SUBJECT: Creating offenses for certain cybercrimes

COMMITTEE: Government Transparency and Operation — committee substitute recommended

VOTE: 7 ayes — Elkins, Capriglione, Gonzales, Lucio, Shaheen, Tinderholt, Uresti

0 nays

WITNESSES: For — (*Registered, but did not testify*: Meredyth Fowler, Independent Bankers Association of Texas; Mark Mendez, Tarrant County; Vincent Giardino, Tarrant County Criminal District Attorney's Office; Caroline Joiner, TechNet; Justin Yancy, Texas Business Leadership Council; Michael Goldman, Texas Conservative Coalition; Thomas Parkinson)

Against — None

On — W. Scott McCollough, Data Foundry, Inc.; (*Registered, but did not testify*: Sacha Jacobson)

BACKGROUND: Penal Code, ch. 33 governs computer crimes, including gaining access to a computer or computer system for various reasons without the consent of the owner. Penalties range from a class C misdemeanor (maximum fine of $500) to a first-degree felony (life in prison or a sentence of five to 99 years and an optional fine of up to $10,000).

DIGEST: CSHB 9 would create new offenses under Penal Code, ch. 33 for electronic access interference, electronic data tampering, and unlawful decryption.

Electronic access interference. CSHB 9 would make it a crime for a person to intentionally interrupt or suspend access to a computer system or network without the effective consent of the owner, unless the person was a network provider acting for a legitimate purpose. An offense would be a third-degree felony (two to 10 years in prison and an optional fine of

up to $10,000).

It would be a defense to prosecution that the person acted with intent to lawfully seize, search, or access a computer, system, or network for legitimate law enforcement purposes.

It would be an affirmative defense to prosecution that the actor was working for a communications common carrier or electric utility and the act was committed in the course of employment and was necessary to render service or to protect the rights or property of the carrier or utility.

Electronic data tampering. The bill would make it a crime for a person to knowingly and without the owner's consent:

- alter data as it transmitted between two computers in a computer network or system; or
- introduce malware or ransomware, as defined in the bill, onto a computer or computer network or system without a legitimate business reason.

An offense would be a class A misdemeanor (up to one year in jail and/or a maximum fine of $4,000) unless the person acted with the intent to defraud or harm another or to alter, appropriate, damage, or delete property, in which case the offense would be:

- a state-jail felony (180 days to two years in a state jail and an optional fine of up to $10,000) if the aggregate amount involved was at least $2,500 but less than $30,000;
- a third-degree felony (two to 10 years in prison and an optional fine of up to $10,000) if the aggregate amount involved was at least $30,000 but less than $150,000;
- a second-degree felony (two to 20 years in prison and an optional fine of up to $10,000) if the aggregate amount involved was at least $150,000 but less than $300,000 or any amount less than $300,000 and the computer, network, or system was owned by the government or a critical infrastructure facility; or

- a first-degree felony (life in prison or a sentence of five to 99 years and an optional fine of up to $10,000) if the aggregate amount involved was $300,000 or more.

In certain cases, conduct could be considered as one offense and the value of the benefits obtained or losses incurred could be aggregated in determining the grade of the offense. The aggregate amount would include the value of money, service, or property appropriated or any expenditure required by the victim to determine whether data or property was affected or to restore, recover, or replace any data affected.

The bill would provide an exception to the offense of altering data as it transmitted between two computers if the act was committed in the course of employment for certain service providers and was consistent with accepted industry technical specifications. This exception would apply to those working for an internet service provider, a computer service provider, an information service provider, an interactive computer service, an electronic communications service, or a cable or video service provider.

For the crime of altering data, it would be an affirmative defense to prosecution that the actor was working for a communications common carrier or electric utility and the act was committed in the course of employment and was necessary to render service or to protect the rights or property of the carrier or utility.

Unlawful decryption. The bill would make it a crime to decrypt encrypted private information without the owner's consent. An offense would be a class A misdemeanor unless the person acted with the intent to defraud or harm another or to alter, appropriate, damage, or delete property, in which case the offense would be:

- a state-jail felony if the aggregate amount involved was less than $30,000;
- a third-degree felony if the aggregate amount involved was at least $30,000 but less than $150,000;

- a second-degree felony if the aggregate amount involved was at least $150,000 but less than $300,000 or any amount less than $300,000 and the computer, network, or system was owned by the government or a critical infrastructure facility; or
- a first-degree felony if the aggregate amount involved was $300,000 or more.

It would be a defense to prosecution that a person under contract with the owner was providing services related to security, including assessing or maintaining the security of the information or of a computer, network, or system.

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

SUPPORTERS SAY:

CSHB 9 would mitigate concerns that current law does not address many cybercrimes by updating state law to criminalize certain cyber activities and reflect current technologies. Under the bill, it would be an offense to interfere with access to a computer system, tamper with electronic data, or unlawfully decrypt encrypted private information.

Current law covers cybercrimes that are carried out through direct access, such as computer trespass, but many cybercrimes are perpetrated by criminals who use malware, ransomware, or other means to get a person to unknowingly facilitate the criminal activity on that person's own device. These activities can harm citizens, businesses, and governments, but they may not constitute currently defined computer crimes. By focusing on the activities and not the technology, this bill would create a more lasting approach to address all types of cybercrime.

While there may be concerns that actors could be deterred from performing security research, the bill would create a defense to prosecution for those who decrypt encrypted private information to provide security services pursuant to a contract with the owner.

OPPONENTS SAY:

CSHB 9 would make intentionally interrupting or suspending access to a computer network or system without the owner's consent a third-degree felony in every case, but not all denial of service attacks have the same scope and therefore should not be treated equally. For example, some attacks may target the network of a governmental entity or critical infrastructure while others affect smaller networks. Access may be interrupted or suspended for an hour or for days. It would be better to start the offense at a misdemeanor or other lesser penalty and allow it to be increased based on the impact to the targeted computer network or system.

Criminalizing the decryption of encrypted data could result in unintended consequences for security research. Governmental entities and companies may employ hackers to test vulnerabilities in their systems to prevent bad actors from infiltrating, but much security research is independent. This bill potentially could criminalize efforts by university researchers or other actors to discover vulnerabilities in systems, creating a deterrent effect. It is important to incentivize people to not only discover vulnerabilities in systems but also to inform entities about the vulnerabilities.

NOTES:

CSHB 9 differs from the bill as filed in several ways, including by:

- creating the offense of unlawful decryption;
- excluding a network provider acting for a legitimate network operation or protection purpose from the offense of electronic access interference;
- specifying that a person committed the offense of electronic data tampering if the person did so knowingly;
- creating an exception to the offense of altering data for employees of certain providers who were acting necessarily in the course of employment; and
- adding and expanding certain definitions.

A companion bill, SB 1020 by V. Taylor, was referred to the Senate Committee on Criminal Justice on March 6.