# BILL ANALYSIS

C.S.H.B. 9
By: Capriglione
Government Transparency & Operation
Committee Report (Substituted)

## BACKGROUND AND PURPOSE

Interested parties contend that current law pertaining to cybercrime is outdated because it focuses on the technology used rather than the activity perpetrated. C.S.H.B. 9 seeks to implement a more lasting approach to addressing cybercrime by making certain acts of electronic access interference, electronic data tampering, and unlawful decryption criminal offenses.

## CRIMINAL JUSTICE IMPACT

It is the committee's opinion that this bill expressly does one or more of the following: creates a criminal offense, increases the punishment for an existing criminal offense or category of offenses, or changes the eligibility of a person for community supervision, parole, or mandatory supervision.

## RULEMAKING AUTHORITY

It is the committee's opinion that this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

## ANALYSIS

C.S.H.B. 9 amends the Penal Code to create the third degree felony offense of electronic access interference for a person, other than a network provider acting for a legitimate network operation or protection purpose, who intentionally interrupts or suspends access to a computer system or computer network without the effective consent of the owner. The bill establishes as a defense to prosecution for the offense 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 law enforcement purpose.

C.S.H.B. 9 creates the Class A misdemeanor offense of electronic data tampering for a person who knowingly alters data as it transmits between two computers in a computer network or computer system without the effective consent of the owner and for a person who knowingly introduces malware or ransomware onto a computer, computer network, or computer system without the effective consent of the owner and without a legitimate business purpose. The bill enhances the penalty for the offense if the person acted with the intent to defraud or harm another or alter, appropriate, damage, or delete property and establishes penalty enhancements ranging from a state jail felony to a first degree felony, depending on the aggregate amount involved and if the computer, computer network, or computer system is owned by the government or a critical infrastructure facility. The bill specifies that when benefits are obtained, a victim is defrauded or harmed, or property is altered, appropriated, damaged, or deleted in violation of the bill's provisions, whether or not in a single incident, the conduct may 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 may be aggregated in determining the grade of the offense. A person who is subject to prosecution for the offense of electronic data tampering and any other Penal Code offense may be prosecuted for

either or both offenses.

C.S.H.B. 9 establishes that software is not ransomware for purposes of an electronic data tampering offense if the software restricts access to data because authentication is required to upgrade or access purchased content or because access to subscription content has been blocked for nonpayment. The bill excepts from such offense officers, employees, and agents of certain service providers who commit the proscribed act 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 person's employer and whose alteration of data was consistent with accepted industry technical specifications.

C.S.H.B. 9 establishes as an affirmative defense to prosecution for the offense of electronic access interference and the offense of electronic data tampering involving altering data as it transmits between two computers in a computer network or computer system without the owner's effective consent 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.

C.S.H.B. 9 creates the Class A misdemeanor offense of unlawful decryption for a person who decrypts encrypted private information without the effective consent of the owner. The bill enhances the penalty for the offense if the person acted with the intent to defraud or harm another or alter, appropriate, damage, or delete property and establishes penalty enhancements ranging from a state jail felony to a first degree felony, depending on the aggregate amount involved and if the computer, computer network, or computer system is owned by the government or a critical infrastructure facility. The bill establishes as a defense to prosecution for such offense that the actor's conduct was pursuant to a contract 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. A person who is subject to prosecution for the offense of unlawful decryption and any other Penal Code offense may be prosecuted for either or both offenses.

C.S.H.B. 9 includes the amount of any expenditure required by a victim of a computer crime to attempt to restore, recover, or replace any data altered, acquired, appropriated, damaged, deleted, or disrupted in the definition of "aggregate amount" for purposes of statutory provisions relating to computer crimes.

**EFFECTIVE DATE**

September 1, 2017.

**COMPARISON OF ORIGINAL AND SUBSTITUTE**

While C.S.H.B. 9 may differ from the original in minor or nonsubstantive ways, the following comparison is organized and formatted in a manner that indicates the substantial differences between the introduced and committee substitute versions of the bill.

| INTRODUCED | HOUSE COMMITTEE SUBSTITUTE |
| --- | --- |
| SECTION 1. This Act may be cited as the Texas Cybercrime Act. | SECTION 1. Same as introduced version. |
| No equivalent provision. | SECTION 2. Section 33.01, Penal Code, is amended by amending Subdivision (2) and |

adding Subdivisions (11-a), (13-a), (13-b), and (13-c) to read as follows:

(2) "Aggregate amount" means the amount of:

(A) any direct or indirect loss incurred by a victim, including the value of money, property, or service stolen, appropriated, or rendered unrecoverable by the offense; or

(B) any expenditure required by the victim to:

(i) determine whether data or [~~verify that~~] a computer, computer network, computer program, or computer system was [~~not~~] altered, acquired, appropriated, damaged, deleted, or disrupted by the offense; or

(ii) attempt to restore, recover, or replace any data altered, acquired, appropriated, damaged, deleted, or disrupted.

(11-a) "Decryption," "decrypt," or "decrypted" means the decoding of encrypted communications or information, whether by use of a decryption key, by breaking an encryption formula or algorithm, or by the interference with a person's use of an encryption service in a manner that causes information or communications to be stored or transmitted without encryption.

(13-a) "Encrypted private information" means encrypted data, documents, wire or electronic communications, or other information stored on a computer or computer system, whether in the possession of the owner or a provider of an electronic communications service or a remote computing service, and which has not been accessible to the public.

(13-b) "Encryption," "encrypt," or "encrypted" means the encoding of data, documents, wire or electronic communications, or other information, using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized access to, such information.

(13-c) "Encryption service" means a computing service, a computer device, computer software, or technology with encryption capabilities, and includes any subsequent version of or update to an encryption service.

SECTION 2. Chapter 33, Penal Code, is amended by adding Sections 33.022 and

SECTION 3. Chapter 33, Penal Code, is amended by adding Sections 33.022,

33.023 to read as follows:

Sec. 33.022. ELECTRONIC ACCESS INTERFERENCE. (a) A person 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) An offense under this section is a third degree felony.

(c) 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 law enforcement purpose.

Sec. 33.023. ELECTRONIC DATA TAMPERING. (a) In this section:

(1) "Malware" means computer software used to:

(A) gather data without the effective consent of the owner of the data;

(B) gain access to a computer, computer network, or computer system without the effective consent of the owner; or

(C) disrupt the operation of a computer, computer network, or computer system without the effective consent of the owner.

(2) "Ransomware" means malware that demands a ransom payment to:

(A) restore access to a person's property; or

(B) not publish the person's data.

(b) A person commits an offense if the person:

(1) alters data as it transmits between two computers in a computer network or computer system without the effective consent of the owner; or

(2) introduces malware, including ransomware, onto a computer, computer network, or computer system without the effective consent of the owner.

(c) An offense under this section is a Class

33.023, and 33.024 to read as follows:

Sec. 33.022. ELECTRONIC ACCESS INTERFERENCE. (a) A person, other than a network provider acting for a legitimate network operation or protection 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) An offense under this section is a third degree felony.

(c) 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 law enforcement purpose.

Sec. 33.023. ELECTRONIC DATA TAMPERING. (a) In this section:

(1) "Malware" means computer software used to:

(A) gather data without the effective consent of the owner of the data;

(B) gain access to a computer, computer network, or computer system without the effective consent of the owner; or

(C) disrupt the operation of a computer, computer network, or computer system without the effective consent of the owner.

(2) "Ransomware" means a computer contaminant or lock that restricts access by an unauthorized person to a computer, computer system, or computer network or any data in a computer, computer system, or computer network under circumstances in which a person demands money, property, or a service to remove the computer contaminant or lock, restore access to the computer, computer system, computer network, or data, or otherwise remediate the impact of the computer contaminant or lock.

(b) A person commits an offense if the person knowingly alters data as it transmits between two computers in a computer network or computer system without the effective consent of the owner.

(c) A person commits an offense if the person knowingly introduces malware or ransomware onto a computer, computer network, or computer system without the effective consent of the owner and without a legitimate business purpose.

(d) An offense under this section is a Class

A misdemeanor, unless the person acted with the intent to defraud or harm another or alter, damage, or delete property, in which event the offense is:

(1) a state jail felony if the aggregate amount involved is $2,500 or more but less than $30,000;

(2) a felony of the third degree if the aggregate amount involved is $30,000 or more but less than $150,000;

(3) a felony of the second degree if:

(A) the aggregate amount involved is $150,000 or more but less than $300,000; or

(B) the aggregate amount involved is any amount less than $300,000 and the computer, computer network, or computer system is owned by the government or a critical infrastructure facility; or

(4) a felony of the first degree if the aggregate amount involved is $300,000 or more.

(d) When benefits are obtained, a victim is defrauded or harmed, or property is altered, damaged, or deleted in violation of this section, whether or not in a single incident, the conduct may be considered as one offense and the value of the benefits obtained and of the losses incurred because of the fraud, harm, or alteration, damage, or

deletion of property may be aggregated in determining the grade of the offense.

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

A misdemeanor, unless the person acted with the intent to defraud or harm another or alter, appropriate, damage, or delete property, in which event the offense is:

(1) a state jail felony if the aggregate amount involved is $2,500 or more but less than $30,000;

(2) a felony of the third degree if the aggregate amount involved is $30,000 or more but less than $150,000;

(3) a felony of the second degree if:

(A) the aggregate amount involved is $150,000 or more but less than $300,000; or

(B) the aggregate amount involved is any amount less than $300,000 and the computer, computer network, or computer system is owned by the government or a critical infrastructure facility; or

(4) a felony of the first degree if the aggregate amount involved is $300,000 or more.

(e) 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, the conduct may 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 may be aggregated in determining the grade of the offense.

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

(g) Software is not ransomware for the purposes of this section if the software restricts access to data because:

(1) authentication is required to upgrade or access purchased content; or

(2) access to subscription content has been blocked for nonpayment.

(h) It is an exception to the application of Subsection (b) that:

(1) the person was an officer, employee, or agent of:

(A) an Internet service provider;

(B) a computer service provider;

(C) a provider of information service, as that term is defined by 47 U.S.C. Section 153;

(D) an interactive computer service, as that term is defined by 47 U.S.C. Section 230;

(E) an electronic communications service,

| | |
|---|---|
| | as that term is defined by Article 18.20, Code of Criminal Procedure; or<br>(F) a cable service provider or video service provider, as those terms are defined by Section 66.002, Utilities Code;<br>(2) the person committed the proscribed act 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 person's employer; and<br>(3) the alteration of data was consistent with accepted industry technical specifications. |
| No equivalent provision. | Sec. 33.024. UNLAWFUL DECRYPTION.<br>(a) A person commits an offense if the person decrypts encrypted private information without the effective consent of the owner.<br>(b) An offense under this section is a Class A misdemeanor, unless the person acted with the intent to defraud or harm another, or alter, appropriate, damage, or delete property, in which event the offense is:<br>(1) a state jail felony if the aggregate amount involved is less than $30,000;<br>(2) a felony of the third degree if the aggregate amount involved is $30,000 or more but less than $150,000;<br>(3) a felony of the second degree if:<br>(A) the aggregate amount involved is $150,000 or more but less than $300,000; or<br>(B) the aggregate amount involved is any amount less than $300,000 and the computer, computer network, or computer system is owned by the government or a critical infrastructure facility; or<br>(4) a felony of the first degree if the aggregate amount involved is $300,000 or more.<br>(c) It is a defense to prosecution under this section that the actor's conduct was pursuant to a contract entered into with the owner for the purpose of:<br>(1) assessing or maintaining the security of the information or of a computer, computer network, or computer system; or<br>(2) providing other services related to security.<br>(d) A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections. |

| | |
|---|---|
| SECTION 3. Section 33.03, Penal Code, is amended. | SECTION 4. Substantially the same as introduced version. |
| SECTION 4. The change in law made by this Act applies only to an offense committed on or after the effective date of this Act. An offense committed before the effective date of this Act is governed by the law in effect on the date the offense was committed, and the former law is continued in effect for that purpose. For purposes of this section, an offense was committed before the effective date of this Act if any element of the offense occurred before that date. | SECTION 5. Same as introduced version. |
| SECTION 5. This Act takes effect September 1, 2017. | SECTION 6. Same as introduced version. |