

# SENATE APPROPRIATIONS COMMITTEE FISCAL NOTE

**BILL NO.** Senate Bill 726

**PRINTER NO.** 829

**AMOUNT**

See Fiscal Impact

**FUND**

General Fund

**DATE INTRODUCED**

May 28, 2021

**PRIME SPONSOR**

Senator Phillips-Hill

**DESCRIPTION**

Senate Bill 726 amends Title 18 (Crimes and Offenses) of the Pennsylvania Consolidated Statutes by adding a new Subchapter F to provide for the offense of ransomware and impose duties on the Office of Administration.

This legislation amends Chapter 76 of Title 18 by adding a new Subchapter F (Ransomware) that makes the possession, use, sale, threat to use ransomware or inducement of another person to commit one of these acts a crime, authorizes civil actions by victims of a ransomware attack and requires the Office of Administration to study the susceptibility, preparedness and ability to respond on the part of Commonwealth agencies to ransomware attacks.

Section 7672 (relating to definitions) provides for certain definitions, of which include:

- “Commonwealth agency” is any of the following:
  - 1) The Governor’s Office;
  - 2) A department, board, commission, authority or other agency of the Commonwealth that is subject to the policy supervision and control of the Governor;
  - 3) The Office of the Lieutenant Governor;
  - 4) An independent department;
  - 5) An independent agency;
  - 6) A municipality;
  - 7) A school district;
  - 8) An intermediate unit;
  - 9) An area career or technical school;
  - 10) A charter or cyber school;
  - 11) A community college;
  - 12) A State-owned institution;
  - 13) A State-related institution;
  - 14) A court or agency of the unified judicial system; or
  - 15) The General Assembly.

# SENATE APPROPRIATIONS COMMITTEE

## FISCAL NOTE

- “Ransomware” as follows:
  - 1) A computer contaminant or lock placed without authorization into a computer, computer system or computer network that does any of the following:
    - Restricts access to a computer, computer system or computer network or to any data held within, coupled with a demand for payment of money or other consideration to:
      - A. Remove the contaminant or lock;
      - B. Restore access to the computer, computer system or computer network; or
      - C. Otherwise remediate the impact of the contaminant or lock.
    - Transforms data into an unreadable or unusable form without the use of a confidential process or key.

Section 7673 (relating to prohibited actions) provides that a person may not, with the intent to extort money or other consideration from another person or a Commonwealth agency for the purpose of removing a computer contaminant or lock, restoring access to a computer, computer system, computer network or data or otherwise remediating the impact of a computer contaminate or lock:

- Knowingly possess ransomware;
- Use ransomware without authorization;
- Sell, transfer or develop ransomware;
- Threaten to use ransomware; or
- Induce another person to commit the above acts.

The above-mentioned prohibitions do not apply to the use of ransomware for research purposes by an authorized agent of the Commonwealth or the federal government.

Section 7674 (relating to grading of offenses) generally provides that if a person is convicted of, found guilty of or pleads guilty or nolo contendere in a court of record to one of the acts described in section 7673, the person shall be subject to the following:

- Misdemeanor of the first degree, punishable by a term of imprisonment, the maximum of which is not more than five years, and a fine not exceeding \$10,000, if the consideration sought is less than \$10,000;
- Felony of the third degree, punishable by a term of imprisonment, the maximum of which is not more than seven years, and a fine not exceeding \$15,000, if the consideration sought is at least \$10,000 but less than \$100,000;
- Felony of the second degree, punishable by a term of imprisonment, the maximum of which is not more than ten years, and a fine not exceeding \$25,000, if the consideration sought is at least \$100,000 but less than \$500,000; or

# SENATE APPROPRIATIONS COMMITTEE

## FISCAL NOTE

- Felony of the first degree, punishable by a term of imprisonment, the maximum of which is more than ten years, and a fine not exceeding \$25,000, if the consideration sought is greater than \$500,000.

All offenses, except for an offense classified as a felony of the first degree, shall be classified one degree higher if the commission of the offense:

- Is a second or subsequent offense;
- Involves the infliction of a physical injury; or
- Involves a computer, computer system or computer network, of a court or agency of the unified judicial system.

Section 7675 (relating to forfeiture) provides that upon conviction of an offense under this subchapter, the court may direct the forfeiture of any computer, computer system, computer network, software or data that is used during the commission of the offense or used as a repository for the storage of software or data illegally obtained in violation of this subchapter.

Section 7676 (relating to limitation of time) provides that an action to prosecute an offense under this subchapter must be commenced within three years from the date of discovery of the commission of the offense.

Section 7677 (relating to notification) provides for timely notification of a ransomware attack to appropriate Commonwealth agencies, the Office of Administration and the Federal Bureau of Investigation.

Section 7678 (relating to payments) provides that, after December 31, 2021, state and local taxpayer money or other public money may not be used to pay an extortion attempt involving ransomware unless the Governor authorizes payment in the event of a declaration of disaster emergency under 35 Pa.C.S. § 7301 (relating to general authority of Governor).

Section 7679 (relating to civil actions) authorizes civil actions by a person or Commonwealth agency to bring an action in the event of a violation of this subchapter to recover any one or more of the following:

- 1) Actual damages;
- 2) Punitive damages; and
- 3) Reasonable attorney fees and other litigation costs reasonably incurred.

Section 7680 (relating to remedies not exclusive) provides that commencement of a criminal prosecution or civil action under this subchapter shall not prohibit or limit the same under any other law.

Section 7681 (relating to Office of Administration) requires the Office of Administration to study the susceptibility, preparedness, and ability to respond to on the part of Commonwealth agencies to ransomware attacks. The Office of Administration shall:

- 1) Develop guidelines and best practices to prevent a ransomware attack;
- 2) Evaluate current data encryption and backup strategies;

# **SENATE APPROPRIATIONS COMMITTEE FISCAL NOTE**

- 3) Evaluate the availability of tools to monitor unusual access requests, computer viruses and computer network traffic;
- 4) Develop guidelines for Commonwealth agencies on responding to a ransomware attack;
- 5) Develop law enforcement response strategies to identify the source of a ransomware attack; and
- 6) Provide recommendations on legislative or regulatory action to protect Commonwealth agencies from a ransomware attack.

The Office of Administration shall prepare and transmit to the General Assembly a report related to the nature of and number of ransomware attacks on Commonwealth agencies no later than July 1 of each year. Commonwealth agencies shall cooperate with the Office of Administration in providing the necessary information for the preparation of the report.

This act shall take effect in 60 days.

## **FISCAL IMPACT:**

This legislation provides that a conviction under this new subchapter is classified from a misdemeanor of the first degree up to a felony of the first degree. Using the Department of Corrections' minimum marginal cost of \$29.44 per inmate/per day, the Commonwealth would incur additional annual costs of approximately \$107,456 for every ten defendants sentenced to a State Correctional Institution.

Prevention of ransomware and network security are considered part of the Commonwealth's Information Technology department's cybersecurity program and current duties. Any costs related to the Office of Administration fulfilling the additional duties within this legislation would be minimal and capable of being accommodated within the agencies' current workload and budget.