State of Illinois

Cybersecurity Strategy

2021-2025

Section I: Executive Overview

Introduction

Information Technology (IT) is central to national and state security, the economy, and public health and safety. Businesses, governments, academia, and individuals are all increasingly dependent upon Information Technology for essential services and daily life. It is the expectation that the systems providing services are secure and resilient.

Developing a State Cybersecurity Strategy is the first step in helping secure systems the public relies upon. The purpose of this strategy is to establish a clear vision for the State of Illinois' cybersecurity with goals, objectives, and desired outcomes that address current gaps in cybersecurity. Each objective will be achieved through actionable items and deliverables that measure progress and maturity. While this strategy is a four-year plan, it is a living document which will be revisited and refined based on the ever-evolving threat landscape, emerging technologies, and current needs.

Scope

This strategy establishes a framework for a whole-of-state approach to cybersecurity. It is structured to provide clear direction over the next four years for mitigating risks and addressing cyber threats across the state. Partnerships with federal, state, local and private sectors will be utilized and leveraged to accomplish the goals and objectives of the strategy.

Vision

A strong, secure, and resilient cybersecurity environment that facilitates and promotes best practices, reduces risk to critical services, and protects personal privacy and data.

Illinois Cybersecurity Goals and Objectives: 2021-2025

The State of Illinois has established five cybersecurity goals based upon identified gaps and current risks across the state. Each goal contains supporting objectives that further define how to meet the goal. Each of these supporting objectives has a desired outcome, as well as actionable programs or initiatives that can be measured to track progress in achieving each objective.

Goal One: Build a Culture of Cyber Awareness - Build and enhance cyber awareness and training across all sectors.

Goal Two: Prepare and Plan for Cyber Incidents - Develop practices, processes and the overall planning required to protect valuable information, resources, and services.

Goals Three: Mature Cyber Capabilities - Mature cyber competencies through the utilization of best practices to help organizations make risk-based decisions for improving cybersecurity.

Goal 4: Build a Cyber Workforce - Promote the improvement and advancement of a well-trained cybersecurity workforce in Illinois.

Goal 5: Collaborate and Share Information – Create and expand partnerships to foster continual learning and information sharing to ensure the safety and resiliency of digital infrastructure.

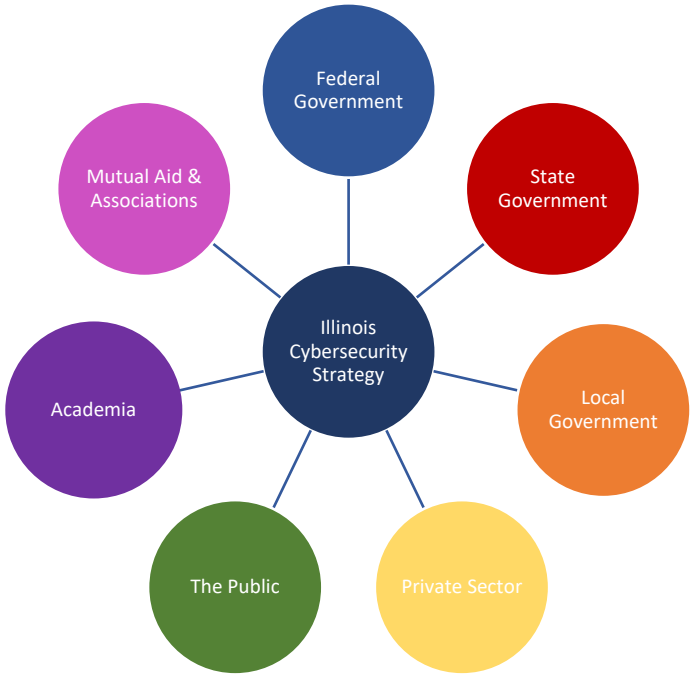
Coordination with Partners and Stakeholders

This cybersecurity strategy will require coordinated planning, support, and investments from a variety of stakeholders in order to mature cybersecurity across the state. The Executive Cybersecurity Oversight Committee (ECOC) will coordinate an integrated approach to cybersecurity and work towards successful implementation of this Strategy.

Illinois is comprised of various levels of government, academia, private entities, nonprofit groups, associations, and the public. In this time of greater dependency on IT resources by all, many gaps have been identified in cybersecurity across the state. Gaps include budget limitations, a limited qualified workforce, and a general deficiency of cybersecurity maturity across all sectors. To help build a more cyber-secure state, Illinois will leverage existing partnerships and forge new partnerships to begin building a more cyber- secure state. This coordinated outreach will extend into all corners of the state to meet organizations where they are in their journey to maturity and to help them understand their specific risks. Current partnerships

include publicly and privately owned utilities, city and county governments, and associations representing local fire departments, law enforcement, public health agencies, and schools.

All coordination efforts will be based on best practices, such as the Cybersecurity Framework, the CIS Top 20 Security Controls, and the Risk Management Framework. Each entity in the state will need to focus its maturity efforts on its own individual risks. Some of the measurable actions in the Strategy are focused on outreach to help assess and mitigate these individual risks. Training efforts will range from basic awareness to more advanced level courses, especially for those tasked with securing critical IT systems that serve the public. Workforce development begins with S.T.E.A.M. educational opportunities in the K-12 sector and moves to increased post-secondary learning opportunities to help develop a more advanced cyber workforce.



Evaluating and Updating the Strategy

Measuring progress is a key component of successfully implementing the State Cybersecurity Strategy. The effective use of state and federal money, as well as the efficient use of existing resources, is critical and requires metrics that will properly track and measure the desired outcomes. To that end, the Strategy includes a desired outcome and several actionable initiatives for each objective. These initiatives provide a means to assess progress towards the Strategy's goals and objectives. Each measurable initiative can be assessed with various metrics over the life of the Strategy. A comprehensive assessment of the Strategy will be conducted at least twice during its life. This will allow for progress updates as well as any needed adjustments based on the ever-evolving threat landscape.

Section II: Risk Profile

Illinois' economy, security, and way of life depend on a stable, safe, and resilient cyberspace. The Department of Homeland Security stated "Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services." Governments, schools, private sectors, and the public face an array of cyber-related threats designed to access sensitive information, steal money, force ransom payments, and disrupt essential services. These threats come from a variety of sources, utilize different attack methods, and take advantage of vulnerabilities and human error.

Public and private sector entities throughout the nation have been affected by cyber-attacks carried out by various threat actors, including nation states, hacktivists, and criminals. While Illinois, like most states, must prepare for the possibility of a cyber-attacks against critical infrastructure, attacks are more commonly financially motivated cybercrimes that have a high degree of success in disrupting business, public safety, or delivery of services, or stealing money from individuals. The rise of "ransomware" (i.e., malicious software that renders computer files inaccessible and demands a ransom to either restore the files or avoid the release of sensitive data) has affected continuity of operations at many government agencies and private sector entities.

The threat landscape can be assessed through four variables, each of which can be represented in multiple ways:

1. The Threat Actor (Attacker)
    a. External
    b. Internal

2. The Intention
    a. Monetary
    b. Political
    c. Sociological

3. The method of attack (attack vectors)
    a. Malware
    b. Social Engineering
    c. Hacking
    d. Credential Compromise
    e. Web Attacks
    f. DDoS
    g. Other

4. The Vulnerability
    a. Technical
    b. Human

As noted above, threat actors can be external or internal. External cyber threats are based on a variety of intentions and take advantage of system vulnerabilities. These vulnerabilities could be technical in nature or simple human error. As an example, those motivated by monetary gain might look to steal information that they can sell or ransom. A nation state could be motivated to sell proprietary business information or sensitive government data. A threat actor could take advantage of an unpatched vulnerability to gain access to data. They could also take advantage of human error via a successful phishing scam where an employee clicks on a malicious link to malware that enables the transfer of sensitive information. The CrowdStrike 2021 Global Threat Report details a number of attacks using the Global COVID-19 Pandemic to target victims.

Hacktivists, another example of an external threat actor, continue to be a problem across the state. These hackers, or hacking organizations, are often politically or sociologically motivated. They often target government services, critical infrastructure, law enforcement, or schools. These attackers employ state-of-the-art stealth tactics to avoid being discovered and are often supported directly or indirectly by nation-states or domestic extremism. While the intended impact of such attacks may be political or sociological, they can take many forms, such as website defacement, rendering services unavailable, or releasing of sensitive data to cause harm or embarrassment. Any interference in the confidentiality, integrity, or availability of data is a problem for any organization.

Internal threats are usually employees, commonly referred to as accidental or malicious insiders. In the first case, the employee or vendor is not intentionally causing harm. They may not understand that their actions are causing harm by exposing sensitive data or compromising processes. In the case of a malicious insider the intent changes. The employee or vendor understands the harm they can inflict and knowingly exposes sensitive data or compromises processes.

New forms of malware and other methods of attacks are created every day. In contrast, new vulnerabilities continue to be discovered, and patches and updates continue to be released to mitigate those vulnerabilities. Despite the everchanging types of attacks and vulnerabilities, the formula of the threat landscape is the same. Threat Actor + Intention + Method + Vulnerability = Cybersecurity attack. The element representing each variable can change, but the overall equation does not change. Good information sharing and intelligence helps any organization stay abreast of which threat actors are active, the specific methods of attack they are using, and the vulnerabilities they are trying to exploit. Staying focused on organizational vulnerabilities, and understanding and identifying the other variables, helps minimize the number and success of cyber-attacks.

Headlines tend to focus on the threat actor, the intention, or the method of attack. However, the vulnerabilities of a system are its true weaknesses. This Cybersecurity Strategy is focused on maturing cyber best practices so entities can help themselves mitigate those vulnerabilities and their overall risk.

Section III: Cyber Goals and Objectives for 2021-2025

1. **Goal One: Build a Culture of Cyber Awareness** – Build and enhance cyber awareness and training across all sectors.
   - Objective 1: Identify opportunities to educate the public on ways to prevent cybersecurity attacks and protect personal information.
   - Objective 2: Create access to security awareness training for local units of government, school employees, law enforcement, and critical infrastructure.
   - Objective 3: Train state government employees to help protect the information and assets with which they are entrusted.
   - Objective 4: Support and attend cyber security trainings to improve technical capabilities.

2. **Goal Two: Prepare and Plan for Cyber Incidents** – Develop practices, processes, and the overall planning required to protect valuable information, resources, and services.
   - Objective 1: Identify and disrupt cyber-attacks to minimize adverse impacts.
   - Objective 2: Improve and expand statewide security incident response capabilities.
   - Objective 3: Promote and facilitate joint training and exercise scenarios.
   - Objective 4: Support public and private sector partners to secure critical systems that serve the public.

3. **Goal Three: Mature Cyber Capabilities** – Mature cyber competencies through best practices that help organizations make risk-based decisions for improving cybersecurity.
   - Objective 1: Promote a risk-based approach to cybersecurity.
   - Objective 2: Establish regional volunteer cyber response teams.
   - Objective 3: Develop and disseminate best practices and tools to advance cyber maturity across all sectors.

4. **Goal 4: Build a Cyber Workforce** - Promote the improvement and advancement of a well-trained cybersecurity workforce in Illinois.
   - Objective 1: Advocate for cybersecurity careers and create hands on opportunities for K-12 students to experience.
   - Objective 2: Expand partnerships with Higher Education to help build tomorrow's cyber workforce.
   - Objective 3: Enhance the public sector cyber workforce.

5. **Goal 5: Collaborate and Share Information** – Create and expand partnerships to foster continual learning and information sharing to ensure the safety and resiliency of digital infrastructure.
   - Objective 1: Forge and nurture partnerships with critical infrastructure sectors to ensure the resiliency of critical systems.
   - Objective 2: Identify, evaluate, and share information on the threats and vulnerabilities impacting the state.
   - Objective 3: Expand and foster partnerships with federal, state, and local governments, private sector and non-governmental organizations, and academia to foster situational awareness and advance cybersecurity efforts in Illinois.

Appendix A

Alignment of the State Strategy with the NIST Cybersecurity Framework	Identify	Protect	Detect	Respond	Recover
Goal 1 - Building a Cyber Risk Aware Culture					
Objective 1: Identify opportunities to educate the public on ways to prevent cybersecurity attacks and protect personal information.					
Objective 2: Create access to security awareness training for local units of government, school employees, law enforcement, and critical infrastructure.					
Objective 3: Train state government employees to help protect the information and assets with which they are entrusted.					
Objective 4: Conduct, support, and attend cyber security trainings to improve technical capabilities.					
Goal 2 - Preparing and Planning for Cyber Events					
Objective 1: Identify and disrupt cyber-attacks to minimize adverse impact.					
Objective 2: Improve and expand statewide security incident response capabilities.					
Objective 3: Promote and facilitate joint training and exercise scenarios.					
Objective 4: Support public and private sector partners to secure critical systems serving the public.					
Goal 3 - Maturing Cyber Capabilities					
Objective 1: Promote a risk-based approach to cybersecurity.					
Objective 2: Establish regional volunteer cyber response teams.					
Objective 3: Develop and disseminate best practices and tools to advance cyber maturity across all sectors.					
Goal 4 - Building a Cyber Workforce					
Objective 1: Advocate cybersecurity careers and create hands on opportunities for K-12 students to experience.					
Objective 2: Expand partnerships with Higher Education to help build tomorrow's cyber workforce.					
Objective 3: Enhance the public sector cyber workforce.					
Goal 5 - Collaborating and Information Sharing					
Objective 1: Forge and nurture partnerships with critical infrastructure sectors to ensure the resiliency of critical systems.					
Objective 2: Identify, evaluate, and share information on the threats and vulnerabilities impacting the state.					
Objective 3: Expand and foster partnerships with federal, state, local governments, private sector, non-governmental organizations, and academia to foster situational awareness and advance cybersecurity efforts in Illinois.					