TechTarget Security Media
SearchSecurity.com
INFORMATION SECURITY
INFORMATION SECURITY DECISIONS

SearchWindowsSecurity.com
SearchSecurity.com
INFORMATION SECURITY

Guide to Creating a Secure Access Control Environment

Creating a Secure Access Control Environment, a guide featuring content from *Information Security* magazine, SearchSecurity.com and SearchWindowsSecurity.com, offers tips on avoiding costly password incidents and formulating new access control policies. Data can be compromised by trusted users who intentionally -- or accidentally -- harm a system through sabotage or data stealing. This guide aims to assist system admins and managers in establishing controls and policies that protect the enterprise from these threats. Included in the guide are 10 quick tips that offer expert advice on password policy considerations as well as new alternatives for passwords used company-wide to access applications. Also covered, will be advice for managers on building and implementing a new identity and access management architecture.

TechTarget
The Most Targeted IT Media

Resource Guide

Table of Contents

Section 1: Amazing Access

Section 2: 10 Tips in 10 minutes: Password Policy Considerations

Section 3: Passwords Still the Weakest Link

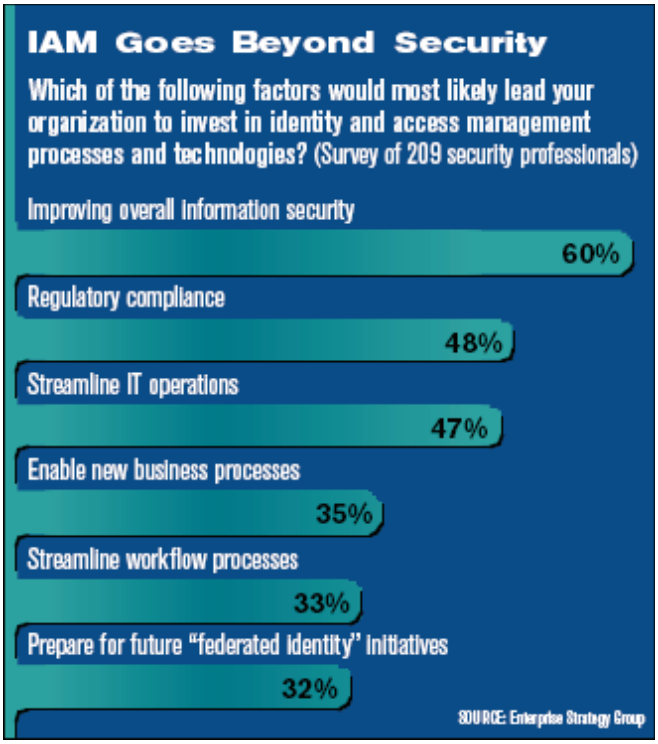
Resources From Symark

Section 1: Amazing Access

By Jon Oltsik

July 2005 | *Information Security* magazine

Finding a comprehensive identity and access management architecture requires leadership to navigate the technology and implementation labyrinth.



No need to beat around the bush—passwords stink. No one—users, administrators, security pros—likes them, and for good reason.

Despite password policies, users persist in repeating poor password choices—their dog's name, birthdays, favorite colors. Getting them to apply fixed alpha-numeric combinations at least seven characters long is a security fantasy, but shops trying to enforce strong password policies often discover that passwords aren't free. Heck, they aren't even cheap.

According to recent statistics, 25 to 30 percent of all help desk calls are password-related, the average cost per call is $25, and the average user makes roughly four of these calls per year. Then, there are the omnipresent dangers of skilled social engineers who are able to con even the savviest of users into revealing their passwords.

It's time to place authentication in its rightful place as an important component in a comprehensive identity and access management (IAM) architecture.

But, since IAM goes beyond security, it should be approached with a holistic enterprise perspective and not just focused solely on authentication.

After years of languishing on the back burner, IAM will become a major enterprise focus area in the next 24 to 36 months, driven by new business initiatives, regulatory compliance and the need for process efficiency.

Security managers must seize this opportunity and provide IAM leadership on four levels: building a planning team, mapping access requirements, designing an access control architecture and implementing the solution.

The IAM Team

When embarking on an IAM project, security managers must gather a team of application, systems, access, network and directory managers and administrators from various business units across the enterprise. Of course, each department's security should have strong representation within the IAM team.

This team's purpose is to define the IAM business requirements—not to architect a technical solution. Each participant must represent his department's needs while collaborating to address overall business requirements. The team's ultimate goal is threefold:

1. Assess current problems by developing a list of IAM financial, operational and organizational issues. The team members will define the business risks, operational overhead and organizational issues associated with each problem so the IAM solution can be aligned with overall business goals.

2. Define goals by prioritizing short- and long-term objectives based on business value. The team will address tactical operational and security issues, but think strategically about business and regulatory requirements. Will the company outsource any business processes in the next few years? Will the organization need to create roles and access policies for "extended enterprise" applications to service outsiders? Are there any pending or anticipated deadlines for regulatory compliance? A model solution should enable business flexibility, improve security and cut operational costs.

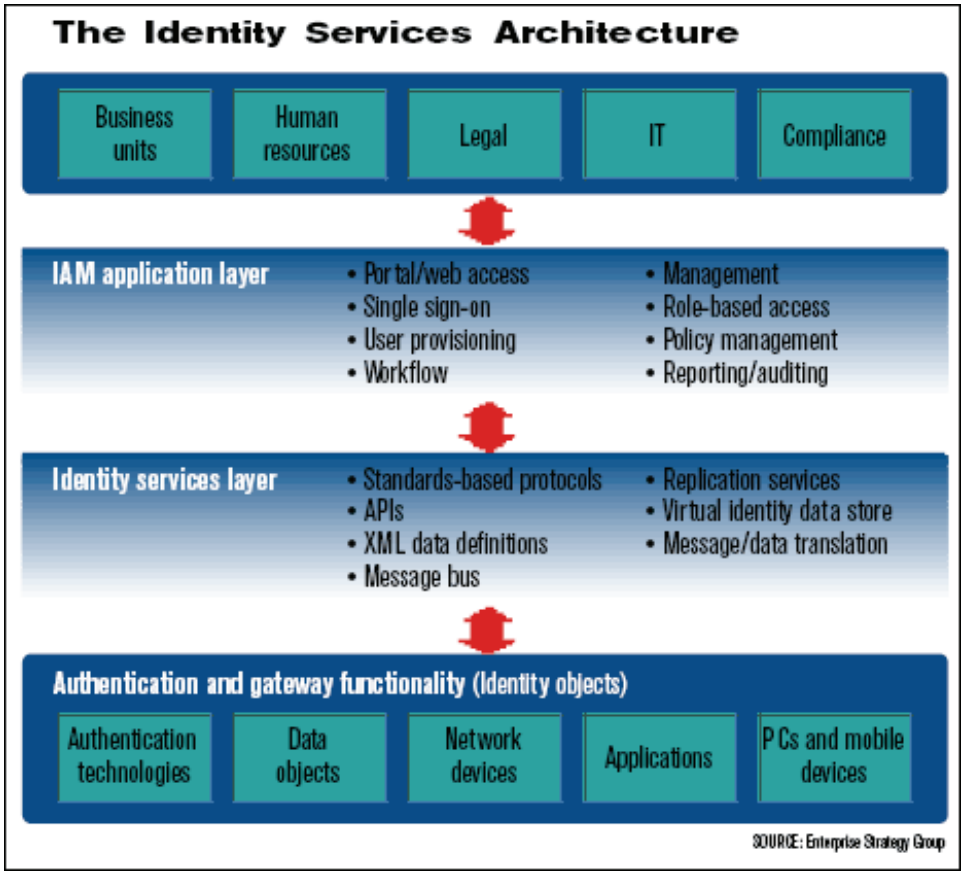
3. Pool funds from various business units. While the IT department can certainly build and manage the technology, all business groups should invest in the process. Enterprises may allocate money to IAM projects, but it's quite common for business departments to contribute from their budgets.

During this initial phase, the security group's job is to help the organization fully appreciate the business risks associated with current IAM architectures—weak passwords, poor controls and multiple identity stores. Security managers should avoid the temptation to play "Chicken Little" with constant warnings about security breaches and identity theft that don't amount to much.

Rather, security managers should balance paranoia with hard operational facts—the process of managing and monitoring multiple RADIUS servers, VPNs and network directories requires loads of financial and human resources and is strewn with costly inefficiencies—both human and technical. Quantifying security inefficiencies loses as a result of breaches and future savings—or as some call return on security investment (ROSI)—will be important and well-received input.

Plotting Access

Access control isn't just about keeping bad guys out—it's about controlling who gets into the infrastructure and limiting where they can go. Mapping access needs is a crucial phase of an IAM project, since this is when security managers need to determine which users and devices will have access to specific applications and data and from which locations (intranet, mobile computers, kiosks).



During this phase, the IAM development team needs to catalog all systems and applications; each system should be rated in terms of how critical it is to the business and assigned a value.

It's important to note the process for user provisioning, management and monitoring, and, in terms of the technical information, to note whether each system has open or proprietary application interfaces and IAM infrastructure, the type of operating system, and whether the application is in a steady-state of operation or due for a near- term upgrade.

Enterprises also need to assign a level of sensitivity to data as it is being created, amended, enhanced, stored and transmitted. Data classification can be an arduous and time-consuming task, and many companies simply ignore it. At the very least, security managers should classify obvious confidential and regulated data, and assign it a level of minimum protection.

Many enterprises make the mistake of using existing access rules and accounts as baselines for new systems.

Security mangers should use the opportunity of a new IAM infrastructure to recast all access rights. Rather than focusing on the "who," best practices dictate that companies should focus on "what" (what asset?) and "why" (does this person need access to this system/data?). Building role-based access provisioning in this way will help bolster security and ease the compliance auditing both during and after the process.

With an inventory of assets, data and access roles, security managers can define rules for authentication and authorization by selecting a security model that helps meet enterprise objectives without impeding business operations. In terms of authorization, security managers can now help map existing roles and groups to the assets they truly need and secure critical systems enterprise-wide with "need to know" security.

Enterprises also need to create standard processes for account creation, change management and deletion by documenting the current workflow, approval and provisioning process, looking for inefficiencies and opportunities for automation. Once designed, the model process can be complemented with auditing, automation and provisioning tools from vendors like BMC Software, Computer Associates, Courion, Consul, IBM Tivoli, Novell and RSA Security. Given the complexities of this phase, companies often cut corners—and run into security and compliance problems down the line. CISOs must step in to make sure that this doesn't happen; successful access mapping will lead to perpetual security and operations benefits.

Striving for Scalability

Identity and access management spans the entire enterprise; in building an IAM solution, enterprises must define an appropriate architecture that allows them to start small, grow gracefully and, most important, avoid all-encompassing solutions that demand million-dollar investments and multiyear implementations.

To maximize benefits while avoiding technical lock-in, IAM services should feature a layered architecture based upon standard protocols (i.e., RADIUS, LDAP, X.509), data formats and APIs. There are three basic layers in the IAM services architecture:

1. Identity Objects (i.e. user, device, file, application, etc.) sit at the bottom of the stack. They define anything with an identity that needs to be mapped to access policies and monitored for compliance. Identity objects vary based on company size, global locations and government regulations.

2. Identity Services provide middleware like messaging, directory, replication and data services that link identity objects to IAM applications. Identity objects will take direct advantage of the identity services, while legacy objects with their own IAM infrastructure will rely on specific gateway and data translation (i.e., metadirectory, XML translation, etc.) functionality.

3. Application Layer provides business, security and operations functionality through the identity services layer. Identity and access management applications will plug into the identity services layer through a handful of standard interfaces from leading software vendors and IAM infrastructure providers (i.e., Java, ASP/.NET, C++, etc.). As other standards evolve (such as authentication protocols like RSA Security's OTPS or VeriSign's OATH), enterprises will be able to integrate best-of-breed IAM technologies into existing architectures.

Security managers may be in unfamiliar territory during this phase as they tend to think in terms of "best-of-breed" products rather than architectural solutions. They need to focus on protecting corporate operations, long-term scalability and business needs by designing an identity management architecture, and then filling in tactical needs with standards-based tools that have an eye toward future integration.

The Final Frontier

This phase includes setting up a test bed, building a prototype, rolling out an early adoption phase and then pushing the project into production.

Though this sounds fairly straightforward, security managers must continue to oversee the deployment to ensure that design and operational goals are met.

An IAM project has no shortage of moving parts, so it's easy to get lost or have some minor problem cascade into a major showstopper. Security managers must keep meticulous records on the implementation process to troubleshoot the inevitable kinks and avoid any future problems.

To ensure progress, security managers must also make training an ongoing process. Users must be taught the mechanics of the IAM, so they will understand the protections, processes and limitations on their access rights. And, business managers must be educated on the need for maintaining IAM integrity. Shortcuts and ad hoc processes and mechanisms will undermine the IAM efficiency and, ultimately, overall security.

Unanticipated security vulnerabilities or process problems will crop up—and security managers must stay on top of them. With a project of this significance, it's better to delay deployment than to roll out systems that frustrate users and don't work.

Overall, patience is a virtue. This project will require time, money and loads of cooperation. Security managers should approach IAM as politicians—not police officers.

Identity is truly an area where security and business initiatives go hand-in-hand, so savvy security managers can use this critical project as a way to improve security, formalize controls, reduce operating overhead and support business initiatives.

About the Author

Jon Oltsik is a senior analyst and storage industry veteran at the Enterprise Strategy Group, focused on information security. Send your thoughts on this article to feedback@infosecuritymag.com.

Section 2: 10 Tips in 10 Minutes: Password Policy Considerations

By SearchWindowsSecurity.com

17 Jan 2005 | SearchWindowsSecurity.com

Tip #1: Know What Makes Up a Strong Password Policy
A strong password policy can go a long way. A strong password policy will:

- Insist on frequent password changes
- Require long passwords composed of random combinations of upper and lowercase letters, numbers and special characters
- Not allow blank passwords
- Check to ensure passwords are not repeated
- Prevent the use of any part of the user's name or user ID
- Not allow the use of common dictionary words

- Excerpted from Roberta Bragg's Hardening Windows systems' book excerpt Strengthen the password policy

Tip #2: Create Logical Policies
Changing the password policy for an organization may be a rather large undertaking. If users can now use blank passwords or short ones, and if they do not have to meet complexity rules, making them comply with more restrictive rules may prove to be beyond your authority. This is something that you should evaluate, and it is really of the utmost importance. No single change can have as much impact on the security of your networks.

You can, however, immediately improve the security of your networks by creating a logical password policy for a select group of individuals: those who have elevated privileges in the enterprise, in the domain, or on some systems. A prime target for such a policy are system and network administrators. IT admins and their management should be receptive to changes that will improve information security.

Perhaps you can spearhead change by making the adoption of a strong password policy the result of working together to improve security. Working out ways to strengthen the policy without making it overly difficult to adhere to will make it easier to obtain and implement a stronger organization-wide password policy.

- Excerpted from Roberta Bragg's Hardening Windows systems' book excerpt Strengthen the password policy

Tip #3: Change Policy for Local Accounts
Local accounts on servers and workstations cannot be entirely eliminated. Windows computers that are domain members retain their local account databases. Any accounts in these databases cannot be managed by the domain password policy. A password policy for these accounts should also be in place. This policy can be a very strong policy. In many organizations, local accounts are not used, with the exception of some administrative accounts on some servers. If accounts are not used, then password policies can be very restrictive; if accounts are used, then password policies should be very restrictive, and it should not be difficult to obtain approval, since many of these computers are controlled by IT.

Local password policies for NT 4.0 computers, and for those Windows computers joined in a Windows NT 4.0 domain, must be configured on the local system, or via custom scripts. Local password policies for computers joined in a Windows 2000 or Windows Server 2003 domain can be set and managed via Group Policy. Remember, password policies set at the OU level affect only the local user accounts of the computers in the OU. To use Group Policy to manage the password policy of local user accounts:

- Place the accounts of servers for which the same password policy is required, in the same OU.
- Create a GPO and link it to the OU.
- Open the GPO for editing and modify the password policy.
- Close the policy.

- Excerpted from Roberta Bragg's Hardening Windows systems' book excerpt Strengthen the password policy

Tip #4: Change Policy for Individual Accounts

In addition to domain password policy and local password policy, changes can be made at the account level. That is, you can impact the password policy of an individual account. In many cases, changing policy at the account level is a way to prevent the weakening of password policy for the domain. Options may also strengthen policy.

For example, in some cases, it may be required to store a password using reversible encryption. This is not recommended; however, it is still better to do so for a couple of accounts, using the Store Password Using Reversible Encryption option, than it is for all accounts in the domain. Another questionable option is Password Never Expires.

Expiring passwords is a way to make sure users change their passwords. Blocking this action weakens that technical control. However, if accounts are used by services, then passwords must be manually changed—the service program will not recognize or respond to reminders to change passwords and will simply be locked out when the password expires. Using the account level option allows the domain-level password policy to require periodic password changes. Incredibly, I still find domains where no user accounts are required to change passwords, because service accounts cannot.

While both of these options can weaken individual account protection, setting account level policy can strengthen protection for an individual account. For example, the option Smart Card Is Required for Interactive Logon can be set for an individual account. Long before smart cards can be installed as the primary authentication mechanism for an organization, it may be possible to require their use by administrators, or by other privileged users.

Finally, other options are temporary controls that can do much to prevent unauthorized account usage, the goal of a password policy in the first place. These options include:

- User Must Change Password at Next Logon
- Account Is Disabled
- Account Is Sensitive and Cannot Be Delegated

- Excerpted from Roberta Bragg's Hardening Windows systems' book excerpt Strengthen the password policy

Tip #5: Know How to Expire Passwords
Because there can only be one password policy for a domain, whatever you set for the password expiration will be in effect for all users, with the exception that you can set an account to not expire at all. There are two possible solutions to this problem:

1. Create a separate domain for the high-risk areas, which would have other advantages as well, as they could manage other differences (length of password, history, account lockout, etc.).

2. While there is only one enforceable password expiration policy per domain, there is no reason not to procedurally insist on group passwords being changed on whatever schedule. Scripts could also be written to check on this and possible e-mail users who failed to follow the policy, or make some other changes that would be effective in enforcing the policy. Of course, writing custom software could also be used to enforce more frequent password changing.

- Excerpted from Roberta Bragg's Can we have more than one password policy?

Tip #6: Determine Who Should Have Stronger Passwords
Just because the generic password policy for all users is set at one level and partially enforced by technical controls, you should still have another, stronger password policy for administrators and others with sensitive accounts. While only one password policy per domain can be technically enforced, you can require some users to have stronger passwords. You'll have to give them further training, requiring longer passwords and other techniques. You may have to audit them by using a cracking/audit tool, but it will be worth it.

- Excerpted from Roberta Bragg's Hardening user passwords

Tip #7: Manage Multiple Unique Passwords
The reason for using a unique password for every account is to limit the risk. If someone obtains a password or cracks an account, you want to limit them from getting access to more data. For example, if you have two accounts, one with administrative privileges, and one without, I hope you have a different password for each of them. It is always a good rule to have different account passwords. Certainly, however, you must weigh this risk against the risk posed by writing down or otherwise storing passwords.

Writing down passwords or storing them electronically is not in itself bad—it's where and how you store the recording. Having a PDA file of your passwords and no encryption on the PDA and no password on the PDA is not very secure. Locking the list up somewhere or having an encrypted file on a device that is not accessible from the network might be reasonably secure. You are going to have to weigh the risk of each possible solution to the problem. And one other caveat… if the 16 passwords at work exist because 16 different resources must be accessed, it may be that having the same password for some of the accounts may not be as large a risk. After all, a good single-sign-on implementation might provide you a single account that allows you to access all resources. Remember, no security rule is absolute. There are super "best practices" that must be tempered by the organizations and situations "best security."

- Excerpted from Roberta Bragg's How to manage multiple unique passwords

Tip #8: Enable Complex Passwords
When complex passwords are enabled, existing accounts that do not meet the requirements are unaffected until the password is changed. It's recommended that you require a password change the next time they log on. However, in a larger environment, you may want to stagger this requirement, and in any organization, make sure this does not catch users by surprise. Provide ample warning, training and above all, solicit support from all management. Nothing is worse than implementing new security without support.

- Excerpted from Roberta Bragg's Enabling complex passwords

Tip #9: Know When to Disable Default Password Filter
Normally when a custom password filter is installed, it replaces the Windows password filter or even the entire logon process. When a log on is attempted, Windows looks at all valid password filters, so preventing the use of its own is important if you want to rely on yours entirely. You may have already written your own, though you can find an example script. Microsoft also reveals its own passfilt.dll and instructions on how to write and use your own filter.

Now, to prevent Windows from using passfilt.dll simply requires setting the password policy to NOT require complexity. This setting is at "Windows Settings/Security Settings/Password Policy/Password must meet complexity requirements." Simply change it to disabled if it is enabled. If your password filter is also checking for password size, history and other Windows password settings, you can set them to null here as well. I wouldn't, however, change the "Store passwords using reversible encryption" setting. It's disabled by default for a reason. It allows storing passwords in an easily recoverable form. This is required by some classic non-Windows clients, and that's why its available. It is generally used as a user account variable and not as a system wide variable and only if necessary.

- Excerpted from Roberta Bragg's Disabling the default Windows password filter

Tip #10: Enforce Password Policy
If your password policy does not exceed the technical controls Windows offers, setting those controls for enforcement will suffice. However, no password policy should be without requirements, including failure to post passwords on monitors, not sharing passwords and so on. In addition, there are technical controls you may want that cannot be done in the Windows password policy, such as requiring number placement in the middle of passwords.

Use the following strategies to enforce password policies:

- First, purchase and use a password auditing tool. These tools can be used to provide information on how long it may take to crack a password—even weak passwords. While you may not be able to tell if numbers are placed in the middle of a password, you can tell if a password is easily cracked and not in policy.
- Second, do periodic site searches looking for passwords that are written down.
- Third, include a punishment for non-compliance in your security policy. If there is a violation, there should be consequences.

- Excerpted from Roberta Bragg's Hardening user passwords

Section 3: Passwords Still the Weakest Link

By Niall McKay, Contributor

26 Jan 2006 | SearchSecurity.com

Last November, a man named Pok Soeng Kwong, was convicted with sabotaging the computer network of his former employer, America Flood Research Inc. in Plano, Tx., and causing $600,000 in damages. Two months earlier, Carl Shea, a former program manager of a Silicon Valley debt collection company called Bay Area Credit Services Inc., was convicted of deleting 50,000 customer records, causing $100,000 in damages. And before than, in June, Roman Meydbray, the former IT manager of Morgan Hill, Calif.-based Creative Explosions, Inc., pleaded guilt of unlawful access and damage to the company's computer systems.

Former or disgruntled staff commit up to 70% of security breaches, according to Washington-based Diligence LLC, a risk-management company. Often these insiders exploit lax password management policies that provide systems administrators, computer programmers (often offshore contract workers) and others access to service account and administrative passwords, even long after they leave the company. Not only are these common passwords often shared, but also they are infrequently changed.

Unauthorized access and theft of propriety information increased by 30% in 2005, according to the most recent CSI/FBI Computer Crime and Security Survey. The two organizations peg the average loss at about $300,000 per incident.

Application-to-application or service-account passwords—typically used by systems administrators—can be tricky to manage. Since they're used to enable applications to communicate, they're hard-coded or written into middleware. This makes them difficult to change, especially when they are often widely known within an organization.

"In the past six months, managing administrative and privileged passwords has become in item on many corporations' agenda," said Jonathan Penn, principal analyst with Cambridge, Mass.-based Forrester Research. "I believe that this is being driven by the auditors who are now going after the shared-level passwords to make sure that the corporations are meeting Sarbanes-Oxley [internal control reporting] security requirements."

Information security firms such as Cyber-Ark Software Inc. in Dedham, Mass. and Symark Software in Agoura Hills, Calif. have upgraded their password-management tools to support service-account passwords.

The software gives each staff member an account on the password management system. The staff member logs into the system, which authenticates the user before allowing access to an application. In this way, users never know the shared password to access the application, and can neither share it nor use it after leaving the company. Security and network administrators easily add or delete users and set individual or role-based access privileges, while also quickly changing database and other application passwords through these types of "password enhancement" products.

Cyber-Ark's Password Vault and Symark's PowerKeeper software use 256-bit Advanced Encryption Standard to secure the information on the box and to secure traffic to and from client machines. Each user has a virtual vault where their passwords are kept so that router administrators, for example, only have access to the router password section.

"In a large corporate environment, administrative passwords are cumbersome to manage," said David Ross, Unix team leader with the Calgary, Alberta-based Husky Energy Inc., which uses Symark's PowerKeeper. "So the auditors like to see that the company has this under control."

Even more importantly, he adds, is the ability to provide an audit trail so that, if necessary, auditors can clearly see who has been accessing which applications.

Large corporate accounting scandals like WorldCom and Enron have heightened the importance of maintaining a complete audit trail for any large transactions. And even those companies that don't fall under SOX compliance, like Husky Energy, are trying to abide by the law due to U.S. business partnerships and to remain competitive.

In the meantime, it appears smaller public companies trying to meet their SOX deadline are among the interested.

"We have seen a big increase in demand for our password products," said Ellen Libenson, Symark's vice president of product marketing, "because smaller companies with a market capitalization of 75 million shares outstanding will need to comply with the Sarbanes-Oxley section 404 by July 2006."

And the clock is ticking.

Resources From Symark

Symark Protects Your Vital Digital Assets from the Inside Out.
Symark PowerBroker enables administrative delegation of the UNIX/Linux "root" or "superuser" password on a granular level and centrally manages access to "privileged" accounts! PowerBroker strikes the perfect balance between protection and productivity by giving system administrators, security officers, and auditors the tools to uniformly manage and record access to servers and the applications running on them. Create and enforce security policies that meet regulatory compliance. Take PowerBroker for a test drive by downloading an evaluation copy today!

Read the SANS Institute White Paper: PowerBroker vs. *sudo*
This paper, written by the SANS Organization, compares and contrasts the differences in features and functionality between Symark PowerBroker and the open source access control product sudo. "If there is a need for a system that will provide an audit trail and solidly enforce security policy such as is required by HIPAA, SOX, etc. to prove regulatory compliance, PowerBroker has the built-in tools to handle that task." –SANS

Bringing Heterogeneous UNIX/Linux Networks into Compliance with the Sarbanes-Oxley Act
This document discusses how an organization can use identity and access management solutions for UNIX and Linux operating systems to meet SOX section 404 requirements for effectiveness of internal controls for financial reporting requirements.

Administrative Passwords Are The "Keys to the Kingdom"
Administrative passwords are the Keys to the Kingdom. Symark PowerKeeper® is a secure appliance for generating, managing, and storing administrative passwords. It offers a secure release mechanism for passwords, and can automatically change the password on a managed system based on the parameters you control. Not only does it ensure that a strong password is utilized, it closes the existing issue of someone knowing the password prior to it being put under control. A great compliment to PowerBroker as it provides secure storage of the "root" or "superuser" password.

Managing Roles Is Safer Than Managing Users
Symark PowerPassword UME identity management solution provides more than user provisioning. PowerPasswords' advanced Login Policies enable you to control not only who logs in but what groups or defined roles may login to what. PowerPassword enables highly granular password and policy configuration and logging to fully protect servers containing sensitive data dramatically improving compliance.

About Symark

Symark helps enterprises protect their vital digital assets from the inside out and secures them from damage or theft by trusted users. Our products strike the perfect balance between protection and productivity by giving system administrators, security officers, and auditors the tools to uniformly manage authentication and authorization across the network while administering access to machines, applications, and files, and effectively enforcing security policies to meet regulatory compliance. Our PowerBroker® and PowerPassword® products address the inherent security gaps in native UNIX/Linux operating systems and provide a superior alternative to freeware and homegrown programs. Our PowerKeeper® network appliance securely automates administrative password generation, encryption, and storage across multiple platforms such as Windows, UNIX, Linux, and AS/400. Our commitment to quality products and superior technical support has made us the leading vendor of UNIX and Linux security management software worldwide.

Please contact us at:

Symark Software
30401 Agoura Road
Agoura Hills, CA 91601
800-234-9072 toll free
818-575-4000 direct
Email: info@symark.com
Website: www.symark.com

Symark Software UK
Suite 345 Warren Street
London W1T 6AF
England
Telephone: 0870-458-6224
Fax: 0870-458-6225
Email: emeainfo@symark.com

Symark Software Japan
Broad Corporation
6F, 2-27-20, Bunkyo-ku,
Hongo, Tokyo 113-0033 Japan
Email: info@broad-corp.co.jp
Website: http://www.broad-corp.co.jp/

Symark Software Mexico
IMAXSERV
Sales Contact: Wilfredo Barraza
Email: wilfredobarraza@webtelmex.net.mx
Telephone: 011 5255 5525-4660

Symark Software Korea
I'VE TECH Co., Ltd
7F Dongsung Bldg, 17-8 Youido
Seoul Korea
Telephone: 82-2-780-9700
Fax: 82-2-785-1122