

BILL ANALYSIS

C.S.H.B. 3396
By: Hernandez Luna
Criminal Jurisprudence
Committee Report (Substituted)

BACKGROUND AND PURPOSE

Observers note that a breach of computer security offense is a Class B misdemeanor when there is no proof of actual monetary damages. It is further noted that there also is no enhanced punishment for committing this offense when monetary damages are not incurred or evidenced. A breach of computer security, as interested parties note, may include obtaining personal identifiers from a computer system, which is often a precursor to the crime of identity theft, obtaining access to credit card sales logs or employment applications, and obtaining access to a governmental computer network. In addition, the parties note that it is difficult to prove the amount of actual monetary damages immediately resulting from a network intrusion.

C.S.H.B. 3396 seeks to address this issue by providing enhanced penalties for breach of computer security offenses that involve computers owned by the government or certain public and private utilities considered to be critical infrastructure facilities.

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. 3396 amends the Penal Code to enhance the penalty for breach of computer security from a Class B misdemeanor to a state jail felony if the defendant has been previously convicted two or more times of a computer crime or the computer, computer network, or computer system knowingly accessed without the owner's effective consent is owned by the government or a critical infrastructure facility.

C.S.H.B. 3396, in the provision of law establishing a range of penalties based on the aggregate amount involved in an offense of breach of computer security in which the actor knowingly obtains a benefit, defrauds or harms another, or alters, damages, or deletes property, instead makes that range of penalties apply if the actor commits an offense of breach of computer security with the intent to obtain a benefit, defraud or harm another, or alter, damage, or delete property.

C.S.H.B. 3396, in that same range of penalties, removes the minimum aggregate amount involved in the offense that classifies the offense as a third degree felony to make it a third degree felony if the aggregate amount involved is less than \$100,000 and removes the Class A misdemeanor and state jail felony penalties for amounts below that removed minimum. The bill, in that same range of penalties, makes it a second degree felony if the aggregate amount involved in the breach of computer security offense is any amount less than \$200,000 and the computer, computer network, or computer system is owned by the government or a critical infrastructure facility. The bill makes it a second degree felony if the actor obtains the identifying information of another by accessing only one computer, computer network, or computer system and makes it a first degree felony if the actor obtains the identifying

information of another by accessing more than one computer, computer network, or computer system.

C.S.H.B. 3396 establishes a defense to prosecution for breach of computer security if the actor 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. The bill defines "critical infrastructure facility" and provides for the meaning of "identifying information" by reference. The bill makes conforming and nonsubstantive changes.

EFFECTIVE DATE

September 1, 2011.

COMPARISON OF ORIGINAL AND SUBSTITUTE

C.S.H.B. 3396 contains a provision not included in the original providing for the meaning of "identifying information."

C.S.H.B. 3396 differs from the original, in the provision of law establishing a range of penalties for breach of computer security based on the aggregate amount involved in the offense, by removing the minimum aggregate amount that classifies the offense as a third degree felony to make it a third degree felony if the aggregate amount involved is less than \$100,000, whereas the original makes it a state jail felony if the aggregate amount involved is less than \$20,000 and retains the range of amounts that makes the offense a third degree felony.

C.S.H.B. 3396 contains provisions not included in the original making it a second degree felony breach of computer security offense if the actor obtains the identifying information of another by accessing only one computer, computer network, or computer system and making it a first degree felony if the actor obtains the identifying information of another by accessing more than one computer, computer network, or computer system.

C.S.H.B. 3396 contains a provision not included in the original establishing a defense to prosecution for breach of computer security if 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.