STATE OF NORTH CAROLINA

CYBERSECURITY STRATEGIC PLAN
2025-2030

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Table of Contents

From the State Chief Information Security Officer

Cybersecurity is a critical concern in today's digital age, where threats are constantly evolving. The current state of cybersecurity is challenging, North Carolina public entities are targets for cyber threat actors who are using advanced tactics, techniques, and procedures; new tools; and exploitative technologies, which can present cybersecurity challenges as dynamic as the cyber threat landscape itself. Threat actors, ranging from sophisticated nation-state groups to organized cybercriminals are working continuously to circumvent security measures and achieve their objectives – cause disruptions.

As we increasingly rely on digital systems and interconnected technologies, the opportunity for attack increases, presenting cyber threat actors with the chance to exploit both known and unprecedented vulnerabilities. The dark web allows even less skilled cyber threat actors to launch attacks, while emerging technologies introduce new vulnerabilities. The shortage of skilled cybersecurity professionals exacerbates these challenges, leading to outsourcing to third-party vendors who may also face cybersecurity issues. Staying ahead of threats requires proactive measures, continuous learning, and the integration of cutting-edge technologies.

The Cybersecurity Strategic Plan helps entities align their cybersecurity efforts with six key goals. While aimed at the state level, it can strengthen any organization's program. The Department of Information Technology (DIT) and Enterprise Security & Risk Management Office (ESRMO) believe these goals will advance cybersecurity initiatives through teamwork and collaboration.

Bernice Russell-Bond, CISSP, MBA, PMP

NC State Chief Information Security Officer

State of North Carolina Cybersecurity Vision

North Carolina government entities will form a secure and resilient cybersecurity environment by using their resources efficiently, collaboratively, and effectively to create a risk-aware culture that prioritizes the protection of online government services, critical infrastructure, and North Carolinian information.

State of North Carolina Cybersecurity Goals

Our statewide cybersecurity strategy will fortify North Carolina' cybersecurity landscape by:

Goal 1: Reducing the **cyber threat surface** through robust **risk management** .

Goal 2: Establishing an **accountability model** for Statewide CISO practices.

Goal 3: Enhancing the state's **cybersecurity governance** capabilities.

Goal 4: Fostering a prevalent **culture of cybersecurity awareness and education**.

Goal 5: Improving **resilient**, uninterrupted business critical operations during and after cyberattacks; and

Goal 6: Instituting workforce programs dedicated to **nurturing and advancing cybersecurity professionals**.

This comprehensive approach to cybersecurity ensures the protection of North Carolinian data, the reliability of digital services, and the overall trustworthiness of the state's online infrastructure.

Goal 1: Threat Surface Management

Reduce North Carolina' cyber threat surface through comprehensive risk management.

Overview

To safeguard digital assets from potential cyber threats, North Carolina will embrace a comprehensive risk management approach that incorporates cutting-edge tools, robust processes, thorough methodologies, and proven governance. By continually monitoring, analyzing, and addressing cyber risks, North Carolina can proactively identify vulnerabilities and stay one step ahead of cyber threat actors.

Challenge

North Carolina organizations face an array of cybersecurity challenges. These cybersecurity challenges can be difficult to address due to complicated and evolving factors, such as cyber risk tolerance, ever-evolving cyber threats, dynamic landscape of defensive tooling, and vulnerability management practices. To best address these challenges, North Carolina organizations must first understand their current risks and cybersecurity capabilities. Then, organizations can determine how to securely integrate new and evolving technology and updated processes into their operations. Additionally, reducing the attack surface through a comprehensive vulnerability management program is necessary to help organizations limit potential attack points.

Strategies

1. Adopt an effective risk-based vulnerability management approach by understanding what must be protected and quantifying the risk of that information or system being compromised.
2. Implement data classification and tagging as well as consistent security categorization of systems and information technology assets .
3. Apply zero trust architectural strategy and principles where feasible to define minimal baselines for good cyber hygiene of IT assets.
4. Collaborate and communicate with other North Carolina entities to support a whole-of-state approach to cybersecurity.

Outcomes

- Increased commitment to data classification and a better understanding of an organization's cyber risks.
- Improved systems protection and threat intelligence.
- Emphasize a risk-based approach that optimizes vulnerability management and ensures the highest level of security while prioritizing vulnerabilities based on the potential impact and likelihood of exploitation, ensuring that resources target the most critical threats first.
- Integrate real-time threat intelligence, understand their organization's unique risk profile, and leverage advanced analytics to make proactive, informed decisions about patching, mitigation, and remediation.

Enterprise Security Risk Management Office (ESRMO) Initiatives

ENDPOINT DETECTION AND RESPONSE PROGRAM

ESRMO's endpoint detection and response (EDR) solution provides around-the-clock management of real-time continuous monitoring with rules-based automated response and analysis capabilities. ESRMO's EDR solution covers tablets, workstations, laptops, and physical and virtual servers. The program is currently monitoring and protecting over 50,000 IT assets.

ESRMO's solution is available to state agencies at no cost through ESRMO's Managed Security Services (MSS). Following a statewide approach ESRMO is aiming to have the MSS available to all T1 and T2 counties within the next year at no additional cost.

ASSESSMENT SERVICES

ESRMO funds comprehensive security assessments, penetration tests, and web application vulnerability scans to state agencies, institutions of higher education, and public junior colleges. These services gauge the maturity of an organization's security programs, providing insights into the strengths and weaknesses that help management prioritize security budgets and resources. ESRMO and partner assessors (e.g. National Guard) shares test results with the assessed organization's staff to facilitate remediation.

THIRD-PARTY RISK MANAGEMENT TOOLS

To implement vulnerability management, ESRMO utilizes specialized third-party tools to enhance proactive identification, assessment, and remediation of potential security vulnerabilities. These tools offer a comprehensive and streamlined approach that facilitates efficient vulnerability detection, risk prioritization, and mitigation strategies. ESRMO is aiming to have some tools available to Tier 1 and Tier 2 counties within the next year at no additional cost.

Goal 2: Statewide CISO Accountability

Clarifying the purpose, impact, and relationships the statewide Chief Information Security Officer (SCISO) has with public sector entities.

Overview

Creating a clear accountability model for SCISO practices ensures consistent security standards, aligned risk management, and transparent oversight across all state agencies. This model clarifies roles and expectations and ensures the SCISO has the authority to guide agency practices and strengthens coordination across public sector entities.

Challenge

In 2015, Department of Information Technology (DIT) was established to simplify the technology function, create economies of scale, secure data and accelerate growth. Through exceptions, exemptions, and tactical priorities, the authority of the SCISO has diminished over time. With the new and emerging risks in our technology-first society, now is the time to revisit the authority and clarity of the SCISO function. This goal will look to correct:

- Fragmented practices that result in inconsistent controls and maturity levels across agencies.
- Limited visibility to risk exposure, compliance, and readiness.
- Lack of enforcement mechanisms.
- Inadequate response coordination.

Strategies

1. Define roles and responsibilities. Clarify the SCISO oversight role plus Shared Service offerings from Enterprise Security & Risk Management Office (ESRMO), the agency CISO responsibilities and chosen service providers.
2. Standardize SCISO governance practices and reporting under statewide mandated standards / frameworks.
3. Document and mature SCISO shared service offerings and measure the public sector utilization.
4. Create accountability mechanisms including funding/incentives for compliance and improvement. Develop escalation and remediation processes for agencies that fall behind.

Outcomes

- Statewide risk transparency so legislators and leadership can see where risks exist and how they're being addressed.
- Better use of resources with shared investments in tools, talent, and training.

ESRMO Initiatives

SCISO ACCOUNTABILITY CHARTER

Build, validate, and socialize an up-to-date playbook for why the function was put in place. Clarify the core functions and measures of success. Fortify the team to be able to meet the expectations and clarify performance management. With a True North defined for the team, they will be able to support the state with more confidence and consistency.

CYBERSECURITY, RISK, PRIVACY, AND DATA MANAGEMENT CENTER OF EXCELLENCE

Build the framework, repository, and communications system necessary for agencies and organizations in the public sector to collaborate fully in these areas. Reduce redundancy and accelerate learning by building a culture and platform for learning, sharing, and connecting.

MONTHLY OPERATIONS REVIEW

Implement core metrics on both the governance and shared service functions that ESRMO offers. With consistent measures of maturity, adoption, and performance, the team will know when they are on or off track. Measuring what needs to be managed is an essential step in moving forward.

POLICY MODERNIZATION

Gather the experts and solidify the approval processes to quickly and effectively modernize policies to match the current state of threats and risks in Cyber, Privacy, and Data Management. Keep modernization as part of the operating model to support the adoption of emerging technologies and to serve the expanding needs of the public sector.

Goal 3: Governance

Strengthen North Carolina' cybersecurity governance capabilities.

Overview

Good cybersecurity governance helps North Carolina protect its information and systems in a clear, organized way. It makes sure security efforts follow state and federal rules and helps everyone stay accountable and transparent. This builds public trust. With strong governance, the state can make smart decisions about cybersecurity and keep those efforts aligned with its bigger goals. In the end, it helps keep information safe, systems running, and public confidence strong.

Challenge

Cybersecurity policies can be complex, challenging to understand, and even harder to accurately interpret. Balancing multiple audit and compliance requirements with daily operations, which often involve intricate and time-consuming processes, can be demanding for North Carolina entities.

Strategies

- Adopt comprehensive cybersecurity policies that outline the acceptable use of technology, password management, data handling, and reporting procedures, making it easy for people to understand security requirements.
- Ensure the organization's leadership is informed of cybersecurity's importance, encourage them to prioritize cybersecurity, and establish channels for communications on cybersecurity-related topics and updates.
- Adopt actionable, meaningful, and relevant metrics to effectively monitor progress in improving cybersecurity maturity.
- Ensure executives and business units are accountable for cybersecurity risk.
- Educate identified data owners on risk, governance, and effective security control implementation and monitoring.
- Contribute expertise and best practices to the statewide knowledge base by participating in statewide and national governance initiatives.
- Adopt standards around the data use with emerging technologies, including artificial intelligence (AI) and quantum computing.

Outcomes

- Quantified and qualified risk profiles for public sector functions providing the legislature with transparency and clarity in cyber/data risks.
- A Cybersecurity, Privacy, and Data Management Center of Excellence to foster knowledge share, collaboration, and a definitive authority for best practices in the state.
- Timely, accurate, and thorough risk reports that support legislative decision making.
- Improved understanding of the risks of an entity's digital assets and compliance with cybersecurity laws and regulations, leading to an increased level of accountability, ownership, and resource allocation.
- Enhanced collaboration among stakeholders within the information security community.
- Transparent Risk Posture with a consistent statewide view of cyber and data-related risks. Leading to a clearer articulation of vulnerabilities, threat levels, and maturity across agencies.
- Better use of public funds by reducing duplicative efforts and costly inconsistencies across agencies with the promotion of shared services and common tools, driving economies of scale.

- Strengthen public trust and compliance by demonstrating the state's commitment to protecting personal information.
- Aligns cybersecurity, privacy, and data strategies with state priorities that the foundation for innovation, AI readiness, and digital transformation.

ESRMO Initiatives

STATEWIDE INFORMATION SECURITY MANUAL

Based on industry standards and best practices, the Statewide Information Security Manual is the foundation for security in the state of North Carolina. It provides state agencies with a baseline for managing information security and making risk-based decisions.

These policies were developed with the assistance of subject matter experts and peer-reviewed by agency representatives using NIST 800-53 revision 5 controls as the framework. The policies align to 18 NIST control families, including previous policies and addressing NIST 800-53 control gaps, as appropriate.

NORTH CAROLINA RISK AND AUTHORIZATION MANAGEMENT PROGRAM

A statewide baseline for cybersecurity, providing consistency in the approach to ensure confidentiality, integrity and availability (CIA) of our systems and data is a foundational requirement. Establishing a risk and authorization management program (e.g. GovRAMP) provides a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process the data of a state agency. ESRMO will look to establish the North Carolina Risk and Authorization Management Program. This program aims to reduce the risk of using third-party cloud services through assessing the security practices of the cloud service provider.

Goal 4: Education

Build a culture around cybersecurity awareness.

Overview

Embedding cybersecurity into North Carolina' culture is an ongoing process that requires commitment and engagement from all levels of North Carolina government. Promoting a shared responsibility for cybersecurity by providing comprehensive policies, protocols, training, and communications will strengthen North Carolina organizations and improve the security of the state.

Challenge

Meeting the ongoing and ever-increasing security challenges facing the state will require North Carolina to equip employees with the skills and knowledge to understand cybersecurity risks, including the best ways to avoid those risks and limit their impact to North Carolina organizations.

Strategies

Educate state employees and the public about cybersecurity awareness through diverse, updated training with various delivery methods.

- Build and develop partnerships with public and private sector entities to encourage customers and employees to stay informed about emerging cyber threats, new security measures, and end-user best practices.
- Find and offer access to relevant training opportunities that include up-to-date and tailored content to meet specific organizational objectives.
- Incorporate a broader variety of training delivery methods such as interactive games, scenario-based learning, simulations, and workshops.
- Regularly assess the effectiveness of cybersecurity awareness programs and training efforts by gathering feedback from customers, conducting surveys, tracking progress, and measuring the impact of training initiatives

Outcomes

- A well-trained workforce that stays current on best practices in cybersecurity, which, in turn, encourages employees to promptly report potential security breaches without fear of blame or retribution.
- Enhanced statewide cybersecurity awareness, leading to an increased level of security over North Carolina's data.
- Reduced risk of compromise due to lack of employee awareness or carelessness.
- Increased personal understanding of cyber risks that will carry over to the workplace
- Better public support for cyber practices

ESRMO Initiatives

CYBERSECURITY AWARENESS AND EDUCATION

As a statewide leader in information security, ESRMO provides education and support at no cost to state agencies, institutions of higher education, and local governments through a variety of methods, such as offering end-user security awareness training, providing access to technical

research and advisory services, hosting educational webinars and events, and organizing Cybersecurity Awareness Month activities.

INFORMATION SECURITY FORUM

The Information Security Forum (ISF) will be an annual educational conference bringing together security and IT professionals from public sector organizations across the state of North Carolina. This premier conference—which state and local government employees are eligible to attend at no cost—focuses on cybersecurity trends and current issues.

NORTH CAROLINA CYBER INFORMATION SHARING PORTAL

ESRMO is collaborating to create the North Carolina Cyber Information Sharing Portal (NCCISP) to provide a forum for North Carolina entities to share information regarding cybersecurity threats, best practices, and remediation strategies. The NCCISP is open at no cost to state agencies, local government, public and private institutions of higher education. The NCCISP provides access to intelligence and educational opportunities and allows members to participate in real-time information sharing.

INFOSEC ACADEMY

The ESRMO Security Academy will provide training for cybersecurity staff from state agencies, cities, counties and institutions of higher education to grant skills for increasing the security of both their respective organizations and the state. Interested participants must receive approval from their organization's CISO/ISO before registration and should be employed in positions related to cybersecurity. ESRMO also requires that all participants complete the North Carolina Cyber Baseline course, which is updated every two to three years with the latest security, information technology, and legislative changes. The ESRMO Security Academy strengthens the state's cybersecurity posture and is an essential function of government.

Goal 5: Resilience

Maintain continuous business critical operations when responding to and recovering from—cyberattacks.

Overview

Technology shapes how the government serves the public, so resilience must be a top priority. North Carolina must equip its organizations to plan for, adapt to, and recover from cyberattacks that threaten critical services. Strong response and recovery capabilities will keep essential operations running, even during serious disruptions. By investing in planning, training, and trusted partnerships, North Carolina will build organizations that stay operational under pressure and bounce back quickly from cyber incidents. This resilience is vital to meeting the state's immediate and long-term goals.

Challenge

Cyber disruptions are not a matter of "if" they are a matter of "when." Every government organization must be prepared to deliver essential services even while under cyberattack. That means building and maintaining strong contingency plans, including business continuity and disaster recovery strategies, is non-negotiable.

Two major challenges threaten this readiness. First, many organizations fail to invest the time, expertise, and effort needed to build realistic, flexible, and organization-specific plans that work in a crisis. Second, even well-designed plans often collect dust. The plans are never tested, never updated, and ultimately useless when disaster strikes.

Cybersecurity is a core government function. Without a tested plan and a disciplined approach to vulnerability management, agencies put public services, employee safety, and public trust at risk.

Strategies

- Identify and develop plans to prepare organizations to re-establish essential functions in the event of a cyber disruption.
- Implement corrective actions identified from past cybersecurity incidents and exercises.
- Hardwire resilience into agency operations by proactively identifying critical functions and develop targeted, tested continuity plans.
- Turn lessons into action. Require every agency to track, implement, and audit corrective actions from real incident and tabletop exercises. Build the lessons into training, system configurations, and contingency updates.
- Institutionalize continuous testing and validation. Use results to inform leadership decisions and refine readiness.
- Mandate shared risk visibility through a statewide cyber risk dashboard for executive and legislative leaders. Highlight agency-level vulnerabilities, plan maturity, and system dependencies.
- Create a resilience maturity model, setting a statewide standard for what 'resilient' means. Benchmark agencies against it annually.

Outcomes

North Carolina organizations that can proactively manage vulnerabilities and risks while reducing operational costs and ensuring the continuity of critical business operations.

- A tested disaster recovery plan for North Carolina organizations that ensures business continuity and has established service baselines.
- Identified essential functions of North Carolina organizations that are resilient during a cyber incident.
- A statewide and cross-functional culture of preparedness that reduces cybersecurity incident impacts and improves response time to address critical cybersecurity incidents.
- Cybersecurity professionals have access to the tools they need to maintain cybersecurity baselines and meet business objectives while successfully mitigating risks.
- Rapid restoration of public technology services in the event of an incident or attack.
- Reduced impact of cyber incidents because of actionable continuity plans.
- Increased accountability and learning, where corrective actions are standard practice.
- Real-time visibility for decision makers.
- Confidence in crisis response and stronger public trust because routine drills and plan validations define the steps.

ESRMO Initiatives

CYBERSECURITY INCIDENT RESPONSE TEAM

ESRMO's Cybersecurity Incident Response Team (CIRT) aims to safeguard critical assets of the state by sharing threat intelligence and providing incident response support to eligible organizations, including onsite and remote security incident management support. The CIRT offers various cybersecurity preparedness activities—such as tabletop exercises and incident response training—to enhance North Carolina organization readiness. Furthermore, the CIRT offers computer forensics and analysis services to investigate incidents effectively. CIRT works collaboratively with the NC Joint Cybersecurity Task Force (JCTF).

CYBER OPERATIONS

ESRMO Cyber Operations offers critical support to state agencies, customers of the state data center, and eligible partners. Operating around-the-clock, ESRMO Cyber Operations provides a comprehensive range of services, including IP and domain name blocking, vigilant monitoring and prompt alerting for suspicious activities, expert incident response guidance and support, intelligence gathering, and information sharing.

AGENCY INCIDENT RESPONSE REPORTING

Agency entities in North Carolina are required to report cybersecurity incidents to ESRMO. After discovering a cybersecurity incident, entities have 24 hours to submit an initial incident report to ESRMO. Within 14 days of recovering from the incident, the impacted entity will be required to report an analysis of the cause of the incident. Reporting incidents to ESRMO gives the state a more comprehensive view of the cyber threat landscape in North Carolina. Additionally, ESRMO continues to share anonymized threat intelligence with members of the NCCISP, which can help prevent additional attacks.

STATEWIDE INCIDENT RESPONSE PREPAREDNESS

ESRMO maintains the Statewide Cybersecurity Incident Response Plan, which outlines the method and tactics North Carolina will take to respond to a statewide cybersecurity incident. ESRMO will also start and lead a Statewide Incident Response Working Group, a collaboration among multiple state agencies that facilitate a whole-of-state approach when responding to significant cybersecurity incidents.

Goal 6: Workforce Development

Establish programs to support and develop cybersecurity professionals.

Overview

To ensure a talented, strong, and robust workforce for the future, North Carolina should have programs in place to identify, train, and develop cybersecurity talent. Partnerships between state and local government organizations, universities, school districts, and junior colleges are key to developing programs that build, retain, and recruit the talent needed for the future.

Challenge

The shortage of qualified and skilled cybersecurity professionals underscores the necessity for programs that attract and retain talent. Effectively addressing these challenges requires focused efforts to enhance recruitment strategies, promote cybersecurity as an appealing career path, and allocate ample resources to cultivate a resilient and proficient cybersecurity workforce.

Strategies

North Carolina government entities should:

- Dedicate additional funding to cybersecurity positions.
- Partner with K-12 and higher education organizations to develop innovative workforce training and internship opportunities for future cybersecurity professionals.
- Develop programs to upskill existing government employees and fill vacant cybersecurity roles.

Outcomes

- An increase in qualified cybersecurity professionals to fill open positions.
- An increase in training and educational opportunities for potential and existing employees in the cybersecurity workforce.
- An increase in interest in cybersecurity as a career path among North Carolina students.

ESRMO Initiatives

REGIONAL OPERATION CENTERS

ESRMO is looking to establish regional security operational centers (RSOC) in two new locations. These RSOCs employ, educate, and increase the cybersecurity skills of college students and veteran apprentices (who work under trained cybersecurity professionals) while providing threat research, monitoring, and mitigation services for customers. ESRMO, through the RSOCs, can help secure local government entities such as cities, counties, and independent school districts from cyber threat actors while concurrently increasing the quality and quantity of cybersecurity analysts in North Carolina.

ESRMO INITIATIVES INTERNSHIP PROGRAM

ESRMO's internship program provides college students with experiential learning opportunities to gain practical experience in a profession related to their college degree plan and career interests. ESRMO interns learn new skills, get exposure to different work environments, and receive mentorship and guidance from professionals within the agency. ESRMO's goal with the cyber internship program is to create a positive learning experience, instill a sense of belonging, and prepare interns for full-time employment, perhaps at ESRMO or another state agency.

VETERAN APPRENTICESHIP

ESRMO is committed to the successful reentry of military veterans into the civilian workforce and employment. Military service members also possess a wide variety of cross-functional skills, have undergone advanced technical training, and are adept at working with new and emerging technologies. Because of these values, skills, and training, military veterans are highly sought after candidates for ESRMO apprenticeship. Military veterans, therefore, are uniquely qualified to serve the North Carolina government and help ESRMO achieve its mission of leading the state's technology strategy, protecting state technology infrastructure, and transforming how North Carolina government serves Carolinians.

Definitions / Terms

Cyber Threat Surface

The cyber threat surface (also known as the **attack surface**) refers to the total sum of all the potential points where an unauthorized user (attacker) could try to enter or extract data from a digital environment. It includes all the ways an organization's systems, users, and processes could be exploited or attacked.

Cyber Risk Management

Risk management in cybersecurity is the ongoing process of identifying, assessing, prioritizing, and mitigating risks to an organization's digital assets, systems, and data. Its goal is to reduce the likelihood and impact of cyber threats to acceptable levels, enabling the organization to operate securely and confidently.

Cybersecurity Governance

The way an organization makes decisions and sets rules to keep its digital systems and data safe.

Risk-based Vulnerability Management

A cybersecurity approach that focuses on identifying and fixing the vulnerabilities that pose the greatest risk to an organization — instead of trying to fix everything equally.

Data Classification and Tagging

The process of organizing and labeling data based on its level of sensitivity, importance, or type, so that it can be protected, managed, and used appropriately.

Consistent Security Categorization

Consistent security categorization of systems and information technology assets means applying a standardized process to evaluate and label each system or asset based on the **sensitivity of the information it handles and the potential impact** if that information were compromised.

Endpoint Detection and Response (EDR)

A cybersecurity technology that continuously monitors devices (like laptops, servers, or mobile phones) to **detect suspicious activity**, **investigate threats**, and **automatically respond** to potential attack.