BILL ANALYSIS

C.S.H.B. 2397
By: Miller, Sid
Criminal Jurisprudence
Committee Report (Substituted)

BACKGROUND AND PURPOSE

The criminal investigations division of the Office of the Attorney General of Texas is tasked with the investigation of certain computer crimes that fall under the offense of breach of computer security. Often, a criminal illegally obtains access to a computer network with the intent to steal another's identifying information, financial information, or trade secrets, all of which do not necessarily have a monetary amount attached. Since penalties for breach of computer security currently vary based on the monetary amount involved in the commission of the offense, there is concern that authorities have experienced difficulty in enforcing punishment for these computer-related crimes. C.S.H.B. 2397 seeks to remedy this situation and provide penalties for the offense that are based both on monetary value and on the specific circumstances under which the offense is committed.

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. 2397 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. 2397, 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. The bill, 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 makes conforming changes by removing the Class A misdemeanor and state jail felony penalties. 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. 2397 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. 2397 omits a provision included in the original increasing the penalty for breach of computer security from a Class B misdemeanor to a third degree felony. The substitute contains provisions not included in the original defining "critical infrastructure facility" and enhancing the penalty for breach of computer security 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 is owned by the government or a critical infrastructure facility.

C.S.H.B. 2397 differs from the original by making the range of penalties for the commission of a breach of computer security apply to the commission of the offense with the intent to obtain a benefit, defraud or harm another, or alter, damage, or delete property and establishing the base penalty for the range as a third degree felony, whereas the original makes it a second degree felony to knowingly obtain a benefit, obtain the identifying information of another, defraud or harm another, or alter, damage, or delete property in committing a breach of computer security offense and removes the range of penalties established for the offense based on the amount of damage.

C.S.H.B. 2397 contains a provision not included in the original making it a second degree felony breach of computer security offense if the aggregate amount involved in the 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 or the actor obtains the identifying information of another by accessing only one computer, computer network, or computer system. The substitute differs from the original by making it a first degree felony breach of computer security offense if the actor obtains the identifying information of another by accessing more than one computer, computer network, or computer system, whereas the original makes it a first degree felony if in committing the offense the actor knowingly obtains a benefit, obtains the identifying information of another, defrauds or harms another, or alters, damages, or deletes property and accesses more than one computer, computer network, or computer system without the effective consent of the owner.

C.S.H.B. 2397 contains a provision not included in the original establishing 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 substitute retains provisions of law repealed in the original authorizing conduct relating to the offense of breach of computer security to be considered as one offense and the value of the benefits obtained and of the losses incurred as a result of the offense to be aggregated in determining the grade of the offense, whether or not the conduct occurred in a single incident. The substitute differs from the original in nonsubstantive ways.