NASCIO
Representing Chief Information
Officers of the States

NASCIO Staff Contact:
Charles Robb
Issues Coordinator
crobb@AMRms.com

Protecting the Realm: Confronting the Realities of State Data at Risk

All About the Data

Information is the lifeblood of any organization, and to an ever-increasing extent, that information exists and is most valuable in electronic form. In the case of public agencies, and state governments particularly, the economy and speed with which data can be captured and employed to transact public business is remarkable. Data are aggregated and analyzed to support implementation and management of public programs, captured into records that preserve evidence of those transactions, shared among agencies to reduce costs and enhance services, and published or disseminated to allow transparency or as a resource to citizens and business. All contribute to the sense that the enterprise is almost literally, all about the data.

A data-centric view of this critical resource, however, is not one commonly held by public agencies themselves. Despite continuing improvement through modernization, state governments remain rife with stove-piped applications and information assets, and agencies vary in the extent to which they manage their resources. Data is frequently understood to be "owned" by individual business units rather than by the agencies and the larger enterprise. Furthermore, the expansion of the volume and the proliferation of the kinds of data maintained by agencies have made it almost impossible to maintain an inventory of the resources in a very meaningful sense, and equally challenging to establish degrees of protection appropriate to the classes of data being stored.

This situation, combined with the same characteristics that make electronic information valuable in the first place – portability, ease of copying, transmissibility and the like – mean there are increasing vulnerabilities and risks that data will be disseminated or shared when it should not be, or that it will be lost, stolen, or otherwise misused. It is equally possible that it will not be available when it should be, or that it will be destroyed when evidence of governmental activity is still needed.

State CIOs are fully aware of the criticality of protecting data and of the fact that the continued success of the organizations they support depends on rock-solid reliance on doing business electronically and maintaining citizen trust. Here, however the track record of governments is not perceived to be particularly good, with sixty-five percent of citizens in one national survey expressing little confidence that government can be trusted to maintain records about them appropriately.[1] Every breach, public or private, fairly or unfairly, diminishes that confidence and inhibits progress.

How Are We Doing?

The statistics are startling. To date, over 236 million records containing sensitive, personal information have been breached or compromised since January 2005.[2] As instances of individual data breaches continue to infiltrate the headlines of mainstream media organizations, data protection and data security[3] have emerged as vital parts of any organization's IT security program. For private sector organizations, protecting data can include protecting customers' and employees' personal information as well as information that is covered by intellectual property or trade secret laws.

For state governments, however, the data protection and security burden is enormously heightened. The relationship of citizens to their state governments does not allow opt-in when it comes to furnishing information – it is a relationship that begins with birth and likely extends years beyond the individual's life. As states push to conduct every transaction possible through electronic means in order to provide services and drive down costs, the volume of information they collect, maintain, and protect grows constantly. Simultaneously they manage these information assets in an environment that must provide openness and transparency while still protecting the information from loss and misuse.

With many agencies at varying levels of maturity in their IT security programs, State CIOs must find ways to harmonize data protection and raise all agencies and state-affiliated organizations to a common level of data protection.

Ensuring strong data protection that provides for the confidentiality, integrity and availability of a state's data and information assets has many benefits, including:

- Ensuring that information and data are available in order to carry out **government operations and citizen services**
- Protecting the **privacy** of citizens
- **Establishing regulatory compliance** and reducing **legal risk**, stemming from such laws and standards as HIPAA and Payment Card Industry (PCI) compliance
- Protecting the **government's knowledge assets**

In this environment, states are faced with the mandate of ensuring strong data protection across the vast state enterprise. With many agencies at varying levels of maturity in their IT security programs, State CIOs must find ways to harmonize data protection and raise all agencies and state-affiliated organizations to a common level of data protection. This brief explores at a high level the elements of data protection that are critical for state government information and then provides starting steps for inventorying and classifying state data assets across the enterprise.

The Big Picture—Data Management

Data touches so many facets of a State CIO's responsibilities because it is at the heart of how state government conducts business and serves its citizens. For State CIOs, it impacts multiple efforts, including Security, Privacy, Collaborative Information Exchange, Disaster Recovery, Business Continuity and Identity Management.[4] Since most data and information are now in electronic form or "born digital," state government, as an enterprise, must manage the systems, databases and applications that hold that information and find ways to ensure that the information's confidentiality, integrity and availability are not compromised. While

state CIOs do not own the information or data of other state agencies they service, it is their responsibility to facilitate its management. If this is going to happen, it is up to them to coordinate the efforts and commitment needed from data owners, agency, business and IT staff, and those responsible for enterprise information security and asset management.

As a result of the growing value of data and information as knowledge assets, data management is emerging as a discipline unto itself. It addresses the broad spectrum of data-related issues including:

- Data Governance
- Data Architecture, Analysis and Design
- Database Management
- **Data Security Management**
- Data Quality Management
- Reference and Master Data Management
- Data Warehousing and Business Intelligence Management
- Document, Record and Content Management
- Metadata Management[5]

All of the elements of data management must work in tandem to constantly ensure that states' knowledge assets are protected, reliable and properly managed. A solid foundational governance structure serves as a starting point for a holistic and methodical approach to the management of state data. A state's Enterprise Architecture (EA) program can provide this solid foundation, since it is a government-wide, multi-disciplinary, multi-stakeholder effort that is driven by the business needs of government. Within that framework, state CIOs can help ensure data protection efforts are consistent across the enterprise.

NASCIO has addressed these issues in its April 2008 research brief, ***Data Governance - Managing Information As An Enterprise Asset: Part I - An Introduction.*** This brief covers the primary elements of state data protection and starting points for determining what information assets states possess and how to organize and classify them. NASCIO's Enterprise Architecture Committee will continue to address the issue of the CIO's role in data governance in subsequent briefs.

The Link to Enterprise Architecture

The organizational structure of a state's Enterprise Architecture (EA) program is the logical framework to attack the problems associated with protecting data. Through the EA's governance, domain structures, policies and individual standards, data ownership and responsibility issues can be resolved and efforts can be made to conduct needed inventories and data classification. Protective strategies can then be identified and pursued.

It is likely that life cycle management standards already exist within the states's EA framework, so the task of the CIO is to ensure architects and developers integrate available data protection and classification models with pre-existing life cycle management standards or models, to establish better control of data resources.

As with other EA efforts, it is obviously easier to produce a model for establishing control than it is to execute it. At the same time, for many states, the *process* of developing the architectural model will create a coherent picture that didn't previously exist. Further, EA provides the operating discipline for assigning resources in the most coherent and cost-effective way possible. In that sense, establishing the data protection effort in the EA program should be considered foundational.

All of the elements of data management must work in tandem to constantly ensure that states' knowledge assets are protected, reliable and properly managed. A solid foundational governance structure serves as a starting point for a holistic and methodical approach to the management of state data.

Primary Elements of Data Protection for State CIOs

A holistic approach to data protection is needed to ensure that all of the moving parts of state government data management are functioning cohesively. There is a set of *primary elements* that a state must have in place as part of its overall IT security program, which are necessary for implementing a consistent approach to data protection. These are noted below. These *primary elements* should be considered as "must haves" in order to ensure proper data protection for the entirety of state government.

> **The Primary Elements of Data Protection for State CIOs:**
> A. Governance Framework - Roles and Responsibilities
> B. Enterprise-Level Policies to Address Data Protection
> C. Risk Assessments
> D. Data Inventory and Classification
> E. Integration of Security Classification with Life cycle Management Processes
> F. Access Controls (Identity Management, Authentication)
> G. Perimeter Security Controls (Anti-Virus, Intrusion Detection)
> H. Mobile Device Security (For both state-issued and employees' personal devices)
> I. Ensuring Regulatory Compliance and Minimizing Audit Risks

Below is a description of each element of data protection as well as any NASCIO resources that may be related to it. Future NASCIO Research Briefs may cover individual elements on a more in-depth basis.

A. Governance Framework – Roles and Responsibilities

The state Enterprise Architecture program encompasses not only IT but the many disciplines that are impacted by data protection, including records management, project management, and legal compliance. As a best practice, data protection activities should therefore reside within the greater umbrella of the state EA program. States must identify and convene the relevant stakeholders within a governance structure. An early priority of governance is to create a common understanding that data and knowledge assets represent *enterprise-owned resources* that must be managed and protected as state enterprise assets. This concept of asset management provides the foundation for examining the state's current, or "as is" level of data protection. The governance process must also define what an appropriate level of data protection, or the "to be" state, would be. This activity looks at available resources, acceptable risk, and may even stage activities that allow state government to migrate through various levels of maturity to eventually bridge the gap between the "as is" and "to be." The governance structure should provide a means for collective decision-making. Adequate authority is also a must to ensure that decisions made by the governance body translate into projects, programs and management initiatives that bring about the "to be" state of improved data protection.

Regarding a state's IT security program, most states have a Chief Information Security Officer (CISO), or the equivalent of that position, to oversee the state's enterprise IT security efforts. Both the State CIO and the State CISO should be included in data protection activities, since the role of the State CISO has evolved through the years to encompass not only technical security-related duties, such as perimeter security, but also administrative security issues, such as policies, procedures, awareness training, compliance audit, and remediation.

Related NASCIO Resources:
- "IT Governance and Business Outcomes—A Shared Responsibility Between IT and Business Leaders," March 2008
- "Born of Necessity: The CISO Evolution—Bringing the Technical and the Policy Together," July 2006
- "A Current View of the State CISO: A

National Survey Assessment," September 2006

B. Enterprise-Level Policies to Address Data Protection

As new technologies emerge and states strive to offer streamlined and efficient citizen services, State CIOs must ensure that the technologies and business processes meet a required minimum level of data protection.

In revising current policies or creating new ones, state government leaders must understand that, at the heart of data protection, is the protection of citizens' personal information as well as homeland security or other sensitive government information. Citizen trust in government's credibility and competence and even public safety hinges on the protection of private and sensitive information. State policies set the stage for implementing data protection.

In developing data protection policy frameworks, the Fair Information Principles provide important considerations that a state should take into account in deciding what personal information it should collect, how it handles, stores and protects that information, and how it eventually disposes of or permanently preserves that information.[6] A principle related to the Fair Information Principles is to limit the amount of sensitive or personal information that state agencies collect only to the amount they need to carry out operations or serve citizens.

An often-overlooked facet of data protection is the need for policies that address not only external threats, such as hackers, but also internal threats posed by employees and contractors. Policies must address the concept of role-based access to personal or sensitive information as well as handling personal information in a way that protects its security. Finally, policies should also specify how and when employees and contractors will receive training and awareness to ensure they understand their individual responsibility

for data protection as well as overall IT security.

Related NASCIO Resources:
- "IT Security Awareness and Training: Changing the Culture of State Government," August 2007
- "Insider Security Threats: State CIOs Take Action Now!" April 2007
- "Keeping the Citizen Trust: What State CIOs Can Do To Protect Citizen Privacy," October 2006

C. Risk Assessments Regarding State Data

An initial step in enhancing a state's enterprise data protection is to identify the current risks to state information assets and prioritize them according to their seriousness and likelihood of occurrence. Steps in a risk assessment include identifying critical information and system assets, determining the current, as-is risks to state information, envisioning the to-be, improved risk level, and then developing strategies, policies, security measures and compliance mechanisms to close the gap between the current and future states. Types of risk assessments can range from self-assessments that agencies conduct to determine the current level of their data protection to risk assessments conducted by an independent third party. In some states, the state or legislative auditor may conduct risk assessments.

Related NASCIO Resource:
- "The IT Security Business Case: Sustainable Funding to Manage the Risks," May 2006 (includes a section on risk assessments, as well as examples)
- "Data Governance – Managing Information As An Enterprise Asset Part 1 – An Introduction," April 2008

D. Data Inventory and Classification

Knowing what information a state government possesses, where it is located and whether it is sensitive and in need of enhanced levels of security protection are critical first steps towards improved data protection. However, in the state government

Citizen trust in government's credibility and competence and even public safety hinges on the protection of private and sensitive information.

environment, this is a particularly daunting task, because states are vast enterprises with many agencies and quasi-governmental entities that possess large amounts of personal and other sensitive information. ***The second part of this brief addresses steps State CIOs can take to begin this data inventorying and classification process.***

E. Integration of Classification with Life Cycle Management Processes

State government data and information are fluid by their very nature, but at the same time, data, information, and records all have a "life cycle." Information is initially collected by states with a specific business purpose and then used during business processes. Thereafter, it may be used for secondary purposes which may or may not involve passage out of the original business units or systems that maintained it. It then may be stored for varying lengths of time depending upon statutory requirements and/or its importance and long-term value to state government. A small percentage of state government information that carries with it historical value may be preserved permanently. However, most information does have a limited life, whether several hours or several years. At the end of its life, it is normally disposed of or destroyed.

In developing improved data protection, states must consider not only the primary elements of data protection but must consider them in the context of the information life cycle. For example, enterprise data protection frameworks should address how information is collected, used, handled and stored, and then disposed of or preserved. Moreover, during the data classification process, state agencies must determine what information they collect, store, use and either dispose of or preserve.

The most formal life cycle model states are likely to use today relevant to IT is the systems development life cycle model or SDLC. The March 2008 National Institute of Standards and Technology draft publication, Security Considerations in the System Development Lifecycle (NIST Special Publication 800-64 Revision 2; http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-64-Rev.%202), contains detailed guidance for incorporating security requirements into the information system development life cycle, and state CIOs are urged to employ guidance provided there.

F. Access Controls

Managing access to information is a critical element of data protection. This includes password management, identity management and authentication functions to ensure that only authorized individuals have access to personal or sensitive information. In the current environment of data breaches that originate from within, this is especially important. A framework that addresses which employees have a business need to view legally protected or sensitive information is a starting point for solid access controls, which should then be supported by appropriate technology solutions. In addition, employees have certain responsibilities for protecting access to their workplace devices, such as desktop computers and laptops. Some of these security measures can be automated. For example, employees can be required, through a technology solution, to use a password of a specified complexity or multi-factor authentication in order to access their desktop computers and network resources.

Related NASCIO Resources:
- "Insider Security Threats: State CIOs Take Action Now!", April 2007
- "The Year of Working Dangerously— Parts I and II: The Privacy Implications of Wireless in the State Government Workplace," August and September 2005
- "Who Are You? I Really Wanna Know: E-Authentication and its Privacy Implications," December 2004

G. Perimeter Security Controls

Controlling the perimeter of a state's computer network and systems helps to ensure that external attacks do not compromise the information and services within those networks and systems. Common perimeter security controls include routers, firewalls, intrusion detection systems, virtual private network (VPN) devices and enterprise-class anti-virus, anti-spyware and spam filter solutions. States also may consider enhancing application layer security, since concerns have been raised in recent years that, as perimeter security has improved, threat vectors may now target the application layer.

Related NASCIO Resources:
- "Welcome to the Jungle: The State Privacy Implications of Spam, Phishing and Spyware," February 2005
- "The Real Phantom Menace: Spyware and its State Implications," January 2005

H. Mobile Device Security

It has been well-documented that many data breaches have resulted from lost or stolen mobile devices, such as laptops, personal digital assistants (PDAs), and thumb drives. The encryption of information both at rest and in transit has become one way that states and other entities have addressed data protection concerns with mobile devices.

States must also be aware that they should not only protect data on state-issued mobile devices but also on personal devices employees may bring to work with them, where such devices are not prohibited. Recent changes in civil procedure relating to e-discovery now put personally owned equipment used for state business in the line of fire for seizure as evidence. Unless employees are prohibited from using personal devices for business purposes, citizens' personal or sensitive information may well be stored on them. Moreover, employees seeking to cause damage to the state can and do use portable devices to download and take state information from the workplace.

State CIOs must ensure that data protection activities address mobile device security. Policy-driven technology solutions can be implemented to prevent the transfer of sensitive information to portable storage devices.

Related NASCIO Resources:
- "The Year of Working Dangerously— Parts I and II: The Privacy Implications of Wireless in the State Government Workplace," August and September 2005
- "Insider Security Threats: State CIOs Take Action Now!", April 2007

I. Ensuring Regulatory Compliance and Minimizing Audit Risks

An essential element of strong data protection is ensuring that state employees follow policies and procedures that are put in place. Coordination with state human resource officials is necessary so that employees understand that IT security and data protection are part of their job responsibilities. State CIOs or CISOs should pursue efforts to include IT security compliance and data protection as items covered by employee performance evaluations. By ensuring compliance, risks of unfavorable findings during state or regulatory audits can be minimized. State CIOs should note, however, that audits related to the privacy of personal and sensitive information may include new elements upon which states will be audited. Close attention to such new audit elements may be necessary to ensure the fairness and helpfulness of the audit process.

While not a panacea, automation can be a significant help in discovering where the sensitive data is and what can be done with data that is found in the wrong place. Policy-based automation is gaining in popularity in both the public and private sector as organizations seek to move toward better protection against data loss and more proactive oversight for all data types and devices.

States must also be aware that they should not only protect data on state-issued mobile devices but also on personal devices employees may bring to work with them…

- "IT Security Awareness and Training: Changing the Culture of State Government," August 2007
- "Insider Security Threats: State CIOs Take Action Now!" April 2007

Where to Start—Know What You Have and How to Classify It

Information and data are assets of state government and they must be managed as any other physical state assets, such as buildings, furniture and vehicles. As part of managing government information and data, states must start with determining what information and data they possess. The next step is to organize or classify that information and data, since different types of information and data require different types of security protections.

Understand How Data Inventory and Classification Supports the State's Overall IT Security Posture: Inventorying what data a state possesses and characterizing that data relative to value and vulnerability. The level of data protection is then applied, based on that characterization or risk assessment. The risk assessment process determines the classification of data. The classification then prescribes the appropriate data protection measures that will be employed. This process must be applied consistently across the enterprise. State CIOs can provide the necessary guidance to agencies on how to conduct data inventories and classification efforts.

Initially, State CIOs will likely need to demonstrate *why* these activities are so vital to a state's overall IT security posture. For example, Ohio has taken steps to demonstrate the critical importance of its data classification efforts by mapping its data classification policy back the requirements of the state's overall IT security framework. Ohio's data classification effort supports all of the elements of the state's security framework, including:
- Risk management

- Confidentiality
- Integrity
- Availability
- Protect, detect and respond
- Identification and authentication
- Access control and authorization
- Security audit logging
- Security management and administration[7]

On a broader scale, data classification also can help to facilitate state electronic records (e-records) management efforts, since a preliminary step in managing e-records across the state enterprise is to know what information a state possesses and how sensitive that information may be.

Make the Application of Data Classification Broad: In preparing policies that support agency data classification, State CIOs must be sure that those policies are broad enough to include not only state employees but also others who have access to state data, including contractors and temporary employees. Service level agreements and contract terms and conditions regarding IT and non-IT contractors should include clauses regarding data classification.[8]

Define Who Has Responsibility for Data Classification: While the State CIO may have responsibility for establishing policy for the state enterprise regarding data classification, agencies normally have responsibility for conducting data classification in accordance with state policy. For example, Arkansas' data classification policy suggests that a small group of agency officials, such as individuals familiar with an agency's IT resources or data, including the CIO, IT manager or database administrator, should be responsible for conducting data classification.[9]

In Ohio, agencies also serve as the data classification authority for the information they collect and maintain. Each agency is required to designate an "information owner" from a business or program area to be responsible for the data classification process. The information owner must work with agency IT personnel in developing

appropriate security requirements for each classification labeling or category as part of this process. Finally, information owners also have responsibility for ensuring that data that is shared with other agencies is properly classified and protected according to a data sharing agreement that documents how shared data will be treated.[10]

Define A Process or Methodology for Data Classification: Although state data classification processes will differ from state-to-state, the general steps remain fairly consistent across the states. First, agencies must determine what information they possess, including information that may be located in IT systems, networks, and on IT devices, including mobile devices and even state employees' personal devices that they use in part for business purposes. From there, agencies then must determine what types of personal or other sensitive information are contained within IT systems or on IT devices. Some states, such as Arkansas, also require IT systems to be categorized according to their criticality to state government operations. After the categorization process has occurred, agencies will then determine what security measures apply to each category of sensitive information and implement appropriate controls accordingly. Final steps in the process include educating and training employees regarding their role in data classification activities and periodically revisiting data classification policies, categories and security measures to ensure that they are up-to-date with types of information held by an agency and any laws or regulations that may apply to agency information.

Provide for Training and Awareness Regarding Data Classification: As part of a state's overall approach to IT security awareness and training for state employees as well as contractors and others, states should include a component regarding data classification. Employees must understand their responsibility for ensuring data protection and proper classification. For example, Ohio's data

classification policy includes specific provisions for education and awareness related to data classification. At a minimum, Ohio agencies must include the following elements:

- Process for identifying and assigning labels and guidelines for state data
- Distribution and disclosure of guidelines
- Impact of risk of data loss, disclosure, release or modification
- Reporting incidents such as theft, disclosure, or unauthorized modification[11]

State Examples of Data Classification—Ohio, Arkansas, and Iowa
The following states have established data classification policies and processes for state agencies. They are detailed below and demonstrate different approaches to how data classification can be established and implemented.

Ohio: Ohio's data classification policy was established by the State CIO and requires agencies to make classification a part of their overall risk assessment process. During the process, information and data are labeled by each agency according to confidentiality and criticality. At the same time, the policy recognizes that other state and federal laws may require additional, more specific labels. For confidentiality, agencies must classify information as "public" (must be released according to public records laws), "limited access" (may be released by an agency if the agency chooses to waive a public records law exception and places conditions or limitations on the release), or "restricted" (prohibited from release by state or federal law or treated by the agency as highly confidential). These three categories are derived from the Ohio Attorney General's legal guidance on Ohio's public records law. Information also is classified according to its criticality. With criticality, the potential impact of a compromise is evaluated in terms of financial loss to the state, legal liability, public trust, or harm to the public health and welfare. Information is categorized for criticality as "low" (insignificant or no risk), "medium" (limited

risk), "high" (significant risk), or "very high" (catastrophic risk). Again, agencies are tasked with determining any other special information labeling based on additional state or federal law.

Responsibility for classifying data is assigned to the information/business owner, not the information technology function. According to Ohio's policy, the information owner is to be someone from a business or program. Preferably the information owner would be someone who understands why the data is being collected, how it is used, who is to have access to it, and the potential impact of the loss of confidentiality, integrity or availability. This individual develops access guidelines for data in each classification. The information owner also coordinates the sharing of data with other agencies to ensure that there is a documented data sharing agreement and that the shared data is consistently classified and secured.

Ohio's policy requires agencies to develop a data classification methodology that addresses:

- Whether existing laws, regulations or agreements regulate information and how it is handled through the information life cycle;
- A structured decision process at the agency-level to determine appropriate information labels;
- Data maintenance guidelines based upon the results of the classification process for how information is to be secured throughout the information life cycle, including the creation, access, storage, modification, retention, archive, disposal, and distribution of data; and
- A process to regularly review data classification labels and adjust them per regulatory changes.

The policy also addresses issues related to handling compiled data and summary data. Compiled data – data from multiple sources that are combined to create a more comprehensive view of the subject of the data – must be classified according to the most sensitive level of classification

of any individual piece of data within the compilation. However, summary data – data that draws from various information sources and is analyzed and presented as trend data without revealing confidential data – may be classified at a less restrictive level.[12]

Alongside its data classification policy, Ohio also published a data classification resource kit. This resource kit came out of a standing, multi-agency committee on data protection. In it, agencies are given functional guidance in the form of a classification framework and a high-level classification process template that can be built upon. The resource kit also provides two examples of agency practices that helped those respective agencies to engage in the data classification process.

Arkansas: Arkansas' data classification policy, established by the State Security Office, tasks agencies with responsibility for data classification activities. However, agencies do not have to take a complete inventory of their data and systems but rather must examine their data and systems generally. The state's policy then sets out a two step process for agencies that involves first identifying systems and data and then classifying agency data and systems according to a grid system.[13]

During the first step, agencies must identify major databases and systems. However, the state's guidelines caution that agencies must include databases and systems that contain sensitive information, even if they appear to be insignificant at first. In addition to databases and IT systems, other systems that should be included in the process are phone networks, websites, email systems and networks.

The second step involves the classification of agency systems and data according to sensitivity and criticality. Arkansas' guidelines provide a great deal of detail to assist agencies in classifying their data and systems properly. Sensitivity levels range from unrestricted to extremely sensitive.

At the far ends of the spectrum, "unrestricted" information is open public data with no distribution limitations, while "extremely sensitive" information, if compromised, could have "severe financial, health or safety repercussions." An example of "unrestricted" information would be press releases, formal statements, and reports that are freely made available by the state. On the other hand, information in a law enforcement database would likely be considered to be "extremely sensitive."

At the spectrum's mid-range are "sensitive" and "very sensitive" classifications. "Sensitive" information includes the majority of a state's information that is available through open records requests or other similar processes but to which direct access is limited to authorized individuals. Examples include:
- Most data elements in state personnel records
- Driver history records
- Employment and training program data
- Firearm permits
- Real estate appraisal data
- Personnel data
- Building code violations data
- Collective bargaining data
- Federal contracts data
- Historical records repository data
- Occupational licensing data

On the other hand, "very sensitive" data is only available to internal authorized individuals and may be regulated by state or federal law. It is intended for use only by those employees who have a legitimate business need for the information. Examples include:
- Social Security Numbers
- Most home addresses
- Attorneys' files
- Comprehensive law enforcement data
- Domestic abuse data
- Educational records
- Foster care data
- Health and medical data
- Library borrower's records
- Signature imaging data
- Welfare records/data

- Credit card numbers
- Competitive bids
- Civil investigative data
- Criminal history data
- Economic development assistance data
- Food assistance programs data
- Head Start data
- Juvenile delinquent data
- Counselors' data
- Trade secrets data

Regarding the classification of Arkansas agencies' information according to criticality, there are three levels—"not critical," "critical," and "extremely critical." Issues of prioritization for business continuity and disaster recovery purposes drive this categorization process. For example, "extremely critical" systems must be critical to public health or safety and must be protected by a disaster recovery plan that would allow for the resumption of operations within a very short period of time. However, "critical systems" are required in order to administer functions of state government. For those systems, a business continuity plan must allow for the continuation of operations within a certain period of time until those systems can be restored.[14]

Iowa: According to the data classification policy established by Iowa's State CIO, all agencies must classify their data as well as information derived from that data, at a minimum, as "public" or "confidential." "Public" information is all information that is not included in any other data classification category, while "confidential" information is protected by federal or state law. In addition, agencies may classify information as "sensitive" if it is not protected by federal or state law but could cause a negative impact to state government operations or services or citizens if compromised. Agencies then set security standards for the protected classes of information. The state's data classification standard recommends that agencies consider different states of data, including at rest, in transit, and in use when setting such standards. All forms of data should also be considered, including local and

networked databases, documents, spread-sheets, messaging, paper, and backup media. Finally, Iowa's Information Security Officer has authority to assess agency compliance with the state's data classification standard and issue notifications of noncompliance to agencies.[15]

Managing the Risks to Data– Start Simple and Execute

With a focus on broader awareness, developing a security architecture and IT security investments, state governments have made significant progress in recent years protecting the realm. However there is still much to be done to adequately protect the data held in trust by state government. Citizens expect it. However, it is clear that the public generally has low expectations of state government's ability to protect their most sensitive personal information from harm. Because of this eroding trust and confidence with state institutions, data protection is more critical than ever. Despite the pressures, the enormity and complexity of the enterprise data protection task has hindered states from making substantial progress. The lessons learned from other public sector initiatives illustrate the path to enterprise data protection is not easy. The approach must be simplified and critical data at risk addressed from an *enterprise* view with an understandable classification schema. Collaboration across the enterprise will provide a firm foundation for future action. This can only happen if state agencies are actively engaged in this process. There is no doubt that leadership is a critical success factor and State CIOs have the opportunity, and the challenges, to assume the leadership role.

The lessons learned from other public sector initiatives illustrate the path to enterprise data protection is not easy. The approach must be simplified and critical data at risk addressed from an enterprise view with an understandable classification schema. Collaboration across the enterprise will provide a firm foundation for future action.

An *enterprise risk management framework* for data protection is necessary as the first step to risk reduction. Key questions must be posed to the stakeholders to enhance agency-level accountability and promote the adoption of best practices. The key question for state CIOs is clearly defining the roles and responsibilities for action – who is responsible for the security and protection of these data? What are the data that the state needs to protect and where are these data within the state agencies? Is access to these data controlled through clearly articulated policies and processes? What is the decision process for redaction and removal? Is there a process in place for periodic audits to monitor compliance with state policies? Even with appropriate controls in place, bad things will happen. Is a data breach response and notification process outlined? Most importantly, as the risks are addressed and gaps identified, will an enterprise data protection framework and corresponding policies be accepted and followed? These are tough questions for State CIOs and underscore the complex challenges of data protection in state government.

Appendix I: Resources

Link to Educause Data Classification Policy
http://connect.educause.edu/term_view/
Data+Classification+Policies

AR
http://www.dis.state.ar.us/poli_stan_
bestpract/pdf/DataClassificationGuide.pdf

http://www.nascio.org/events/2006Annual/
presentations/NASCIO%20101706%20Priv
acy%20Elkins.pdf

IA
http://www.state.ia.us/itd/standards/
enterprise_it/12_data_classification.html

MN
http://www.osa.state.mn.us/other/
Statements/dataclassification_0705_
statement.pdf

OH
Data Classification Policy
http://www.oit.ohio.gov/IGD/policy/pdfs_
policy/ITP-B.11.pdf

Data Classification Resource Kit
http://www.oit.ohio.gov/IGD/policy/pdfs_
policy/Data_Classification_Resource_Kit.
pdf

Data Classification Toolkit
https://wiki.internet2.edu/confluence/
display/secguide/Data+Classification+
Toolkit

Appendix II: Endnotes

[1] Government Privacy Trust Survey, Ponemon Institute, 2006.

[2] "A Chronology of Data Breaches," the Privacy Rights Clearinghouse, August 12, 2008, http://www.privacyrights.org/ar/ChronDataBreaches.htm.

[3] Note that while differences in terminology do exist between "data" and "information," they will be used interchangeably throughout this brief and refer to the knowledge assets of state government that exist in electronic form and that contain sensitive or personal information.

[4] "Electronic Records Management and Digital Preservation: Protecting the Knowledge Assets of the State Government Enterprise—Part I: Background, Principles and Action for State CIOs," NASCIO, May 2007, http://www.nascio.org/committees/ea/index.cfm#pubs.

[5] Introduction and Project Status for DAMA-DMBOK (Data Management Body of Knowledge), Data Management Association (DAMA), November 2007, http://www.dama.org/files/public/DI_DAMA_DMBOK_Guide_Presentation_2007.pdf.

[6] Fair Information Principles, the Federal Trade Commission, June 2007, http://www.ftc.gov/reports/privacy3/fairinfo.shtm. The Fair Information Principles focus on the following key areas: Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security, and Enforcement/Redress.

[7] Ohio Data Classification Policy.

[8] Ibid.

[9] Arkansas Data Classification Policy

[10] Ohio Data Classification Policy

[11] Ohio Data Classification Policy.

[12] Ohio Data Classification Policy.

[13] To view an example of Arkansas' grid system, please see Doug Elkins' PowerPoint Presentation from the NASCIO Annual Conference in 2006.

[14] Arkansas Data Classification Policy.

[15] Iowa Data Classification Policy.