a half dozen disparate product evaluations, adding time and cost to the implementation process while their organizations remain insecure.

Source: Enterprise Security Group, 2005

The convergence market will grow rapidly in the next five years as enterprise risk management points more companies to greater security efficiencies and effectiveness.

Source: Forrester Research, 2005

1. SECURITY TECHNOLOGY IS EXPLODING.

The transition from film-based photo cards to digital ID systems occurred relatively slowly, over the course of 20 years. Today, major advances in card security emerge at a significantly faster pace.

Areas of innovation are numerous. They include discrete technologies, such as customized holographic imagery, UV ink, micro-printing and laser-retrievable text; new combinations of platforms, such as contactless smart cards and biometric templates; fresh applications of familiar technologies, such as smart chip-enabled e-passports; and new international standards for device interoperability.

Although this rapid innovation increases overall security, it makes your organization's planning decisions much tougher.

2. CARD APPLICATIONS ARE CONVERGING.

With more potential points of vulnerability to contend with, many organizations are consolidating their lines of defense. Instead of deploying a separate solution for every possible threat, forward-thinking companies are using secure ID cards that enable both physical access to facilities and logical access to networks. This approach greatly simplifies the security infrastructure, eliminating the need for separate cards, databases, passwords and procedures. It is also much less expensive to administer and manage. These measurable gains in efficiency and cost are important indicators for the future of secure IDs, pointing the way toward cards that consolidate even more applications, such as cashless payment, time and attendance, and secure tracking of individuals and equipment.

10 CRITICAL THINGS

As much as 50% of security breaches at large companies happen from the inside.

Source: Computer Security Institute, 2001

3. POINT-OF-ENTRY VERIFICATION REQUIRES MORE THAN A VISUAL ID.

Consider these trends: Rising numbers of temporary, part-time and flex-time workers. High employee turnover. Greater reliance on outsourcing. Add them up and you get a constant stream of unfamiliar faces entering your facilities. This makes it impossible for security staff to memorize all the employees, visitors and vendors they encounter. In fact, many security personnel are themselves contract workers who do not put in the regular hours necessary to recognize authorized visitors on sight.

Effective point-of-entry verification requires a failsafe digital solution, driven by a central image database. This allows security teams at any location to compare the person in front of them with that individual's photo and data pulled up immediately on a local workstation, then confirm his or her identity and security clearance at a glance.

4. SECURITY AND ASSET MANAGEMENT ARE NOW A SINGLE FUNCTION.

Over recent years, issues surrounding the valuation of intellectual property and intangible assets for tax purposes have become increasingly common and the values involved increasingly significant. This trend reflects the growing importance of intellectual property, and intangible assets more generally, in the value of business operations.

Source: PricewaterhouseCoopers, 2005

The role of your security team has expanded dramatically with the advent of mobile and wireless computing — and with the skyrocketing value of intellectual property. Security professionals no longer have the narrow task of gatekeeping at building entrances. Instead, they are responsible for tracking and safeguarding physical and intellectual assets. In other words, they have evolved into total asset managers.

To operate as securely and efficiently as possible, organizations must equip security staff with a single, integrated solution for performing point-of-entry verification, tracking physical assets and protecting intellectual property. A secure, centralized image database provides real-time access to key information from a readily available and easy-to-navigate source.

\$844 billion worth of corporate deals were announced in 2004, up 50% from 2003 levels. U.S. mergers could hit the \$1 trillion mark in 2005.

Source: Kiplinger.com, 2005

5. MERGERS AND ACQUISITIONS CREATE SECURE IDENTITY CHALLENGES.

Mergers and acquisitions are two of the greatest challenges facing professionals in security, human resources and IT departments.

The need to create and quickly implement a strong, consistent corporate identity is obvious. But what about individual identity? Who is authorized to enter a facility? Remove property? Access the network? Who is employed and who is a contractor? How do you track the intellectual and physical assets that belong to each enterprise involved in the transaction?

Mergers and acquisitions also often involve layoffs and heavy turnover, providing fertile ground for confusion and resentment — and inviting opportunities for workplace theft, violence and sabotage.

All of which makes security a top concern, and makes a centralized image database — accessible anywhere in the world by authorized users — invaluable for your enterprise. It allows you to know precisely who's who and who has access to specific facilities and privileges.

6. EVERYONE BENEFITS FROM A SECURE ID DATABASE — NOT JUST SECURITY.

Most people see security departments as the sole beneficiaries of integrated identity management solutions. While security executives often take the lead in implementing identity solutions, most organizations quickly discover that the benefits of instant access to ID images and demographic data stretch far beyond the security team.

With instant access to secure identity information, teams in risk management, real estate, IT, human resources and marketing can do their jobs with more impact and higher efficiency. Enterprises should strive to make this information readily available to employees in all departments.

Historically, a multitude of separate systems handle identity management functions. For example, one program handles provisioning, another manages passwords, LDAP stores authentication information, and each application (or administrator) maintains individual user access-control lists. Keeping these separate functions maintained, synchronized and up to date is a resource-intensive, costly proposition.

Source: Intelligent Enterprise Magazine, 2004

10 CRITICAL THINGS

As online scams get more sophisticated, passwords are becoming hopelessly outmoded. Yet many businesses and nearly all consumers still rely on passwords as the primary means of verifying who they say they are.

Source: CNET News.com, 2005

The increased use of biometric-enhanced Machine Readable Travel Documents (MRTDs) will lead to speedier passage of travelers through airport controls, heightened aviation security and added protection against identity theft.

Source: International Civil Aviation Organization, 2003

7. ONE-FACTOR AUTHENTICATION IS ON THE WAY OUT.

The number of factors involved in an identity verification — whether visual or virtual — increases security exponentially. One-factor authentication requires a single piece of data (a password) or a single document (a photo ID card). Many organizations still rely on one-factor authentication for granting access to facilities and networks. Unfortunately, it provides a bare minimum of security, because an unauthorized visitor only needs to steal one password or alter one document.

Two-factor authentication combines the individual components. For example, an employee scans an ID card and types in a password to gain access to a secure network. Two-factor authentication is quickly eclipsing one-factor authentication as the minimum basic standard for secure access.

Three-factor authentication offers even greater protection, requiring an individual to produce something they know (a password), something they have (an ID card) and something they are (a biometric scan). As three-factor systems become more affordable to implement, they will be ideal for securing your organization's most critical facilities, such as R&D labs.

8. BIOMETRICS AND SECURE IDENTITY DOCUMENTS ARE MERGING.

Fingers, hands and eyes all have unique, measurable attributes that can be used for positive identification. That's why biometrics are now being incorporated into the full range of secure documents, including ID cards, visas and passports. It's also why truly effective identity solutions offer biometrics as an option.

Typically, an individual must submit to a biometric scan to acquire the secure document. The scanned information is then converted into a binary template, which can be saved in a centralized database and encoded into a contactless smart card chip within the secure document.

This helps organizations protect themselves in new ways. For example, if a photo ID card also contains a biometric template, unauthorized visitors would easily be detected — even if they had altered the photo on the card or expertly disguised themselves. Biometrics are also an effective solution for remote authentication, where a visual confirmation is impossible.

The most insidious damage [of online fraud] is to a bank's reputation.

Source: Bank Technology News, 2004

9. IDENTITY IS CENTRAL TO THE SUCCESS OF YOUR BRAND.

All too often, key elements of brand identity, including logo usage and badge design, are handled at the local level. Even if you issue clear guidelines, local execution often varies. This inconsistency can erode an enterprise's identity and brand. These investments are worth protecting.

With a centralized image database at the core, a secure identity solution helps eliminate inconsistencies and strengthen your organization's image. For example, you can post approved ID designs and logo treatments on your network. This allows everyone to issue consistent photo IDs, and gives you precise control over the variables that reinforce a strong global brand. Even more important, it helps reduce the risk of unauthorized individuals exploiting inconsistencies in ID design to breach your security protocols.

10. IT ALL STARTS WITH A PLAN.

Today, secure identity information impacts every department in the enterprise, from marketing to human resources, IT to risk management. It takes calculated, strategic thinking to make the most of this critical, far-reaching function.

Visual and virtual identification have become central to protecting people, property and profits — and consequently, developing an integrated secure identity solution has become an absolute necessity. Photo ID cards with smart card, biometric, radio frequency (RF) and other technologies, combined with a centralized image database, provide a long list of security, productivity and identity benefits that no enterprise can afford to ignore.

Datacard Group provides a complete range of digital identity systems for corporations, government agencies, schools and other enterprises of all sizes. **For more information, call 1.800.944.4216 ext. 6606. You can also email identity@datacard.com or visit www.datacard.com.**