BILL ANALYSIS

Senate Research Center

H.B. 9
By: Capriglione et al. (Taylor, Van)
Criminal Justice
5/18/2017
Engrossed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Unlike traditional computer trespass, modern cybercrimes no longer infiltrate their targets directly. Instead, criminals use ransomware, malware, and other methods where an unsuspecting person unknowingly facilitates crimes on their own devices. Ransomware, for example, locks people out of their devices with valuable information unless a payment is made to the criminal. H.B. 9 address the activity, not the technology, to ensure a more lasting approach to addressing cybercrime.

H.B. 9 creates an offense for intentionally interrupting or suspending access to a computer system or network without the effective consent of the owner with an exception for law enforcement purpose. For example, this change would criminalize "Denial of Service" attacks. The bill defines "ransomware" for prosecution purposes in a way that captures wrongdoers without preventing service providers from employing security measures on their networks. H.B. 9 also creates an offense for intentionally altering data as it transmits between two computers through deception and without a legitimate business purpose. Allowing network interference for legitimate business purposes allows organizations to regulate and conduct maintenance on networks without violating the provisions of the bill. Offenses in the bill start at a Class A misdemeanor and scale upwards depending on the amount defrauded.

H.B. 9 amends current law relating to cybercrime and creates criminal offenses.

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. Authorizes this Act to be cited as the Texas Cybercrime Act.

SECTION 2. Amends Section 33.01, Penal Code, by amending Subdivision (2) to redefine "aggregate amount" and adding Subdivisions (11-a), (13-a), (13-b), and (13-c) to define "decryption," "decrypt," or "decrypted," "encrypted private information," "encryption," "encrypt," or "encrypted," and "encryption service."

SECTION 3. Amends Chapter 33, Penal Code, by adding Sections 33.022, 33.023, and 33.024, as follows:

> Sec. 33.022. ELECTRONIC ACCESS INTERFERENCE. (a) Provides that a person, other than a network provider or online service provider acting for a legitimate business purpose, commits an offense if the person intentionally interrupts or suspends access to a computer system or computer network without the effective consent of the owner.
>
> > (b) Provides that an offense under this section is a third degree felony.
> >
> > (c) Provides that it is a defense to prosecution under this section that the person acted with the intent to facilitate a lawful seizure or search of, or lawful access to,

a computer, computer network, or computer system for a legitimate enforcement purpose.

Sec. 33.023. ELECTRONIC DATA TAMPERING. (a) Defines "ransomware."

(b) Provides that a person commits an offense if the person intentionally alters data as it transmits between two computers in a computer network or computer system through deception and without a legitimate business purpose.

(c) Provides that a person commits an offense if the person intentionally introduces ransomware onto a computer, computer network, or computer system through deception and without a legitimate business purpose.

(d) Provides that an offense under this section is a Class A misdemeanor, unless the person acted with the intent to defraud or harm another, in which event the offense is a certain felony depending on the aggregate amount involved.

(e) Authorizes the conduct, when benefits are obtained, a victim is defrauded or harmed, or property is altered, appropriated, damaged, or deleted in violation of this section, whether or not in a single incident, to be considered as one offense and the value of the benefits obtained and of the losses incurred because of the fraud, harm, or alteration, appropriation, damage, or deletion of property to be aggregated in determining the grade of the offense.

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

(g) Provides that software is not ransomware for the purposes of this section if the software restricts access to data because authentication is required to upgrade or access purchased content or access to subscription content has been blocked for nonpayment.

Sec. 33.024. UNLAWFUL DECRYPTION. (a) Provides that a person commits an offense if the person intentionally decrypts encrypted private information through deception and without a legitimate business purpose.

(b) Provides that an offense under this section is a Class A misdemeanor, unless the person acted with the intent to defraud or harm another, in which event the offense is a certain felony.

(c) Provides that it is a defense to prosecution under this section that the actor's conduct was pursuant to an agreement entered into with the owner for the purpose of assessing or maintaining the security of the information or of a computer, computer network, or computer system or providing other services related to security.

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

SECTION 4. Amends Section 33.03, Penal Code, to provide that it is an affirmative defense to prosecution under Section 33.02 (Breach of Computer Security) or 33.022 that the actor was an officer, employee, or agent of a communications common carrier or electric utility and committed the proscribed act or acts in the course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the communications common carrier or electric utility.

SECTION 5. Makes application of this Act prospective.

SECTION 6. Effective date: September 1, 2017.