Key NC Cybersecurity Legislation

G.S. 143-800, amended by SL2021-180

G.S. 143B-1320, amended by SL2021-180

G.S. 143B-1379(c), amended by SL2021-180

Article 84, Various Technology Regulations.

GS143-800: State entities and ransomware payments.

UNC SCHOOL OF GOVERNMENT

(a) No State agency or local government entity shall submit payment or otherwise communicate with an entity that has engaged in a cybersecurity incident on an information technology system by encrypting data and then subsequently offering to decrypt that data in exchange for a ransom payment.

(b) Any State agency or local government entity experiencing a ransom request in connection with a cybersecurity incident shall consult with the Department of Information Technology in accordance with G.S. 143B-1379.

(c) The following definitions apply in this section:
(1) Local government entity. – A local political subdivision of the State, including, but not limited to, a city, a county, a local school administrative unit as defined in G.S. 115C-5, or a community college.

Cybersecurity Incident Reporting Requirement

UNC SCHOOL OF GOVERNMENT

G.S. 143B-1379(c), amended by SL2021-180

(c) Local government entities, as defined in **G.S. 143-800(c)(1)**, shall report cybersecurity incidents to the Department. Information shared as part of this process will be protected from public disclosure under G.S. 132-6.1(c). Private sector entities are encouraged to report cybersecurity incidents to the Department.

.

A Significant Cybersecurity Incident…

- **G.S. 143B-1320(a)(14a)** Ransomware attack. – A cybersecurity incident where a malicious actor introduces software into an information system that encrypts data and renders the systems that rely on that data unusable, followed by a demand for a ransom payment in exchange for decryption of the affected data.

- **G.S. 143B-1320(a)(16a)** Significant cybersecurity incident. – A cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, or public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:

  a. Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information: 1. That is not releasable to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or 2. That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.
  b. Incidents that involve information that is not recoverable or cannot be recovered within defined timelines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through additional measures and has a high or medium functional impact to the mission of an agency

Methods of Contact to Report Cybersecurity Incident

UNC SCHOOL OF GOVERNMENT

- **NC EM 24 Hr Watch:** 800-858-0368 (monitored 24/7)
- **NCLGISA Strike Team:** itstriketeam@nclgisa.org or (919) 726-6508 (monitored 24/7)
- **MCNC NOC: 877-466-2736**
- **FBI IC3: https://www.ic3.gov/**
  - If you have a situation involving financial fraud, please contact the FBI first because there is a ~72 hour window for fund recovery before it is moved off-shore.
- **NCDIT:** https://it.nc.gov/resources/cybersecurity-risk-management/statewide-cybersecurity-incident-report-form