Identity management is one of the hottest IT topics in the industry today, with the Gartner Group expecting identity and access management (IAM) to be the fastest-growing product category through 2007, with over 10 percent compound growth rates from 2003 to 2007.

But what makes this mission-critical issue even more complex is the new phenomenon of multiple identities. No, this is not a psychotherapy term. It is a growing recognition that each user on the computer network is responsible for a multitude of identities, and that the growing trend of computer-to-computer transactions adds exponentially to what you might call the "Identity Crisis" in business computing.

The blizzard of activity every day, every second, on your company’s extended computer networks is a fisherman’s stew of direct sign-on events using good old-fashioned passwords, and thousands, perhaps millions, of interconnected “events” that require some form of authentication and monitoring to ensure not only security, but also user productivity.

The right people getting the right information at the right time is a precious but elusive goal since the beginning of the IT revolution. Just as technology and IT management savvy has evolved to the point where the information and the timing is right—down to the nanosecond—new waves of anxiety are erupting over the notion of “right user.”

In today’s worm infested, virus plagued global Internet, CIOs, network managers, and security experts run the risk of locking legitimate (and time-starved) business people right out of their systems. Why? Either because of simple password amnesia or other attempts to oversecure applications with hair-trigger security measures punishing good users making simple access mistakes.

ENOUGH COMPLEXITY FOR ONE DAY?

Now realize that an authorized user who enters the computer network spawns any number of sibling identities as they interact with Web-based applications that must re-authenticate each time the user is handed off to the next application.

In his writing for Network World, industry watcher Dave Kearns described it this way: “Identity management is anything but linear.”
TAMING IDENTITY CREEP

Like they say, you can’t solve a problem unless you know you have one. Trite as it may sound, that is precisely the situation in identity management and its subsets, like authentication, provisioning, and the like. The market is just now beginning to see the problem as more than a case of conventional password management, nor is the solution new authentication hardware. Identity management is no longer simply a security problem. It is a business problem that continues to grow in complexity and hinders employee productivity and business economics.

In any technology scenario, the moment things become non-linear is the moment at which you must reorient your frame of reference and all your assumptions about what’s working and what isn’t. Antibiotic-resistant germs won’t go away like their predecessors by shoving more penicillin at them. It’s time to rethink the cure.

MAPPING THE IDENTITY GENOME

In proposing a solution to this great identity crisis, we will define identity management as “the ability to create, verify, authorize, and monitor users and resources.” Now that the definition is out of the way, how do we go about solving it?

Unfortunately, there is no one single psychotherapy session that will resolve this identity crisis. The realm of identity management is a convoluted one that spans a number of subsets—each of which demands attention in its own right. In most organizations, information on a user’s identity can be found in any number of locations—and in many directories. According to the META Group, the location of internal user data averages 22 separate points, while external user information can be found in 6. No wonder many IT professionals have looked for the biggest impact of identity management in directory consolidation. In this process, all users are placed on a single directory, and authentication policies can be more readily set for applications and other resources. This is a very extensive and expensive integration process, but at the end at least you know where all of your identities are.

Provisioning

Provisioning is the process of adding and removing users from your network and applications. For companies with hundreds of thousands of users, simply managing this first step is an exorsize in frustration. Many vendors provide automation solutions in this category, but as in directory consolidation the drawbacks are integration, cost, and resources for all but the largest companies. Most mid-sized companies today handle provisioning manually. However, they face a grave security
risk in the cycle time it takes to revoke a fired or down-sized employee’s credentials.

**Authentication**

Authentication is the most visible part of identity management. Users authenticate based on system requirements, resources, level of security required, or if they are coming onto the network from inside or outside the perimeter.

Figure 1 only shows the tip of the iceberg when it comes to the authentication nightmare a network administrator faces when providing users access to network resources. There are differing methodologies like smart cards, tokens, or biometrics. The type and frequencies of access points also are exploding with users coming into the enterprise through VPN, wireless, and other channels. Users are struggling with multiple and confusing logon protocols. And help desk costs are going through the roof.

There are two facts when it comes to identity management and authentication today:

1. There is no silver bullet for authentication.
2. Identities are growing exponentially faster than present authentication methods can handle.

**Self-Service Password Reset**

Self-service password reset is a process that allows employees to manually reset a lost password and is useful for large
companies that are wrestling with skyrocketing help desk costs. New research from the Aberdeen Group says hundreds of thousands of dollars a year are at stake for small to medium sized businesses, and upwards of $35 million a year for a large enterprise (over 100,000 users)—just for password-related help desk calls. Again, great for companies with tens of thousands of users. Not so practical for the rest of us.

Enterprise Single Sign On

Enterprise single sign on has been touted by many in the technology community as the silver bullet when it comes to identity management. Like the proverbial pendulum, SSO has swung to both extremes:

- Implanted as a centralized solution based on a monolithic model in which a centralized location stores all credentials, then as an inline proxy to distribute the credentials as different servers request them.
- Or shifted all the way to the desktop, which provided tremendous user flexibility but hindered the ability of IT to centrally manage, control or audit user access.

For large organizations with sizable IT resources, centralized SSO deployments made business sense. But for most companies, they cost too much money and dilute scant IT resources with application changes and custom integration.

All of these are for big companies with lots of resources. But the question remains—if you have less than 10,000 employees with a heterogeneous mix of applications, how do you streamline the set of identity management problems?

Current technologies that are intelligently adapted to the new, multidimensional aspect of identity management can provide practical solutions in the near term. A new generation of hybrid SSO technologies, for example, takes proven techniques for password management into the matrix-world of multiple identities with multiple login protocols without requiring the extensive infrastructure re-working associated with earlier SSO deployments.

Distributed SSO architecture seems to hit the sweet spot in the middle of the two extremes (see Figure 2). It offers the convenience and flexibility of client-side SSO but utilizes centralized administration and management to ensure full integration and security across the enterprise. In a distributed SSO solution, a central credential store, managed by an enterprise administrator, maintains all user credentials in a central location.

Inline processing for handling application credentials is performed only on the client, after authentication and successful download of credentials from the central store. Here’s how it typically works:
A user logs into a distributed server.
- Authentication takes place using one or more modalities.
- All applicable credentials are cached on the local desktop.
- The user attempts to access an application.
- The application responds with its challenge/response mechanism.
- A listener application on the desktop intercepts the application challenge and looks up the credentials for the application in a local user store.
- The listener application submits the credentials to the application by proxy.
- The application evaluates the credentials as if they had been input by the user.

The distributed SSO approach has several advantages:
- It is seamless and easy for users and does not introduce new dialogs or forms that must be understood.
- It keeps credentials centralized and secure; it supports multiple applications; and it supports centralized administration and control, including de-provisioning and logging/auditing.

How does the poor overworked, underappreciated IT administrator continue to meet all these needs by not trying to solve everything with one silver identity management bullet?
Despite what vendors say, they can’t do it—at least not within a time frame or budget anyone can afford to spend. I propose you start by not trying to map the entire identity management genome. Start by consolidating the way your users login to their applications and network resources.

One User—One Password

This is an idea whose time has come. When it comes to resolving the identity crisis in business computing today, mid-sized companies must win the battle—then worry about the war.

Omar Hussain is the SVP Marketing and Operations of Imprivata, providers of Imprivata OneSign, a SSO security appliance. He can be reached at ohussain@imprivata.com.