BILL ANALYSIS

Senate Research Center
85R13335 ADM-D

S.B. 1477
By: West
Criminal Justice
4/12/2017
As Filed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Ransomware is a malicious software that is introduced onto a computer, network, or system for the purpose of preventing the owner or authorized user of the affected machines from accessing information. The person who introduced the software requests that the owner of the effected machines make a payment or give some other consideration for the release of the system from the ransomware. Ransomware targets can range from individual users, to large corporations, to police stations, to hospitals and law firms.

Not all ransomware targets are created equal. Law firms and hospitals have especially sensitive information, and people's livelihoods and health are at stake. There are also special concerns with regards to law enforcement, who may be prevented from performing their jobs or may lose control of particularly sensitive information.

The Federal Computer Fraud and Abuse Act does address harm through manipulation of medical information, but otherwise classifies the crime based on aggregate cost of the harm. There is not much consideration given to whether the attacker intended to go after especially delicate information, other than financial information covered by the Fair Credit Reporting Act. It also does not make available a means of recourse for Texas law enforcement, instead leaving crimes of this nature to the sole jurisdiction of the federal government.

S.B. 1477 scales the crime based on price of ransom, but also escalates the crime based on the sensitivity of the information targeted. The sensitivity of information is defined as "privileged information": information protected by the attorney-client privilege or by the Health Insurance Portability and Accountability Act (HIPAA). Targeting privileged information immediately raises the offense to a minimal felony level, with the harm done to effected persons being a consideration for escalating the offense to a higher-degree felony. S.B. 1477's "attorney-client privilege" information protection would also escalate the crime for most instances of targeting police departments because of ongoing prosecutions with the district attorney. These escalations would thereby disincentivize criminals from targeting hospitals, law practices, and law enforcement.

As proposed, S.B. 1477 amends current law relating to ransomware, and creates a criminal offense.

RULEMAKING AUTHORITY

This bill does not expressly grant any additional rulemaking authority to a state officer, institution, or agency.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Chapter 33, Penal Code, by adding Section 33.023, as follows:

Sec. 33.023. RANSOMWARE ATTACK AND EXTORTION. (a) Defines "privileged information" and "ransomware."

(b) Provides that a person commits an offense if the person intentionally introduces ransomware onto a computer, computer network, or computer system

without the effective consent of the owner and demands payment or other consideration to remove the ransomware, restore the owner's access to the computer, computer network, or computer system, or otherwise mitigate the effects of the ransomware.

(c) Provides that, except as provided by Subsection (d), an offense under this section is a Class C misdemeanor if the value of the payment or other consideration demanded is less than $100, a Class B misdemeanor if the value of the payment or other consideration demanded is $100 or more but less than $750, a Class A misdemeanor if the value of the payment or other consideration demanded is $750 or more but less than $2,500, a state jail felony if the value of the payment or other consideration demanded is $2,500 or more but less than $30,000, a felony of the third degree if the value of the payment or other consideration demanded is $30,000 or more but less than $150,000, a felony of the second degree if the value of the payment or other consideration demanded is $150,000 or more but less than $300,000, and a felony of the first degree if the value of the payment or other consideration demanded is $300,000 or more.

(d) Provides that an offense under this section, if it is shown on the trial of the offense that the defendant knowingly restricted a victim's access to privileged information, is a state jail felony if the value of the payment or other consideration demanded is less than $2,500; a felony of the third degree if the value of the payment or other consideration demanded is $2,500 or more but less than $30,000, or a client or patient of a victim suffered harm attributable to the offense; a felony of the second degree if the value of the payment or other consideration demanded is $30,000 or more but less than $150,000, or a client or patient of a victim suffered bodily injury attributable to the offense; and a felony of the first degree if the value of the payment or other consideration demanded is $150,000 or more, or a client or patient of a victim suffered serious bodily injury or death attributable to the offense.

(e) Authorizes a person who is subject to prosecution under this section and any other section of this code to be prosecuted under either section or both sections.

SECTION 2. Makes application of this Act prospective.

SECTION 3. Effective date: September 1, 2017.