SENATE AMENDMENTS

2nd Printing

By: Capriglione, Elkins, Blanco, et al. H.B. No. 9

A BILL TO BE ENTITLED

AN ACT

relating to cybercrime; creating criminal offenses.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. This Act may be cited as the Texas Cybercrime Act.

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 3. Chapter 33, Penal Code, is amended by adding Sections 33.022, 33.023, and 33.024 to read as follows:

Sec. 33.022. ELECTRONIC ACCESS INTERFERENCE. (a) 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) 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, "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 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) 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) 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:

(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.

Sec. 33.024. UNLAWFUL DECRYPTION. (a) A person commits an offense if the person intentionally decrypts encrypted private

information through deception and without a legitimate business purpose.

(b) 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:

(1) a state jail felony if the aggregate amount involved is 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.

(c) 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:

(1) assessing or maintaining the security of the information or of a computer, computer network, or computer system; or

(2) providing other services related to security.

(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 4. Section 33.03, Penal Code, is amended to read as follows:

Sec. 33.03. DEFENSES. It is an affirmative defense to prosecution under Section 33.02 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. 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 6. This Act takes effect September 1, 2017.

ADOPTED

MAY 24 2017

Secretary of the Senate

FLOOR AMENDMENT NO. 1 BY: Lonnie Burton

Amend H.B. No. 9 (senate committee printing) as follows:

(1) In the recital to SECTION 2 of the bill (page 1, line 26), strike "(13-b), and (13-c)" and substitute "(13-b), (13-c), and (15-a)".

(2) In SECTION 2 of the bill, amending Section 33.01, Penal Code (page 1, between lines 59 and 60), insert the following:

(15-a) "Privileged information" means:

(A) protected health information, as that term is defined by Section 182.002, Health and Safety Code;

(B) information that is subject to the attorney-client privilege; or

(C) information that is subject to the accountant-client privilege under Section 901.457, Occupations Code, or other law, if the information is on a computer, computer network, or computer system owned by a person possessing a license issued under Subchapter H, Chapter 901, Occupations Code.

(3) In SECTION 3 of the bill, strike added Section 33.023(d), Penal Code (page 2, lines 29-44), and substitute the following:

(d) Subject to Subsections (d-1) and (d-2), an offense under this section is a Class C misdemeanor.

(d-1) Subject to Subsection (d-2), if it is shown on the trial of the offense that the defendant acted with the intent to defraud or harm another, an offense under this section is:

(1) a Class C misdemeanor if the aggregate amount involved is less than $100 or cannot be determined;

(2) a Class B misdemeanor if the aggregate amount involved is $100 or more but less than $750;

(3) a Class A misdemeanor if the aggregate amount

involved is $750 or more but less than $2,500;

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

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

(6) a felony of the second degree if the aggregate amount involved is $150,000 or more but less than $300,000; and

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

(d-2) If it is shown on the trial of the offense that the defendant knowingly restricted a victim's access to privileged information, an offense under this section is:

(1) a state jail felony if the value of the aggregate amount involved is less than $2,500;

(2) a felony of the third degree if:

(A) the value of the aggregate amount involved is $2,500 or more but less than $30,000; or

(B) a client or patient of a victim suffered harm attributable to the offense;

(3) a felony of the second degree if:

(A) the value of the aggregate amount involved is $30,000 or more but less than $150,000; or

(B) a client or patient of a victim suffered bodily injury attributable to the offense; and

(4) a felony of the first degree if:

(A) the value of the aggregate amount involved is $150,000 or more; or

(B) a client or patient of a victim suffered serious bodily injury or death attributable to the offense.

(4) In SECTION 3 of the bill, strike added Section 33.024(b), Penal Code (page 2, line 65, through page 3, line 11),

and substitute the following:

(b) Subject to Subsections (b-1) and (b-2), an offense under this section is a Class C misdemeanor.

(b-1) Subject to Subsection (b-2), if it is shown on the trial of the offense that the defendant acted with the intent to defraud or harm another, an offense under this section is:

(1) a Class C misdemeanor if the value of the aggregate amount involved is less than $100 or cannot be determined;

(2) a Class B misdemeanor if the value of the aggregate amount involved is $100 or more but less than $750;

(3) a Class A misdemeanor if the value of the aggregate amount involved is $750 or more but less than $2,500;

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

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

(6) a felony of the second degree if the value of the aggregate amount involved is $150,000 or more but less than $300,000; and

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

(b-2) If it is shown on the trial of the offense that the defendant knowingly decrypted privileged information, an offense under this section is:

(1) a state jail felony if the value of the aggregate amount involved is less than $2,500;

(2) a felony of the third degree if:

(A) the value of the aggregate amount involved is $2,500 or more but less than $30,000; or

(B) a client or patient of a victim suffered harm

attributable to the offense;

(3) a felony of the second degree if:

(A) the value of the aggregate amount involved is $30,000 or more but less than $150,000; or

(B) a client or patient of a victim suffered bodily injury attributable to the offense; and

(4) a felony of the first degree if:

(A) the value of the aggregate amount involved is $150,000 or more; or

(B) a client or patient of a victim suffered serious bodily injury or death attributable to the offense.

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

May 25, 2017

TO: Honorable Joe Straus, Speaker of the House, House of Representatives

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB9** by Capriglione (Relating to cybercrime; creating criminal offenses.), **As Passed 2nd House**

No significant fiscal implication to the State is anticipated.

The bill would amend the Penal Code relating to computer crimes to create the offenses of electronic access interference, electronic data tampering, and unlawful decryption. The bill also would provide criminal penalties for these offenses and certain defenses to prosecution.

The Office of Court Administration indicates any increased caseload would likely be absorbed within existing resources. This analysis assumes the provisions of the bill addressing felony sanctions for criminal offenses would not result in a significant fiscal impact on state correctional agencies.

The bill would take effect September 1, 2017 and would apply only to an offense committed on or after the effective date of the Act.

Local Government Impact

According to the Texas Association of Counties, the fiscal impact to counties is not anticipated to be significant.

A Class A misdemeanor is punishable by the fine of not more than $4,000, confinement in jail for a term not to exceed one year, or both. Costs associated with enforcement, prosecution, and confinement could likely be absorbed within existing resources. Revenue gain from fines imposed and collected is not anticipated to have a significant fiscal implication.

Source Agencies: 212 Office of Court Administration, Texas Judicial Council, 696 Department of Criminal Justice

LBB Staff: UP, KJo, LM, AKU, LBO, RC

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

April 23, 2017

TO: Honorable John Whitmire, Chair, Senate Committee on Criminal Justice

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB9** by Capriglione (Relating to cybercrime; creating criminal offenses.), **As Engrossed**

No significant fiscal implication to the State is anticipated.

The bill would amend the Penal Code relating to computer crimes to create the offenses of electronic access interference, electronic data tampering, and unlawful decryption. The bill also would provide criminal penalties for these offenses and certain defenses to prosecution.

The Office of Court Administration indicates any increased caseload would likely be absorbed within existing resources. This analysis assumes the provisions of the bill addressing felony sanctions for criminal offenses would not result in a significant fiscal impact on state correctional agencies.

The bill would take effect September 1, 2017 and would apply only to an offense committed on or after the effective date of the Act.

Local Government Impact

According to the Texas Association of Counties, the fiscal impact to counties is not anticipated to be significant.

A Class A misdemeanor is punishable by the fine of not more than $4,000, confinement in jail for a term not to exceed one year, or both. Costs associated with enforcement, prosecution, and confinement could likely be absorbed within existing resources. Revenue gain from fines imposed and collected is not anticipated to have a significant fiscal implication.

Source Agencies: 212 Office of Court Administration, Texas Judicial Council, 696 Department of Criminal Justice

LBB Staff: UP, KJo, LM, AKU, LBO, RC

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

March 29, 2017

TO: Honorable Gary Elkins, Chair, House Committee on Government Transparency & Operation

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB9** by Capriglione (Relating to cybercrime; creating criminal offenses.), **Committee Report 1st House, Substituted**

No significant fiscal implication to the State is anticipated.

The bill would amend the Penal Code relating to computer crimes to create the offenses of electronic access interference, electronic data tampering, and unlawful decryption. The bill also would provide for criminal penalties for these offenses and certain defenses to prosecution.

According to the Office of Court Administration, any increased caseload would likely be absorbed within existing resources. This analysis assumes the provisions of the bill addressing felony sanctions for criminal offenses would not result in a significant fiscal impact on state correctional agencies.

The bill would take effect September 1, 2017 and would apply only to an offense committed on or after the effective date of the Act.

Local Government Impact

According to the Texas Association of Counties, the fiscal impact to counties is not anticipated to be significant.

A Class A misdemeanor is punishable by the fine of not more than $4,000, confinement in jail for a term not to exceed one year, or both. Costs associated with enforcement, prosecution, and confinement could likely be absorbed within existing resources. Revenue gain from fines imposed and collected is not anticipated to have a significant fiscal implication.

Source Agencies: 212 Office of Court Administration, Texas Judicial Council, 696 Department of Criminal Justice

LBB Staff: UP, LBO, LM, AKU, RC

LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

March 19, 2017

TO: Honorable Gary Elkins, Chair, House Committee on Government Transparency & Operation

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB9** by Capriglione (Relating to cybercrime; creating criminal offenses.), **As Introduced**

No significant fiscal implication to the State is anticipated.

The bill would amend the Penal Code relating to computer crimes to create two criminal offenses: electronic access interference and electronic data tampering. The bill also would provide for criminal penalties for these offenses and certain defenses to prosecution.

According to the Office of Court Administration, any increased caseload would likely be absorbed within existing resources. This analysis assumes the provisions of the bill addressing felony sanctions for criminal offenses would not result in a significant fiscal impact on state correctional agencies.

The bill would take effect September 1, 2017 and would apply only to an offense committed on or after the effective date of the Act.

Local Government Impact

According to the Texas Association of Counties, the fiscal impact to counties is not anticipated to be significant.

A Class A misdemeanor is punishable by a fine of not more than $4,000, confinement in jail for a term not to exceed one year, or both. Costs associated with enforcement, prosecution and confinement could likely be absorbed within existing resources. Revenue gain from fines imposed and collected is not anticipated to have a significant fiscal implication.

Source Agencies: 212 Office of Court Administration, Texas Judicial Council, 696 Department of Criminal Justice

LBB Staff: UP, LBO, LM, AKU, RC, JGA

LEGISLATIVE BUDGET BOARD
Austin, Texas

CRIMINAL JUSTICE IMPACT STATEMENT

85TH LEGISLATIVE REGULAR SESSION

May 25, 2017

TO: Honorable Joe Straus, Speaker of the House, House of Representatives

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB9** by Capriglione (Relating to cybercrime; creating criminal offenses.), **As Passed 2nd House**

The provisions of the bill addressing felony sanctions are the subject of this analysis. The bill would amend the Penal Code to create the offenses electronic access interference, electronic data tampering, and unlawful decryption. Under the provisions of the bill, certain individuals who intentionally interrupt or suspend access to a computer system or network without the effective consent of the owner could be prosecuted for electronic access interference, a third degree felony. The bill would also make electronic data tampering, intentionally altering data as it transmits between two computers in a computer network or system or introducing ransomware onto a computer or a computer network or system through deception and without a legitimate business purpose, a criminal offense. Intentionally decrypting encrypted private information through deception and without a legitimate business purpose as outlined in the bill's provisions would be unlawful decryption, a criminal offense. The punishments for electronic data tampering and unlawful decryption would range from a misdemeanor to a felony with the punishment based on intent, the type of system or network involved, the amount of pecuniary loss, and other circumstances of the offense.

A first degree felony is punishable by confinement in prison for life or a term from 5 to 99 years; a second degree felony for a term from 2 to 20 years; a third degree felony for a term from 2 to 10 years; and a state jail felony is punishable by confinement in state jail for a term from 180 days to 2 years or Class A misdemeanor punishment. In addition to confinement, most felony offenses are also subject to an optional fine not to exceed $10,000.

Creating an offense is expected to result in increased demands on the correctional resources of the counties or of the State due to a potential increase in the number of individuals placed under supervision in the community or sentenced to a term of confinement within state correctional institutions. However, this analysis assumes the provisions of the bill addressing felony sanctions would not result in a significant impact on the demand for state correctional resources.

Source Agencies:
LBB Staff: UP, LM, AKU

LEGISLATIVE BUDGET BOARD
Austin, Texas

CRIMINAL JUSTICE IMPACT STATEMENT

85TH LEGISLATIVE REGULAR SESSION

April 23, 2017

TO: Honorable John Whitmire, Chair, Senate Committee on Criminal Justice

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB9** by Capriglione (Relating to cybercrime; creating criminal offenses.), **As Engrossed**

The provisions of the bill addressing felony sanctions are the subject of this analysis. The bill would amend the Penal Code to create the offenses electronic access interference, electronic data tampering, and unlawful decryption. Under the provisions of the bill, certain individuals who intentionally interrupt or suspend access to a computer system or network without the effective consent of the owner could be prosecuted for electronic access interference, a third degree felony. The bill would also make electronic data tampering, intentionally altering data as it transmits between two computers in a computer network or system or introducing ransomware onto a computer or a computer network or system through deception and without a legitimate business purpose, a criminal offense. Intentionally decrypting encrypted private information through deception and without a legitimate business purpose as outlined in the bill's provisions would be unlawful decryption, a criminal offense. The punishments for electronic data tampering and unlawful decryption would range from a misdemeanor to a felony with the punishment based on intent, the type of system or network involved, and the amount of pecuniary loss.

A first degree felony is punishable by confinement in prison for life or a term from 5 to 99 years; a second degree felony for a term from 2 to 20 years; a third degree felony for a term from 2 to 10 years; and a state jail felony is punishable by confinement in state jail for a term from 180 days to 2 years or Class A misdemeanor punishment. In addition to confinement, most felony offenses are also subject to an optional fine not to exceed $10,000.

Creating an offense is expected to result in increased demands on the correctional resources of the counties or of the State due to a potential increase in the number of individuals placed under supervision in the community or sentenced to a term of confinement within state correctional institutions. However, this analysis assumes the provisions of the bill addressing felony sanctions would not result in a significant impact on the demand for state correctional resources.

Source Agencies:
LBB Staff: UP, LM, AKU

LEGISLATIVE BUDGET BOARD
Austin, Texas

CRIMINAL JUSTICE IMPACT STATEMENT

85TH LEGISLATIVE REGULAR SESSION

March 29, 2017

TO: Honorable Gary Elkins, Chair, House Committee on Government Transparency & Operation

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB9** by Capriglione (Relating to cybercrime; creating criminal offenses.), **Committee Report 1st House, Substituted**

The provisions of the bill addressing felony sanctions are the subject of this analysis. The bill would amend the Penal Code to create the offenses of electronic access interference, electronic data tampering, and unlawful decryption.

Under the provisions of the bill, an individual who intentionally interrupts or suspends access to a computer system or network without the effective consent of the owner could be prosecuted for electronic access interference, a third degree felony. The bill would also make altering data as it transmits between two computers in a computer network or system without the effective consent of the owner or introducing malware or ransomware onto a computer or a computer network or system without the effective consent of the owner punishable as criminal offense. Decrypting encrypted private information without the effective consent of the owner as outlined in the bill's provisions would also be a criminal offense. The punishments for electronic data tampering and unlawful decryption would range from a misdemeanor to a felony with the punishment based on intent, the type of system or network involved, and the amount of pecuniary loss.

A first degree felony is punishable by confinement in prison for a term from 5 to 99 years; a second degree felony for a term from 2 to 20 years; a third degree felony for a term from 2 to 10 years; and a state jail felony is punishable by confinement in state jail for a term from 180 days to 2 years or Class A Misdemeanor punishment. In addition to confinement, all felony level offenses are also subject to an optional fee not to exceed $10,000.

Creating an offense is expected to result in increased demands upon the correctional resources of counties or of the State due to a potential increase in the number of individuals sentenced to a term of supervision in the community or a term of incarceration within state correctional institutions. However, this analysis assumes implementing the provisions of the bill would not result in a significant impact on the demand for state correctional resources.

Source Agencies:
LBB Staff: UP, AKU, LM

LEGISLATIVE BUDGET BOARD
Austin, Texas

CRIMINAL JUSTICE IMPACT STATEMENT

85TH LEGISLATIVE REGULAR SESSION

March 19, 2017

TO: Honorable Gary Elkins, Chair, House Committee on Government Transparency & Operation

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB9** by Capriglione (Relating to cybercrime; creating criminal offenses.), **As Introduced**

The provisions of the bill addressing felony sanctions are the subject of this analysis. The bill would amend the Penal Code to create two new offenses: electronic access interference and electronic data tampering. Under the provisions of the bill, an individual who intentionally interrupts or suspends access to a computer system or network without the effective consent of the owner could be prosecuted for electronic access interference, a third degree felony. The bill would also make altering data as it transmits between two computers in a computer network or system without the effective consent of the owner or introducing malware onto a computer or a computer network or system without the effective consent of the owner punishable as criminal offense. The punishment for electronic data tampering would range from a misdemeanor to a felony with the punishment level based on intent, the type of system or network involved, and the amount of pecuniary loss.

A first degree felony is punishable by confinement in prison for a term from 5 to 99 years; a second degree felony for a term from 2 to 20 years; a third degree felony for a term from 2 to 10 years; and a state jail felony is punishable by confinement in state jail for a term from 180 days to 2 years or Class A Misdemeanor punishment. In addition to confinement, all felonies are also subject to an optional fee not to exceed $10,000.

Creating an offense is expected to result in increased demands upon the correctional resources of counties or of the State as a result of additional individuals placed under supervision in the community, incarcerated in state correctional institutions, or placed under parole supervision. However, this analysis assumes implementing the provisions of the bill would not result in a significant impact on the demand for state correctional resources.

Source Agencies:
LBB Staff: UP, LM, AKU