DRAFT
Date of Last Revision: August 31, 2004

Nebraska Information Technology Commission
Strategic Initiatives

Strategic Plan For
Security and Business Resumption

Objectives

This initiative will define and clarify policies, standards and guidelines, and responsibilities related to the security of the state's information technology resources. Information security will serve statutory goals pertaining to government operations and public records. These include:

1. Insure continuity of government operations (Article III, Section 29 of the Nebraska Constitution; Nebraska Revised Statutes Sections 28-901 and 84-1201);
2. Protect safety and integrity of public records (Nebraska Revised Sections 28-911, 29-2391, and 84-1201);
3. Prevent unauthorized access to public records (Nebraska Revised Statutes Sections 29-319, 81-1117.02, and 84-712.02);
4. Insure proper use of communications facilities (Nebraska Revised Statutes Section 81-1117.02); and
5. Protect privacy of citizens (Nebraska Revised Statutes Section 84, Article 7).

Benefits

A strategy for security and business resumption of information technology systems is essential for meeting the statutory objectives listed above. In addition, there are several federal laws and regulations regarding privacy and security of information. These include HIPAA (Health Insurance Portability and Accountability Act), IT Requirements for Public Health Preparedness and Response for Bioterrorism (Center for Disease Control), Sarbanes-Oxley Act of 2002, Help America Vote Act of 2002 (HAVA), Graham-Leach-Bliley Act (GLBA), and the Family Education Rights and Privacy Act (FERPA).

Some of the federal laws carry substantial penalties. In particular, HIPAA imposes civil penalties of up to $25,000 per person, per year, per standard as well as criminal penalties from $50,000 and one year in prison to $250,000 and 10 years in prison (when malice, commercial advantage and personal gain are involved).

Security is also important for protecting critical systems that impact large numbers of people in the state. A few examples include:

- Unemployment assistance ($2.2 million paid out per week to 18,000 people)
- Child support ($4.4 million paid per week to 20,000 recipients)
- Medicaid claims (156,000 claims per week; $21.4 million payments per week)
- NFOCUS payments for multiple human services programs ($26 million paid each month for 185,000 cases)
- State accounting and payroll system
- Law enforcement
- Tax collection
- Homeland Security functions

The FBI conducts an annual survey of computer security issues affecting U.S. corporations, government agencies, financial institutions, medical institutions, and universities. The 2004 CSI/FBI Computer Crime and Security Survey included the following findings:

- 79% of survey participants reported one or more security incidents;
- 78% reported virus attacks;
- 59% reported insider abuse of Net access;
- 49% reported laptop/mobile theft;
- 39% reported system penetration;
- 37% reported unauthorized access to information;
- 15% reported abuse of wireless networks;
- 10% reported misuse of public web applications, and
- 7% reported web site defacement.

The 2004 survey is available at: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf.

An additional justification for attention to computer security issues is the National Strategy to Secure Cyberspace, published by the Department of Homeland Security in February 2003. One of the priorities of the national cyberstrategy is "Securing Governments' Cyberspace." The foundation for the federal government's cybersecurity includes:

- Assigning clear and unambiguous authority and responsibility for security priorities;
- Holding officials accountable for fulfilling those responsibilities, and
- Integrating security requirements into budget and capital planning processes.

The national cyberstrategy encourages state and local governments to "establish IT security programs for their departments and agencies, including awareness, audits, and standards; and to participate in the established ISACs (Information Sharing and Analysis Centers) with similar governments."

Adequate security is also essential to expansion of e-government. Surveys show that concerns about security is one reason that the public is cautious about using on-line services, especially for conducting financial transactions or providing personal information.

Current Status

Every version of the Statewide Technology Plan of the NITC has included one or more action items pertaining to security for information technology systems. Past achievements include:

- Establishing the Security Work Group, with broad representation from state government and education sectors, to provide a forum for sharing information and developing standards and guidelines. Agendas and minutes are located at: http://www.nitc.state.ne.us/tp/workgroups/security/index.htm).
- Adopting a comprehensive set of security policies in January 2001 by the NITC. These policies include: Information Security Management, Access Control, Disaster Recovery, Education, Training and Awareness, Individual Use, Network Security, and Security Breaches and Incident Reporting.
- Publishing three security handbooks tailored to security officers, IS technical staff, and the general user.
- Offering training on the use of the security handbooks.
- Developing detailed information on:
    - Incident Response and Reporting Procedures;
    - Disaster Recovery Planning Procedures;
    - Wireless Local Area Network Guidelines;
    - Remote Access Guidelines.
- Sponsoring a Security Awareness Day (July 15, 2002).

All NITC policies, handbooks, procedures and guidelines are available at: http://www.nitc.state.ne.us/standards/index.html (under Security Architecture).

In 2002, the Nebraska Emergency Management Agency (NEMA) added a provision to the State Emergency Operations Plan that requires "Each state agency and local government (to develop) a continuity of operations plan and a disaster plan for information technology." In 2003, NEMA awarded $75,000 to the Department of Administrative Services (DAS) for a "Continuity of Operations Study". DAS has contracted with a company specializing in developing business continuity plans. The outcome will be a complete business continuity plan for all divisions of DAS. It will also provide a template that can be used for other agencies. By including a 'train-the-trainer' concept as well as involving multiple agencies in the project, DAS intends to encourage development of business continuity plans in all agencies.

The NITC has also funded two security audits. In March 2004, Omnitech conducted a limited security assessment of the state's network. The external vulnerability scan identified a total of 2,720 potential vulnerabilities with the following breakdown: 91 high-risk, 640 medium risk, and 2,989 low risk. Twelve agencies had one or more high-risk vulnerabilities. Agencies are in the process of evaluating the assessments and what steps they need to take. Not all of the potential vulnerabilities can or should be removed but all of the high and medium risk vulnerabilities will be accounted for by the agency responsible for the host that is vulnerable. In 2003, the results were 3,262 potential vulnerabilities (136 high risk, 1,182 medium risk, and 1,944 low risk). Seventeen agencies last year had one or more high-risk vulnerabilities.

These summary statistics indicate some progress in reducing the number of potential vulnerabilities, but the March 2004 results underscore the need for more attention on

securing our information assets. These potential vulnerabilities may expose state government to the risk of disruption of services, legal liability, and financial loss.

Several agencies have undertaken special projects and initiatives to improve security of information technology systems. These include:

- Department of Administrative Services
  - Implemented layered security and firewall management of the state's network;
  - Developed directory services capability for better authentication and identity management;
  - Updating the disaster recovery plan for Information Management Services Division;
  - Distributing security notices from the Multi-State Information Sharing and Analysis Center to agency security contacts.
- Health and Human Services
  - Designated a security officer for information technology;
  - Implemented HIPAA Privacy and Security regulations;
  - Developing agency security policies and procedures;
- Department of Roads
  - Designated a security officer for information technology;
  - Updating the disaster recovery plan for information technology services;
  - Developing agency security policies and procedures.
- University of Nebraska
  - In collaboration with DAS-IMServices, NU is developing a shared, fast recovery capability, through mutual assistance of physically distant data centers. Fiber optic cable has been installed between the State and University.
  - Hired a University Information Security Officer
  - Work is progressing on the design and implementation of a Directory Service / Identify Management System.
  - Disaster recovery plan is going through major revisions to update and incorporate new options.
  - UN has implemented various firewalls in locations where it is needed.
  - Implemented a University-wide security focus group to share information, patch management, awareness training, incident reporting, and other educational opportunities.
  - University-wide licensing for McAffee Anti-Virus Software
  - Implemented various federally mandated regulations (HIPAA, GLBA, FERPA).
- Multiple Agencies
  - Implementing recommendations stemming from the March 2004 Network Perimeter Security Sweep.

Future

Security is a continuous effort to manage the risk to information systems. The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected. Security must be balanced against other business needs, such as providing public access or remote access to information.

The previous section demonstrates the progress that is being made. Further improvement in security and disaster recovery is needed in several areas:

- Monitor and reduce the number of vulnerabilities of computer systems;
- Provide better patch management, including enforcement of patch management policies;
- Promote survivability of systems as a security strategy;
- Demonstrate the ability to recovery critical computer systems following a disaster, including table top exercises of disaster recovery plans;
- Improve awareness on the part of users regarding security policies and sound security practices;
- Insure adequate security for wireless systems through encryption capabilities and other means;
- Deploy intrusion detection and protection technologies to protect critical infrastructure;
- Provide redundant services for critical infrastructure such as additional Internet access points;
- Plan for additional infrastructure to extend the distances for shared disaster recovery facilities.

Finding cost effective and workable solutions to these problems is essential to a good security program for state government.

Recommended Actions

(NOTE: These recommendations are still subject to change, pending additional advice from those entities that are participating in this strategic initiative.)

A. Promote disaster planning for information technology systems, in conjunction with agency business continuity plans

Disaster recovery plans for information technology must be linked to an overall agency business continuity plan. A strategy for security and business resumption must encourage completion of agency business continuity plans in order for disaster recovery plans for information technology to be effective. Because many agencies depend on DAS for networking and computing services, it is essential that DAS develop a disaster recovery plan for its facilities and services.

Actions include:

1. Conduct an “executive overview” briefing (orientation exercise) explaining the progress and current and future activities in the development of disaster recovery plans.
   a. Lead Entity: DAS – IMServices, DAS Division of Communications, and CIO
   b. Timeframe: December 31, 2004
   c. Funding: No funding required for this task

2. Encourage agencies to develop agency business continuity plans and disaster plans for information technology by seeking funding sources, providing training on developing plans, and providing technical assistance. The focus should be at the business level.
   a. Task: Identify funding sources
      (1) Lead Entity: DAS Risk Management and CIO (subject to approval by DAS)
      (2) Timeframe: November 30, 2004
      (3) Funding: No funding required for this task
   b. Task: Identify next set of agencies for developing business continuity plans
      (1) Lead Entity: DAS Risk Management and CIO (subject to approval by DAS)
      (2) Timeframe: February 1, 2004
      (3) Funding: The cost of preparing business continuity plans by agency is itemized in the DAS contract. Sources of funding have not been identified.

3. Identify and develop procedures for common elements that should be addressed in all or most business continuity plans and disaster recovery plans for information technology.
   a. Task: Investigate and communicate the availability of insurance to cover costs relating to replacement, repair and recovery services
      (1) Lead Entity: DAS Risk Management (subject to approval by DAS)
      (2) Timeframe: December 31, 2004
      (3) Funding: No funding required for this task
   b. Task: Develop and communicate policy and procedures for expedited purchasing of goods and services related to a disaster
      (1) Lead Entity: DAS Materiel with DAS IMServices as a critical stakeholder (subject to approval by DAS)
      (2) Timeframe: March 31, 2005
      (3) Funding: No funding required for this task
   c. Task: Investigate and document arrangements with major vendors for rapid response in replacing information technology equipment and software
      (1) Lead Entity: DAS IMServices
      (2) Timeframe: June 30, 2005
      (3) Funding: No funding required for this task

B. Implement shared disaster recovery facilities

Mission critical systems have three common requirements. Recovery times must be measured in hours, not days or weeks. Recovery facilities should be physically separated so that they will not be affected by a single disaster. There must be staff available to assist with the recovery efforts. Achieving these requirements is very expensive. Sharing disaster recovery facilities, and establishing a collaborative approach to disaster recovery is one strategy for managing costs. DAS IMServices and the University of Nebraska are jointly developing a fast recovery capability using mutual assistance of physically separated data centers

Actions include:

1. Develop a shared recovery capacity serving state government and the University of Nebraska.
   a. Lead Entity: DAS IMServices and NU
   b. Timeframe: ongoing
   c. Funding: The cost and source of funding have not been determined.
2. Evaluate feasibility of additional infrastructure to extend the distances for shared disaster recovery facilities.
   a. Lead Entity: DAS IMServices and NU
   b. Timeframe: ongoing
   c. Funding: The cost and source of funding have not been determined.
3. Conduct a briefing for state agency information technology staff (orientation exercise) describing the disaster recovery activities that will be performed by IMServices and the disaster recovery testing that has been completed.
   a. Lead Entity: DAS IMServices
   b. Timeframe: March 31, 2005
   c. Funding: No funding required for this task.

C. Encourage testing and updating of disaster plans

Testing is the only way to insure that a disaster recovery plan is adequate and the organization is able to implement its plan.

Actions include:

1. Evaluate current status of testing and recommend testing strategies for different kinds of systems
   a. Lead Entity: CIO
   b. Timeframe: June 30, 2005
   c. Funding: No funding required for this task.

D. Conduct annual independent security audits

In the latest computer crime survey by the FBI, 82 percent of respondents indicated that their organizations conduct security audits. Multiple federal programs require periodic computer security audits, including HIPAA, HAVA, and Bioterrorism grants from the Center for Disease Control. Computer security audits are a widely accepted best practice across the public and private sector.

Actions include:

1. Request funding for the CIO to contract for security audits.
   a. Lead Entity: CIO
   b. Timeframe: September 1, 2004
   c. Funding: No funding required for this task
2. Investigate opportunities for aggregating efforts of several state agencies that face federal requirements for security audits.
   a. Lead Entity: CIO
   b. Timeframe: November 1, 2004 (and on-going)
   c. Funding: No funding required for this task
3. Prepare RFP and Scope of Work

a. Lead Entity: CIO (with assistance from Security Work Group)
b. Timeframe: January 31, 2005
c. Funding: If technical assistance is required for preparing the RFP, the cost will be paid either from the NITC grant or the budget of the Office of the CIO.

4. Conduct 2005 Security Audit
   a. Lead Entity: CIO
   b. Timeframe: April 30, 2005
   c. Funding: A grant application is pending before the NITC. The CIO is requesting funding for annual security audits as part of the FY2006 / FY2007 budget request.

E. Implement centralized directory services

An analysis of security risks identified the need for an Enterprise Directory that provides identity management, single sign on, and role-based/policy-based authorization. In response to this need, IMServices is now implementing a directory services system that will be available to all agencies. Under the direction of the CIO and the NITC, a Work Group was established to make recommendations regarding business rules, polices and procedures for implementation. The system will provide single (or reduced) sign-on using role based authentication and authorization

Actions include:

1) Establish an authentication standard to be submitted to the NITC to seek approval by the March 2005 meeting
   a) Propose standard to State Government Council
      - Lead Entity: IMServices
      - Timeframe: September 16, 2004 meeting
      - Funding: No funding required for this task
   b) Propose standard to NITC Technical Panel
      - Lead Entity: IMServices
      - Timeframe: December 14, 2004 meeting
      - Funding: No funding required for this task

2) Content Management offerings to customers
   a) Provide Role-based content management based upon folders (for IMS pilot)
      - Lead Entity: IMServices
      - Timeframe: October 31, 2004
      - Funding: IMServices
   b) Provide full search capabilities to IMS folders
      - Lead Entity: IMServices
      - Timeframe: October 31, 2004
      - Funding: IMServices
   c) Expand the Content Management taxonomy to other agencies -
      - Lead Entity: IMServices
      - Timeframe: January 31, 2005
      - Funding: IMServices
   d) Provide integration between content management and Microsoft Office products (Word, Excel, and PowerPoint)

- Lead Entity: IMServices
- Timeframe: January 31, 2005
- Funding: IMServices

e) Provide customized search engines based upon agency/application specific criteria
- Lead Entity: IMServices
- Timeframe: May 31, 2005
- Funding: IMServices

3) Two-factor authentication
   a) Propose standard to NITC Directory Workgroup
      - Lead Entity: IMServices
      - Timeframe: September 31, 2004 meeting
      - Funding: No funding required for this task
   b) Propose standard to SGC
      - Lead Entity: IMServices
      - Timeframe: November 18, 2004 meeting
      - Funding: No funding required for this task

4) Pilot single sign-on
   a) Provide Web-Based Single sign-on (WSSO) guideline to any client/application that desires it.
      - Lead Entity: IMServices
      - Timeframe: September 31, 2004
      - Funding: IMServices

F. Implement incident reporting requirements

Very few agencies are complying with the NITC's incident reporting requirements. Centralized reporting serves the goal of increasing awareness of vulnerabilities and threats to state government as a whole. In particular, centralized reporting is necessary to discern patterns, identify areas of vulnerability, allocate resources, and develop statewide solutions. Centralized reporting does not substitute for internal reporting to management, reporting to law enforcement, or mobilizing a computer security incident response team (CSiRT). Agencies should develop procedures for internal and external reporting that will meet the needs of centralized reporting with little or no additional work.

Actions include:

1. Review incident reporting procedures to determine need for changes in what is reported and the reporting requirements.
   a. Lead Entity: CIO
   b. Timeframe: December 31, 2004
   c. Funding: No funding required for this task

2. Communicate reporting requirements to agencies.
   a. Lead Entity: CIO
   b. Timeframe: March 31, 2005
   c. Funding: No funding required for this task

G. Network Security and Network Management

DAS Division of Communications (DOC) has made changes to implement a layered approach to network security. DOC and many agencies have focused more attention on network management, including patch management, virus protection, and intrusion detection.

Actions include:

1. Configure all assets behind the state's firewall system
   a. Lead Entity: DOC
   b. Timeframe: December 31, 2004
   c. Funding: DOC
2. Implement intrusion detection and prevention
   a. Lead Entity: DOC
   b. Timeframe: March 31, 2005
   c. Funding: DOC
3. Improve VPN capabilities
   a. Lead Entity: DOC
   b. Timeframe: March 31, 2005
   c. Funding: DOC
4. Provide encryption across the state's Wide Area Network
   a. Lead Entity: DOC
   b. Timeframe: December 31, 2004
   c. Funding: DOC