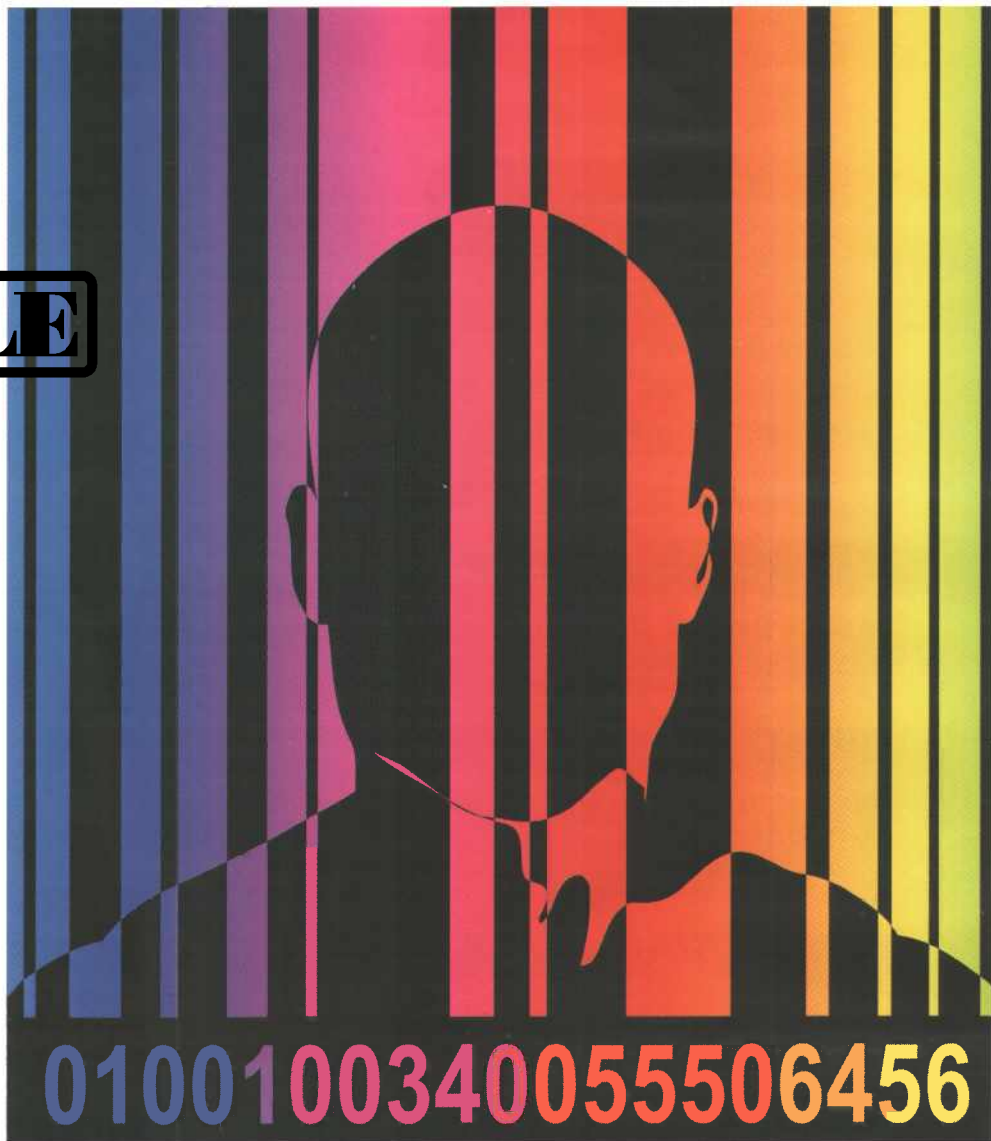


SAMPLE

GROWING PAINS



Government agencies struggle with identity, access management

By Jim Ebzery

In government IT systems, identity and data can last a lifetime. This is unlike the corporate world where both often expire—for example, when an employee leaves or a project is completed. Government organizations store sensitive information about citizens, projects, security threats and historical events—sometimes forever—and this information is generated at an enormous rate. Concurrently, the complexities of accessing data also have increased. In today’s on-demand information age, more government employees are accessing sensitive files, and an increasing number of citizens are using government computer systems and Web sites to view public information or access services.

Infinite storage of confidential information and rising numbers of people requiring access to that information lend themselves to the possibility of critical data breaches. Complex IT environments, where national security information and critical citizen data are stored, need to be protected in an efficient, cost-effective way, and access rights should be granted

only to people who require that data.

A FAILING GRADE

In 2007, officials from the Commerce and State departments met with the Homeland Security Committee to explain three separate security breaches that compromised sensitive government data. These incidents ranged from opened virus-infected e-mail attachments to hackers using international networks and malicious software to gain access to government networks. These were not isolated incidents, according to the Department of Homeland Security’s National Cyber Security Division. In 2006, NCSA received roughly 24,000 reports of government security breaches that included hackers probing networks for vulnerabilities and cases of unauthorized access to government information.

These occurrences led many government agencies to receive poor or failing grades for their security practices in 2006, based on the Federal Information Security Management Act. The agencies were then graded based on assessments

and information submitted annually to the White House Office of Management and Budget. The report cards for all agencies were released in 2007, and the government earned an overall C- for its security. DHS earned a D.

FISMA is not the only federal law demanding better government security. HSPD-12 establishes a government-wide standard for identification credentials—or smart cards—that deliver a common, two-factor authentication method for accessing physical and logical assets. Many agencies are scrambling to meet the law’s requirements by the October deadline.

Mandates, fear of security breaches, public mistrust and fines are all factors driving most government agencies to reevaluate ways in which sensitive information is protected. Older, “check box” technology has given way to complex, integrated infrastructures to better protect computer systems.

With all this new technology, why are government agencies still failing to meet data security guidelines? Using next-generation technology to protect infor-

mation is just the first step in the long data security journey. There are certain best practices government agencies should implement to provide the most comprehensive protection against insider and targeted attacks. Identity and access management tools provide an integrated approach for ensuring the right people have access to the right information without interrupting productivity.

BEST PRACTICES

To successfully implement an identity and access management project, agencies should outline definitive goals and ensure the right solutions are in place for policy enforcement, automated user provisioning, federated identity, endpoint security and password management.

Policy enforcement grants users secure access to appropriate resources according to their relationship and roles. Policies are often enforced through an automated user provisioning solution, which also eliminates tedious, labor-intensive manual procedures that can cause security lapses from personnel changes. User provision-

SAMPLE



ATTENTION: CAMERA SURVEILLANCE DEALERS

Be the **King** of Your
Own Business
and **Rule** Your Market!

Join the **only** CCTV
Dealer Program
in the industry that is
100% Dealer Driven!

**CALL 1-800-521-3993
TODAY!**

Home of the Free Camera
Surveillance Program

- FREE LEAD PROGRAM
- Earn \$8,000 on a \$6.00 a day sale
- Market Your Own Name
- Get More Leads from our Lead program
- Grow YOUR Business
- Give FREE DVR, Monitor and Cameras for Warranty Service
- Daily FUNDING

www.alarmking.com

Circle 45 on card.

power + UTP video/data transmission



HubWay[®]8S Passive UTP Transceiver Hub with Integral Camera Power

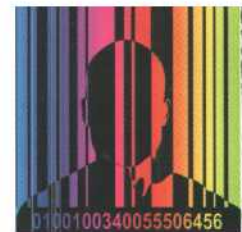
- Transmits UTP video, RS422/RS485 data and power over a single CAT-5 (or higher) structured cable
- 8 channels of quality video up to 750 ft.
- Power LED indicators
- Individually selectable 24VAC or 28VAC power outputs
- Compatible with 24VAC and/or 12VDC fixed or PTZ cameras
- 115VAC or 230VAC input
- Space saving 1U EIA 19" rack mount chassis
- Lifetime Warranty – Made in the USA



1.888.258.7669 • www.altronix.com

More than just power.™

IT SECURITY



ing tools update access rights automatically when roles change or an employee leaves, giving government agencies the capability to revoke access in real time. With role-based provisioning, systems are never vulnerable, and companies can maintain visibility into use of information and resources.

An identity and access management infrastructure with federated identity helps agencies securely access resources across their shared networks. By leveraging multiple identity standards, including Liberty Alliance, WS-Security and SAML, federated identity verifies access from a variety of applications, thus minimizing or eliminating interoperability issues among agencies. Agencies also need to connect to their IT infrastructure through mobile devices or endpoints, including laptops and PDAs. Endpoint security management provides integrated security for USB, wireless, data and application control, and supports policy-based management.

There is a correlation between the number of passwords a user must remember and the likelihood that one will be stolen. Single sign-on is the foundation for efficient password management and a requirement of FISMA and other mandates. Single sign-on means employees, partners and the general public only have to remember one password or login routine to access all the applications they are authorized to use. This reduces the likelihood of users resorting to vulnerable written reminders—such as a yellow sticky note that could end up in the wrong hands.

OTHER CONSIDERATIONS

Implement identity and access management projects in stages rather than all at once, and evaluate the technologies needed for a particular organization. Keep in mind that not all technologies initially may be required, but most ultimately are used. Avoid solutions that disrupt existing systems during deployment, align early-stage deliverables to primary needs to highlight quick-win return on investment and build internal support for the project. Finally, focus on the total project cost over time and not just the cost of software or support.

Due to the information they house, government computer security systems are particularly vulnerable to cyber criminals, malicious insiders and amateur hackers looking for fame. Given the sensitive data and the increase in sophisticated attacks, agencies should use the best technology available to protect information. Identity and access management provide the features and capabilities necessary, but only if agencies implement solutions that provide the level of security needed, such as federated identity, automated user provisioning and single sign-on. Without leveraging the best of these tools, government agencies will continue to receive failing grades for IT security.



Jim Ebzery is the senior vice president of identity and security management at Novell.