SUBJECT: Describing breach of computer security to specify obtaining data

COMMITTEE: Criminal Jurisprudence — committee substitute recommended

VOTE: 6 ayes — Herrero, Moody, Canales, Hunter, Shaheen, Simpson

0 nays

1 absent — Leach

WITNESSES: For — (*Registered, but did not testify*: Jessica Anderson, Houston Police Department)

Against — (*Registered, but did not testify*: Mark Bennett, Harris County Criminal Lawyers Association)

On — Kate Murphy, Texas Public Policy Foundation

BACKGROUND: Penal Code, sec. 33.02 establishes penalties for breach of computer security involving the intent to harm or defraud another or to alter, damage, or delete property. The penalty for such an offense ranges from a a state-jail felony (180 days to two years in a state jail and an optional fine of up to $10,000) 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) depending on the entity that owns the computer, network, or system and the aggregate dollar amount of the loss incurred by the victim.

DIGEST: CSHB 896 would expand the description of breach of computer security involving the intent to harm or defraud another or to alter, damage, or delete property. It would be a crime for a person to access a computer, computer network, or computer system owned by the government, a business, or another commercial entity:

- in violation of a clear and conspicuous prohibition by the owner or a contractual agreement to which the person had expressly agreed; and

- with the intent to obtain or use a file, data, or proprietary information stored in the computer, network, or system.

For a breach of computer security crime described above, the bill would create a defense to prosecution if the actor's conduct was taken pursuant to a contract with the owner of the computer, network, or system to:

- assess the security of the computer, computer network, or computer system; or
- provide other security-related services.

The bill would take effect September 1, 2015, and would apply only to an offense committed on or after that date.

SUPPORTERS SAY:

CSHB 896 would make it easier to prosecute computer hackers who maliciously breach computer security without necessarily demonstrating intent to defraud or harm another or alter, damage, or delete property. This intent can be difficult to prove under current law because hackers often take information or data for reasons other than to cause harm to the owner. For example, some hackers are simply interested in accessing, disseminating, or selling information that does not belong to them. This bill would allow proof of obtaining or using a file, data, or proprietary information stored in the computer, network, or system to serve as proof of intent to defraud or harm another or alter, damage or delete property.

This bill primarily would be used to target individuals who commit crimes significant enough to be punished under the more severe penalties in Penal Code, sec. 33.02. It would place an emphasis on hacking that causes a significant amount of damage and on individuals who hack into government or critical infrastructure facility computers, networks, and systems.

OPPONENTS SAY:

CSHB 896 is overly broad and would criminalize activities that are not generally considered hacking. It would criminalize accessing computers, networks, or systems in violation of contractual agreements if the person intended to obtain or use a file, data, or proprietary information. That

provision could be used to prosecute violations of terms of service agreements, which the vast majority of the public do not read. Any time someone accesses any website or network, that person could be using data — and if that person did so in violation of a terms of service agreement, that person could be prosecuted under this bill. There is already extensive law that protects parties to contracts, and the criminal justice system should not be used to enforce these contracts.

OTHER OPPONENTS SAY:

Language in the bill as introduced would have made it easier for a prosecutor to convict a defendant of the offense in question by showing that a hacker who accessed a computer without permission did so with intent to obtain a benefit and not necessarily with intent to cause harm or damage property. It is not clear that CSHB 896 would allow a prosecutor to obtain a conviction for a breach of computer security described in the bill without first demonstrating that the offender intended to defraud or harm another or alter, damage, or delete property.

NOTES:

The committee substitute differs from the filed bill in that CSHB 896 would add to the description of a breach of computer security under Penal Code, sec. 33.02(b-1) that the person, in violation of a clear prohibition or contractual agreement, accessed a computer, network, or system owned by a government or business or other commercial entity with the intent to obtain or use a file, data, or proprietary information stored within.

CSHB 896 removed language in the bill as introduced that would have created an offense for a person who, in violation of a clear prohibition or contractual agreement, breached computer security with the intent to obtain a benefit. The committee substitute also would create a defense to prosecution for actions taken under contract to assess the security of a computer, network, or system.

The companion bill, SB 345 by Huffman, was approved by the Senate on April 9 and referred to the House Criminal Jurisprudence Committee on April 15.