Comprehensive Information Security Funding Strategy

March 15, 2010

Table of Contents

Executive Summary 3

CHAPTER 1 – Introduction 5

CHAPTER 2 – Program Costs 8

CHAPTER 3 – Funding Sources 11

CHAPTER 4 – Service Management 15

APPENDIX A 16

- **Detailed Security Service Descriptions** 16
- **Information Security Portfolio Management** 17
- **Information Security Risk Management** 18
- **Policies and Standards Management** 19
- **Information Security Architecture** 20
- **Security Awareness** 21
- **Access Management** 22
- **Intrusion Monitoring** 23
- **Malicious Program Detection** 24
- **Security Information Management** 25
- **Vulnerability Management** 26
- **Threat Management** 27
- **Security Incident Response and Forensics** 28
- **Information Asset Management** 29
- **Physical Security** 30
- **Business Continuity** 31
- **Data Privacy** 32

Appendix B 33

Appendix C 35

Executive Summary

This Comprehensive Information Security Funding Strategy Report is submitted by the Office of Enterprise Technology (OET) in response to the 2009 legislative requirement (MN Laws 2009, Chapter 101, Article 1, Section 10) to prepare a funding strategy for the State's Enterprise Security Program.

Since it was created in 2006, the Enterprise Security Office has worked diligently to create an effective statewide Enterprise Security Program, directing its limited resources toward the crucial building blocks – strategic planning and enterprise policy development - that make possible a more comprehensive, long-term program. The program has also purchased and piloted some, but not all, of the key technical tools necessary to protect the State's digital infrastructure and the data upon which government depends.

Through strong governance and a spirit of collaboration among the state agencies that collectively comprise our most important lines of defense, the Enterprise Security Program has laid the necessary foundation for security measures that will maintain a reasonable level of risk to our systems and information in a world where cyber threats continue to grow at an alarming pace.

Now the hard work of implementing the policies and deploying the tools begins.

While the overarching focus of this report is on the financial structure necessary to provide adequate protection to the State's information technology resources, the report also identifies the core focus areas that comprise a robust program, and outlines the challenges – financial and otherwise – that face us.

Funding Strategy Recommendation: Funding for executive branch security currently comes from two sources – a general fund appropriation to the Office of Enterprise Technology ($4.2 million) and resource allocations within individual agencies (an estimated $4 million). To continue the progress now being made, the report recommends that:

- The State continues the existing general fund appropriation as the primary funding source for shared executive branch security services. This is the most efficient and equitable way to share costs. Generally funded costs are recovered through the statewide indirect cost process, which allocates costs to all fund types. Currently this allocation method is based on the percentage of total IT dollars spent per agency. The resulting recoveries are deposited back into the general fund as non-dedicated revenue.
- Any expansion of security services beyond the executive branch should be funded through charges to entities, based on use. Appendix A outlines the individual security services and their underlying costs, upon which fees for service would be based.
- Absent general funding, OET recommends accounting for Enterprise Security Program costs and recoveries in the enterprise technology fund. Under this alternate approach, the costs would be allocated to all agencies based on their percentage of the total statewide IT expenditures. Table 3-2 lists the potential allocation percentages for the largest executive branch agencies.

Additional Recommendations

1. **Program Elements**: Sixteen core security services need to be provided to align the security program with generally accepted best practices and meet legal compliance requirements. The services range from foundational governance activities, such as development of baseline policies and standards, to detailed technical services, such as continuous vulnerability management.

   The estimated annual cost for the full program outlined in this report - if there is no consolidation of the overall IT infrastructure (see recommendation #4) - is approximately $19 million. This is more than twice the current combined expenditure within the executive branch. However, in light of the current fiscal crisis, this report does not recommend an increase in overall security expenditures at this time.

2. **Service Management**: This report recommends a "hybrid" approach to the management of security services, centralizing most of the security functions in a manner that maximizes resources, while maintaining some localized staff and activity to ensure that the systems and data within individual agency environments remain secured.

3. **Service Scope**: The report assumes that security services will be provided to 77 executive branch entities. However, many of the outlined security services can be extended very cost-effectively to other government entities as well. Providing centralized and standardized security services beyond the executive branch to other branches of state and local government can improve the security of shared infrastructure such as the state network and may, in fact, bring down the per-entity cost to the State of a standardized security environment.

4. **Streamlining to Bring Down Costs and Improve Security**: Improvements to the executive branch's overall IT environment would significantly improve the security profile of the State and make appropriate levels of risk far more affordable. In particular,

   - The current decentralized information technology environment is inherently difficult and costly to secure. Consolidating technology operations into two data centers will reduce the amount that needs to be spent on security *by about $4 million annually,* reducing the overall anticipated cost from $19 million to $15 million.

Conclusion

Effective security policy is about managing risk. The State of Minnesota – or any other public or private organization – can never afford or create a completely risk-free IT environment, particularly as new technologies proliferate and cyber threats mushroom. Protecting our digital infrastructure at a reasonable level of risk must be the goal, one that we can only reach through prudent investments, shared resources and effective management.

Presently, the State faces a high level of risk due to lax security controls and an inadequate investment in tools, people and processes. At its current funding level, the State's investment in security stands at 2 percent of its total IT budget, compared to an industry standard of 5.4 percent - 6.2 percent. The result is a litany of Legislative Audit reports that highlight our vulnerability:

> *"The State of Minnesota does not have adequate continuity of operations plans to ensure the timely recovery of critical services and operations in the event of a disruption."*
>
> *State of Minnesota Continuity of Operations Plans*
> *Report 08-07, March 2008*
>
> *"Small agencies in Minnesota state government generally do not have adequate security controls over their computer systems, which creates an unacceptable risk of unauthorized access to not public data and disruption to state functions."*
>
> *Small Agencies' Information Security Controls*
> *Report 09-16, April 2009*

This report outlines the best route to bringing Minnesota's investment closer to the norm and our risks to a more acceptable level. In the process, we equitably share the costs of ensuring that our physical and digital resources are protected, government services remain operative, and we maintain the trust of Minnesota's citizens, whose data and lives we hold in trust.

CHAPTER 1 – Introduction

The threat landscape is worsening.

The current rate of technology advances and mobile tools increase citizens' demand for continuous access to online government services. The rapidly expanding use of the Internet has increased connectivity between government entities, third parties, and users of state services, and has created a more "open government." However, the increase in connectivity and reliance on information systems by agencies also increases the State's risk posture, making 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. The December 2008 Cyberspace Policy Review by the Commission on Cybersecurity for the 44th Presidency states the challenge plainly: "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration."

The State responds.

Established in 2006, the Office of Enterprise Technology's Enterprise Security Office (ESO) has the responsibility to "ensure overall security of the state's information and technology systems and services." *(Minnesota Statutes, Section 16E.01)* The ESO uses a multi-pronged approach that combines preventative and reactive strategies to keep our IT assets safe:

Policy and planning: Setting clear enterprise-wide standards and policies that protect our assets and lessen the likelihood of attacks.

Architecture: "Baking" security tools and best practices into new systems that we build and buy.

Security tools: Developing a shared toolset that isolates vulnerabilities, monitors systems, detects and neutralizes attacks, and conducts forensics.

Education: Training users about cyber dangers and the best practices that keep us out of trouble.

Practice: Practicing recovery plans so that government business is uninterrupted in case of attack or disaster.

The State's current activity level and progress made in these five areas is outlined in Appendix C.

We must move forward, even in uncertain times.

The 2009 Legislature (MN Laws 2009, Chapter 101, Article 1, Section 10) required the Office of Enterprise Technology (OET) to prepare a funding strategy to stabilize and continue the important work of the State's Enterprise Security Program. This Comprehensive Information Security Funding Strategy Report is submitted in response to that request.

To develop this report, OET worked closely with state agencies and various established IT governance bodies in order to gain an understanding of their information security needs and capabilities. OET also surveyed other state governments and sought the advice of outside experts with extensive information security experience, including the implementation of a security program for a local Fortune 100 company.

Although the resulting report specifically deals with the costs and funding of enterprise security, OET first needed to answer a series of foundational service questions:

1. *What information security services must be provided to align with generally accepted best practices and meet legal compliance requirements?*

Sixteen core security services comprise the comprehensive security program. They range from foundational governance activities to detailed technical services, such as continuous vulnerability management. These services are detailed in Appendix A, and include:

- Security Portfolio Management
- Risk Management
- Standards & Policy
- Security Architecture
- Security Awareness & Training
- Access Management
- Intrusion Monitoring
- Malicious Program Detection
- Security Information Management
- Vulnerability Management
- Incident Response & Forensics
- Threat Management
- Asset Management
- Physical Security
- Business Continuity
- Data Privacy

2. *Which government entities should be the beneficiaries of these services?*

The report assumes that security services will be provided to 77 executive branch entities. However, it is important to note that many of the 16 security services outlined in this report can be extended very cost-effectively to other government entities as well. Since its inception in late 2006, the Enterprise Security Program has been inundated by calls from counties and other government entities that need help addressing complex cyber security threats. Appendix B specifies the program's current scope as well as the entities outside the executive branch that could leverage investments made by the Enterprise Security Program.

3. *What is the best way to manage security services?*

The historical decentralized approach to information security has not worked. For years, each state agency was forced to address information security risks on its own. This approach has resulted in a decentralized environment in which important security duties are either performed inconsistently or, due to resource constraints, not at all.

The Office of the Legislative Auditor's information security audit work affirms the inadequate current state of information security controls and the inherent deficiencies in a decentralized environment. The ongoing array of deficient audit reports paint a clear picture that the historical strategy of addressing cyber security threats agency-by-agency has not worked.

The Enterprise Security Program was created in 2006 to remedy these shortcomings. Under the leadership of our State's first Chief Information Security Officer, OET has embarked on a multi-year plan to improve security and more effectively leverage resources. However, cost figures in this report reflect the fact that the State of Minnesota has historically underfunded information security and that there is a large backlog of work to be done.

The most important success factor going forward will be how well we share the limited resources available today – including people, processes, and tools.

This plan proposes a primarily centralized security structure in which financial and human resources are consolidated, but sufficient agency presence is maintained in order to ensure the security of individual systems and environments.

CHAPTER 2 – Program Costs

Chapter Conclusion

The annual cost to deliver comprehensive information security services to the executive branch is projected to be about $19 million. This is more than twice the current investment.

Given the current budget crisis, OET recommends continuing the existing $4.2 million general fund investment, which will allow the Enterprise Security Program to keep making progress until the State is in a better financial position.

The current decentralized information technology environment is inherently difficult and costly to secure. Consolidating technology operations into two data centers will reduce the projected security costs by about $4 million annually, from $19 million to $15 million.

The amount spent today on information security in Minnesota state government falls well below industry norms. Though it is difficult to compile exact figures, we estimate that Minnesota's executive branch spends about 2 percent of its total information technology budget on information security. The industry standard is much higher, ranging from 5.4 percent - 6.2 percent (Table 2-1).

OET estimates an annual cost of $19 million per year to fully deliver people, processes and tools for services in the comprehensive program represented by the services in Appendix A. The estimate is based on the cost to secure the decentralized IT environment we have today.

This full funding would increase the percentage the State spends on security to about 4.7 percent of the total information technology budget – still less than industry standards, but more appropriate to address the State's serious security challenges and to reach an acceptable level of risk.

Table 2-1: Proposed State Security Spending Versus Industry Benchmarks

	Gartner	IREC	Federal Government	Executive Branch Current	Executive Branch Proposed
Security as a Percent of Total Technology Spending	5.4%	5.6%	6.2%	2%	4.7%
Security Spending per Employee	$510	$623	Unknown	$235	$550

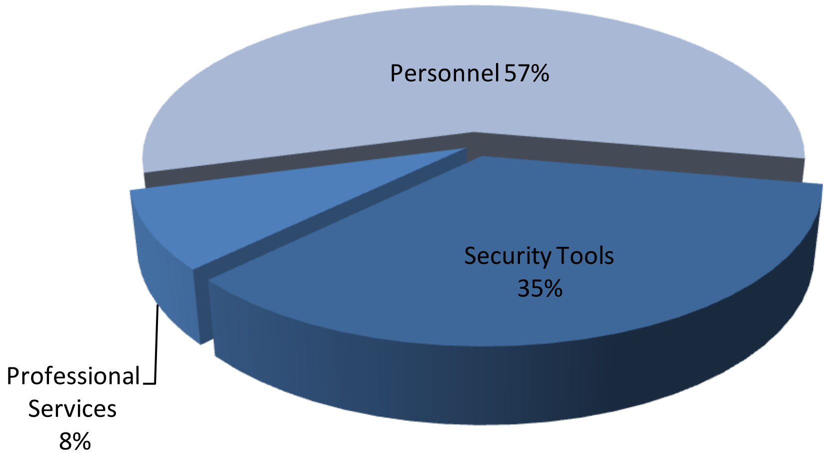
In its most recent report, Gartner estimates that most organizations typically allocate about 5.4 percent of their total information technology budget to security, an estimate that is slightly less than the 5.6 percent figure recently published by the Information Risk Executive Council (IREC). And finally, according to the Office of Management and Budget, the federal government spends about 6.2 percent of its total information technology budget on security at civilian agencies. The percentage spent on security in defense agencies is much higher.

Table 2-2 identifies what it would cost to deliver each security service over the next five years. As depicted in Figure 2-1, personnel account for about 57 percent of the total security service costs. However, the figure also demonstrates that the State will need to make a substantial ongoing investment in sophisticated security tools.

Table 2-2: Estimated Annual Costs per Security Service (In Thousands) for the Proposed Comprehensive Program

Security Services	2011	2012	2013	2014	2015
Enterprise/Portfolio	$647	$1,833	$1,789	$1,782	$1,851
Risk Management	$611	$1,486	$1,527	$1,424	$1,468
Policy & Standards Management	$306	$560	$560	$559	$578
Security Architecture	$460	$883	$870	$758	$783
Security Awareness & Training	$360	$650	$668	$685	$704
Access Management	$5,118	$4,405	$3,474	$2,706	$2,726
Intrusion Monitoring	$1,585	$1,305	$1,334	$1,345	$1,376
Malicious Program Detection	$806	$967	$985	$984	$1,003
Security Information Management	$2,503	$2,683	$1,606	$1,058	$1,083
Vulnerability Management	$817	$1,105	$1,134	$1,163	$1,194
Incident Response & Forensics	$567	$855	$844	$843	$874
Threat Management	$212	$212	$218	$223	$230
Asset Management	$460	$739	$721	$702	$721
Physical Security	$262	$280	$268	$273	$280
Business Continuity	$1,450	$1,450	$1,269	$1,310	$1,354
Data Privacy	$880	$1,324	$1,335	$1,047	$1,059

Figure 2-1
Security Program Annual Costs by Type for the Proposed Comprehensive Program



Program Cost Recommendations

1. **Continue present enterprise security funding levels**: Given the current fiscal crisis, it will be extremely difficult for the State to find dollars sufficient to fully fund the Enterprise Security Program as outlined above. However, even in these trying financial times, it will be vital to keep making progress on the information security plan in which we have already invested and upon which state security depends. Maintaining the current $4.2 million annual funding for enterprise activity and the current agency expenditures (estimated at an annual $4 million) will allow the State to continue progress in all 16 security service areas.

2. **Centralize security resources:** Centralizing the information technology environment and resources leads to better security. For example, a single state-of-the-art new Enterprise Vulnerability and Threat Management System gives every agency and MnSCU campus the ability to continuously assess all computers for exploitable security vulnerabilities, an issue discussed in many legislative audit reports. Before the rollout of this system, very few agencies had the people, processes, or tools to perform these vital functions. A single system provides the capability to all at a much lower cost.

3. **Simplify and consolidate the IT environment:** The executive branch has a complex and decentralized information technology environment that is extremely costly to secure. Today there are 36+ executive branch data centers to protect. Making matters worse, across these disparate environments there has been virtually no focus on product standardization. Collectively, this means that the Enterprise Security Program is now in the difficult position of needing to defend everything, everywhere, with very limited resources.

   Consolidating the number of data centers to two would reduce future information security costs *by about $4 million annually,* from the projected $19 million to $15 million. Most of the savings would come from reductions in the number of expensive security devices, such as intrusion detection sensors.

CHAPTER 3 – Funding Sources

Chapter Conclusion

The most efficient way to pay for and recover Enterprise Security Program costs for the executive branch is by continuing to use a general fund appropriation for enterprise activity. Generally funded costs are recovered today through the statewide indirect cost process, which allocates costs equitably to all fund types.

Non-executive branch entities that may benefit from Enterprise Security Program services should be charged through a rate structure, based on usage.

With increased demands for online government services, information security has become an essential cost of doing business. High profile data breaches now dominate the media, leaving little doubt about whether information security services are necessary. The more pressing questions today are not whether security is necessary, but:

- What is the appropriate investment in security services?
- What is the best way to fund and recover the costs?

To answer these questions, OET turned to the private sector and other state governments to seek out best-of-breed funding and cost recovery models.

In a recent research study by the Information Risk Executive Council (IREC),

- 37 percent of organizations fund information security centrally and do not recover costs from individual units.
- Of the 63 percent with mechanisms to recover information security costs from business units, most simply pool and allocate all security costs to business units based on their respective share of the total information technology spend.
- Very few organizations went through the effort of allocating security costs on a service-by-service basis.

Funding Source Recommendations

OET recommends a funding and cost recovery model that is a hybrid of the two common “best practices” cited above. The recommendation is similar to what is in place today.

1. **Executive Branch Security Services**

We recommend that the State continues to cover the Enterprise Security Program with a general fund appropriation. Minnesota Management and Budget (MMB) currently uses the statewide indirect cost process to allocate these costs equitably across all fund types, such as the federal fund and others.

The indirect cost methodology spreads a portion of the $4.2 million Enterprise Security Program costs to those agencies that are not generally funded, thereby reducing the overall fiscal impact on the general fund. The specific allocation method is based on each agency and each fund’s representative share of the total statewide IT spend. MMB sends each agency indirect cost bills. Amounts recovered get re-deposited into the general fund as non-dedicated revenue.

Benefits of a general fund approach include:

- **It is simple.** General fund appropriations make it very easy to track and manage costs in the State’s accounting system. All recoveries are made through one common indirect cost recovery process, managed by MMB.
- **It is efficient and equitable.** The indirect cost recovery process is well understood and accepted by agencies as a normal business practice. It also provides a very efficient way to distribute costs equitably to other fund types, without undue complexity. Finally, the indirect cost recovery process meets the federal cost allocation requirements.

- **Keeps overhead costs low and focus on security.** Use of this approach reduces the amount of time spent on rate-setting, billing, and accounts receivable functions. Particularly with a new security program, it is important to focus on security issues, rather than cumbersome administrative processes.
- **Clarifies that security services are a utility.** Costs that are billed and recovered through the statewide indirect cost process are considered utility services. For example, through this process all agencies help shoulder the cost of the central accounting and human resource functions. The Enterprise Security Program should be considered a utility service as well.
- **Aligns with best practices.** During our research, we found that most organizations that allocated costs used a process very similar to the statewide indirect cost process, managed by MMB. Very few organizations developed rates for specific security services.
- **Funds key security activities that cross jurisdictional lines**. For example, the Enterprise Security Office serves as a single point of contact for all security events in the State of Minnesota. Each day the office receives security alerts from the United States Computer Emergency Response Team (US-CERT) and other private sector entities. Many of these alerts pertain to security breaches and hacking activities that cross jurisdictional lines, impacting cities, counties, school districts, higher education institutions, and other branches of state government. Using its people and tools, the Enterprise Security Office helps all government organizations diagnose and remedy security problems.

2. **Security Services for Entities Outside the Executive Branch**

We recommend that security services be provided to non-executive branch entities through standard rates charged for the incremental cost of using the services, using the Enterprise Technologies Fund.

Today only a few security services have matured to a point that they could be extended to entities outside the executive branch. However, Table 3-1 identifies the security services that could be extended to other units of government in the future, and defines the relevant cost basis for each.

Table 3-1
Proposed Mechanism for Assigning Rates to Non-Executive Branch Government Entities

Service Description	Difficulty to Extend	Billing Unit
Enterprise/Portfolio	Hard	Per Engagement
Risk Management	Medium/Hard	Per Assessment/Audit
Policy & Standards Management	Medium/Hard	Per Document
Security Architecture	Medium	Per Project
Security Awareness & Training	Medium	Per Person Trained
Access Management	Medium/Hard	Per User ID
Intrusion Monitoring	Easy/Medium	Per Device Monitored
Malicious Program Detection	Medium	Per Endpoint/License
Security Information Management	Easy/Medium	Per Device Monitored
Vulnerability Management	Easy/Medium	Per Devices Monitored
Incident Response & Forensics	Medium	Per Incident
Threat Management	Easy	Per Info Feed
Asset Management	Medium/Hard	Per Device
Physical Security	Hard	Per Piece of Equipment
Business Continuity	Medium/Hard	Per Size of Entity
Data Privacy	Medium	Per Endpoint/License

Alternate Funding Approach

Absent general funding, OET recommends accounting for all Enterprise Security Program costs and recoveries in the enterprise technology fund. Under this approach, a simple way to recover Enterprise Security Program costs would be to allocate the costs to all agencies, based on each agency's percentage of the total statewide IT expenditures. This approach achieves some, but not all, of the benefits of the preferred general fund/indirect cost recovery approach, discussed above.

Using fiscal year 2009 data, we estimated the respective percentage of the total statewide IT expenditures for each of the 77 executive branch agencies. As illustrated in Table 3-2, the Department of Human Services (DHS) has the largest technology budget, representing about 23% of the executive branch total. Under the alternate funding approach, DHS would be billed about $955,000 if the budget for the Enterprise Security Program remains at $4.2 million.

Table 3-2
Security Cost Allocations under an Alternate Funding Approach

Agency	Percent of Executive Branch IT Spend	Current Security Allocation
Human Services	22.75%	$955,382
Transportation	13.69%	$575,064
Public Safety	10.32%	$433,560
Revenue	8.99%	$377,662
Employment and Economic Development	7.23%	$303,517
Health	5.88%	$246,800
Natural Resources	4.57%	$191,982
Corrections	3.84%	$161,282
Enterprise Technology	3.82%	$160,490
Minnesota Management and Budget	2.97%	$124,642
Education	2.24%	$94,139
Pollution Control	1.98%	$82,962
Administration	1.69%	$71,022
Secretary of State	1.68%	$70,488
Commerce	1.41%	$59,067
Labor and Industry	1.09%	$45,939
All Others	5.86%	$246,002
Total	**100.00%**	**$4,200,000**

OET believes that there are distinct disadvantages to this alternative funding approach and strongly recommends against its use because of:

- **Increased costs.** Increased overhead costs would result from monthly billing, accounts receivable, and cash management activities.
- **Increased security risk.** Our interviews with smaller entities indicate that many would simply be unable to pay additional costs without corresponding increases to their funding base. The viability of this model depends on allocating and recovering all costs. If some entities cannot pay, the result would be a corresponding erosion of the funding pool that benefits all entities - including those that can pay. Cutting off or refusing security services to entities that cannot pay is not an acceptable option, particularly since security incidents today spread extremely fast across entity boundaries. OET would not support a funding methodology that could result in less or no security for some agencies, putting the entire State at risk.
- **Cumbersome fiscal constraints.** Statutory and federal mandates limit cash balances in the enterprise technology fund, making it challenging to build the necessary reserves to purchases enterprise security tools. Currently, the Master Lease Program gives OET a mechanism to purchase and spread the cost of hardware over its useful life. However, many security tools have large software start up and refresh costs, which cannot be funded through the Master Lease Program. Under this funding model, it will be very difficult for OET to avoid federal penalties and comply with statutory cash limits.

CHAPTER 4 – Service Management

Chapter Conclusion

The most efficient way to manage security services is centrally. However, in Minnesota's decentralized technology environment, a hybrid delivery approach for security is most appropriate. Under a hybrid approach, all executive branch entities will share common security tools and processes. However, sufficient resources would remain in agencies to perform localized security functions.

The historical approach of delivering security services on an agency-by agency basis has not been successful. The State's enterprise direction calls for a more centralized delivery model that promotes resource sharing and addresses complex security problems more holistically.

The private sector is already adopting this strategy, as outlined in a report recently published by the Information Risk Executive Council. According to this study,

- More than 86 percent of organizations in North America now deliver information security services through a centralized model.
- Twelve percent use a decentralized model.
- Two percent deliver information security through a shared service organization.

Service Delivery Recommendations

1. Centralized and Decentralized Services

   OET recommends a hybrid approach to security service delivery in which all executive branch entities share common security tools and processes, but leave sufficient staff at the agency level to perform localized security functions. This is particularly important in the current IT environment at the State, which is highly decentralized. If the overall IT environment becomes more consolidated, centralization of security services will follow suit.

   The level of centralization will depend on the individual service, as depicted in Table 4-1.

Table 4-1: Proposed Security Service Delivery Method

Enterprise/Portfolio	Hybrid
Risk Management	Hybrid
Policy & Standards Management	Hybrid
Security Architecture	Hybrid
Security Awareness & Training	Hybrid
Access Management	Fully Centralized
Intrusion Monitoring	Hybrid
Malicious Program Detection	Hybrid
Security Information Management	Fully Centralized
Vulnerability Management	Fully Centralized
Incident Response & Forensics	Fully Centralized
Threat Management	Hybrid
Asset Management	Hybrid
Physical Security	Fully Centralized
Business Continuity	Hybrid
Data Privacy	Hybrid

APPENDIX A

Detailed Security Service Descriptions

The following is a detailed breakdown of security services that make up a comprehensive enterprise security plan. Services include:

- Security Portfolio Management
- Risk Management
- Standards & Policy
- Security Architecture
- Security Awareness & Training
- Access Management
- Intrusion Monitoring
- Malicious Program Detection
- Security Information Management
- Vulnerability Management
- Incident Response & Forensics
- Threat Management
- Asset Management
- Physical Security
- Business Continuity
- Data Privacy

Information Security Portfolio Management

Enterprise security portfolio management provides the enterprise management and reporting of all information security functions.	
Scope	• Required for all executive branch
Management	• Centralized, with some larger agencies having on-site staff to assist with business alignment
Activities	• Management of overall enterprise information security program and services • Management of the security framework that defines o Governance and cross-agency collaboration o Policy, standards, and guidelines o Compliance o Roles, responsibilities and qualifications for security personnel • Vendor and other third-party management
Expected outcomes	• An improved information security posture for the executive branch. • Greater visibility of information security risks and coordinated mitigation strategies for those risks. • Strategic and tactical plans that meet long-term priorities of executive leadership. • Proactive leveraging of state and vendor resources. • Increased efficiencies through reduction of redundant processes and tools.

Estimated Annual Costs for Security Service (In Thousands)

	2011	**2012**	**2013**	**2014**	**2015**
People	$431	$1,581	$1,645	$1,710	$1,779
Tools	$0	$0	$0	$0	$0
3rd Party	$216	$252	$144	$72	$72
Total	$647	$1,833	$1,789	$1,782	$1,851
FTEs	3	11	11	11	11

Detailed cost assumptions:

- Assumes the development of a formal Portfolio Management Capability in FY 2012, including a CISO, a manager for each security area (governance, management, and operations) and a team of 7-8 information security officers within larger agencies.
- Third-party costs include the construction of processes and procedures, creation of reports and metrics, agency information security evaluations to determine needs, and assessments to determine information security posture.

Information Security Risk Management

Information security risk management identifies, quantifies, and prioritizes security risks. The risk management program includes processes for performing risk assessments, tools to track risks, and communication of risk. As risks are identified, follow-on processes are determined for appropriate mitigation.

Scope	• Required for all executive branch
Management	• Hybrid model: centralized security risk management program with agencies' participation
Activities	• Risk assessment of new and existing systems and entities using a risk assessment tool or process, prioritizing systems based upon criticality. • Analysis of risk assessment data. • Implementation of controls to eliminate or compensate the risk findings. • Executive and business reporting of risks and mitigation strategies. • Tracking of identified risks.
Expected outcomes	• Balanced approach to identifying and assessing security risks. • Risk mitigation strategies that realize the appropriate security level at an affordable cost. • Executive and stakeholder understanding and acceptance of residual risk.

Estimated Annual Costs for Security Service (In Thousands)

	2011	2012	2013	2014	2015
People	$431	$1,006	$1,047	$1,088	$1,132
Tools	$0	$300	$300	$300	$300
3rd Party	$180	$180	$180	$36	$36
Total	$611	$1,486	$1,527	$1,424	$1,468
FTEs	3	7	7	7	7

Detailed cost assumptions:

- Assumes the development and management of an informal Risk Management capability in FY 2011. A formal Risk Management Program would begin in FY 2012 with an increase to 7 FTEs with some deployed to larger agencies.
- Tool costs are based upon the selection of a Governance, Risk, and Compliance tool for Risk Management, deployed in FY 2012. This tool would also be leveraged by Policy & Standards, Business Continuity and other areas.
- Third party costs are for the establishment and development of processes and procedures for Risk Assessment, Mitigation, Reporting, and Tracking.

Policies and Standards Management

Policies and Standards would manage the lifecycle of enterprise security program's policies, standards, and guidelines. It would also drive the enterprise toward compliance with the policies, standards, and regulatory requirements across the executive branch.

Scope	• Required for all executive branch
Management	• Centralized management, with some larger agencies having additional agency-specific policies and standards.
Activities	• Maintenance of enterprise policies through regular reviews to assess changes in regulatory requirements, security best practices, and business priorities. • Maintenance of supporting enterprise standards. • Management of an exception or variance process. • Enterprise-wide information security metrics reporting. • Coordination of compliance assessment with Risk Management. • Compliance reporting, communication, and tracking.
Expected outcomes	• A comprehensive set of information security policies and standards for the State of Minnesota executive branch. • Security policy and standards in accordance with applicable legislation, industry guidance, and best practices. • Benchmarks against to measure and report compliance via score cards.

Estimated Annual Costs for Security Service (In Thousands)

	2011	2012	2013	2014	2015
People	$288	$431	$449	$466	$485
Tools	$0	$75	$75	$75	$75
3rd Party	$18	$54	$36	$18	$18
Total	$306	$560	$560	$559	$578
FTEs	2	3	3	3	3

Detailed funding assumptions:

- Assumes the continued build out of policy and standards and the creation of compliance assessment procedures in FY 2011. FY 2012, the team is 3 FTEs and has established a formal program including maintenance and deployment of a Governance, Risk, and Compliance (GRC) tool.
- Tool costs are based upon the leverage of a GRC tool that would be shared with other information security capability areas.
- Third party costs are related to creating processes and procedures for compliance and maintenance.

Information Security Architecture

Security architecture represents the combination of security requirements into a set of processes, tools, and procedures used for the design and implementation of information systems.	
Scope	• Required for all executive branch
Management	• Hybrid of central and localized management. Larger agencies will have in-house Security Architecture capabilities for specific agency needs.
Activities	• Enterprise requirements analysis. • Setting of IT security standards. • Standardization of common security tools and controls. • Coordination with IT project management functions.
Expected outcomes	• A system of processes and procedures that ensures security requirements are part of each IT project life-cycle. • Specified security requirements ensures vulnerabilities and risks are appropriately mitigated during IT development. • Efficiency gains by the use of standardized tools, processes, and templates.

Estimated Annual Costs for Security Service (In Thousands)					
	2011	**2012**	**2013**	**2014**	**2015**
People	$288	$575	$598	$622	$647
Tools	$100	$200	$200	$100	$100
3rd Party	$72	$108	$72	$36	$36
Total	$460	$883	$870	$758	$783
FTEs	2	4	6	6	6

Detailed cost assumptions:

- Assumes an ad-hoc/informal security architecture group in FY 2011 and a formal enterprise-level capability developed in FY 2012.
- The Security Architecture team expands from two employees in FY 2011 to six by FY 2013 and becomes a centralized service.
- Tool costs are based upon security architecture tools that assess code and assist with the deployment of IT solutions.
- Third party costs are based upon process and program creation assistance and third party architecture reviews, when required.

Security Awareness

The focus of Security Awareness services is to achieve a long term shift in the mind-set of employees, leaders and consultants towards security by promoting a cultural and behavioral change within an organization. Security aware means you understand that there is the potential for some people to deliberately or accidentally steal, damage, or misuse the State's data.

Scope	• Required for all executive branch. Many organizations require formal security awareness training for all workers when they join the organization and periodically thereafter. Security awareness services have unique focuses towards executive leaders, the end users, the information technology professional, and the information security professional.
Management	• Hybrid management. Larger agencies will have in-house security awareness capabilities.
Activities	• Analysis of needed awareness, training and education within the enterprise; understanding audiences and the proper vehicles are for messaging • Creation of messages and vehicles for dissemination • Measuring effectiveness of awareness for business and compliance goals • Identification of specialized training and education needs • Tracking and reporting of security awareness, training and education
Expected outcomes	• Government leaders understand and support the information security program. • All state employees and contractors receive initial and ongoing security training appropriate to their job duties.

Estimated Annual Costs for Security Service (In Thousands)

	2011	2012	2013	2014	2015
People	$288	$431	$449	$466	$485
Tools	$0	$75	$75	$75	$75
3rd Party	$72	$144	$144	$144	$144
Total	$360	$650	$668	$685	$704
FTEs	**2**	**3**	**3**	**3**	**3**

Detailed cost assumptions:

- Assumes starting informally in FY 2011, developing into a formal Security Awareness & Training capability by FY 2012. The number of employees would expand from two in FY2011 to three by FY 2012 as it becomes a centralized service.
- Tool costs include user management and training tools.
- Third party costs include assistance in creation of materials and processes for the program, and specialized technical training.

Access Management

Access management manages the identities for users and devices, and controls access to system resources based on these identities. Logical access to IT systems, networks and data must ensure users and devices have access to only those systems for which they are properly authenticated and authorized to access. The capability must provide the ability to rapidly search, identify, and verify who and what is accessing the systems. This function is a critical aspect of meeting security and compliance requirements for any organization.

Scope	• Capability and common tools are needed across all agencies.
Management	• Hybrid management. Larger agencies will use common tools in a decentralized approach.
Activities	• Determining business requirement for access control. • Management of authentication and authorization. • Creation of evidence for all assessments, audits, and compliance activities. • Management of operating system access. • Management of network access controls.
Expected outcomes	• Access controls for executive branch information systems that meet business needs. • People and entities that conduct business with state government have appropriate and timely access to the necessary resources and data. • State information resources and data are protected from being used or accessed inappropriately. • A phased, enterprise approach that identifies loop holes in control points. • Improved compliance with industry regulations. • Reduced overall effort of IT administration; improved employee productivity. • A scalable approach that enables IT expansion.

Estimated Annual Costs for Security Service (In Thousands)					
	2011	**2012**	**2013**	**2014**	**2015**
People	$1,438	$1,725	$1,794	$1,866	$1,940
Tools	$3,500	$2,500	$1,500	$750	$750
3rd Party	$180	$180	$180	$90	$36
Total	$5,118	$4,405	$3,474	$2,706	$2,726
FTEs	10	12	12	14	14

Detailed cost assumptions:

- Assumes the current solutions will continue in FY 2011 while a decision is made to continue, update and expand or commence building new and improved solutions.
- The scope of computer systems covered by a centralized access control toolset will steadily expand into FY 2014.
- The team will consist of ten FTEs in FY 2011 expanding to fourteen in FY 2014.
- Assumes the acquisition of a well-established and robust tool.

Intrusion Monitoring

Intrusion monitoring includes the people, processes, and products to detect and prevent events that may damage the state's information resources. Intrusion detection is the process of monitoring the events occurring in a computer system and network; analyzing them for signs of possible incidents that are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents.

Scope	• Capability and common tools are needed across all agencies.
Management	• Centralized management. Larger agencies may have on-site personnel for investigative purposes.
Activities	• Providing resource to planning and architecture in development and placement of technologies to prevent intrusions to Minnesota's network and systems. • Coordination of all associated changes and maintenance activities to ensure that monitoring technologies are functioning properly. • Reporting on intrusion related events to business management. • Investigation of critical events to determine if the event resulted in a compromised of state data.
Expected outcomes	• All state computer systems are continuously monitored for adverse information security events. • Better situational awareness to make informed security decisions. • Prevention of unwanted behavior on state networks and systems.

Estimated Annual Costs for Security Service (In Thousands)

	2011	2012	2013	2014	2015
People	$431	$719	$748	$777	$808
Tools	$1,100	$550	$550	$550	$550
3rd Party	$54	$36	$36	$18	$18
Total	$1,585	$1,305	$1,334	$1,345	$1,376
FTEs	3	5	5	5	5

Detailed cost assumptions:

- Assumes continued intrusion monitoring in its current limited state and development of a formal function in FY 2011.
- Intrusion Monitoring would expand the number of employees from three to five by FY 2012 as it becomes a centralized service.
- Process improvements occur at the end of FY 2013 to leverage first-year knowledge of formal operations.
- Tool costs include current license, support, maintenance, and operations costs of already-purchased hardware.
- In FY 2011, additional appliances will be required for a complete enterprise solution.
- Third party costs include development of processes and the Intrusion Monitoring Program.

Malicious Program Detection

Malicious Program Detection identifies and manages software designed to maliciously infiltrate a computer system without the owner's informed consent. Malicious software, (also known as malware), includes computer viruses, worms, trojans, root kits, spyware, dishonest adware, crime ware and other unwanted software.

Scope	• Capability and common tools are needed across all agencies.
Management	• Hybrid management. Larger agencies will use common tools and processes.
Activities	• Detection and analysis, containment, eradication and recovery from a virus/spyware outbreak. • Alerts and periodic reporting on virus/spyware activity, update activity, virus spread, virus cleanup, trend analysis, and other reporting metrics which show level of risks to the State. • Management of antivirus software on e-mail and internet facing external gateways.
Expected outcomes	• Successful detection and mitigation of malicious software on servers, desktops, laptops and other mobile devices before they can do any harm. • The prevention of malicious software from entering Minnesota's network and information systems.

Estimated Annual Costs for Security Service (In Thousands)

	2011	2012	2013	2014	2015
People	$288	$431	$449	$466	$485
Tools	$500	$500	$500	$500	$500
3rd Party	$18	$36	$36	$18	$18
Total	$806	$967	$985	$984	$1,003
FTEs	2	3	3	3	3

Detailed cost assumptions:

- Assumes operating in an informal state in FY 2011 and the development of a formal Enterprise Malicious Program Detection capability in FY 2012.
- Expansion of the number of employees from two in FY 2011 to three by FY 2012 as it becomes a centralized service for the vast majority of agencies.
- Tool costs include $15 per endpoint for license costs for malware protection software.
- Third party costs are to assist with the establishment of processes and procedures for a centralized program.

Security Information Management

Security information management (SIEM) refers to the collection of data – typically event logs files – into a central repository for trend analysis. SIEM products generally are comprised of software agents that run on computer systems and communicate information about security-related events to a centralized server which displays the information in real-time reports, charts, and graphs and issues alerts for immediate response.

Scope	• Capability and common tools are needed across all agencies.
Management	• Centralized management.
Activities	• Management of security event logs and repository. • Correlation of security events from different log sources. • Generation of needed reports and logs for compliance reporting. • Assistance with the profiling of assets and known vulnerabilities.
Expected outcomes	• Streamlined handling of incident information in the security incident response process. • Near real-time notification of security events. • Relevant state computer systems are continuously monitored for adverse information security events. • Better situational awareness that recognizes and prevents unwanted behavior on the network or on the system.

Estimated Annual Costs for Security Service (In Thousands)

	2011	2012	2013	2014	2015
People	$431	$575	$598	$622	$647
Tools	$2,000	$2,000	$900	$400	$400
3rd Party	$72	$108	$108	$36	$36
Total	$2,503	$2,683	$1,606	$1,058	$1,083
FTEs	3	4	6	6	6

Detailed cost assumptions:

- Assumes the development of the service in FY 2012 and the full deployment in FY 2013, including a State Security Operations Center. It would operate in a limited manner in FY 2011.
- SIM would expand the number of employees from three in FY 2011 to six by FY 2013 for a nearly complete centralized service.
- Tool costs are based upon current license, support, maintenance and operations costs plus additional hardware needed for the first two years to complete an enterprise solution. A hardware refresh is forecasted for $4 million in FY 2017.
- Third party costs are to develop processes and assist in the setup of the service.

Vulnerability Management

Vulnerability management is the information security practice of identifying, classifying, remediating, and mitigating known vulnerabilities in computing systems. Vulnerability management is designed to proactively prevent the exploitation of an IT vulnerability that exists within an organization. Typically these system vulnerabilities are identified and classified by robust scanning toolsets. While many vulnerabilities are remediated with applying a patch fix, not all vulnerabilities have related patches; thus, security professionals must not only be aware of applicable vulnerabilities and available patches, but also other methods of remediation (e.g., device or network configuration changes, employee training) that limit the exposure of systems to vulnerabilities.

Scope	• Capability and common tools are needed across all agencies.
Management	• Centralized management. Larger agencies will use common tools.
Activities	• Management of processes and tools that identify weaknesses in software development processes. • External and internal assessment on technology security controls throughout Minnesota's networks and systems to discovery vulnerabilities. • Routine vulnerability scanning of critical devices. • Coordination of resolution and follow-up for any discovered vulnerabilities. • Assessment reporting. • Notification of system patches, testing and deployment of patches, measuring of compliance through scans to ensure patches have been applied, or vulnerabilities have been corrected
Expected outcomes	• Continuous vulnerability monitoring of state computer systems • Problems identified and remediated before they are exploited by hackers. • A more secure environment through routine assessments.

Estimated Annual Costs for Security Service (In Thousands)					
	2011	**2012**	**2013**	**2014**	**2015**
People	$431	$719	$748	$777	$808
Tools	$350	$350	$350	$350	$350
3rd Party	$36	$36	$36	$36	$36
Total	$817	$1,105	$1,134	$1,163	$1,194
FTEs	3	5	5	5	5

Detail cost assumptions:

- Assumes operation in its current informal state in FY 2011, and the development of a formal Vulnerability Management function in FY 2012.
- Expands the number of employees from 3 in FY 2011 to 5-6 by FY 2012 when it becomes a completely centralized service.
- Includes process improvement at the end of FY 2012 to leverage the first-year knowledge of formal operations.
- Tool costs include current license, support, maintenance and operations costs of previously purchased hardware.
- Includes a refresh of hardware in FY 2016 for $2 million.

Threat Management

Threat management is a security service that communicates or makes users aware of information security threats and vulnerabilities that exist both internally and externally so they can be managed.	
Scope	• Capability is needed across all agencies.
Management	• Centralized. All agencies will leverage the information from this service.
Activities	• Analysis of information security threats and their potential impact. • Storage and tracking of threats across the executive branch. • Communication and reporting of relevant threats and information security news, alerts and bulletins to the appropriate entities.
Expected outcomes	• Appropriate parties have threat information in time to react and prevent damage. • Threats are tracked and reported in a manner that assist in their analysis, mitigation, and management.

Estimated Annual Costs for Security Service (In Thousands)					
	2011	**2012**	**2013**	**2014**	**2015**
People	$144	$144	$150	$155	$162
Tools	$50	$50	$50	$50	$50
3rd Party	$18	$18	$18	$18	$18
Total	$212	$212	$218	$223	$230
FTEs	1	1	1	1	1

Detail cost assumptions:

- Assumes the development of an Informal Threat Management capability in FY 2011 with a one person team to developing the processes and procedures and perform outreach.
- Tool costs include the purchase of feeds and a tool to track and manage threats.
- Other Governance, Risk and Compliance Tools and Security Event and Information Tools maybe utilized for this, too.

Security Incident Response and Forensics

The security incident management and computer forensics function determines the cause, scope, and impact of incidents. The goal is to stop unwanted activity, limit damage, and prevent recurrence. Information security incidents include everything from a lost or stolen laptop to rampant computer virus infections to defacement of State web sites to other events that could cause prolonged system outages.	
Scope	• Capability is needed across all agencies.
Management	• Centralized. Larger agencies would continue to perform this function in the near term.
Activities	• Management of incident case assignment and the security investigation processes. • Mobilization/activation of emergency and general incident response services. • Investigations of email, employee internet access, network access, system access, etc. • Reporting on all associated activity included in the scope of an investigation; centralized logging and management of incidents for reporting. • Manage third party forensics where applicable.
Expected outcomes	• Improve ability to identify and isolate incidents, thereby limiting damage to state systems and data. • Fewer cross-agency infections. • Reduced costs through the sharing of staff and expensive forensic investigation tools. • Coordinated response to information security incidents, including assessment, triage, containment and preservation of evidence.

Estimated Annual Costs for Security Service (In Thousands)					
	2011	**2012**	**2013**	**2014**	**2015**
People	$431	$719	$748	$777	$808
Tools	$100	$100	$60	$30	$30
3rd Party	$36	$36	$36	$36	$36
Total	$567	$855	$844	$843	$874
FTEs	3	5	5	5	5

Detailed cost assumptions:

- Assumes operation in its current informal state in FY 2011, and the deployment of a formal Enterprise Incident Response & Forensics in FY 2012.
- Incident Response & Forensics would expand the number of employees from three in FY 2011 to five by FY 2012 when it becomes a centralized service.
- Includes process improvement at the end of FY 2012 to leverage the first-year knowledge of formal operations.
- Tool costs include various investigation and forensic tools and the expansion of those to an enterprise license, a incident and investigation tracking tool and e-discovery tools.
- Third party costs include creation of processes and procedures.

Information Asset Management

Information asset management is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision-making for the environment. Developing an inventory of information assets, defining owners of assets, establishing acceptable use policies and classifying and labeling information are all information security functions that can be implemented to ensure information and assets receive appropriate protection. This security service includes three functions: inventory of assets, designated ownership of assets, and acceptable use of assets.

Scope	• Capability is needed across all agencies.
Management	• Hybrid model. Smaller agencies use centralized service; larger agencies use centralized tools and processes.
Activities	• Maintenance of an information asset inventory that records asset owner, location, and acceptable uses. • Classification and prioritization of information assets. • Management and tracking of information assets. • Communication and reporting of information asset to appropriate tools and parties.
Expected outcomes	• A secure environment maintained through comprehensive inventory, classification, and tracking of all information assets. • Security resources are appropriately applied to protect the most critical information assets.

Estimated Annual Costs for Security Service (In Thousands)					
	2011	**2012**	**2013**	**2014**	**2015**
People	$288	$431	$449	$466	$485
Tools	$100	$200	$200	$200	$200
3rd Party	$72	$108	$72	$36	$36
Total	$460	$739	$721	$702	$721
FTEs	2	3	3	3	3

Detailed cost assumptions:

- Development of an Informal Asset Management capability in FY 2011 with two FTEs.
- Formal capability deployed in FY 2012, with a team of three FTEs.
- Tool costs include the purchase of an asset management tool or module.
- Third party costs include assistance with development of processes.

Physical Security

This service includes physical and environmental measures that prevent or deter threats from accessing a facility, resource, or information stored on physical media. It can be as simple as a locked door or as elaborate as multiple layers of armed security guards. The goal is to convince potential attackers that the likely costs of attack exceed the value of making the attack.	
Scope	Capability is needed across all agencies.
Management	Hybrid model. Smaller agencies use centralized service; larger agencies use centralized tools and processes.
Activities	Maintenance of perimeter and entry controls, external and environmental controls, office and facility controls. Management of access to public access. Management of off-site usage and removal of equipment. Proper equipment destruction.
Expected outcomes	Information systems are protected from physical threats. Continuous monitoring prevents or limits the impact of environmental threats.

Estimated Annual Costs for Security Service (In Thousands)

	2011	2012	2013	2014	2015
People	$144	$144	$150	$155	$162
Tools	$100	$100	$100	$100	$100
3rd Party	$18	$36	$18	$18	$18
Total	$262	$280	$268	$273	$280
FTEs	1	1	1	1	1

Detailed cost assumptions:

- Assumes one FTE liaison to other areas (security, facilities) to ensure physical security requirements are deployed where information systems are kept.
- Tool costs include physical controls needed for laptops and other data devices; this does not include any costs for facility security or data center security.
- Third party costs assist with the establishment of this capability its processes.

Business Continuity

Business continuity is the activity performed by an organization to ensure that critical business functions will be available to customers, citizens, regulators, and other entities at the time of a disaster. Business Continuity refers to those activities performed daily to maintain service, consistency, and recoverability, not to reactive planning at the time of a disaster.

Scope	• Capability is needed across all agencies.
Management	• Hybrid service to assist business owners and ensure proper plans are in place.
Activities	• Business impact analysis and identification of critical and non-critical information systems. • Business continuity and disaster recovery planning for systems to be restored or returned to service. • Testing and analysis of business continuity and disaster recovery plans. • Maintenance of processes and procedures. • Training of employees in their roles of the business continuity plans.
Expected outcomes	• Critical business functions continue and normal operations can be restored after a disruption or disaster. • A comprehensive test, training and exercise program validates and improves continuity and recovery planning. • State services are prioritized with appropriate recovery strategies for critical information systems. • Faster recovery of priority government services during a crisis. • Reduced costs through leveraging shared recovery environment. • Increased ability to share staff during times of crisis through adoption of a common plan format, processes, and tools.

Estimated Annual Costs for Security Service (In Thousands)

	2011	2012	2013	2014	2015
People	$1,006	$1,006	$1,047	$1,088	$1,132
Tools	$300	$300	$150	$150	$150
3rd Party	$144	$144	$72	$72	$72
Total	$1,450	$1,450	$1,269	$1,310	$1,354
FTEs	7	7	7	7	7

Detailed cost assumptions:

- Assumes the development of a formal Enterprise Business Continuity capability in FY 2012 that includes Risk Assessment, Business Impact Analysis, Recovery Strategy Development, Business Continuity Plans, Disaster Recovery Plans, Testing Processes and Maintenance Process.
- Assumes 7 FTE to support analysis, development and planning (this does not included people within the agencies that create the business continuity plans nor the expenses around recovery sites or backup equipment).
- Tool costs include software to assist with all of the above component.

Data Privacy

Data privacy is the aggregation of tools and process designed to protect data. This would include encryption for data at rest, data loss prevention tools to restrict the transfer of sensitive data, and the monitoring of the use of sensitive data.	
Scope	• Capability is needed across all agencies.
Management	• Hybrid management. Smaller agencies use centralized service • Larger agencies use centralized tools and processes.
Activities	• Proper destruction of data. • Management of tools and process to protect data in all stages, from storage to transmission, including databases, servers, laptops, etc. • Development of an effective communications program. • Helping business units understand their needs/challenges, assess potential impacts, propose potential resolutions, and assist with compliance, as appropriate.
Expected outcomes	• Data is appropriately protected, handled, and disposed of, regardless of medium (paper, electronic, other) or state (storage, processing, transmission).

Estimated Annual Costs for Security Service (In Thousands)

	2011	2012	2013	2014	2015
People	144	$288	$299	$311	$323
Tools	$700	$1,000	$1,000	$700	$700
3rd Party	$36	$36	$36	$36	$36
Total	$880	$1,324	$1,335	$1,047	$1,059
FTEs	1	2	2	2	2

Detailed cost assumptions:

- Assumes operating in an informal state in FY 2011, and the development of a formal Data Privacy capability in FY 2012.
- Expands the number of employees from one in FY 2011 to two by FY 2012, when it becomes a centralized service for the vast majority of agencies.
- Tool costs include data privacy software costs per endpoint per year.
- Costs do not include any forecasted increases in usage.
- Third party costs are to assist with the establishment of processes and procedures for a centralized program.

Appendix B

Executive Branch Entities currently in scope for the Enterprise Security Program

Accountancy Board

Administration Department

Administrative Hearings Office

Aging Board

Agriculture Department

Amateur Sports Commission

Animal Health Board

Architecture & Engineering Board

Arts Board, Minnesota

Asian-Pacific Council

Attorney General

Barber & Cosmetologist Examiners

Behavioral Health & Therapy Board

Black Minnesotans Council

Campaign Finance Board

Capitol Area Architect

Center for Arts Education, Perpich

Chicano Latino Affairs Council

Chiropractic Examiners Board

Combative Sports Commission

Commerce Department

Corrections Department

Dentistry Board

Dietetics & Nutrition Practices Board

Disability Council

Education Department

Emergency Medical Services Board

Employment & Economic Development Department

Explore Minnesota Tourism

Faribault Academies

Gambling Control Board

Governor

Health Department

Higher Education Facilities Authority

Human Rights Department

Human Services Department

Humanities Commission

Indian Affairs Council

Investment Board

Iron Range Resources & Rehabilitation

Labor & Industry Department

Lieutenant Governor

Lottery

Marriage & Family Therapy Board

Mediation Services Bureau

Medical Practices Board

Military Affairs Department

Minnesota Management and Budget

Natural Resources Department

Nursing Board

Nursing Home Administrations Board of Examiners

Office of Enterprise Technology

Office of Higher Education

Ombudsman for Mental Health & Mental Retardation

Ombudsperson for Families

Optometry Board

Peace Officers Standards and Training Board

Pharmacy Board

Physical Therapy Board

Podiatric Medicine Board

Pollution Control Agency

Private Detectives Board

Psychology Board

Public Safety Department

Public Utilities Commission

Racing Commission

Revenue Department

Secretary of State

Sentencing Guidelines Commission

Social Work Board

State Auditor

Transportation Department

Uniform Laws Commission

Veterans Affairs Department

Veterinary Medicine Board

Water & Soil Resources Board

Zoological Garden Board

Other Entities that Could Benefit From Enterprise Security Services

Quasi State Agencies
Historical Society
Housing Finance Agency
Metropolitan Airports Commission
Metropolitan Council
Metropolitan Mosquito Control District
Metropolitan Sports Facilities Commission

Retirement Systems
Public Employees Retirement Association
Minnesota State Retirement System
Teachers Retirement Association

Higher Education
Minnesota State Colleges and Universities
University of Minnesota

Minnesota State Legislature
House of Representatives Offices
Senate Offices
Legislative Reference Library
Legislative Auditor
Revisor of Statutes
Legislative Coordinating Commission

Minnesota Judicial Branch
MN Supreme Court
MN Court of Appeals
MN District Courts
Public Defense Board
Tax Court
Workers’ Compensation Court of Appeals

Local Government
K-12 School Districts
Cities and Counties

Appendix C

Today's proactive security efforts for executive branch agencies

*A FIVE-YEAR JOURNEY TO PROGRAM MATURITY**

Policy and Planning

70% Completed

What has been done

- Cross-agency strategic and tactical security planning
- Program based on nationally recognized framework
- Cross-agency participation in the program's governance process
- Majority of fundamental polices defined and published
- Policy adoption begun by executive branch entities

Still to do

- Complete risk management policies and establish enterprise information risk management practices
- Full adoption of the polices by all executive branch agencies
- Program performance metrics

Architecture

15% Completed

What has been done

- Published minimum standard requirements in four core security disciplines:
- Security Incident
- Vulnerability Management
- Continuity of Operations
- Physical / Environment Security

Still to do

- Full adoption of the existing standards by all executive branch entities
- Complete standards for remaining 14 core security disciplines
- Integration of Security Architecture into Enterprise Architecture
- Security requirements integrated into various development processes

Security Tools

20% Completed

What has been done

- Process for information security incidents at the enterprise level
- Processes to identify and address vulnerabilities across agency systems
- Process for accessing the impact of disasters
- Detection of weaknesses in externally-facing information systems
- Piloted additional network monitoring tools for intrusions and malicious activity
- Establish data gathering and metrics reporting for vulnerability management

Still to do

- Additional tools and processes for the remaining 14 core security disciplines
- Expansion of monitoring capability across all executive branch agencies
- Integration of security of tools and processing into the Enterprise Architecture
- Data gathering requirements and reporting across core security disciplines.

*Based on the Capability Maturity Model SM developed by Carnegie Mellon University as a tool for objectively assessing the maturity of government business processes

Education **15%** Completed

What has been done

- Planning practitioners trained on continuity of operations practices
- Continuity of operations plans for a majority of critical information systems
- Vulnerability management training started for practitioners
- Initial integration and training of enterprise security incident management
- Basic security awareness training events for larger agencies
- Targeted education and awareness to key stakeholders and security practitioners
- External vulnerability management metrics in use to reduce the risk of known vulnerabilities within information systems
- Some executive branch agencies are mitigating internal vulnerabilities based on the vulnerability management metrics

Still to do

- Full security awareness program for employees, contractors, and other personnel
- Complete continuity of operations plans for all information systems
- Complete security incident management processes for key personnel
- Essential broad training on various levels for future core security disciplines
- Consolidation of security metrics to establish an enterprise risk profile

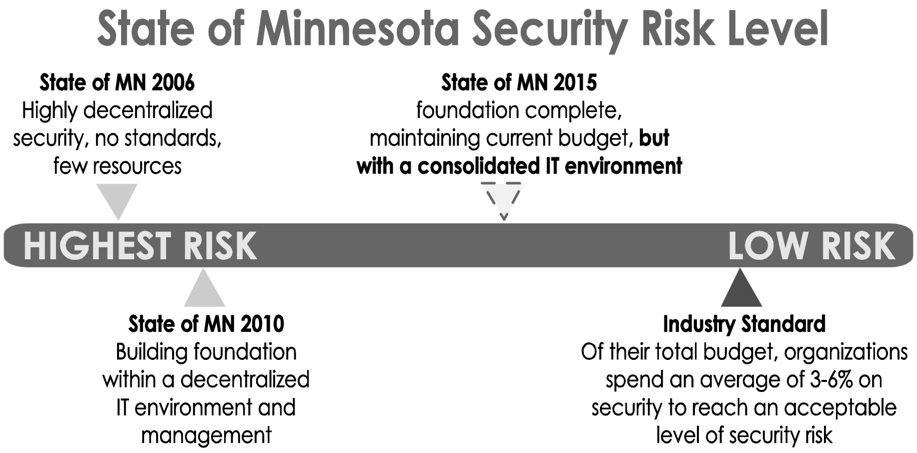
Practice **5%** Completed

What has been done

- Regular testing of continuity of operations plans by some agencies
- Regular testing for vulnerabilities in all externally-facing information systems
- Regular testing for vulnerabilities in a portion of internal information systems
- ACF2 Mainframe Access Control

Still to do

- Regular testing of continuity of all agency operations plans
- Regular testing for vulnerabilities in all internal information systems
- Continuous improvement through use of consolidated security program metrics and risk profile
- Full executive branch agency adoption of policies



State of Minnesota Security Risk Level

State of MN 2006
Highly decentralized
security, no standards,
few resources

State of MN 2015
foundation complete,
maintaining current budget, **but**
with a consolidated IT environment

State of MN 2010
Building foundation
within a decentralized
IT environment and
management

Industry Standard
Of their total budget, organizations
spend an average of 3-6% on
security to reach an acceptable
level of security risk