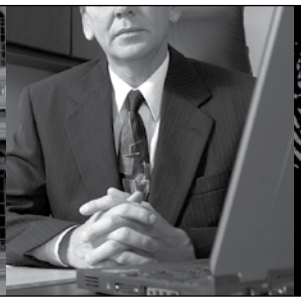
A STRATEGY PAPER FROM CENTER FOR DIGITAL GOVERNMENT

I AM WHO I SAY I AM:

The Role of Identity and Access Management in Government

Introduction: Ripped from the Headlines

Whether managing risk or avoiding threats, the impact is the same — public sector organizations are spending a significant portion of their information technology (IT) budgets on information security, as high as 10 percent in some cases. The reason is clear — recent headlines tell the story:

- Privacy breach puts U.S. total over 100 million[1]
- Another Government Security Breach[2]
- Security Breaches Afflict Most Enterprises, Government[3]
- Voters' Information Exposed [to hackers] on Website[4]

The issue of information security is so pervasive that one Web site even publishes a "Security Breach Weekend Roundup"[5] without a hint of irony. That said, the cost of preventing a security breach pales in comparison to the cost of addressing such a breach after the fact. A recent study of 14 organizations that experienced an IT security breach revealed $69.8 million in direct costs associated with the breaches.[6]

Investing in preventative measures and addressing security breaches are necessary but not sufficient in developing and maintaining a sound and sustainable information security program. The cost of not being prepared or inappropriately responding to an incident goes well beyond dollars and cents. Incidents such as the theft of a laptop containing sensitive information or hackers gaining illegal access to personal information belonging to hundreds of thousands of people further diminish the public's trust of government, and obtaining data necessary to conduct government's business becomes even more difficult.

One potential response to security threats is to institute the use of IAM — identity and access management. As its name suggests, IAM is the convergence of two previously discrete fields into an important new discipline, defined by one industry source this way: "Identity and access management refers to the processes, technologies and policies for managing digital identities and controlling how identities can be used to access resources."[7]

Government's dual nature as both a provider of key identifiers to which others refer, such as driver's licenses and Social Security numbers, and holder of vital public records, makes information security a critical issue for public sector organizations. This white paper discusses the drivers, responses and challenges associated with information security. It also outlines solutions and suggestions for implementing a comprehensive information security program, focusing on the challenges and benefits associated with IAM.

Drivers and Responses: Assessing and Managing Risk

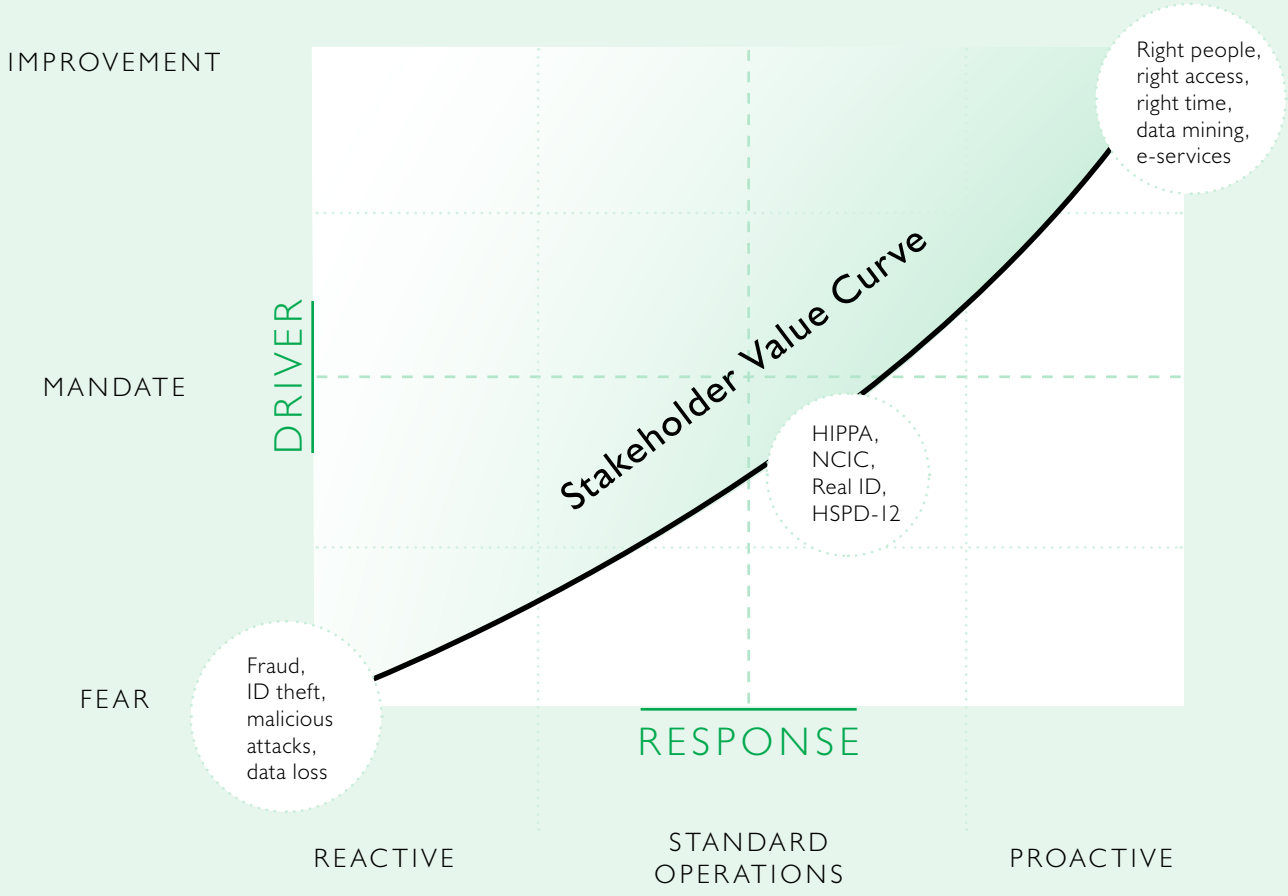
Managers need to sort through which risks are most likely to materialize and which could cause the most damage to the business, then spend their money where it will be most useful.

*– **Robert D. Austin** and **Christopher A.R. Darby**[8]*

While much of the focus is on prevention of, or response to threats, leading public sector organizations understand that they must identify and address risks and the associated impact likely to occur in their environment. Additionally, public sector leaders understand that total protection is difficult, if not impossible, to achieve. "The key mistake people make is that they think about it [information security] wrong. They think, 'How do I avoid the threat?' when they should be thinking, 'How do I manage the risk?'," says Bruce Schneier, founder and chief technical officer of an Internet security company and author of *Secrets & Lies: Digital Security in a Networked World* (John Wiley & Sons, 2000).[9]

Since organizations, public or private, simply cannot afford to address every threat that exists, they must identify the risks most likely to impact their organization. Agencies must then determine the impact of those risks, and identify security mandates to which they must comply. Once relevant issues and mandates are identified, standard risk management practices, as well as project prioritization and resource allocation, can be used to address the most pressing issues.

FIGURE 1



DEFINITIONS RELEVANT TO FIGURE 1:

HIPAA – the Health Insurance Portability and Accountability Act (HIPAA). According to the Centers for Medicare and Medicaid Services' (CMS) Web site, the Administrative Simplification (AS) provisions of HIPAA require the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The standards encourage the widespread use of electronic data interchange in the U.S. health care system.

NCIC – The Federal Bureau of Investigation describes the National Crime Information Center (NCIC) as a "computerized index of criminal justice information such as criminal record history information, fugitives, stolen properties and missing persons. It is available to federal, state, and local law enforcement and other criminal justice agencies and is operational 24 hours a day, 365 days a year."

Real ID – The Real ID Act will create national standards for state-issued driver's licenses identification cards, and must be implemented nationwide by May 2008. According to the act, the electronically-readable ID cards must include, at a minimum: name, birth date, sex, ID number, a digital photograph, address, and a "common machine-readable technology" that the Department of Homeland Security will decide on. The card must also include "physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes."

HSPD-12 – Homeland Security Presidential Directive 12 (HSPD-12) requires all federal employees and contractors to be given a common identification card that can be used anywhere and everywhere, with single sign-on to computer systems, as part of three-factor authentication involving biometrics. See http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.

Data mining – Wikipedia describes data mining as "the process of automatically searching large volumes of data for patterns using tools such as classification, association rule mining and clustering."

e-services – are fully executable online services that have in some cases replaced paper-based systems. They are often databased and searchable and/or provide online citizen interaction.

malicious attacks – intentional or unintentional attacks against information systems. These attacks can take a wide variety of forms including illegal access, spread of malicious code and denial of service attacks. With the ubiquity of the Internet, it is possible to launch an attack from anywhere in the world, to anywhere in the world, at any time, and new, unexpected forms of attacks crop up regularly.

While counterintuitive on first blush, organizations can turn information security from just a new necessary cost of doing business into an opportunity to further improve the overall IT environment.

Fear may be a great motivator — as is its bureaucratic equivalent of risk aversion — but they are by no means the only business, functional and policy drivers that cause public agencies to seek ways to better manage information security. While fear strongly influences behavior, the reasons for implementing an information security program vary from reactive (for example, preventing fraud and malicious attacks) to proactive (making access to information and services more convenient, for instance). When asked in interviews with the Center for Digital Government, state and local government IT leaders most often identified three drivers of their information security efforts:

1. Facilitation of business processes and e-services including promoting internal collaboration;
2. Compliance with federal, state, and local mandates; and
3. Risk management, such as security and access control.

Additionally, state and local IT leaders identified financial transactions and protecting personal identification information as their highest priorities for their information security programs. Protecting medical, legal and law enforcement information also ranked high on their list of priorities.[10]

Figure 1 illustrates the value of the nature of responses to security incidents as seen against the drivers that helped shape the response. Stakeholder value — as realized by government, elected officials, partners and citizens — rises as the response moves away from reactive toward proactive, and the focus of the drivers moves beyond fear and simple compliance with mandates toward improving operations and access.

In Figure 1, the greatest stakeholder value is realized in the top right quadrant where proactive measures have been taken — including an operational policy framework — that result in the greatest level of improvement in protecting personally identifiable information.

Challenges: The Changing Landscape

Public sector organizations face several challenges as they strive to implement a comprehensive information security program. Those challenges include overcoming the standard fragmented approach to implementing information security, clearly defining responsibilities and assigning accountability, funding a solution, and balancing the needs of protection and access.

Fragmentation

Unlike private sector organizations, government does not have a single unifying purpose. By its very nature, government is fragmented due to its diverse range of lines of business — often spanning the alphabet from "A" (animal services) to "Z" (zoning). This diversity of purpose leads to competition among departments, which in turn can fragment an organization's funding, oversight and implementation of an information security program.

Owing to their heterogeneous and vastly federated structure, it is not surprising that public sector organizations take a variety of approaches to implementing and managing information security initiatives, with a fairly even distribution among three approaches: (a) decentralized or federated, where public agencies operate autonomously; (b) shared responsibility, where agencies are coordinated in a mutual aid and alerting environment; (c) centralized enterprise, where security services are provided and enforced by a central entity. Yet when asked about their preferred or ideal approach to information security for the Center's study, nearly every public sector leader selected the centralized enterprise approach.

Accountability

Another challenge facing government is often the lack of a position responsible for oversight and management of the information security program. Fortunately, public sector organizations are beginning to acknowledge the importance of information security by establishing the position of chief information security officer (CISO). According to a recent survey, many states have a CISO in place and the remainder will have one within the next few years.[11] A CISO is most valuable to an organization when his/her efforts are aligned with those of the organization's risk manager. Working together they can create a cohesive approach that addresses all aspects of information security.

Funding

Public agencies are also wrestling with information security as an unfunded mandate. Indeed, when interviewed, public sector IT leaders stated that compliance with mandates was a top driver of identity and access management (IAM) efforts. Many of these mandates come with costly requirements but no source of funding. Additionally, investments in information security do not often pay for themselves in the short term, making them difficult to sell to policymakers. Finally, when organizations operating in a fragmented manner attempt to take an enterprise approach to implementing an information security program, they often experience difficulty collecting money from all departments and agencies to fund a joint approach.

Balance

Open is open, for better or worse. Closed systems are inherently more secure than open ones. The last decade has been characterized by using the inherently open Internet to exchange data among what were once-closed proprietary networks and systems to large new universes of users. That tension between security and facilitating e-services and internal process improvements is also on the minds of public sector IT leaders in thinking about IAM drivers. Balancing protection and restriction requires thoughtful policies and processes, as well as the proper application of technology. Additionally, communities have varying levels of acceptance of the amount and type of information that they want made easily accessible. Internal issues also arise from IAM implementations that cause employees to change the way they have always conducted business, or access to information becomes more difficult.

DEFINITIONS

Identity Management is an integrated system of business processes, policies and technologies that enable organizations to facilitate and control their users' access to critical online applications and resources — while protecting confidential personal and business information from unauthorized users.[12] This includes the creation of the user entity (functionality typically found in a human resource application), authorization and permissions (single sign-on and password management functionality), and a single point of administration for accounts.[13]

Access management controls user privileges to use certain applications. It is software that lets the good guys into an enterprise network or e-business site and manages the content they have access to and the actions they can perform. An effective access management system incorporates one or more methods of authentication to verify the user, including passwords, digital certificates or hardware or software tokens.[14]

Authentication is the process of attempting to verify the digital identity of the sender of a communication, such as a request to log in. The sender being authenticated may be a person using a computer, a computer itself or a computer program. In a web of trust, authentication is a way to ensure users are who they say they are — that the user who attempts to perform functions in a system is in fact the user who is authorized to do so.[15]

Authorization is the process of verifying that a known person has the authority to perform a certain operation on a given resource. Authentication, therefore, must precede authorization.[16]

Single Sign-On is a specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple software systems.[17]

Solutions: Confronting the New Order of Things

Anonymous log-ons as a guest are dead. I have had one too many FBI letters about who the hell did what, when and why.
*– **Frank J. Monaco**, CIO/VP, Pace University, New York, October 2006*

As information security has become a cost of doing business, knowing all parties to transactions and tracing access to sensitive data and the systems that contain it are vital. At issue is managing risk by being able to define the following: who is authorized to access systems and under what circumstances they have access, and compare that information with who actually accessed systems and the attendant data including when, where and with what result.

Identity and access management (IAM) brings together these two previously discrete practices. Taken together, IAM can help organizations harden their existing information security practices to enable new business functionality, meet regulatory requirements and compliance standards, as well as improve access to information through routine enforcement of security policies, stronger and more consistent authentication, and managed access to sensitive information. A consistent and common IAM program also holds the potential for reducing both operational costs and development time while all applications — old and new — share the benefits of fortified front and back doors.

Key features of IAM include role- and rule-based identity administration from provisioning of employees and customers to role-based access for applications and systems, and auditing of administration, account activity and access rights. An open standards-based[18] IAM solution supports the application programming interfaces (APIs) of existing applications, eliminating or reducing the need for modifications. Instead, open standards-based IAM solutions integrate with an organization's existing infrastructure and applications. Other key features include modularity and interoperability with components from other vendors or even custom applications. Finally, IAM programs should support an organization's information security program.

To those ends, it is important that IAM solutions include the following components:

- Identity administration and provisioning — authorize, control and manage creation, modification and deletion of user identities and access to increase security and reduce administrative costs.
- Host-based access control — manage access to the organizations' IT assets such as systems, files, directories and databases, including centrally defining and distributing policies that control access.
- Extranet access management — secure Web content, regulate access and provide access to internal and external Web resources to provide centralized identity and access management.
- Single sign-on — provide secure and combined access to applications and databases supporting multiple forms of authentication including passwords, tokens and biometric authentication.
- Biometric/strong authentication — strong or multifactor authentication is the most trustworthy. It brings together a number of components so the whole is greater than the sum of its parts. Biometric authentication (including fingerprints, eye retinas and irises, facial patterns and hand measurements) measures and analyzes human physical and behavioral characteristics. Something the authorized person would have is combined with something the person would know.[19]
- Web services access management — controls access to Web services based on identity in order to protect Web services.
- Mainframe access controls — supports mainframe environments including user account management and provides consolidation of system log information with the centralized audit program.
- Monitoring and auditing — ensures that all events and activities associated with identities and resources are monitored and tracked across the enterprise to allow auditors to know who created what identity and when, what the identity accessed, and when the identity was terminated.

Beyond the Technology: Embracing the Needed and the Inevitable

When interviewed by the Center, public sector IT leaders also identified several factors beyond the technology that are critical for a successful IAM program. These factors include identifying a business case for IAM and understanding that appropriate governance is vital to success.

Return on Investment (ROI)

Public sector IT leaders believe that their policymakers and leaders need to understand that IAM does not easily fit into traditional return on investment models. The payoff is often indirect, in the form of opportunity costs — more access to e-services, or cost avoidance — preventing security breaches or fines from lack of compliance. The desire to immediately recognize a return must be balanced with the overall value of an IAM program. Value is more easily achieved when the IAM program focuses on improving operations in a proactive manner.

Governance

The need for clear lines of authority and collaboration among agencies around shared interest to provide governance and identify funding for a comprehensive, central or shared IAM program was the second most cited need among IT leaders. Without clear leadership and direction, important policy-level decisions are delegated, most often unconsciously, to IT staff. Since these policy-level decisions impact both internal operations and external service delivery, they are best addressed by policymakers through a formal governance process.

Getting Started: Startled and Stunned is Not an Option

When it comes to digital security, there's no such thing as an impenetrable defense. But you can mitigate risk by following sound operating practices.

*— **Robert D. Austin** and **Christopher A.R. Darby**[20]*

While the drivers, responses, solutions and challenges related to IAM are numerous, public sector organizations can get started by building on the foundation already in place in their organization. Many public sector organizations are using passwords, tokens, virtual private network (VPN) technology, lightweight directory access protocol (LDAP), digital certificates and biometric technologies. Although these efforts are familiar, they are often implemented in a fragmented manner. Implementing an IAM program will bring these often fragmented security measures together into a more cohesive approach.

The approach to establishing a more comprehensive, coordinated, value-driven IAM program should sound familiar and include:

- Establishing governance for the IAM program
- Identifying funding and other necessary resources
- Designating who is responsible and accountable for the program
- Determining and prioritizing IAM related needs
- Drafting and distributing related policies and procedures
- Reviewing and revising business processes as needed to support the program
- Identifying and deploying technology based upon the prioritized needs
- Developing and communicating a phased approach to deployment of an IAM solution

Conclusion: The Next Evolution

Organizations on the leading edge are taking their enterprise IAM program to the next level by consolidating responsibility and functionality of logical security with more traditional physical security to provide an integrated solution for the organization. An example of this merged approach is the use of a smart card that electronically identifies an individual, serves as a visual badge, grants access to facilities, and is part of a two or three tiered IAM program that grants access to IT applications and data. While a few public sector organizations have begun to merge logical and physical security programs, most continue to divide responsibilities between the IT department for logical security and a facilities or administrative department for physical security.

Whether the goal is to avoid embarrassing headlines or to improve access to information and services, a comprehensive IAM program will help achieve it. With the number of people using e-government services increasing at the same time the amount and intensity of threats to the digital government environment continue to rise, the time to get started with an IAM program is now.

Endnotes

[1] Robert McMillan, "Boeing privacy breach puts U.S. total over 100 million," securityitwatch.com, 12/15/06.

[2] http://www.internetnews.com/security/article.php/3615831

[3] http://www.eweek.com/article2/0,1895,1986066,00.asp

[4] http://www.numbrx.net/2006/10/24/chicago-voters-information-exposed-on-website/

[5] http://www.numbrx.net/

[6] http://www.computerworld.com/securitytopics/security/story/0,10801,106180,00.html

[7] http://msdn2.microsoft.com/en-us/library/aa480030.aspx.

[8] From "The Myth of Secure Computing," *Harvard Business Review*, June 2003.

[9] Michael Bertin, "The New Security Threats," *Ziff Davis Smart Business,* February 2001.

[10] Based on interviews conducted by the Center for Digital Government, November 2006.

[11] http://www.marketresearch.com/product/display.asp?productid=1327392&g=1

[12] en.wikipedia.org/wiki/Identity_management

[13] www.geneous-software.co.uk/glossary.htm

[14] www.voiceanddata.com.au/vd/admin/glossary.asp and www4.dogus.edu.tr/bim/bil_kay/network/intranets/ch55.htm

[15] en.wikipedia.org/wiki/Authentication

[16] en.wikipedia.org/wiki/Authorization

[17] en.wikipedia.org/wiki/Single_sign_on

[18] A standard with publicly available specifications, which can be implemented by any developer. Open standards are typically developed and maintained by a review process in which all interested parties may participate, in contrast to proprietary standards, which are developed and maintained by a single company. (See www.ssuet.edu.pk/taimoor/books/0-7897-1063-3/appa.htm)

[19] http://en.wikipedia.org/wiki/Biometric

[20] Op. cit., "The Myth of Secure Computing."

100 Blue Ravine Road
Folsom, CA 95630
916.932.1300 phone
916.932.1470 fax

www.centerdigitalgov.com

Underwritten by:

CA's State and Local Government solutions provide government organizations with industry-leading management software to address these challenges. CA's comprehensive portfolio of products and services deliver the right level of technical expertise to help design and implement enterprise architectures that support government objectives, and enable IT staffs to deliver applications aligned with government and agency goals.

CENTER FOR DIGITAL GOVERNMENT

Acknowledgments:
Liza Lowery-Massey, Senior Fellow for the Center for Digital Government, and former CIO for the city of Los Angeles and the city and county of San Francisco
Paul W. Taylor, Ph.D., Chief Strategy Officer for the Center for Digital Government and the Center for Digital Education

The Center for Digital Government, a division of e.Republic, Inc., is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.

The Center's special reports and papers provide two decades of experience and insight into the most important policy and management issues facing governments, and offer strategic approaches for planning and implementing technology, funding sources, and case studies from jurisdictions.