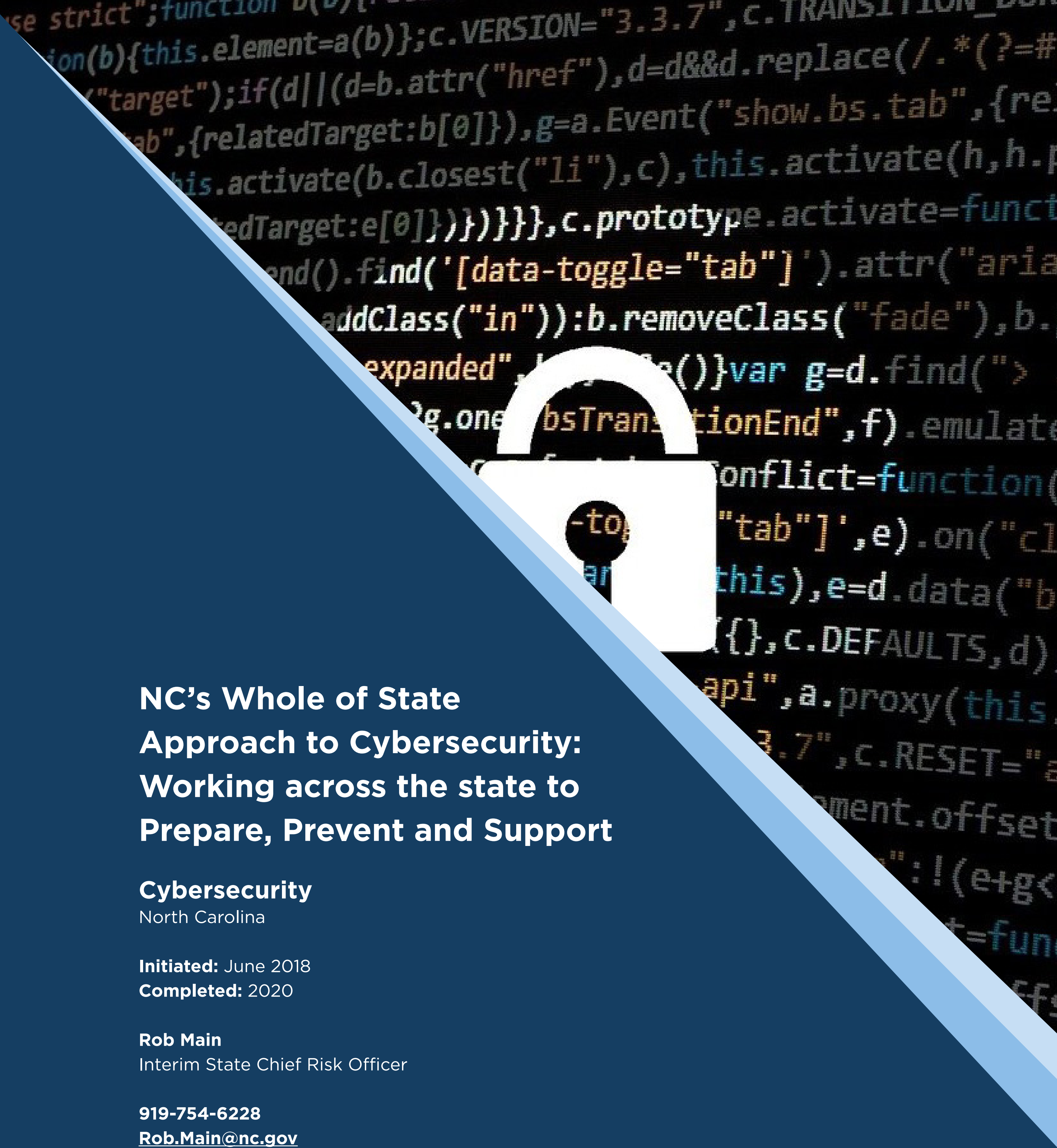

NC's Whole of State Approach to Cybersecurity: Working across the state to Prepare, Prevent and Support

Cybersecurity
North Carolina

Initiated: June 2018
Completed: 2020

Rob Main
Interim State Chief Risk Officer

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

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY
Broadband Infrastructure Office

EXECUTIVE SUMMARY

Cyber incidents continue to be an increasing concern for state, local, and academic institutions in North Carolina. Every year, there has been a noted increase of attacks in the form of ransomware, data exfiltration and extortion and others, which have a devastating impact to our state's critical infrastructure. This trend is forecasted to continue and remain a pervasive occurrence in the upcoming years.

From 2016 to 2019, local governments, community colleges and public school systems in North Carolina reported 17 ransomware attacks of varying degrees to the N.C. Department of Information Technology. In 2020, alone, NCDIT received the same number of reports. Of the 34 attacks since 2016, city or county government entities reported 31 of them.

While we know there is no way to avoid all attacks, North Carolina has adopted a Whole-of-State approach to cybersecurity that is working to prevent and prepare for incidents, and support entities when they occur. This approach has three main components:

1. Data sharing through the NC Information Sharing Analysis Center (NC-ISAC)
2. The creation of the N.C. Joint Cybersecurity Task Force, and
3. Implementing mandatory incident reporting

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. Cyberattacks are evolving and becoming more sophisticated. It is an all hands on deck approach to fighting it. We cannot be siloed in our collection of information. Information sharing is key to preventing cyberattacks from happening and mitigating their impact when they do.

Through North Carolina's comprehensive and collaborative approach, we have been able to provide support to all 100 counties whether it be preventing an event by providing monitoring tools, to providing training and tabletop exercises to actually providing boots on the ground when an incident occurs. The cybersecurity community in NC government has become a big team that supports one another and shares knowledge and experiences.

IDEA

Cyberattacks – from business email compromise to ransomware attacks – are on the rise, and state and local governments are prime targets for cybercriminals. Hackers are increasing their focus on what they call soft targets – education, hospitals, local governments and public administration agencies.

From 2016 to 2019, local governments, community colleges and public school systems in North Carolina reported 17 ransomware attacks of varying degrees to the N.C. Department of Information Technology. In 2020, alone, NCDIT received the same number of reports. Of the 34 attacks since 2016, city or county government entities reported 31 of them.

It is no wonder these "soft targets" are high on hackers' list of targets. County and city governments are at the forefront of providing important services to residents. And these entities do not always have the same technical or financial resources to invest in a robust cybersecurity program, nor do they always have the expertise or human resources to monitor networks for threats, raise awareness among network users or to respond to major cyber incidents. They are the "easy gets," – the "low-hanging fruit," so to speak – for cybercriminals.

The end result, potentially, is great harm to people, businesses and governments in North Carolina in the form of a disruption of services – from soon-to-be homeowners being able to close on a house to the delay of potentially life-saving assistance.

To try to mitigate the risks in this space, North Carolina has adopted a "whole of state" approach to cybersecurity. This approach acknowledges that teamwork is essential for success in the prevention of and preparation for incidents. In North Carolina this is accomplished through a three-pronged approach:

1. The creation of the NC Information Sharing Analysis Center (NC-ISAC) which works to provide a common mechanism for raising the level of cybersecurity readiness and response in state and local governments. The NC-ISAC Cyber Analysis Center receives, vets and correlates information about vulnerability, threat and other significant cyber-related events. NC-ISAC 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 the state agencies and with local government where permissible.
2. The creation of the NC Joint Cybersecurity Task Force, a collaborative of state, local and federal government entities that provides to any government entity in North Carolina – from local and county government administration to K-12 public schools to community colleges – When an entity reports and incident, the state is able to provide subject matter experts, resources, and assistance in various forms ranging from consultation and guidance, to deployment of the NC Joint Cyber Security Task Force to assist as needed. This includes:
   - Incident coordination
   - Resource support
   - Technical assistance
   - On-scene incident recovery

The goals are 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 generally 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
- Leaving the affected entity with a stronger cybersecurity posture

3. Mandatory Cyber Incident Reporting- Reporting cyber incidents as they occur is a method to reduce 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. Proposed legislation is making its way through the 2021 session of the General Assembly which would prevent NC governmental agencies from paying ransom in response to a ransomware incident. This will greatly reduce the likelihood of repeat attacks.

It is important to note that local governments are not required to use state resources to confront cybersecurity challenges, but NCDIT and the cybersecurity task force actively engage local governments to raise awareness of the resources and services that are available.

The Joint Cybersecurity Task Force has been a force multiplier which extends the cyber defensive and incident response capabilities of NC governmental agencies. They are trusted partners across the state with a proven track record of excellence that is worthy of benchmarking across the country. The task force is a textbook example – and one of only a few in the nation – of a collaborative effort among local, state, and federal government entities to prevent and mitigate the effects of cybersecurity incidents. It is what NCDIT refers to as a whole-of-state approach to cybersecurity and should soon become the new normal for cyber defense.

"'State is in our title," says NC State Chief Risk Officer Maria Thompson. "But 'state' doesn't necessarily just mean state agencies."

"It is also NCDIT's job to work with and help protect North Carolina's local jurisdictions," Thompson adds.

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. Cyberattacks are evolving and becoming more sophisticated. It is an all hands on deck approach to fighting it. We cannot be siloed in our collection of information. Information sharing is key to preventing cyberattacks from happening and mitigating their impact when they do.

Regardless of the security controls in place, no government entity is immune from a cyberattack, as the first line of defense against one is often the most flawed and unpredictable – the busy network user who accidentally clicks on a link or attachment in a phishing email, triggering the stealth download and installation of malicious software. Hackers count on it.

IMPLEMENTATION

The NC Joint Cybersecurity Task Force is comprised of NCDIT, which oversees the task force, NC Emergency Management and the NC National Guard Defensive Cyber Operations Team, both divisions of the state's Department of Public Safety. The task force also includes federal partners – such as the FBI and U.S. Department of Homeland Security – and IT professionals at the local-government level who make up what is referred to as the local IT Strike Team.

The IT Strike Team is a group of volunteers and members of the North Carolina Local Government Information Systems Association (NCLGISA), an association of local government IT professionals. Strike team members volunteer their time and skills and, along with the National Guard, serve as boots on the ground to provide on-scene response and recovery services.

When supporting an entity affected by a ransomware attack, the various members of the Joint Cyber Security Task Force:

- Work in tandem to leverage their collective response expertise
- Apply their knowledge of cyberthreats
- Preserve key evidence
- Use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice

The group provides analysis and forensics of security events to conduct threat analysis, damage assessment, containment, eradication and recovery.

The NC Joint Cybersecurity Task Force was formed out of what started in 2018 as a memorandum of understanding between the NCDIT, the NC Department of Public Safety, NC Emergency Management and the NC National Guard, allowing NCDIT to activate the National Guard's cyber unit to support mitigation and recovery operations following a cyberattack without requiring a declaration from the governor. It eventually grew to include federal partners as well as the local IT Strike Team.

As a result of NCDIT's efforts to modernize the state's cybersecurity laws to support better reporting and coordination across government, local and state government entities are required under N.C.G.S. 143B-1379 (passed in 2019) to report cybersecurity incidents to NCDIT within 24 hours of being discovered.
By establishing this law, the state will be able to better prevent, track, and respond to cyber events across the state. The law was not designed to penalize those entities where incidents occur but by reporting the incident, entities will have access to resources that wouldn't otherwise be at their disposal.

Once NCDIT receives a report, the Joint Cybersecurity Task Force conducts initial scoping meetings with the affected entity and continue to hold situation meetings on a regular, if not daily, basis throughout the response and recovery. Topics discussed could include public communication, threat hunting, forensic analysis, network and server reconstitution, endpoint cleaning and environmental hardening and any other issue that might arise.

Knowledge sharing is critical to help mitigate the potential impact of an attack. Because no two cyberattacks are the same and cybercriminals keep making these attacks more sophisticated, there is no template for how to respond. Building off what members learn from previous attacks, the cyber task force looks at each incident individually to determine the best course of action.

IMPACT

The impact the whole of state approach and the collaborative culture it has created in North Carolina is quite remarkable. We are now able to not only share information across the state, but look for trends and assist entities in prevention, preparation and response. When cyber incidents are reported, the task force and its members respond quickly. Below are some of the biggest impacts the task force and its members has had in North Carolina:

Ransomware attacks and other incidents

- **Durham County 2020 Ransomware Attack**
  When Durham County was hit with a ransomware attack in February 2020 it devastated the county's IT infrastructure including all end user devices. The task force immediately responded and offered its assistance. One immediate action was to provide loaner laptops to the county so it could get back up and running as quickly as possible. The NCDIT Enterprise Endpoint Management Team delivered 25 laptops to the Durham County IT group.

  "The cyberattack devastated our county IT infrastructure, including all end user devices, rendering everything useless overnight," said Ari Schein, deputy emergency manager for Durham County Office of Emergency Services. "Loaner laptops from NCDIT and other sources were distributed across the spectrum of mission-essential functions and were able to quickly restore the county to a functional status."

- In addition to supporting Durham County, assistance was provided to 16 additional state, local and academic institutions. This support came in the form of incident response (IR) support, remediation and recovery from ransomware attacks by funding and supporting the National Guard's North Carolina Assessment and Assist Team's IR efforts.

- **Ransomware attacks in both Person and Chatham counties**
  The JCTF Task force mobilized to support the counties. Each engagement began with a scoping assessment and quickly pivoted to actionable tasks which included threat hunting, digital forensics collection and analysis, and the reconstitution of the affected environment. The task force provided resources in the form of personnel, tools, and equipment that the counties lacked.

In 2019, the task force directly supported remediation and recovery for six of the 11 reported ransomware incidents within North Carolina. Below are of the highlights.

- **Columbus County Schools ransomware attack**
  "NCDIT brought together resources from across the state to assist us with rebuilding our network in a way that would be safe and more secure," said Deanne Meadows, superintendent of Columbus County Schools. "The coordinated daily conference calls during the first two weeks ensured that all parties were working in the same direction. Maria Thompson and her team quickly responded to our needs by pulling resources together from across the state. Even a year later, the Enterprise Security and Risk Management team is still involved in checking on our IT team to make sure our network is secure."
- A cyberattack affected a local sheriff's office and 911 operations center in Lincoln County. The task force mobilized resources, put boots on the ground, led the recovery efforts, and coordinated with federal and state partners on threat intel sharing. The result was the sound and secure reconstitution of the electronic environment while concurrently allowing for the continuity of operations.

Event prevention and preparedness

- **Prepared for the 2020 Elections**
  Protecting the 2020 general election results in North Carolina began long before November 3, 2020 votes were cast. Work started a year earlier with a unique, joint collaborative. This group included NCDIT, NC Emergency Management, NC National Guard, NC State Board of Elections and dozens of other local, state and federal partners. As part of their work to protect the election, this group:
  - Synchronized communications between participating organizations to providing cybersecurity practices and training
  - Conducted tabletop exercises
  - Conducted monthly meetings and reviews with the State Board
  - Assessed network infrastructures in the state's 100 counties to identify and remediate issues before the election.

  "As we planned for elections and responded to any cybersecurity issues at the state and county levels, NCDIT and its partners were with us every step of the way," said
  Karen Bell, NC State Board of Elections Executive Director.

- 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

Member organizations of the NC JCFTS provided 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:

- Deployed iSensors on 20 county infrastructures to proactively monitor and block malicious attacks to local networks and to facilitate the information sharing of threats
- 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

Through North Carolina's comprehensive and collaborative approach, we have been able to provide support to all 100 counties whether it be preventing an event by providing monitoring tools, to providing training and tabletop exercises to providing boots on the ground when an incident occurs. The cybersecurity community in NC government has become a big team that supports one another and shares knowledge and experiences.