NASCIO Representing Chief Information Officers of the States

Research Brief

May 2006

Staff Contact: Mary Gay Whitmer, Issues Coordinator, at mwhitmer@AMRms.com or (859) 514-9209.

The IT Security Business Case: Sustainable Funding to Manage the Risks

Security continues to be a high-priority issue for the state CIOs. This fact has been repeatedly confirmed in surveys and polls of the CIOs and in testimony before Congress. At the NASCIO 2005 Midyear Conference, 89% of responding state CIOs ranked security among their top three most important issues. And it only takes a short recitation of some of the statistics about the threats faced by states for the reason for the urgency to become apparent. ***For example, on an average day, Michigan blocks 22,059 spam emails, 21,702 email viruses, 4,239 Web defacements, and 6 remote computer take-over attempts.***[1] Even less populated states face substantial IT threats. Delaware fends off nearly 3,000 attempts at entering the state's network daily. In June 2005, the state saw a spike of 141,000 instances of "suspicious activity" (the most dangerous type of Internet threat) due to a variant of the "mytopb" worm.[2] These are just two of a myriad of statistics that point out the importance for state CIOs to successfully make the business case for sufficient IT security funding. ***Produced under the guidance of NASCIO's Information Security and Privacy Committee, this brief takes a holistic approach to constructing the case for enterprise IT security investment by outlining for the state CIOs the following steps:***

- Understanding state government's IT environment that drives the need for security *(Section I)*
- Constructing an IT security business case in the context of Enterprise Architecture (EA) *(Section II)*
- Starting with an enterprise-wide IT risk assessment *(Section III)*
- Making the case for IT security through demonstrating the risks (bolstered by the IT risk assessment results), the benefits of security, and how security aligns with the state's business needs *(Section IV)*.

I. The World We Live In

Successfully making an IT security business case is far from easy, especially in today's complex world that drives the need for state government IT security. Preventative IT security initiatives also must compete with other IT resource demands that may appear to provide more tangible and immediate business value. The factors below are the primary drivers for IT security.

---

[1] 2006 Michigan IT Strategic Plan, see Appendix F "Cyber-Security," March 2006, <http://www.michigan.gov/documents/AppendixF_149547_7.pdf>.

[2] "Securing Cyberspace: Efforts to Protect National Information Infrastructures Continue to Face Challenges," Testimony of the Honorable Thomas Jarrett, Secretary and CIO, Delaware Department of Technology and Information, before the Subcommittee on Federal Financial Management, Government Information and International Security of the Senate Committee on Homeland Security and Government Affairs, July 19, 2005, <http://hsgac.senate.gov/_files/071905Jarrett.pdf>.

The Diverse and Evolving Threat Environment: A prominent driver of security is the diversity of the current threat environment. Not only must CIOs protect state information systems from attacks and unauthorized access, but they must also take steps to address potential Homeland Security and IT-related threats to critical infrastructure. The risks posed by cyber-crime, including online identity theft, can have a high cost. ***The FBI recently estimated that cyber-crime will cost businesses an estimated $67.2 billion dollars per year.***[3] However, the threats facing states are not only external. States must also protect their information systems and the data within them from ill-intended or even just plain negligent employees. As security threats evolve from spam to spyware to botnets, states may become an increasingly attractive target due to their rich stores of citizens' personal information.

The Pervasiveness of Technology: Today, technology is pervasive, both in the office and in the home. Desktop and laptop computers are an important part of most business and government operations. In their personal lives, citizens have become accustomed to conducting business online with agencies through e-government applications. They now have mobile phones as well as personal digital assistants (PDAs) and other wireless devices that oftentimes are difficult to secure.[4] Such small, cost-effective devices can also present security concerns by placing substantial storage capacity in the hands of those who may use them to discreetly extract data from government or business information systems. As the pervasiveness of technology has grown, so has the depth of citizens' knowledge of how to use technology. Now, state government employees are more tech-savvy than ever. They may have the knowledge to compromise state information systems or obtain access to sensitive information without authorization. Since IT is woven into the fabric of society, unplugging from the Information Age is no longer a viable option. That fact alone makes it all the more important to properly secure technologies used by the states.

The Privacy Imperative: Citizens' privacy and the security of their personal information has risen to prominence as headlines of data breaches and identity theft have become commonplace in mainstream news outlets. For example, in 2005, 9.3 million U.S. citizens were victims of identity fraud. That is about 4.25% of the U.S. population. The total amount of that fraud has cost approximately $54.4 billion dollars.[5] While states have always held a substantial amount of citizens' personal information, from birth records to driver's licenses to benefits information, there is now an increased emphasis on the business value of that information and on sharing it among state agencies and across levels of government. E-government applications have also made it easier for government agencies to collect and store more personal information than with paper-based processes. Within this context, citizens conduct business with the government although their trust in the government's ability to keep that information private is relatively low.[6] In addition, recent security breaches in several states further demonstrate that

[3] "FBI wants businesses' help in fighting cyber crime," Joris Evers, C|Net News, February 16, 2006, <http://news.com.com/FBI+wants+businesses+help+to+fight+cybercrime/2100-7348_3-6040521.html>.
[4] "The Year of Working Dangerously: The Privacy Implications of Wireless in the State Workplace—Parts I and II," the National Association of State Chief Information Officers (NASCIO), 2005, <http://www.nascio.org/nascioCommittees/privacy/>.
[5] "New Research Shows Identity Fraud Growth is Contained and Consumers Have More Control Than They Think," Council of Better Business Bureaus and Javelin Strategy & Research, January 31, 2006, <http://www.bbbonline.org/IDTheft/safetyQuiz.asp>.
[6] "Privacy Trust Survey of the United States Government," Ponemon Institute & the CIO Institute of Carnegie Mellon University, January 31, 2004, <http://cioi.web.cmu.edu/research/2004PrivacyTrustSurveyoftheUnitedStatesGovernmentExecutiveSummaryV.6.pdf>.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com • W :: NASCIO.org

state governments may be increasingly targeted by both external and internal threats due to their rich data stores. ***As other previously targeted sectors, such as the financial services sector, have implemented heightened security measures to deter such incidences, state governments may become a higher priority target for cyber-criminals.***

We're Watching You--State Oversight: As state legislators and auditors have become more aware of IT's prominent role in state government operations, they have heightened their scrutiny of IT expenditures and the security of systems. With pressure growing from legislatures for state agencies and CIOs to be strictly accountable for IT expenditures, there will likely be more legal mandates for accountability that are analogous to the Sarbanes-Oxley Act, which applies to private sector entities. Moreover, as public and private sector data breaches remain in the headlines, the enactment of privacy and information security protections is likely to continue at both the state and federal levels.

The Importance of State IT Security: Driven by the factors discussed above, state IT security and sufficient funding for it have developed into major issues for the state CIOs. State governments should invest in IT security, because states are large, multi-faceted organizations with many agencies that may not always behave in the best interest of the overall enterprise. A recent Computer Security Institute (CSI)/FBI survey found that "[s]tate governments currently have both the largest information security operating expense and investment per employee of all industry/government segments."[7] ***Within this environment, state CIOs must be more ready than ever to make a successful case for continued investment in enterprise IT security in order to keep pace with the ever-evolving threats and changing business demands. However, maintaining a good IT security posture can be one of the most challenging endeavors a state CIO can face.*** This brief offers state CIOs strategies for making the case for continued IT security investment.

II. A Framework for Action: The IT Security Business Case & Enterprise Architecture (EA)

Importance of the IT Security Business Case & EA: IT security is driven by the business needs of state government. Holding an almost incomprehensible amount of citizens' personal information, states must protect the IT systems in which that information exists. From Michigan to Montana, states are recognizing the importance of information security and the privacy imperative in their state IT strategic plans. [8] Since EA supports the development of the business case for IT security, it is important to explore the connection between the two.

[7] "2005 CSI/FBI Computer Crime and Security Survey," Lawrence Gordon, Martin P. Loeb, William Lucyshyn, and Robert Richardson, Computer Security Institute and the Federal Bureau of Investigation, 2005, <http://www.gocsi.com/press/20050714.jhtml>.

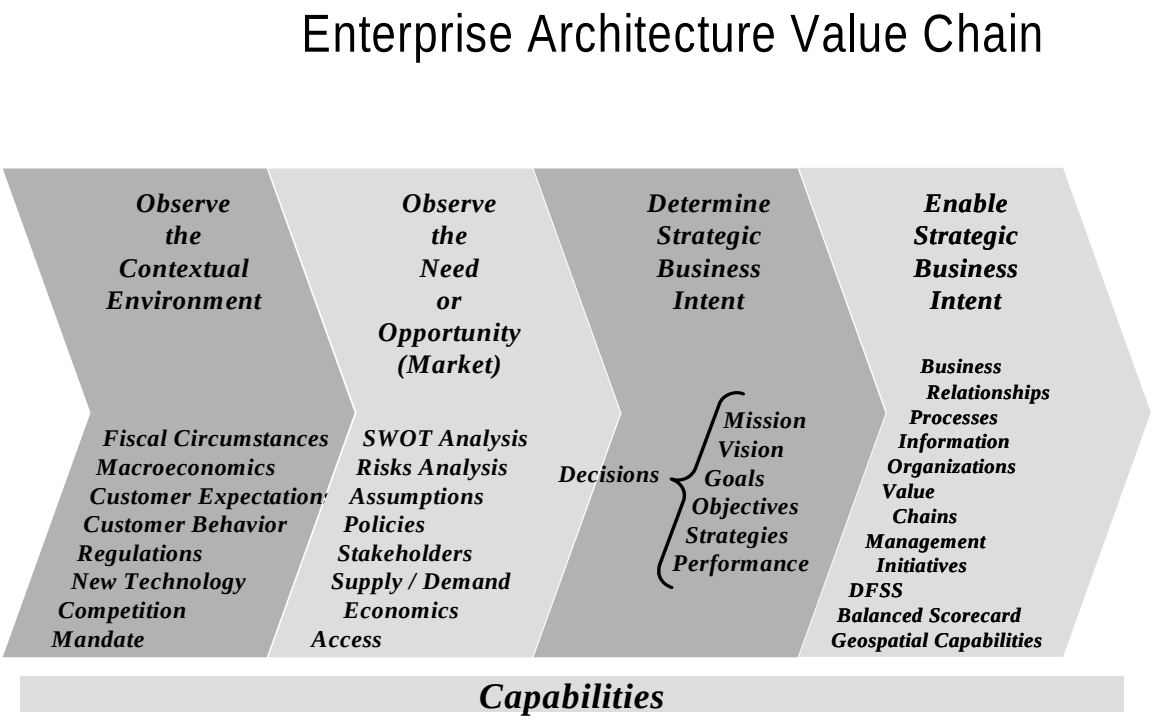
[8] 2006 Michigan IT Strategic Plan, see Appendix F "Cyber-Security," March 2006, <http://www.michigan.gov/documents/AppendixF_149547_7.pdf> and State of Montana Information Technology Strategic Plan 2006 Update, March 1, 2006, <http://itsd.mt.gov/stratplan/MT_IT_Strategic_Plan__Update_2006_Governor's_draft.doc>.

NASCIO & EA: EA is a management engineering discipline with a comprehensive view of the enterprise, including strategic planning; organization development; relationship, information and knowledge management; business process improvement, and operations. It has evolved over the last few years from IT-centric to a broader view of enabling the strategic intent of government. NASCIO's sophisticated and holistic EA program, includes a comprehensive set of publications, including an extensive toolkit and an EA business case summary. For more about NASCIO's EA efforts, please see: <http://www.nascio.org/nascioCommittees/EA/>.

The EA Value Chain--Framework for IT Security Business Cases:

NASCIO's EA Value Chain (see below) supports the development of the IT security business case and involves the following phases:

- **Observe the Contextual Environment**—Competing for funding in an environment of evermore aggressive IT security and privacy threats and the ubiquitous presence of technology in citizens' everyday lives.
- **Observe the Need or Opportunity**—Conducting an enterprise-wide IT risk assessment to determine where weaknesses in information security and privacy protections exist.
- **Determine Strategic Business Intent**—Formulating a mission and goals to address the needs or opportunities identified through the risk assessment. Many states' IT strategic plans reflect goals to protect citizen privacy and strengthen information security.
- **Enable Strategic Business Intent**—Making the IT security business case for the funding necessary to carry out the goal of securing state IT systems and protecting citizen information. States may request funding for risk assessments, processes, systems, management initiatives or training to enable the state's intent to eliminate security vulnerabilities.
- **Capabilities**: Capabilities are the underlying foundational disciplines and mechanisms that make it possible for states to carry out their strategic business intent, such as a state's business case methodology, enterprise architecture, security certification program for state IT staff, project management program or procurement processes.



NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com • W :: NASCIO.org

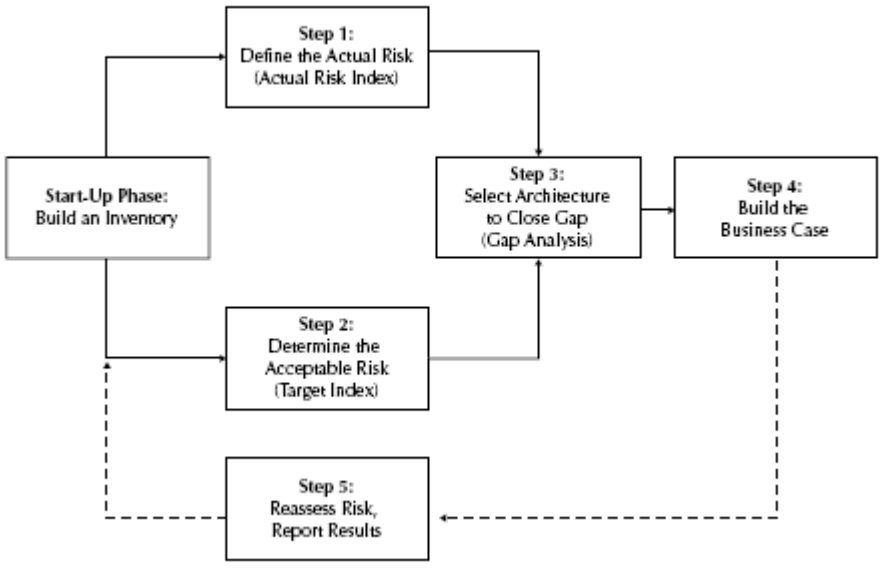
By understanding the environment and conducting an IT risk assessment to determine the state's security needs, a state can formulate its strategic business intent or goal, which will likely involve the protection of citizen privacy and information security. The IT business case then allows the state CIO to carry out the state's strategic business intent by obtaining the resources needed to protect the state's IT systems and data. Fitting a state's security program, including its business case, into its overall EA program serves to ensure that security and adequate funding are built into all stages of the system development life cycle of the state's information systems and is consistent with the federal government's approach. It also is important for agency business leaders to be at the table, because it is at the agency level where states hold vast amounts of sensitive information.

EA & A Risk-Based IT Business Case: Within this framework, the discussion below presents a strategic, risk-based approach to making the case for continued and enhanced funding for state IT security. The approach begins with an IT risk assessment to pin-point current and emerging IT security issues that need to be addressed. Identifying the gaps in IT security and assessing the risks that are associated with them can then serve as concrete support for a successful security business case. This risk-based approach recognizes the difficulties that can be posed by an approach that focuses solely on the hard-dollar return of IT investments, since such savings are often difficult to quantify. After all, the purpose of IT security is to prevent incidences, such as data breaches, that could likely cost the state substantial amounts of resources.

III. A Starting Place—The IT Risk Assessment

Ideally, the IT security business case should be based on a full risk assessment of critical-infrastructure vulnerabilities. According to an October 2002 report produced by NASCIO and the IBM Foundation for the Business of Government that is still very relevant today, a risk assessment should include a complete inventory of critical systems and assets as well as a gap analysis between the actual and ideal levels of IT security as demonstrated below.

Figure 11. Simplified Risk Assessment



"Public-Sector Information Security: A Call to Action for Public-Sector CIOs," Don Heiman, NASCIO, the IBM Business of Government series, October 2002.

Key steps in an overall risk assessment that can be used to support a business case involve the following steps:

- **Determine actual "as is" risk**—Creating an inventory, determining criticality and analyzing the number of people affected if a given asset is lost. This can be reflected in a quantitative formulation that indexes the state's current risk level.
- **Determine the target or "to be" risk**—Calculating the target index level that represents the amount of risk a state is willing to accept.
- **Determine and close the "gaps"**—Analyzing the gap between the "as is" and "to be" risk.[9]

A risk assessment may encompass many areas including the security of applications, systems, data, and networks. Physical and user security as well as security administration and social engineering/human factors may also be part of an IT risk assessment.[10]

Types of IT Risk Assessments: According to NASCIO's 2005 Compendium of Digital Government in the States, thirty-nine state CIOs responded that they offer assessments/audits of agency IT systems. Whether a self-assessment or a third-party assessment, the goal is still the same—to discover the current status of IT security and find ways to fill-in any identified security gaps.

Self-assessments: With this approach, state agencies evaluate the adequacy of their IT security measures. The assessment may be voluntary or required. The state CIO's office typically plays an important role in drafting the self-assessment form that agencies complete.

Do it Yourself—Kansas IT Risk Self-Assessment:

What the State Did: Kansas' risk assessment was instituted in 2003 by the state's IT Security Council. The Security Council developed an IT Security Self-Assessment questionnaire that addressed many facets of IT security, from management to operational to technical controls. The assessment and its various elements were drawn from many sources, including the Federal Information Security Controls Audit Manual (FISCAM) and NIST and are referenced by source for each question. In its first year, the assessment was submitted to 27 state agencies. Sixteen agencies responded on a voluntary basis. Assurance to the agencies of complete confidentiality contributed to the high response rate. Agencies were identified only as a number and all results were communicated to upper IT management on a number-only basis.

The Result: Kansas designed and developed its risk assessment as an integrated process for data acquisition, collection, summarization, and presentation of reports and charts for the Security Council to review. This has provided the Security Council with a common view of the state's IT security posture from a statewide perspective. In July 2004, the State Information Technology Executive Council (ITEC), understanding the value of the IT risk assessment, established a policy requiring the assessment to be completed on an annual basis. All agencies responded to the 2004 risk assessment. Link to risk assessment: http://www.da.ks.gov/itec/itsec/Security_SelfAssessment.doc.

[9] "Public-Sector Information Security: A Call to Action for Public-Sector CIOs," Don Heiman, NASCIO, IBM The Business of Government series, October 2002, <http://www.businessofgovernment.org/main/publications/grant_reports/details/index.asp?GID=151>.

[10] NASCIO Enterprise Architecture Development Tool-Kit, v 3.0, October 2004, <http://www.nascio.org/nascioCommittees/EA/#tool-kit>. Please see Security Domain Blueprint.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com • W :: NASCIO.org

The federal government first articulated an IT security assessment framework in 2000. It intends to take a holistic approach, giving a view of agency components as well as the entirety of each agency as a whole. The framework provides federal agencies with guidance and a template for performing and reporting IT security assessments. The framework approaches assessments using a five-level system in which an agency evaluates each asset to determine its level of IT security. The levels are as follows. At the federal level, the goal is to reach a level 4 or 5 for each IT asset, although states may find that that is not always practical or necessary:

- Level 1: Documented Policy
- Level 2: Documented Procedures for Implementing Policies
- Level 3: Implemented Procedures and Controls
- Level 4: Tested and Reviewed Procedures and Controls
- Level 5: Fully Integrated Procedures and Controls.[11]

Third-Party IT Risk Assessments: Some states choose to bring in a contractor to assist with an IT risk assessment. Below are two examples of states that have employed the assistance of a third-party to conduct their risk assessments. Of note, we have characterized the states below as "more centralized" and "federated" to illustrate the fact that risk assessments vary from state-to-state due to differences in IT governance models, organizational structure, and CIO enterprise authority. However, those characterizations are intended for illustrative purposes only. Given the variety of legal, organizational, political, and cultural differences, states are often difficult to categorize as centralized, federated or decentralized.

North Carolina—Third-Party Assessment in a More Centralized Environment:

What the State Did: Under North Carolina state law, the State CIO is responsible for assessing the ability of state agencies to comply with the state's current enterprise security standards. In 2004, the State CIO conducted such an IT risk assessment. In doing so, the state contracted with a consulting firm to manage the project, normalize the data received from agencies, and produce a draft assessment for the State CIO's review. Because of the size of the project, contractors were engaged to assess various state agencies. The contractors were not allowed to assess agencies where they had performed significant security projects in the past. The assessment was conducted with tools and templates developed by the State Information Security Office's Project Management Office (PMO), which fostered uniformity in the assessment process and consistency in the assessment results.

The Result: The assessment provided a global view of the security posture of the state's executive branch agencies and a snapshot of agency security expenditures. Important for business case purposes, the risk assessment also included specific findings in detail sufficient to permit the state to prioritize and budget for required security enhancement efforts. As a result of the assessment, the State CIO had evidence of the needs when he recommended a substantial funding increase for security.[12]

[11] "Federal Information Technology Security Assessment Framework," the National Institute of Standards and Technology (NIST), Computer Security Division, prepared for the CIO Council's, Security, Privacy and Critical Infrastructure Committee, November 28, 2000, <http://csrc.nist.gov/policies/Federal-IT-Security-Assessment-Framework.pdf>.

[12] "Summary Report: Assessment of Agency Compliance with Enterprise Security Standards," prepared by Gartner, Inc. for the North Carolina State CIO, May 2004, <http://www.iso.scio.nc.gov/pdf/SummaryReportFV02.pdf>.

Ohio—Third-Party Assessment in a Federated Environment:

What the State Did: The Ohio Office of Information Technology (OIT) recognized the need to address security from two perspectives—from the perspective of the state as an enterprise, covering all agencies, and from the perspective of OIT as the primary IT service and infrastructure provider to state agencies. This is important because, in Ohio's federated environment, OIT's role of statewide coordination and leadership for IT is balanced with the agencies' primary responsibility for the IT systems under their control. From the enterprise perspective, OIT first issued a state IT security policy that requires agencies to conduct risk assessments of their IT systems. OIT then used a third-party contractor to perform a security vulnerability assessment of the major agencies' computing and network systems. Reflecting the balance between the roles of agencies and OIT, each agency received a confidential, detailed report of its findings, while OIT received a summary of the overall findings. From the OIT perspective, the contractor was asked to perform a risk assessment related to IT security at OIT because OIT operates as an extension of agencies' IT environments by running the state's primary data center and providing a number of core infrastructure services.

The Result: The agency security vulnerability assessment helped give the agencies a picture of their security needs in light of their agency-specific risk, and it gave OIT an overall picture of the state's IT security needs. The risk assessment of OIT helped identify new initiatives that offer continuing year-over-year improvement to the state's security profile through improving OIT's architectures and systems that support critical agency services. The contractor's formal risk assessment methodology used within OIT was tailored into a process that can be repeated at OIT, and the final product also included a stand-alone guide to conducting the risk assessment methodology in and across state agencies.

Partnering with the State Auditor: Depending upon a state's political and organizational structure, partnering with the State Auditor's office may be an option for agency assessments.

Nebraska—Partnering with the State Auditor:

What the State Did: Each year, the elected Nebraska State Auditor conducts a number of financial audits of state agencies. The Auditor's Office has emphasized audits of financial IT systems. The State Auditor has contracted with an external firm to provide the technical work and provided an external risk assessment and application testing. The State CIO has participated in all appropriate aspects of the audit including the interviews with the contractor and exit interviews with the agencies as well as receiving information to identify areas that need to be addressed. This partnership, now entering its third year, provides an opportunity for the State CIO to work with both the State Auditor and the individual agencies on appropriate options for improvements or necessary changes with the input and influence of the CIO.

The Result: Agencies have observed a strengthening partnership between the Auditor and the CIO's office. This partnership has been valuable in numerous ways. Agencies are beginning to recognize that the CIO's office can be an ally in establishing "best practice" IT behaviors and operations. This is vital because there is a direct tie between the emphasis on security and the operational aspects of the state agencies. Finally, tying the results of the IT assessment to the financial audit of the agency creates a higher level of attention paid to the outcome of the IT assessment within each agency, since all audits are shared publicly by the State Auditor's Office.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com • W :: NASCIO.org

Information Obtained Through a Risk Assessment: Although the method of carrying out an IT risk assessment may vary from state-to-state, the information obtained through the assessment can be used to support the case for continued or additional IT security investment. An IT risk assessment is particularly valuable, because it identifies weaknesses and areas of lacking compliance with existing policies. It may even identify areas in which additional or revised policies are warranted. Areas of focus for Michigan's IT security assessment included:

- Agency security plans
- Audit trails
- Authorize processing (certification and accreditation)
- Contingency and disaster recovery planning
- Data integrity
- Documentation
- Enforcement
- Hardware and systems software maintenance
- Identification and authentication
- Incident response capability
- Logistical access controls
- Personnel security
- Physical security
- Production, input/output controls
- Review of security controls
- Risk management
- Security awareness, training and education.

In addition to an IT security risk assessment, scanning reports for intrusion attempts and penetration testing can provide a state with information regarding the strength of security controls and the level, nature, and source of any penetrations. Virus and other alerts from a variety of government and private sector resources can also be helpful in identifying emerging threats so that a state can make the case for a level of funding necessary to help the state prepare for the new threats it will invariably face in the future. Although much of the information gathered at the agency level may be granular in nature, the aggregated information may paint a picture that simply and clearly demonstrates the need for funding in certain areas. This information can be shared in a summary form with executive, legislative, and judicial branch officials. However, reports from the agency level may be made confidential and kept within the government community so as to avoid tipping off ill-intended parties about specific vulnerabilities. There is also a movement in some states to enact legislation that exempts such types of sensitive information from state information access or sunshine laws.

IV. Armed with Risk Assessment Information—It's Time to Make the IT Security Business Case:

With the EA Value Chain, once a risk assessment has been conducted, a state can formulate its strategic business intent--its goal to protect citizens' privacy and ensure information security. An IT security business case can then help the state to enable its goals.

IT Security Business Case Basics: While the IT security business case has nuances that distinguish it from other types of business cases, it still has many of the same overall goals as other types of business cases. Some of those common goals are:

- Ensuring the credibility of IT and the state IT organization
- Meeting constituent service needs
- Ensuring operational effectiveness and efficiency
- Supporting state policy and providing political returns and stakeholder benefits
- Ensuring enterprise value management.[13]

[13] Business Case Basics & Beyond: A Primer on State Government IT Business Cases," NASCIO, February 2003, <https://www.amrinc.net/nascio/publications/shoppingCart/index.cfm#business>.

The IT security business case can be unique in many respects. One of the most difficult aspects of making the case for IT security is that a state CIO is often asking for the expenditure of funding to prevent a security incident, such as a data breach. It can be difficult to quantify the amount of money that a data breach or other incident could cost. Therefore, it is difficult to place a hard-and-fast ROI calculation at the foundation of an IT security business case. As an alternative, this section will provide a broad range of arguments and examples of how to make the case from a risk management approach, demonstrating that it is worth the investment of funds to mitigate identified risks.

To begin to build the business case, the state CIO will need to establish the estimated cost to improve the state's security architecture and narrow the gaps in security that were identified through the state's risk assessment. For some risks, there could be the possibility of estimating the cost of not addressing the risk. If so, the CIO may choose to rely on such figures to argue that it is worth the cost to avoid certain risks. However, the more likely scenario is that such estimates are not possible. For example, it would be difficult to estimate with a sufficient level of certainty the cost of a data breach, because of the existence of so many variables, such as the type of information compromised, the number of citizens whose information was placed at risk, and the potential amount of financial exposure for citizens.

An IT security business case may support funding for a variety of items including:

- Risk assessment
- Security planning and policy
- Certification and accreditation
- Specific security controls
- Authentication or cryptographic applications
- Education, awareness and training
- System reviews/evaluations
- Contractor reviews, inspections, audits, and other evaluations
- Privacy impact assessments
- Enterprise architecture
- Oversight or compliance inspections
- Development or maintenance of agency reports and corrective action plans
- Contingency planning and testing
- Physical and environmental controls for hardware and software (perimeter defense and firewalls)
- Auditing and monitoring
- Computer security investigations and forensics
- Physical security for facilities and access controls.

The business case also can support the purchase of security products and controls, implementation of security procedures, and personnel-related costs.[14] Although there is a wide-range of items that can be included in the IT security business case, some expenses are more difficult for state CIOs to justify than others. For example, it may be easier to justify obtaining security measures that are readily visible, such as alarm systems and other types of physical security measures for state IT facilities. However, investment in other types of security, such as training and awareness, enterprise content management, and general security management, may be more difficult to justify.

[14] "Integrating IT Security into Capital Planning and Investment Control Process," the National Institute of Standards and Technology (NIST), SP 800-65, January 2005.

Don't Forget the Last Step in the Business Case Process: The last step in making the business case is to implement the measures supported by the business case, reassess their effectiveness and report the results. Arguably, this step may be the most important as the state needs to ensure that it is receiving its money's worth for the cost of securing the state IT infrastructure and resources. Moreover, the IT threat environment is constantly changing and existing security measures may need to be changed or other new initiatives may need to be implemented in order to protect the state. At this stage, the change management discipline comes into play and is vital to ensure the continuity of state operations. Note that, within the EA Value Chain, other state capabilities, such as the project management and procurement disciplines, can help to ensure the smooth realization of the state's strategic business intent to secure its IT infrastructure and systems.

The Traditional Approach to IT Security Business Cases—Demonstrating the Risks and the Consequences:

From a risk-based standpoint, it is important for the state CIO to demonstrate the existing and emerging risks to state IT and clearly show the consequences that will flow from those risks if they occur. The following is a high-level framework for presenting risk-based arguments for IT security funding. This approach tracks how Michigan used its third-party risk assessment results to construct an effective IT security business case.

#1 Demonstrate the Risks: A state can use information from its risk assessment to show quite clearly where funds need to be spent to secure the state's IT resources. Examples of the types of performance measures that might be used are:

- # of virus attacks stopped daily by firewall and intrusion detection systems
- # of hacking attacks stopped monthly.

However, other risks may be more qualitative in nature and stem from a lack of proper policies, procedures, security controls, audit trails, training of state employees and contractors or IT staffing levels.

#2 Demonstrate the Quantifiable Consequences: Some consequences may be quantifiable to an extent and may include estimates for:

- Staff hours per month needed to restore service
- Amount of dollar loss of worker productivity.

#3 Demonstrate the Other Types of Losses that May Occur: Some losses may not be quantifiable, but still should be identified. They include losses related to:

- Citizens' trust and confidence in state government
- The state's ability to deliver services
- Funds invested in the productivity of service workers and IT workers
- Funds invested in the state's online presence
- Savings from online services (especially if citizens revert to in-office or paper-based service offerings)
- Confidential data
- Data integrity
- Damage to business reputation (reputation as a state and a business partner)
- Potential monetary damages from negligence lawsuits and contract breaches
- Political fallout
- Audit findings
- Homeland security threats.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com • W :: NASCIO.org

#4 Highlight Types of Benefits of IT Security: Another way to make the IT security business case is to focus on the positives—those aspects of security that have positive results and are not just risk avoidance-focused. Some of these could be quantifiable and include:

- Reduced expected annual loss (tangible cost reduction)
- Productivity improvement for end users and IT staff (better use of IT staff)
- Added operation benefits (enables projects due to the ability to address security concerns—see next section for more about this)
- Hard cost savings from infrastructure efficiencies.

An Innovative Business Case Approach—Aligning Security with the State's Business Needs: Aligning security with a state's business needs is an important aspect of making the business case. It may be advantageous to show how improved enterprise measures can improve the protection for and reliability of critical functions of government business in the public safety, health, education, human services or financial areas. Note that this is particularly important if multiple levels of government are involved in performing the function. The approach also can be used to include security measures and enhancements as part of the budget for a new IT project or initiative. This is a particularly good approach to take when the state CIO can demonstrate that security measures will make that project possible.

V. Sustaining the Funding Efforts—Priority Action is Required

As reflected in survey after survey, IT security is always a top state CIO priority. ***In a world of pervasive technology where unplugging from it all is not a viable option, sustainable IT security also is not an option—it is a must and a constant goal of the state CIO.*** State CIOs must clearly and successfully articulate the need for IT security funding to protect against current threats and keep pace with ever-emerging security threats. It is also important to take these steps before a security breach occurs—state CIOs must be proactive and prevent security lapses that would otherwise put them quickly in reactive mode. Starting with an IT risk assessment to understand the state's security needs and using that to formulate a risk-based business case, the state CIOs will be able to present in clear terms the urgency and importance of IT security and privacy protection before it is too late and a breach puts citizen trust and state IT transformation at risk.

What CIOs Need to Know

- **The Environment:** IT security is an ever-constant priority of the state CIOs. Security drivers include the diverse and evolving IT threat environment, technology's pervasiveness, heightened citizen privacy concerns, and increasing scrutiny of state IT expenditures. The impact of the security drivers are heightened by the expansiveness of state government IT infrastructure and the fact that a security slip in one agency could have a broad impact on IT systems and information across the state government. And, even as the IT threats increase, state spending on IT security may remain at an unchanged level, making the state CIO have to protect against more threats without a commensurate increase in security resources.
- **The EA Value Chain:** Using Enterprise Architecture (EA) as a framework for constructing a risk-based IT security business case is a way of infusing structure and discipline to the process of obtaining the funding necessary to secure a state's IT infrastructure and systems. Steps provided by the EA Value Chain involve observing the contextual environment, identifying the state's IT security needs (likely using an IT risk assessment), formulating the strategic business intent to address IT

security needs, and carrying out that strategic business intent by making the case for the necessary funding and resources.

- **The Risk Assessment:** Whether performed in-house, with the assistance of a third-party contractor, or by partnering with the state auditor, an enterprise IT risk assessment is key to identifying the state's IT security needs. The risk assessment should inventory all critical state IT systems and assets and provide a gap analysis between the actual and ideal levels of IT security. The results of the risk assessment can then be used to support the state CIO's request for security funding and resources.
- **The IT Security Business Case:** The cost-benefit analysis associated with the IT security business case is made challenging because of the difficulty in calculating the potential cost of a security incident. Hence, CIOs must work in lock-step with state agency business leaders to align security with the state's business needs, showing how security can enable and even enhance the state's ability to address identified business needs and goals.

Appendix A: IT Security Business Case Resources

From NASCIO:

"Public-Sector Information Security: A Call to Action for Public-Sector CIOs," Don Heiman, NASCIO, IBM The Business of Government series, October 2002, <http://www.businessofgovernment.org/main/publications/grant_reports/details/index.asp?GID=151>.

"Business Case Basics and Beyond: A Primer on State Government IT Business Cases," Andris Ozols, NASCIO, February 2003, <https://www.amrinc.net/nascio/publications/shoppingCart/index.cfm#business>.

Other Resources:

State of Texas, Department of Information Resources, Texas Project Delivery Framework, <http://www.dir.state.tx.us/pubs/framework/index.htm>.

"Incorporating and Funding Security in Information System Investments." U.S. Office of Management and Budget (OMB), M-00-07, February 28, 2000, <http://www.whitehouse.gov/omb/memoranda/m00-07.html>.

"Making a Compelling Business Case for Investing in Information Security," Julia Allen, U.S. Computer Emergency Readiness Team (US-CERT), April 29, 2003, <http://www.cert.org/features/green/business_case.html>.

Appendix B: Risk Assessment Resources

From the States:

State of Kansas, IT Security Self-Assessment, Systems Questionnaire, <http://www.da.ks.gov/itec/itsec/Security_SelfAssessment.doc>.

State of Maine, Office of Program Evaluation and Governmental Oversight, <http://www.maine.gov/legis/opega/reports.htm>.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com • W :: NASCIO.org

State of Maryland, Standards Self-Assessment Checklist, December 2004, <http://www.dbm.maryland.gov/dbm_publishing/public_content/dbm_taxonomy/security/prevention/itsecuritypoliciesjuly2003.pdf>. *This checklist is contained in the state's Information Technology Security Policy and Standards, Version 1.2, December 2004. The checklist begins on page 27.*

State of North Carolina, Office of the State CIO, Strategic Initiatives Office, Risk Management Program, <https://rmp.scio.nc.gov/public/default.asp>.

State of North Carolina, Information Security Office, Security Assessment Webpage, <http://www.iso.scio.nc.gov/SecurityAssessment.htm>.

State of Oklahoma, Risk Assessment Statement of Work Requirements Documents, available by contacting Joe Fleckinger, Director, Information Service Division, Office of State Finance, at joe.fleckinger@osf.ok.gov.

Commonwealth of Pennsylvania, Security Assessment Toolkit (for both self or third-party risk assessments), available by contacting Robert Maley, Chief Information Security Officer, Office of Administration/Office of IT, Bureau of Enterprise Architecture, at rmaley@state.pa.us.

From the Federal Government:

"Guide for Information Security Program Assessments and System Reporting Form," Marianne Swanson, Joan Hash, Mark Wilson, and Richard Kissel, the National Institute of Standards and Technology (NIST), Special Publication 800-26, Revision 1, Initial Public Draft, August 2005, <http://csrc.nist.gov/publications/drafts/Draft-sp800-26Rev1.pdf>.

"Guide for Assessing the Security Controls in Federal Information Systems," Ron Ross, Arnold Jackson, Stu Katzke, Patricia Toth, and George Rogers, NIST, Special Publication 800-53A, Second Public Draft, April 2006, <http://csrc.ncsl.nist.gov/publications/drafts/SP800-53A-spd.pdf>.

"Federal Information Technology Security Assessment Framework," NIST, Computer Security Division, November 28, 2000, <http://csrc.nist.gov/policies/Federal-IT-Security-Assessment-Framework.pdf>.

"Security Self-Assessment Guide for Information Technology Systems," Marianne Swanson, NIST, Special Publication, 800-26, November 2001, <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>.

"Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology," Gary Stoneburner, Alice Goguen, and Alexis Feringa, NIST, Special Publication 800-30, July 2002, <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.

From Other Organizations:

CERIAS (The Center for Education and Research in Information Assurance and Security), <http://www.cerias.purdue.edu/>.

The National Association of State Auditors, Comptrollers, and Treasurers (NASACT), <www.nasact.org>.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com • W :: NASCIO.org

Appendix C: Enterprise Architecture & Other Resources

From NASCIO:

"NASCIO Enterprise Architecture Development Tool-Kit, v. 3.0," NASCIO, October 2004, <http://www.nascio.org/nascioCommittees/EA/>. See page 90 of the "Technology Architecture" section for the Security Domain Blueprint.

Other Resources:

"Mapping Your Investments to the Federal Enterprise Architecture," U.S. Office of Management and Budget presentation, August 2005, <http://www.whitehouse.gov/omb/egov/documents/Mapping_Investments.pdf>.

Federal Agency Security Program Manager's Forum, Federal Agency Security Practices, <http://www.csrc.nist.gov/fasp/index.html>.

Appendix D: Sample Business Case Elements

The following are the major facets to the federal agencies' IT business cases as specified by the U.S. Office of Management and Budget in Exhibit 300.

- Summary of spending
- Project description
- Justification
- Performance goals and measures
- Program management
- Alternatives analysis
- Risk inventory and assessment
- Acquisition strategy
- Project and funding plan
- How the IT investment supports and complies with enterprise architecture, security and privacy, and the Government Paperwork Elimination Act (GPEA).

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com • W :: NASCIO.org