SUBJECT: Enhancing the penalties for a breach of computer security

COMMITTEE: Criminal Jurisprudence — committee substitute recommended

VOTE: 8 ayes — Gallego, Christian, Fletcher, Miklos, Moody, Riddle, Vaught, Vo

0 nays

3 absent — Hodge, Kent, Pierson

SENATE VOTE: On final passage, April 17 — 28-0

WITNESSES: For — Katrina Daniels, Bexar County District Attorney's Office; (*Registered, but did not testify:* Marc Chavez, Lubbock County District Attorney's Office; Teresa Clingman, Midland County District Attorney's Office; Kevin Petroff, Harris County District Attorney's Office; Jim Rudd, West Texas Gas Processing L.P., West Texas Gas Inc.; Ballard C. Shapleigh, 34th Judicial District Attorney's Office)

Against — (*Registered, but did not testify:* Matt Simpson, ACLU of Texas)

On — (*Registered, but did not testify:* Douglas Kunkel, DPS)

BACKGROUND: Under Penal Code, sec. 33.02, a person commits an offense by knowingly accessing a computer, computer network, or computer system without the consent of the owner. A breach of computer security is a class B misdemeanor (up to 180 days in jail and/or a maximum fine of $2,000). The penalty increases to anywhere between a class A misdemeanor (up to one year in jail and/or a maximum fine of $4,000) and a first-degree felony (life in prison or a sentence of five to 99 years and an optional fine of up to $10,000) depending on the aggregate amount of monetary value involved.

When benefits are obtained, a victim is defrauded or harmed, or property is altered, damaged, or deleted in violation, 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 may be aggregated in determining the grade of the offense.

DIGEST:

CSSB 1662 would amend Penal Code, sec. 33.02 to create two separate crimes involving the breach of computer security. The first would involve any unauthorized access. The second would involve unauthorized access with intent to obtain a benefit, defraud, or harm another, or alter, damage, or delete property. The bill would enhance penalties for both.

Unauthorized access. A person who knowingly accessed a computer, computer network, or computer system without the effective consent of the owner would be punished with a class B misdemeanor (up to 180 days in jail and/or a maximum fine of $2,000). The penalty would be a state-jail felony if the defendant had previously been convicted two or more times of a computer-related offense under Penal Code, ch. 33 or if the compromised computer, computer network, or computer system was owned by the government or a critical infrastructure facility.

Unauthorized access with intent to harm. A person would commit an offense if with intent to obtain a benefit, defraud, or harm another, or alter, damage, or delete property, the person knowingly accessed a computer, computer network, or a computer system without the effective consent of the owner. The offense would be punishable as a state-jail felony if the aggregate amount involved was less than $20,000. The offense would be 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 $20,000 or more but less than $100,000. The offense would be 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 any amount less than $200,000 and the compromised computer, computer network, or computer system was owned by the government or a critical infrastructure facility. The penalty would be a first-degree felony if the aggregate amount involved was $200,000 or more.

CSSB 1662 would define a “critical infrastructure facility” to be:

- a chemical manufacturing facility;
- a refinery;
- an electrical power generating facility, substation, switching station, electrical control center, or electrical transmission or distribution facility;

- a water intake structure, water treatment facility, wastewater treatment plant, or pump station;
- a natural gas transmission compressor station;
- a liquid natural gas terminal or storage facility;
- a telecommunications central switching office;
- a port, railroad switching yard, trucking terminal, or other freight transportation facility;
- a gas processing plant, including a plant used in the processing, treatment, or fractionation of natural gas;
- a transmission facility used by a federally licensed radio or television station; or
- a cable television or video service provider headend.

The bill would take effective September 1, 2009, and apply to offenses committed on or after the effective date.

SUPPORTERS SAY:

CSSB 1662 would amend the Penal Code, sec. 33.02, to reform the offense of breach of computer security. Under the current statute, it is difficult to measure monetarily the damages caused by a breach of a computer or computer system. While these amounts can be established, it takes a great deal of effort by highly trained computer-forensics teams, whose skills are better used preventing and combating breaches rather than pricing the damage done after an attack.

Under the current statute, criminal penalties for the breach of computer security do not account for breaches that resulted in:

- the theft of personal identification information from a computer system, which is often a precursor to the crime of identity theft;
- access to such information such as credit card sales logs or employment applications;
- access to a government computer network;
- access to a piece of critical infrastructure such as refineries, rail-road computer networks, or utilities.

CSSB 1662 would address these issues by creating two offenses for breach of computer security. The first would involve unauthorized access. The second would cover unauthorized access with intent to harm which would provide appropriate punishments for the theft of information that could lead to identity theft. Both would provide enhancements to deter

repeat offenders and would provide enhancements for a breach of a computer or computer network of a critical infrastructure facility.

According to the LBB, CSSB 1662 would not result in a significant cost to the state.

OPPONENTS SAY:

Enhancement of criminal penalties rarely provides a deterrent effect. Many of the breaches of the computer systems of critical infrastructure in the United States come from outside of the country. Government efforts would be better spent strengthening those systems or requiring higher security standards.

Texas cannot afford to enhance the penalties for its criminal laws. While this enhancement might not be expected to significantly increase the cost of the Texas criminal justice system, every penalty enhancement the Legislature approves contributes to an increase in that cost. The Legislature only should enhance penalties in a measured manner, being sure to look at the overall impact of all enhancements.

NOTES:

The committee substitute differs from the Senate-passed version in that it includes a cable television or video service provider headend in the list of critical infrastructure facilities.