SCHEEF & STONE, L.L.P.
LEGAL COUNSEL BASED ON SOLID PRINCIPLES

Business Cybersecurity
Update

Texas Broadens Unauthorized Access of Computer Law to Specifically Address Insider Misuse

Not that it was really needed, but Texas recently amended its unauthorized access of computers law to specifically address misuse by insiders. Many already read the prior version (one of the broadest) as already prohibiting misuse by insiders. The amended version took effect on September 1, 2015.

BREACH OF COMPUTER SECURITY

Texas' unauthorized access of computers law is titled Breach of Computer Security, Section 33.02 of the Texas Penal Code, a criminal law that has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally, Chapter 143 of the Texas Civil Practice and Remedies Code, titled Harmful Access by Computer.

The civil cause of action permits the recovery of actual damages and reasonable attorney's fees and costs, Tex. Civ. Prac. & Rem. Code 143.002, which is an added benefit for plaintiff's because the Computer Fraud and Abuse Act does not permit the recovery of attorney's fees in most cases. The limitations period is the earlier of five years from the date of the last act or two years from the date the plaintiff had a reasonable opportunity to discover the violation.

PRIOR VERSION OF THE LAW

The Breach of Computer Security law already made it a crime for a person to, "with the intent to defraud or harm another or alter, damage, or delete property … knowingly access[] … a computer, computer network, or computer system without the effective consent of the owner." Tex. Penal Code sec. 33.02 (a).

Consent is not effective if:

"induced by deception … or induced by coercion;"

"given by a person the actor knows is not legally authorized to act for the owner;"

"given by a person who by reason of youth, mental disease or defect, or intoxication is known by the actor to be unable to make reasonable property disposition;"

"given solely to detect the commission of an offense; or"

"used for a purpose other than that for which the consent was given."

Focusing on this last point, the law prohibits a person from (with the intent to defraud or harm another or alter, damage, or delete property) knowingly accessing a computer for a purpose other than that for which the consent was given. That is similar to the Fifth Circuit's Intended-Use Theory for determining unauthorized access under the CFAA, which has been effective in insider misuse cases.

THE AMENDED LAW

The Breach of Computer Security law has been amended, effective September 1, 2015. The new version applies to offenses committed after the effective date. Nothing was removed from the prior version of the law; the following language in blue italics was added as Section 33.02 (b-1)(2) of the Texas Penal Code:

It is a crime for a person to, with the intent to defraud or harm another or alter, damage, or delete property … knowingly access [] … a computer, computer network, or computer system:

(A) that is owned by:
(i) the government; or
(ii) A business or other commercial entity engaged in a business activity;

(B) in violation of:
(i) A clear and conspicuous prohibition by the owner of the computer, computer network, or computer system; or
(ii) A contractual agreement to which the person as expressly agreed; and

(C) with the intent to obtain or use a file, data, or proprietary information stored in the computer, network, or system to defraud or harm another or alter, damage, or delete property.

(f) it is a defense to prosecution under Subsection (b-1)(2) that the actor's conduct consisted solely of action taken pursuant to a contract that was entered into with the owner of the computer, computer network, or computer system for the purpose of assessing the security of the computer, network, or system or providing other security-related services.

PASSING THOUGHTS

The addition of the clear and conspicuous and express contractual agreement requirements for this violation are similar to the baseline requirements for the Fifth Circuit's Intended-Use Theory in applying the CFAA to insider misuse cases. It will be interesting to see how courts apply this new provision vis-a-vis the existing "used for a purpose other than that for which the consent was given." The many discussion points this raises must be continued …

Shawn Tuma (@shawnetuma) is a business lawyer with an internationally recognized reputation in cybersecurity, computer fraud and data privacy law. He is a Cybersecurity & Data Protection Partner at Scheef & Stone, LLP, a full-service business law firm in Texas that represents businesses of all sizes throughout the United States and, through its Mackrell International network, around the world. Contact Shawn at (214) 472-2135 or shawn.tuma@solidcounsel.com.