COLLECTIVE DEFENSE AND SUPPORT: A WHOLE-OF-STATE APPROACH TO CYBERSECURITY

INITIATED JUNE 2018

COMPLETED DECEMBER 2021

Rob Main
State Chief Risk Officer

919-754-6228
Rob.Main@nc.gov

NCDIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

EXECUTIVE SUMMARY

Cyber incidents are an increasing concern for state, local, and academic institutions. Ransomware, data exfiltration, extortion, and other types of cyber-attack have been on the rise for the last several years.

Since 2019 the North Carolina Joint Cybersecurity Task Force has supported more than 60 significant cybersecurity incidents, with 29 of those incidents occurring in 2021. Of the 29 attacks in 2021, local government entities (includes cities, municipalities, counties, local school administrative units, and community colleges) reported 18 of them.

Of the 29 cyberattacks in 2021, local government entities reported 18 of them.

North Carolina has adopted a whole-of-state approach to cybersecurity to prevent and prepare for incidents and support affected entities when they occur. This approach has five main components:

1. Mandatory incident reporting for all state and local government entities
2. Prohibition of ransom payment by any state or local government entity
3. Data sharing through the NC Information Sharing and Analysis Center (NC-ISAAC)
4. Incident preparation and response through the N.C. Joint Cybersecurity Task Force (JCTF)
5. Cybersecurity strategy and planning through the IT Strategy Board Cybersecurity and Privacy Committee

Information sharing and collaboration are crucial in fighting cybercrime. All levels of government must communicate with each other to prevent and mitigate the effects of cybersecurity incidents. We are increasing our vigilance and focus on cybersecurity workforce development as cyberattacks evolve and become more sophisticated. We cannot be siloed in our collection of information - information sharing is key to preventing cyberattacks and mitigating the damage when they occur.
Through North Carolina's whole-of-state approach to cybersecurity and the engagement of the JCTF, we have been able to provide support across the entire state, whether it be preventing an event by providing defensive capabilities, providing training and tabletop exercises, or providing boots on the ground when an incident occurs. Our state's cybersecurity community supports one another and shares knowledge and experiences.

IDEA

North Carolina seeks to ensure awareness of the importance of coordinated, all-inclusive cybersecurity measures and policies at all levels and across all branches of government. Cybersecurity and privacy have gained importance as the pandemic has shifted more government services online and increased expectations of connectivity. State governments have been positioned on the frontlines of protecting citizens as they engage with critical services. We recognize that individualized, piecemeal efforts need to be replaced by a more proactive, comprehensive approach to cybersecurity.

NCDIT's Enterprise Security and Risk Management Office (ESRMO), which has been in existence since 2004, is the state's enterprise entity for cybersecurity concerns. The ESRMO supports the state by providing leadership in the development, delivery, and maintenance of a cybersecurity program that safeguards the state's information and supporting infrastructure against unauthorized use, disclosure, modification, damage, and loss. The ESRMO takes a whole-of-state approach to cybersecurity management, partnering with federal, state, and local entities to gain and share insights that help inform policy and strategy statewide. The ESRMO also works with the state's IT Strategy Board and its Cybersecurity and Privacy committee, which prioritizes cyber needs across the state. The committee and the IT Strategy Board help promote the importance of cybersecurity investment and ensure that state decision-makers are aware of the funding requirements for a robust cybersecurity presence.

The statewide strategy is established based on a gap analysis that considers feedback and recommendations from partners. We also rely on our relationships with local government organizations for regular engagement and communication on their initiatives and needs. We have made a concerted effort to build relationships outside of executive-level agency support, including the establishment of the N.C. Joint Cybersecurity Task Force (JCTF) which consists of the N.C. Department of Information Technology (NCDIT), N.C. Division of Emergency Management, N.C. National Guard Cyber Security Response Force, and the N.C. Local Government Information Systems Association (NCLGISA) Cybersecurity Strike Team.

IMPLEMENTATION

Information-sharing and collaboration are crucial in fighting cybercrime. With our whole-of-state approach, teamwork is essential for success in the prevention of and preparation for incidents.

North Carolina takes a multi-pronged approach to fighting cybercrime:

1. Mandatory Cyber Incident Reporting – Reporting cyber incidents as they occur reduces the risk to citizen-facing services and sensitive data. In 2019 the NC General Assembly passed N.C.G.S. 143B-1379 which required that all local government entities report cyber incidents to NCDIT within 24 hours of discovery.

   While local governments are not required to use state resources to confront cybersecurity challenges, NCDIT and the JCTF actively engage local governments (includes cities, municipalities, local school administrative units, and community colleges) to raise awareness of the resources and services that are available.

2. Prohibition of ransom payment – North Carolina is the first state in the country to prohibit state agencies, local governments, and public educational institutions from making payments in response to ransomware attacks. The prohibition is designed to eliminate the potential financial incentive for cybercriminals to launch ransomware attacks against state and local agencies in North Carolina. The ban became law with the enactment of the state budget appropriations act in November 2021. It also prohibits public entities from otherwise communicating with malicious actors after a ransomware attack – defined as the introduction of software into an information system that encrypts data, renders the system unusable, and issues a payment demand for data decryption.

   The law, Senate Bill 105, also directs public bodies subject to ransomware attacks to consult with NCDIT and empowers the State Chief Information Officer to coordinate statewide response to ransomware attacks and all other cybersecurity incidents Private-sector entities are also encouraged to report ransomware attacks. The ransom payment prohibition and consultation requirements apply to all state agencies and local governments which include (but are not limited to): cities, counties, municipalities, local school administrative units, and community colleges.

3. The NC Information Sharing and Analysis Center (NC-ISAAC) – works to provide a common mechanism for raising the level of cybersecurity readiness and response in state and local governments. The NC-ISAAC Cyber Analysis Center receives, vets and correlates information about vulnerability, threat and other significant cyber-related events. NC-ISAAC provides a central resource for gathering information on cyberthreats to critical infrastructure from state agencies and providing two-way sharing of information between and among state agencies and with local governments where permissible.

4. The N.C. Joint Cybersecurity Task Force (JCTF) – a collaborative of state, local and federal government entities that provides cybersecurity support to any government entity in North Carolina – from local and county government administration to K-12 public schools to community colleges. The JCTF is made up of the NCDIT Enterprise Security and Risk Management Office, N.C. Emergency Management, N.C. National Guard Cyber Security Response Force, and the NCLGISA Cybersecurity Strike Team.

When an entity reports and incident, the state provides subject matter expertise, resources, and assistance in various forms ranging from consultation and guidance to deployment of the JCTF to assist as needed. Support services include:

- Incident coordination
- Resource support
- Technical assistance
- On-scene incident recovery

The JCTF works to remediate and recover infrastructure and data compromised during an attack and to provide training that can help prevent future cybersecurity incidents. Work by the task force varies case to case but often involves:

- Identifying indicators of compromise to stop the spread of malicious software and to reduce the impact of ransomware
- Remediating vulnerabilities in computer networks
- Helping rebuild computer networks and workstations

5. IT Strategy Board Cybersecurity and Privacy Committee – comprised of representatives from the University of North Carolina System, state agency chief information security officers, NCLGISA, National Guard, and private organizations, the committee is tasked with prioritization of cyber needs, helping to set the state's cybersecurity strategies, and ensuring that the whole-of-state approach is comprehensive and effective. The committee meets monthly, working to:

    - Advocate for legislative policies that will help promote statewide cybersecurity and privacy.
    - Improve cybersecurity maturity of local governments to increase trust.
    - Increase education and awareness of cybersecurity and privacy threats for residents of the state in partnership with K-12 schools, Community Colleges, and University Systems.
    - Develop a workforce development/training and education framework for cybersecurity and privacy which includes partnerships with educational institutions for training, support for incident response, and on-the-job training.
    - Encourage programs to support education and awareness of cybersecurity and improve the pipeline and maturity of workforce development for this industry.

This multi-pronged approach allows us to maximize the impact of our monitoring, reporting, strategic prioritization, multi-jurisdictional collaboration, and long-term planning activities.

IMPACT

The North Carolina Joint Cybersecurity Task Force is comprised of the North Carolina National Guard Cyber Security Response Force (NCNG CSRF), the NCDIT, the NCLGISA Cybersecurity Strike Team, and the North Carolina Division of Emergency Management.

Since 2019 the JCTF has supported more than 60 significant cybersecurity incidents, with 29 of those incidents occurring in 2021. North Carolina defines significant cybersecurity incidents as any cybersecurity incident that threatens the availability, confidentially or integrity of data. The JCTF's support is primarily geared toward state and local governments as well as community colleges and K-12 entities; however, all North Carolina critical infrastructure partners, as defined by the Department of Homeland Security, are eligible for JCTF services free of charge.

In 2021 our Task Force supported 29 cybersecurity incident responses with more than 100 events including such as ransomware, supply chain compromises and denial-of-service attacks against voice services. The 29 incidents impacted a variety of entities:

- 8 – County governments
- 8 – Municipal governments
- 5 – State agencies
- 2 – Community colleges/universities
- 2 – SCADA/ICS
- 1 – K-12 entity
- 1 – County rescue squad
- 1 – Regional airport
- 1 – City utility provider

Event prevention and preparedness

Election security

NCDIT, NC Emergency Management, NC National Guard, NC State Board of Elections and dozens of other local, state and federal organizations partner to protect our state's election results. As part of their work to protect elections, this group:

- Synchronizes communications between participating organizations to providing cybersecurity practices and training
- Conducts tabletop exercises
- Conducts monthly meetings and reviews with the State Board
- Assesses network infrastructures in the state's 100 counties to identify and remediate issues before an election.

Incident prevention

Member organizations of the JCTF also provide local public entities with the tools they needed to prevent cyber incidents. In the last two years, as part of the whole-of-state approach, these entities have:

- Conducted cyber tabletop exercises for local government and K-12 organizations being hit heavily by ransomware attacks to build muscle memory on best practice steps to take during a cyber incident, encourage information sharing and expand cyber knowledge

- Extended intrusion detection and prevention services to 42 county governments, school districts and community colleges, adding intrusion detection and prevention services to augment local governments' existing security controls and abilities to defend themselves against cyberthreats.
- Implemented continuous monitoring of external networks for 100 counties as well as executive branch state agencies, 58 community colleges and 118 local education authorities using security scoring mechanisms that report on vulnerabilities identified and changes to the environment Reports are automatically sent to entities when their security posture is impacted by changes. (Community colleges and local education authorities were funded due to the CARES Act.)
- Conducted proactive security assessments on the infrastructure of an additional 23 counties and provided recommended hardening and remediation prioritization

Both the governor and the general assembly have recognized that the whole-of-state approach to cybersecurity and the JCTF are proven and effective strategies for prioritizing the protection of our state's critical infrastructure and key resources. In late 2021, the North Carolina General Assembly approved the 2021-2023 state budget including $7.5 million in annual recurring funding for cybersecurity, which is managed and directed by NCDIT.

NCDIT will devote the new funding to cybersecurity and risk management to strengthen the state's cyber defense and enhance our whole-of-state approach to cybersecurity across all levels of government. With this funding, NCDIT will also initiate the development of a three- to five-year cyber strategic plan by the State Chief Risk Officer, which will guide NCDIT's engagement with local government partners in cybersecurity.

This funding marks the largest increase in recurring cyber funding in NCDIT's history. Previously, the department relied heavily on one-time funding sources, which created uncertainty and undermined the sustainability of cyber programs and initiatives. With this annual recurring funding, the department will be better positioned to undertake long-term initiatives and support local government partners as we together securely reach citizens with the digital services they need.
In addition, in March 2022, Governor Cooper issued Executive Order 254 formally recognizing and establishing the JCTF.

With our comprehensive and collaborative whole-of-state approach we have been able to provide support to the entire state, and with formal recognition and increased funding we will be able to expand these services.