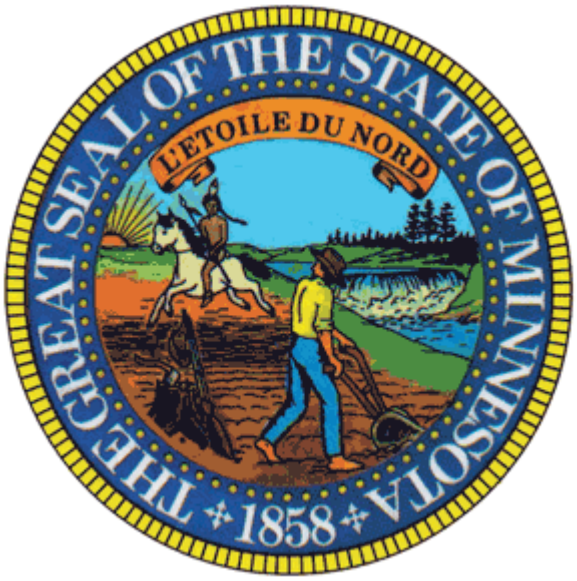
State of Minnesota



Enterprise Security Strategic Plan

Fiscal Years 2009 – 2013

Jointly Prepared By:
Office of Enterprise Technology - Enterprise Security Office
Members of the Information Security Council

State of Minnesota
Enterprise Security Strategic Plan

Contents

Executive Summary

We are pleased to present the first Enterprise Security Strategic Plan for the State of Minnesota. This plan sets priorities for management, control, and protection of the state's information assets.

The 5 year vision includes 19 high-level **strategic objectives** (see chapter 3), grouped into the following 3 categories:

- **Improved situational awareness**, which includes continuous system monitoring and continuous assessment of controls
- **Proactive risk management**, such as solidly articulated requirements and ongoing security training
- **Robust crisis and security incident management**, which allows critical services to continue uninterrupted in a crisis.

This plan also outlines 8 **key initiatives** (see chapter 4) that have been prioritized for delivery during the ensuring 2 years:

- **Security Information and Event Management**: provide enterprise-wide security monitoring
- **Enterprise Vulnerability and Threat Management**: provide ongoing vulnerability assessments of all information technology assets
- **Baseline Policies, Procedures, and Standards**: complete enterprise security policy and standard framework
- **Security Awareness for Employees**: ongoing and comprehensive security awareness program for all state employees
- **Security Awareness for Government Leaders**: annual security awareness event for government leaders and policymakers
- **Identity and Access Management**: centralized and streamlined access control solution for state government
- **Enterprise Business Continuity Program**: ongoing continuity program to address unanticipated disruptions to government services
- **Enterprise Security Incident Management**: enterprise-wide approach to record, identify, and manage information security incidents

Strong executive commitment and support are crucial to the implementation of this plan. We ask that you, as government leaders and policymakers, commit to partner with us in effective problem solving, and be our champions at the highest levels. Successful implementation will ensure information is both protected and available, and that critical government services are available when needed.

Chapter 1 - Introduction

The State of Minnesota recognizes that information is a critical asset. How information is managed, controlled, and protected has a significant impact on the delivery of state services and on the trust instilled in the users of those services. Information assets, including those held in trust, must be protected from unauthorized disclosure, theft, loss, destruction, and alteration. Information assets must be available when needed, particularly during emergencies and times of crisis.

The State of Minnesota's decentralized information technology environment is inherently difficult to secure. Most state agencies still operate their own data centers. Furthermore, the state has not defined or enforced standards limiting the diversity of hardware and software products. In testimony, the Legislative Auditor pointed to undue complexity as a primary factor for the large number of information security audit findings. Current data center consolidation initiatives will simplify the state's information technology environment, making it easier to secure. However, data center consolidation plans are complex and take many years to implement.

The rapidly expanding use of the internet has increased the need for connectivity between government entities, third parties, and users of state services. This increase in connectivity has increased the state's risk posture and made it more difficult to protect information. Cyber crime has skyrocketed over the past few years, shifting from crimes of notoriety to far more serious crimes for financial gain. Attackers have become much more sophisticated in perpetrating and concealing cyber crimes, typically operating in stealth mode with a goal of avoiding detection altogether.

This document is the first enterprise-wide information security strategic plan for the State of Minnesota. It sets priorities for how the enterprise can efficiently and effectively address the management, control, and protection of the state's information assets. It outlines the state's security community's five year vision, articulated as 19 high-level ***Strategic Objectives,*** grouped into three categories.

There are significant gaps between where the state's security community is today and the five year vision. The importance of the strategic objectives was assessed, prioritizing the gaps. The results of this assessment are summarized as ***Key Initiatives***; a two year strategic plan. A set of business and tactical plans detailing the deliverables necessary to achieve the key initiatives are maintained separately.

Figure 1
Security Strategy Alignment

As depicted in Figure 1, this plan attempts to align information security strategic objectives with broader government technology and business strategies. When developing this plan, the strategies outlined in the State of Minnesota Information Technology Master Plan and the 2005 Drive to Excellence Transformation Roadmap were incorporated.

This plan incorporates core information security requirements that must be in place to accomplish major government initiatives efficiently and effectively. These initiatives include data center consolidation and the development of major government business applications, such as the new accounting and procurement system, and centralized electronic licensing.

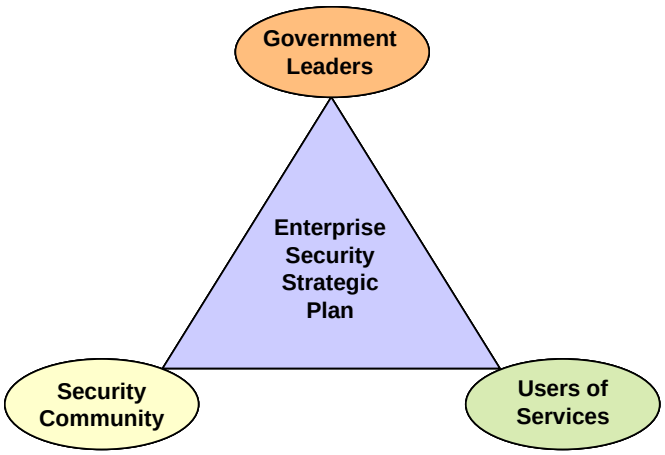
Finally, this plan incorporates global trends, such as:

- More stringent regulatory requirements pertaining to information security
- Increasing sophistication of criminals and politically motivated attackers
- New demands to access data and services through web applications and mobile devices (i.e., laptops, mobile-phones)
- New demands to share data across multiple organizations
- Intense pressure to reduce costs
- A shift from long-term employees to a more temporary and mobile workforce
- The expanding use of software as a service

Stakeholders

Government leaders and policymakers are the primary audience of this plan. From an information security perspective, they need to know the current state, the future vision, and the task necessary to bridge the gap. Achieving the strategic objectives will not be possible without strong executive

Figure 2
Strategic Plan Primary Stakeholders



commitment. Government leaders and policymakers must understand and have confidence in this plan. They must become problem-solving partners by committing resources and helping to remove barriers that impede progress.

The security community itself is also a key audience of this plan. In the past, each government entity was forced to address information security issues on its own. This approach has fostered an environment where critical security duties are simply not done at many government entities. By joining forces to establish a common vision, the security community can ensure that all entities have appropriate information security controls, and can deploy those controls cost effectively.

Finally, business partners and citizens – the end users of government services – have a vested interest in the success of this plan. End users of government services need to have complete confidence that government entities will protect their data from unauthorized disclosure. End users must be confident that critical government services will be available when needed, particularly during times of crisis. Developing this plan demonstrates due diligence to the people and businesses who rely on government services.

Plan Navigation

The plan is organized into three sections:

- **Chapter 2 – Mission and Underlying Core Values** discusses the mission of the Enterprise Security Program, as defined by the security community. It also outlines the core values of a security program necessary to drive the strategic security outcomes in this document.

- **Chapter 3 – Strategic Outcomes** lists the 19 high-level objectives for the State of Minnesota, segregated into three broad categories: Improved Situational Awareness, Robust Crisis and Security Incident Management, and Proactive Risk Management.

- **Chapter 4 – Key Initiatives** discusses the highest-priority projects that the security community hopes to accomplish during the current biennium. Additional details concerning these projects can be seen in the separate Enterprise Security Tactical Plan.

Governance

The State Chief Information Security Officer will lead the effort to deliver the objectives in this plan. To be successful, the State Chief Information Security Officer must align and coordinate agency resources with those in Enterprise Security Office, a part of the Office of Enterprise Technology. Furthermore, these coordinated security efforts must be vetted by all impacted stakeholders through an agreed upon governance process.

Though the governance process is still evolving, current stakeholders that participate in the decision-making process include:

- **State Chief Information Officer.** Under state law, the State Chief Information Officer is responsible for the overall management, direction, and security of the state's information assets.
- **State Chief Information Security Officer.** The State Chief Information Security Officer has delegated authority and is responsible for planning, developing, and deploying the Enterprise Security Program.
- **Information Security Council.** Agency security professionals who comprise the council serve as advisors to the State Chief Information Security Officer. These professionals are responsible for helping develop the enterprise-wide security strategies. They help craft the policies, standards, and systems to achieve the strategic objectives.
- **Chief Information Officer Advisory Council.** This council represents the government technology community as a whole. It is responsible for making sure that security efforts align with and support broader government technology and business initiatives.
- **Commissioners Technology Advisory Board.** This board represents leaders at the highest level in state government, ensuring buy-in and support for enterprise-wide projects and security efforts.

Chapter 2 – Mission and Underlying Core Values

The State of Minnesota's Enterprise Security Program began in June 2006 with the hiring of the first Chief Information Security Officer in the Office of Enterprise Technology. To advance enterprise security, the Chief Information Security Officer promptly established the Information Security Council, an advisory body to help plan, develop, and implement the new program.

With help from the Information Security Council, the Chief Information Security Officer worked to create the following **mission** for the Enterprise Security Program:

> *"The Enterprise Security Program exists to support the efficient delivery of services to government entities and their customers; through a sustainable information security program.*
>
> *The program will accomplish its mission through enterprise information security policies, standards, guidelines, and services that protect the state's information assets and the security interests of the users of state services."*

The security community also agreed on eight core values as a foundation for the new Enterprise Security Program. The program must:

- have an increased focus on security planning activities.
- be comprehensive, clearly outlining the baseline requirements that all agencies must follow.
- ensure that important security decisions are made by people best suited to make those decisions.
- have broad-based support from people who will be expected to implement the provisions.
- be championed by government leaders at the highest levels.
- be supported by appropriate resources, including technical tools, training, and people.
- take advantage of the size of government to leverage financial and human resources to be cost effective.
- include methods to ensure compliance with baseline security requirements.

With this foundation in place, the security community began the difficult task of defining, vetting, and prioritizing long-term security strategies for the State of Minnesota. The result of this effort can be seen in the following chapter.

Chapter 3 - Strategic Outcomes

The high-level strategies outlined in this chapter collectively define where the State of Minnesota needs to be to appropriately manage cyber security risks. The security community believes that it will take at least five years to achieve these strategic outcomes, assuming that there will be sufficient resources for people, processes, and tools. Absent the necessary resources, the strategic outcomes will not change, however, the timeframe to achieve the outcomes will be extended.

The strategic outcomes can be classified into three broad categories:

- **Improved Situational Awareness (Table 1)** – Outcomes in this category will help the state obtain a better understanding of its risk posture. They also will give the state the ability to measure its risk posture with rigorous performance metrics.
- **Proactive Risk Management (Table 2)** – Outcomes in this category will make employees and government leaders more aware of security threats. Also, they will garner the executive support needed for Enterprise Security Program to thrive long-term. Finally, they include various types of preventive controls.
- **Robust Crisis and Security Incident Management (Table 3)** – Outcomes in this category will help the state manage security events more efficiently and effectively, thereby minimizing damage.

Table 1
Improved Situational Awareness

Strategic Outcome Description	Current Biennium Priority
All state computer systems are continuously monitored for adverse information security events.	Yes
Information security controls are continuously assessed for effectiveness.	
Key performance indicators are used to measure the information security program's effectiveness.	
The state has a consolidated and reportable information security risk profile.	

Table 2
Proactive Risk Management

Strategic Outcome Description	Current Biennium Priority
Government leaders at the highest levels understand and support the information security program.	Yes
All state employees receive ongoing security training appropriate to their job duties.	Yes
Information security program requirements are clearly articulated in a framework of policies, procedures, and standards.	Yes
Established relationships between state, local, and federal government entities permit shared security solutions that span traditional parochial boundaries.	
Stakeholders participate in the design and implementation of information security solutions.	
The state attracts, develops, and retains professionals with the appropriate security skills.	
Exploitable technical vulnerabilities in state computer systems are promptly identified and remediated.	Yes
Information security controls adapt rapidly to changing risk conditions.	
People and entities that conduct business with state government have appropriate and timely access to the necessary computer resources and data.	Yes
State computer resources and data are protected from being used or accessed inappropriately.	Yes
Government entities comply with the information security program and other externally mandated compliance requirements.	
Government entities, regardless of size, are supported by security professionals and engaged in the information security program.	
The Office of Enterprise Technology serves as a leader by setting high standards for excellence in information security.	Yes

Table 3
Robust Crisis and Security Incident Management

Strategic Outcome Description	**Current Biennium Priority**
When information security incidents occur, government entities promptly contain, remediate, and manage those incidents.	Yes
Mission-critical services will continue in the event of a crisis.	Yes

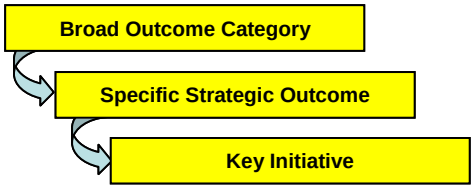
Chapter 4 - Key Initiatives

The Enterprise Security Office and the Information Security Council identified certain security outcomes and specific projects as "high priority." In general, these are areas where our current security controls are lax or have not been applied consistently across the enterprise, resulting in an unacceptable level of risk. In many cases, the security community has developed formal projects to address pressing concerns. In others, security projects are still in the planning stages.

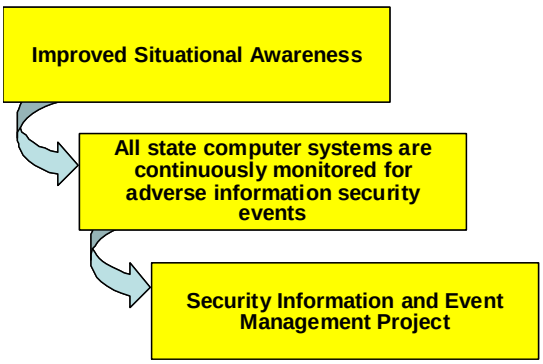
This chapter outlines security projects that the security community believes are high priority. It is not a complete inventory of the work being done by the security community. Rather, it is list of a key initiatives that are planned or are currently under way to address the most pressing risks. Additional details about each key initiative can be found in the Enterprise Security Tactical Plan.

It is important to demonstrate the linkage between key initiatives, long-term strategic outcomes, and the broader strategic outcome categories. Therefore, included with each key initiative in this chapter is a graphic. Figure 3 illustrates the one-to-many relationship between broad strategic outcome categories, specific strategic outcomes, and key initiatives.

Figure 3
Linking Key Initiatives to Outcomes



Initiative #1 – Security Information and Event Management

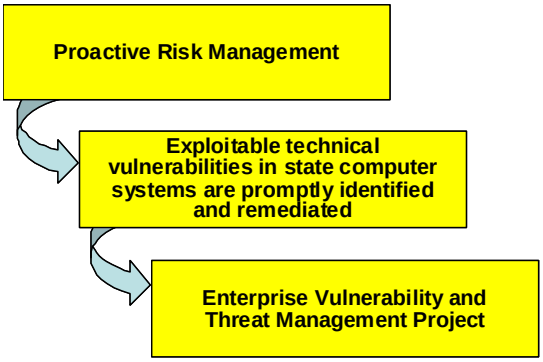


Description: Central system to provide enterprise-wide security monitoring

Key Benefits:

- Improved ability to identify complex cyber attacks
- Reduced time and cost to investigate security incidents
- Consistent and robust monitoring of all agencies, including those with limited resources

Initiative #2 – Enterprise Vulnerability and Threat Management

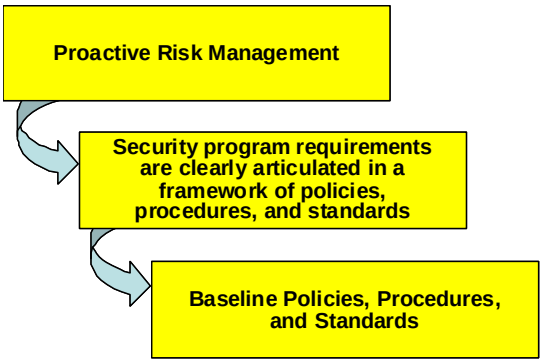


Description: Central system to provide ongoing vulnerability assessments of all information technology assets

Key Benefits:

- State finds and remediates problems before they are exploited by hackers
- Inventory created of all technology assets
- Services offered to all agencies, including those with limited resources

Initiative #3 – Baseline Policies, Procedures, and Standards



Description: Complete enterprise security policy and standard framework

Key Benefits:

- Clear security baselines for all government entities
- Policy-based foundation to measure results
- Consistent application of security controls across the enterprise

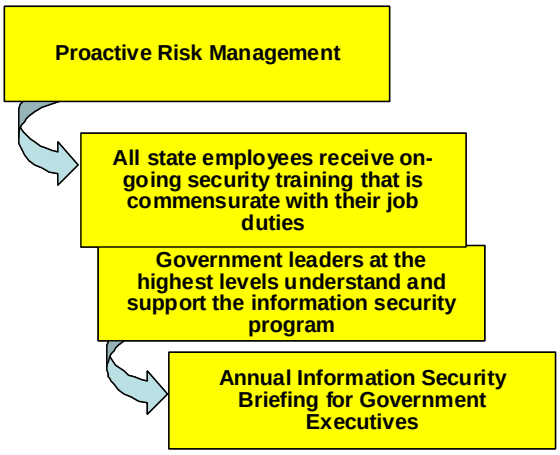
Initiative #4 – Security Awareness for Employees

Description: Ongoing and comprehensive security awareness program for all state employees

Key Benefits:

- Better awareness of security threats capable of impacting government operations
- Fewer security incidents caused by employee mistakes
- Common baseline of knowledge for all employees

Initiative #5 – Security Awareness for Government Leaders

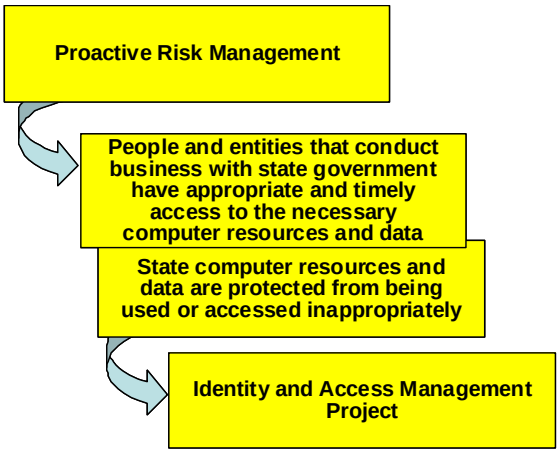


Description: Annual security awareness event for government leaders and policymakers

Key Benefits:

- Clear understanding of all enterprise security initiatives
- Overview of significant information security threats
- Support for the Enterprise Security Program

Initiative #6 – Identity and Access Management

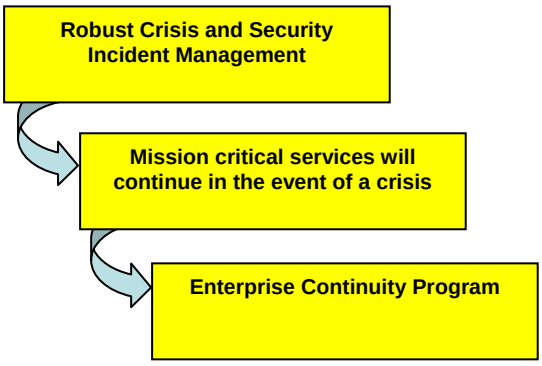


Description: Centralized and streamlined access control solution for state government

Key Benefits:

- Better security through uniform and repeatable access control processes
- Better experience for users of state services by providing all access through a single user ID and password
- Reduced costs to develop new government systems by leveraging an external access control solution

Initiative #7 – Enterprise Business Continuity Program

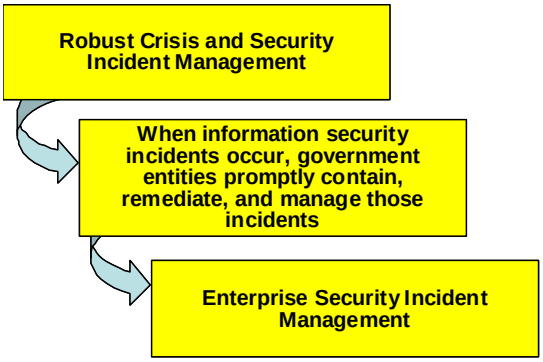


Description: Ongoing continuity program to address unanticipated disruptions to government services

Key Benefits:

- Faster recovery of critical government services during a crisis
- Reduced costs through leveraging shared recovery environment
- Better ability to share staff during times of crisis through adoption of a common plan format and tools

Initiative #8 – Enterprise Security Incident Management



Description: Enterprise-wide approach to record, identify, and manage information security incidents

Key Benefits:

- Ability to limit damage through information sharing
- Fewer cross-agency infections
- Reduced costs through the sharing of staff and expensive forensic investigation tools