Computer Abuse and Data Recovery Act (CADRA) White Paper - August 3, 2014

SUMMARY

The proposed Computer Abuse and Data Recovery Act (CADRA) protects owners, operators and lessees of protected computers and owners of information stored in protected computers from hackers and others who misappropriate passwords or override technologic access barriers in protected computers. CADRA is limited to business operations using protected computers which store business information. "Protected computers" are computers which are password protected or which utilize technological access barriers such as security codes, security tokens, key fobs or other access control devices for hardware, software or digital information.

WHY

Florida businesses need an effective civil remedies statute that provides redress for persons who, without authority, access or take computer data, or destroy computer data or systems. These violators might be insiders, such as disloyal employees or bad contractors, or they could be outsiders who hack into computers taking data and potentially destroying hardware, software and valuable data.

Currently, Florida's Computer Crimes Act, Fla. Stat. §. 815.01 et seq., ("Fla-CCA") is not a viable civil liability statute because, in order to support a claim for civil damages, the violator must be first convicted of a computer crime under the statute. Even if this is achieved, the Fla-CCA specifically excludes employees "acting in the scope of their lawful employment" and Florida courts have interpreted "acting in the scope of their lawful employment" to mean that if they EVER had authorized access, the statute does not apply even if they were no longer employees at the time of the access or if they used the data to intentionally harm the employer.

As for federal remedies, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, ("Fed-CFAA") covers similar issues and also provides for a civil remedy, if the damages exceed $5,000. Unlike the Fla-CCA, the Fed-CFAA has both an "unauthorized access" and "exceeds authorized access" cause of action. Like the Fla-CCA, the Fed-CFAA is primarily criminal in nature, and has been strictly construed by some regional federal appellate courts (the 9th and the 4th Circuits). These courts hold that if the accused has any type of authorized access to the data or computer, then he or she does not violate the Act. Other federal appellate courts (the 1st, 5th, and 7th Circuits), have given a broader interpretation of what is meant by "exceeds authorized access." The 11th Circuit seems to lean towards a broader interpretation of the Fed-CFAA, but the scope of the leading 11th Circuit decision is less than clear on this issue. The criminal conviction prerequisite in the Fla-CCA combined with the circuit split with some appellate courts finding no liability makes civil actions under Fed-CFAA increasingly difficult.

CADRA VIOLATIONS

A CADRA violation occurs when a person knowingly and with intent to cause harm or loss (a) obtains information from a protected computer without authorization and causes harm or loss; (b) causes transmission of a program, code or command without authorization to a protected computer and causes harm or loss or (c) traffics in any password, security code or access device through which access to a protected computer may be obtained without authorization. A person who violates Section 668.803(a), (b) or (c) is liable to the owner of the information used in his or her business stored in the protected computer or the owner, operator or lessee of the protected computer.

The injured party may bring a CADRA action seeking to recover actual damages including loss profits and losses and the violator's profits. The injured party may also seek injunctive or other equitable relief to prevent violation of CADRA and to recover the original and all copies of the information which is subject to the violation. This injunctive relief, for the original and all copies, is important in business disputes. Attorneys fees are available to the prevailing party. The action must be brought within three years of the violation or the reasonable discovery thereof.

CADRA defines the term "protected computer" as a computer storing information used in business when the information and/or the computer has a technological access barrier such as a password, security code or token, key fob, access device or other similar measure. "Without authorization," is a predicate for a CADRA violation and means to circumvent the technological access barrier (for example, a password) to the protected computer without the express or implied permission of the owner. "Without authorization" does not include circumventing a technological measure that does not effectively control access to the protected computer or the information stored therein. "Harm" is defined as including impairment to the integrity, access or availability of the data, program or information. A "loss" is (1) any reasonable cost to the owner of the information or the owner of the protected computer, including the reasonable cost of responding to the violation, conducting a damage assessment and follow-on remediation efforts, (2) economic damages, (3) lost profits, (4) consequential damages including but not limited to interruption of service, and (5) profits derived from a violation.

In conclusion, CADRA will provide Florida businesses with a civil remedy for computer-related abuses, including retrieval of programs, code and information and reasonable compensation for investigation and remediation of computer data-related losses.

Robert Kain, Esq.
Kain & Assoc.
Fort Lauderdale, Fl
rkain@ complexip.com
ofc. 954-768-9002