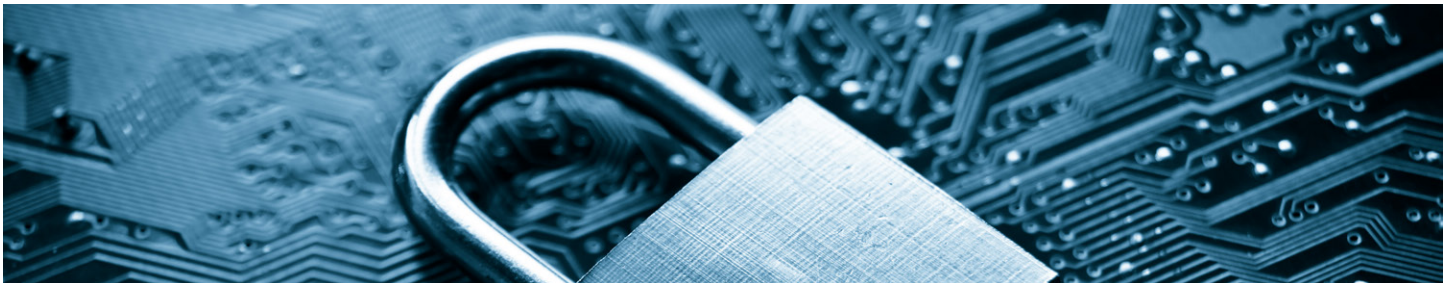
INFORMATION SECURITY STRATEGIC PLAN

JANUARY, 2018

MINNESOTA IT SERVICES

CONTENTS

EXECUTIVE SUMMARY



Information Security exists to help business leaders understand and manage complex technology risks. Business leaders have a fiduciary obligation to protect data from unauthorized loss, disclosure, or alteration, and they must make certain that their systems are available when needed – particularly during times of crisis. Facing an onslaught of catastrophic breaches, business leaders strive to meet new compliance pressures as regulators respond with more mandates. In this increasingly complex and hostile world, business leaders need a trusted advisor to help them succeed and protect their reputation. Information Security fills that role.

Information Security faces unprecedented challenges and extraordinary opportunities. Advanced attacks are becoming more sophisticated and more common, testing the limits of existing capabilities. Businesses' push to digitize compounds the problem and significantly expands the volume of sensitive organizational data vulnerable to attack. These and other trends put great pressure on public and private sector Chief Information Security Officers (CISOs) to develop new strategies and tactics for success.

More than half of CISOs in the United States believe an advanced attack will affect their organization in the next year. The pervasiveness of these threats means CISOs must quickly develop cutting-edge threat intelligence competencies while also improving response plans for when the worst occurs. Every day, attackers use sophisticated tools and techniques to test the defenses of the State of Minnesota and other government entities. Unfortunately, many government entities are not up to the challenge. The result is costly and embarrassing data breaches that erode citizens' confidence in government and cost significant dollars.

Both government and private sector organizations see significant increases in cybersecurity losses due to breaches and reductions in worker productivity. Organizations in the United States now have average annual cyber-crime losses of $15.4 million, according to the Ponemon Institute's 2015 Cost of Computer Crime Study. A 19 percent increase from 2014, this is double the average loss rate of other industrialized nations. A key finding in the report shows that deploying advanced security technologies makes a big difference to significantly reduce cybersecurity losses.

State government has seen an uptick in attacks, which are more sophisticated and targeted

Intense public, media, and regulatory focus on cyber-attacks has sharpened senior executive interest in Information Security. Because of this, the National Association of State Chief Information Officers (NASCIO) named Information Security its number one priority for two consecutive years. NASCIO also spearheaded three studies over the past four years with a leading consulting firm to highlight funding and governance issues that inhibit the effectiveness of state security programs. Information Security has even become a significant issue at the state leadership level, demonstrated in July when 38 governors, including Minnesota's Governor Mark Dayton, signed a compact pledging their commitment to bolstering cybersecurity defenses in their states.

It is important to note that on average state governments spend about two percent of their IT budget on cybersecurity, as opposed to the five percent or more that private sector and federal government civilian agencies spend. While state government spending has been static, Gartner recently announced that the worldwide spend on cybersecurity has been increasing at a seven percent to nine percent rate. It is clear that organizations across the globe are setting the cybersecurity bar higher in response to more advanced and persistent threats. Organizations that do not keep pace are accruing a cybersecurity debt that they eventually must pay to align with industry accepted best practices.

Although the Information Security Strategic Plan does not specifically call for more spending to make security "bigger," it outlines steps that must be taken to make security "better." This plan prioritizes the initiatives for the management, control, and protection of the state's information assets. It identifies 18 major strategies that Minnesota IT Services (MNIT) hopes to achieve over the next five years, resources permitting. The plan also highlights specific milestones for the ensuing year, things that MNIT expects to accomplish with existing resources.

The plan organizes strategies and milestones in four chapters:

- **Proactive Risk Management (Chapter 1)**, which includes activities to prevent adverse security events.
- **Improved Situational Awareness (Chapter 2)**, which includes activities to increase understanding of the state's ongoing cybersecurity posture.
- **Robust Crisis and Incident Response (Chapter 3)**, which allows services to continue uninterrupted in a crisis.
- **Partner for Success (Chapter 4)**, which involves building formal relationships with other entities that are part of the broader cybersecurity ecosystem.

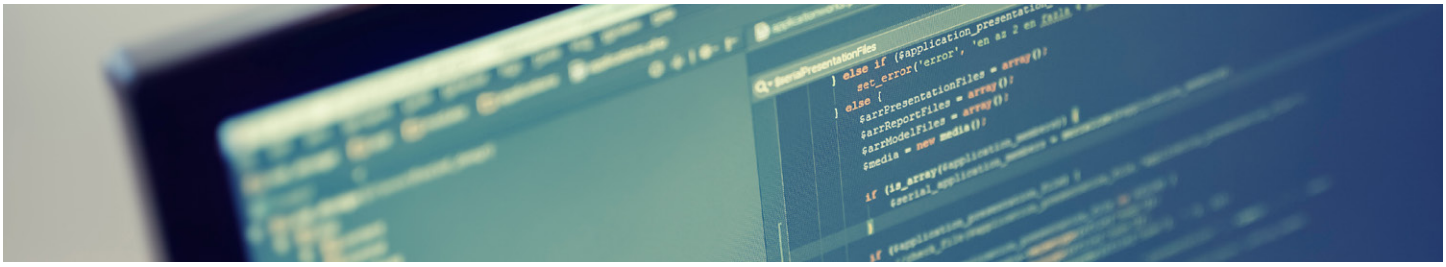
In the complete plan, five year strategies are distinguished from current year tactical milestones. Addressing the five year strategies will require assistance from policymakers and business leaders, who are ultimately accountable for cybersecurity risk, and that authorize spending levels for the state's Information Security Program.

The complete plan also highlights strategies and milestones that address extremely high-risk areas, denoted with a special caution symbol and yellow highlighted text. Resource constraints make it necessary to classify many extremely high-risk areas as five year strategies, rather than items to address during the current fiscal year.

CHAPTER 1 | PROACTIVE RISK MANAGEMENT

Some of the most important security strategies work to prevent adverse security events from happening. With more advanced and persistent threats, large organizations typically run sophisticated tools to help manage cyber risks in real time. An example of one such tool is vulnerability management software, which helps security professionals find and fix security holes before hackers exploit them. Proactive risk management also includes understanding adversaries and designing solutions to combat known threat vectors, such as denial of service attacks. Finally, educating employees is an important preventive defense in an increasingly hostile world, where people are often hackers' target of choice.

This plan also provides business leaders with a much better understanding of cybersecurity risks. MNIT will introduce cyber risk scorecards to our partner agencies' leadership, providing them with ongoing metrics to understand and manage their risk posture. MNIT will also engage business leaders in cyber risk conversations during major system development projects.



Strategy 1: Build Secure Applications

Hackers focus their efforts on business applications, a target of opportunity because they are often accessible from the Internet. Hackers also know that compromising an application can provide access to a treasure trove of backend data. Application security is extremely difficult to get right. Securing applications is technically challenging and now requires sophisticated tools and specialized training to avoid common pitfalls that hackers often exploit.

This strategy includes eight specific desired outcomes.

Strategy 2: Conduct Continuous Risk Assessments

Minnesota must reassess the adequacy of technology controls, because risks to state systems and data constantly change. Hackers relentlessly search for new vulnerabilities in hardware, software, and network devices. Making changes to technology and business practices also can introduce new targets of opportunity for cyber criminals.

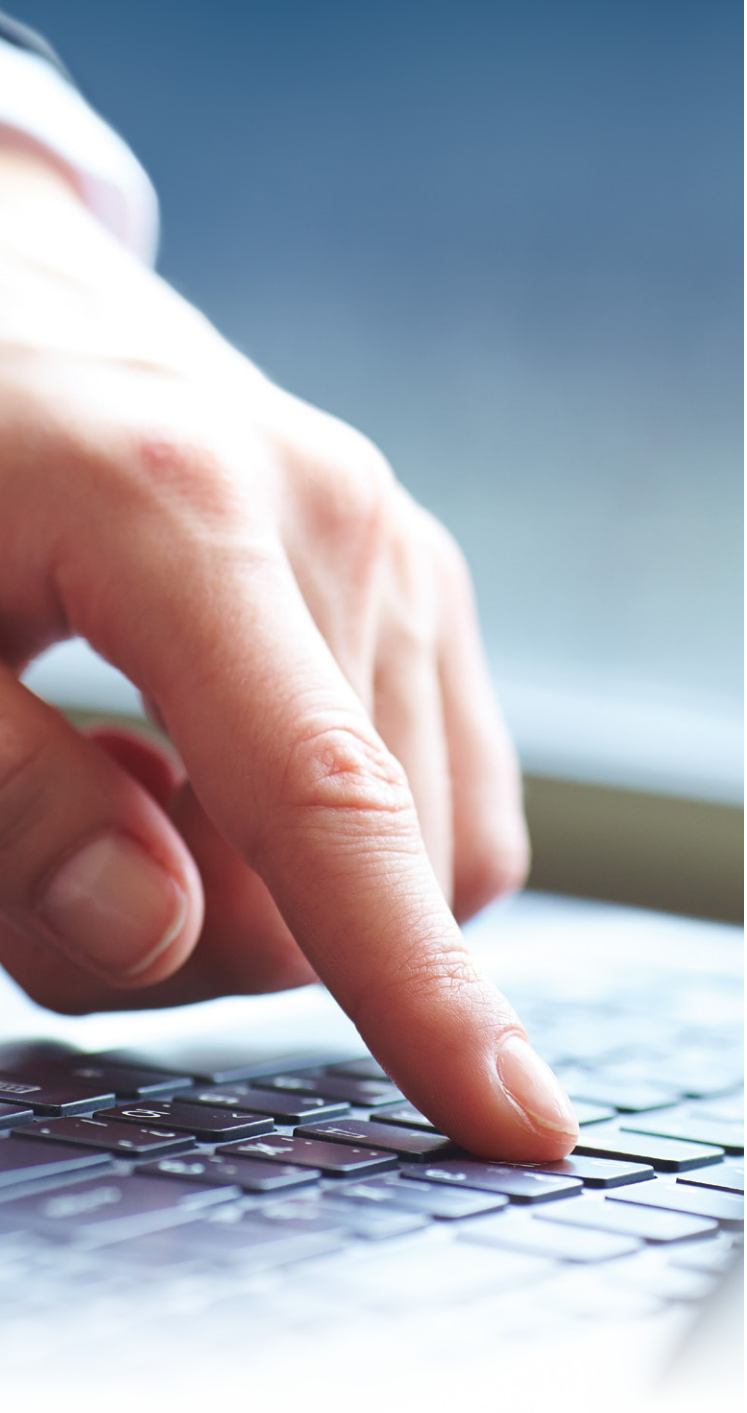
This strategy includes six specific desired outcomes.

Strategy 3: Communicate Security Risks to Agency Leaders

Technology leaders must effectively communicate cybersecurity risks to agency business leaders, who are accountable for cybersecurity risk. Ensuring agency leaders have an understanding of their cybersecurity risk posture fosters a better partnership with Minnesota IT Services to protect state systems and data.

This strategy includes two specific desired outcomes.

Employees are often the weakest link in an organization's security defenses



Strategy 4: Educate Employees about Cyber Risks

Today a large volume of security incidents and breaches result from insecure employee behaviors. Therefore, it is important to educate employees about cyber risks so that they understand what to do to protect state resources and data.

This strategy includes twelve specific desired outcomes.

Strategy 5: Enforce Secure Baselines

Hardware and software delivered by vendors is often insecure by default. Recognizing this out-of-the-box security risk, hackers often target default hardware and software vulnerabilities to compromise systems and steal data. Defining secure configuration baselines and automated build scripts to harden commonly used hardware and software products will combat such attempts from opportunistic hackers. Hardened products promote strong and consistent security, meet regulatory requirements, and align with state policies and standards, thereby minimizing the attack surface available to hackers.

This strategy includes seven specific desired outcomes.

Strategy 6: Improve Access Management

Identity and access management gives people the ability to fulfill their job duties while simultaneously protecting sensitive systems and data from harm. This extremely complicated security area includes:

- Provisioning and managing user accounts
- Granting and managing access to systems and data
- Developing special controls for individuals with extremely powerful clearances
- Organizing oversight encryption tools and processes

This strategy includes fourteen specific desired outcomes.

Strategy 7: Prevent Exploitation of Vulnerabilities

Every computer system has or will have security vulnerabilities. After hackers discover and begin exploiting vulnerabilities, vendors typically take up to several days to update the discovery signatures in their software. MNIT needs to build more robust threat intelligence processes, commonly referred to as "zero day vulnerabilities," to identify and begin remediation of vulnerabilities that are not discoverable with commercial tools. Continuous, proactive scans with special security tools to find and fix security holes mitigate the risk of hackers exploiting newly discovered vulnerabilities. Part of this strategy involves discovering innovative ways to continuously find and fix vulnerabilities in portable and IOT (Internet of things) devices, which are already a target of choice for hackers.

This strategy includes seven specific desired outcomes.

Strategy 8: Validate Security Controls with Independent Assessors

Audits and assessments offer independent validation of the adequacy of security controls. This strategy continues efforts to use independent assessors to validate the adequacy of cybersecurity controls. Independent assessments also help demonstrate compliance with the wide array of regulatory requirements imposed on state agencies, such as:

- Minnesota Government Data Practices Act
- Criminal Justice Information Services Security Policy
- Internal Revenue Service's Publication 1075 Tax Information Security Guidelines for Federal, State and Local Agencies
- Health Insurance Portability and Accountability Act (HIPAA) Security and Privacy Rules
- Social Security Administration (SSA) Electronic Information Exchange Security Requirements and Procedures For State and Local Agencies
- Payment Card Industry (PCI) Data Security Standards
- Federal Information Security Management Act

This strategy includes five specific desired outcomes.

Strategy 9: Prevent Denial of Service Attacks

When hackers use millions of computers to launch a Distributed Denial of Service (DDOS) attack against a service or entity, the barrage of nefarious traffic on the state's wide area network degrades performance for everyone. Globally, these attacks are increasing in frequency and volume. The impact to an organization under direct attack can be devastating, and it often includes the complete loss of vital services.

This strategy includes three specific desired outcomes.

Strategy 10: Obtain Coverage for Catastrophic Cyber Risks

Cybersecurity insurance helps mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and business system damage. Not a substitute for a robust security program, cybersecurity insurance addresses the reality that breaches happen and the resulting losses can be staggering.

This strategy includes two specific desired outcomes.

Strategy 11: Design a Resilient Network

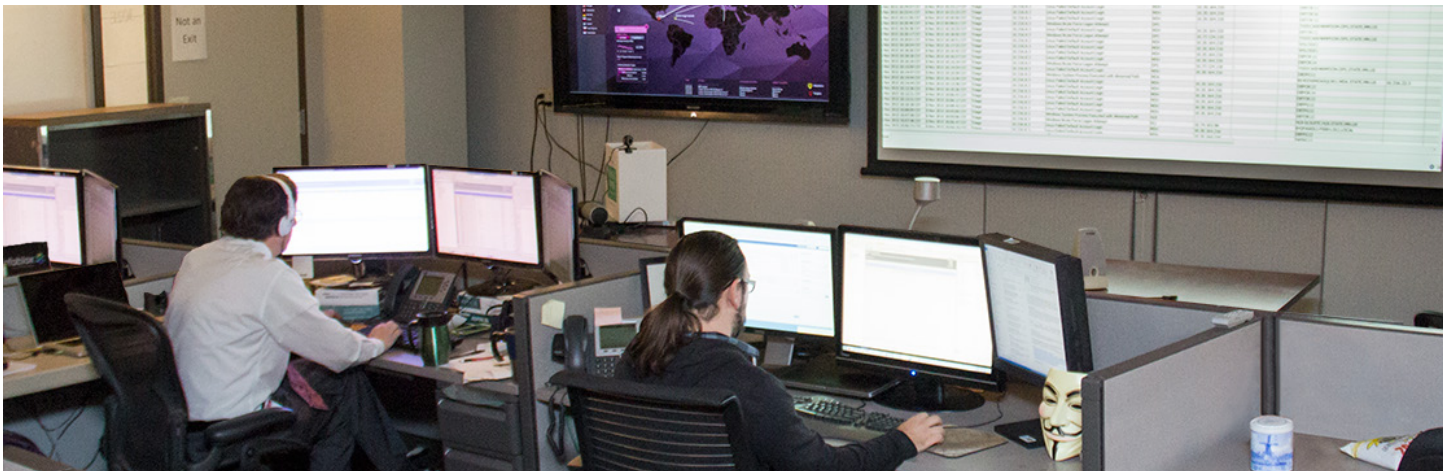
A key tenet of Information Security is defense in depth. A network provides additional layers of defense when it includes state of the art security tools and monitoring processes that smaller organizations simply could not afford when providing networking services on their own. A strong perimeter keeps out unwanted and potentially malicious traffic. Layers of internal segmentation better protect data and limit the impact of security incidents. Finally, oversight and management of an enterprise network will provide a cost-effective path to implement advanced security solutions, such as data loss prevention.

This strategy includes eight specific desired outcomes.

CHAPTER 2 | IMPROVED SITUATIONAL AWARENESS

Situational awareness is key to an effective security program. Awareness of threats, both natural disasters and human motivated, allows for efficient allocation of resources and effective implementation of controls. Awareness of vulnerabilities aids in the prioritization of remediation efforts, and awareness of security events triggers appropriate and timely response actions.

Strategies in this category will help the state better understand its risks and threats and promptly respond to adverse events. They also give the state a more effective measure of its risk posture with rigorous performance metrics.



Strategy 12: Detect Security Anomalies Faster

Security operations – the day-to-day activities of monitoring, auditing, and responding to events – involves correlating vast amounts of information and collaborating with numerous teams. For state government to perform these operations well, data must be available and accurate, tools must be tuned and integrated, and processes must be tested and continuously matured. The continued increase in state IT complexity and 24-hour operation of state systems further increases the need for more effective security operations.

This strategy includes eleven specific desired outcomes.

Strategy 13: Improve Our Understanding of the IT Environment

There is an old adage in the cybersecurity field; you cannot secure what you do not understand. Defining security controls in a world of quickly morphing threats is challenging, particularly in extremely complex and highly diverse environments. This strategy will help the state security program gain a more comprehensive understanding of the business systems that it now supports, including the hardware and software underlying each system.

This strategy includes five specific desired outcomes.

CHAPTER 3 | ROBUST CRISIS AND INCIDENT RESPONSE

It is not possible to prevent every conceivable security incident that could affect state information systems. A balanced Information Security program includes the ability to analyze the circumstances surrounding an incident and to restore normal system functions in a timely manner.

Initiatives in this chapter prepare MNIT for inevitable service interruptions. MNIT must have robust plans to minimize the impact of security incidents. MNIT also must test those plans and recovery processes to keep vital services functioning and data secure in a time of crisis.

Strategy 14: Develop and Exercise Recovery Strategies for Applications

A disaster recovery plan documents the recovery strategies for an information system. It outlines predetermined and approved response and recovery actions that reduce decision-making during a crisis, and it provides a systematic and documented recovery process. Planned disaster recovery actions ensure timely restoration of vital business functions in a time of crisis.

This strategy includes seven specific desired outcomes.

Strategy 15: Respond to Security Incidents Faster

Formal processes to record, validate, prioritize, classify, contain, and eradicate security incidents minimize harm resulting from attacks. Solid relationships and ongoing communication can also help security professionals respond to incidents faster. Simplifying response processes is a key part of this strategy. Further normalizing legacy response processes reduces the time it takes to validate and respond to incidents, particularly in the case of incidents that occur during nonbusiness hours.

This strategy includes six specific desired outcomes.

CHAPTER 4 | PARTNER FOR SUCCESS

With the advent of interconnected systems and the Internet, state government operates in an extremely hostile world. Hacker attacks against state government come from every country, and they never stop. Each day, unscrupulous individuals try to compromise state systems to steal data, shut down vital services, and use our technology infrastructure to launch anonymous attacks against others.

Hacker attack methods evolve daily, forcing security professionals to modify their defenses in a nonstop battle with very high stakes. Success is dependent on threat intelligence. When sophisticated attacks occur, early warning and expert advice can mean the difference between business continuity and catastrophe. Cybersecurity has now evolved into an ecosystem where the success of every organization hinges on timely and actionable threat intelligence.

By using industry intelligence, training the cyber experts of tomorrow, and working with emergency response, MNIT will build the relationships needed to combat cybercrimes now and into the future.

Strategy 16: Use Strategic Partnerships to Improve Security

This strategy includes involvement in the local and national threat intelligence ecosystem. It also includes the expansion of the state's threat intelligence ecosystem, incorporating commercial threat intelligence products on the market now.

This strategy includes five specific desired outcomes.

Strategy 17: Develop a Talent Feeder Program with Higher Education

Continuous partnership with institutions that have cyber programs allows MNIT to show the benefits of working at the state, while also assuring that students have the skills they need to have successful IT careers.

This strategy includes four specific desired outcomes.

Strategy 18: Provide a Cyber Presence in the State Fusion Center

Fusion Centers bring together response organizations to share intelligence to protect local communities. Fusion Centers have historically been geared towards physical threats, but fusion center leaders recognize that cybersecurity threat actors also pose a major risk to society.

This strategy includes two specific desired outcomes.