AMENDED IN ASSEMBLY AUGUST 1, 2016

AMENDED IN SENATE MARCH 31, 2016

AMENDED IN SENATE MARCH 28, 2016

SENATE BILL No. 1137

Introduced by Senator Hertzberg
(Principal coauthor: Senator Beall)
(Coauthors: Senators Anderson, Bates, *Cannella,* Hill, Huff, Liu, ~~and~~ *Stone, and* Wieckowski)
(Coauthors: Assembly Members Brough, *Chang, Chau,* Chávez, Dodd, *Cristina Garcia,* Lackey, *Lopez,* Low, *Maienschein,* and Obernolte)

February 18, 2016

An act to amend Section 502 of the Penal Code, relating to computer crimes.

LEGISLATIVE COUNSEL'S DIGEST

SB 1137, as amended, Hertzberg. Computer crimes: ransomware.

Existing law establishes various crimes relating to computer services and systems, including, but not limited to, knowingly introducing a computer contaminant, as defined. Existing law makes a violation of those crimes punishable by specified fines or terms of imprisonment, or by both those fines and imprisonment.

Existing law defines extortion as obtaining the property of another, with his or her consent, induced by a wrongful use of force or fear. Existing law makes extortion a crime, punishable by imprisonment in a county jail for 2, 3, or 4 years.

This bill would define ransomware as a computer ~~or data contaminant or lock placed in or introduced into a computer system, computer or data in a computer system, or computer that restricts access to the~~

~~system, computer, or data in some way, and under circumstances in which the person responsible for the ransomware demands payment of money or other consideration to remove the contaminant, unlock the computer system or computer, or repair the injury done to the computer system, computer, or data by the contaminant or lock. The bill would provide that a person is responsible for placing or introducing a contaminant or lock into a computer system, computer or data on a computer system, or computer if the person directly places or introduces the contaminant or lock, directs another to do so, or induces another person do so, with the intent of demanding payment or other consideration to remove the contaminant, unlock the computer system or computer, or repair the computer system, computer or data on the computer system, or computer.~~ *contaminant or lock placed or introduced without authorization into a computer, computer system, or computer network that restricts access by an authorized person to the computer, computer system, computer network, or any data therein under circumstances in which the person responsible for the placement or introduction of the ransomware demands payment of money or other consideration to remove the computer contaminant, restore access to the computer, computer system, computer network, or data, or otherwise remediate the impact of the computer contaminant or lock. The bill would provide that a person is responsible for placing or introducing ransomware into a computer, computer system, or computer network if the person directly places or introduces the ransomware or directs or induces another person do so, with the intent of demanding payment or other consideration to remove the ransomware, restore access, or otherwise remediate the impact of the ransomware.* The bill would make it a crime for a person to knowingly introduce ransomware into any computer, computer system, or computer network. The bill would make a violation of this provision punishable by imprisonment in a county jail for 2, 3, or 4 years and a fine not exceeding $10,000. The bill would specify that prosecution under that provision does not prohibit or limit prosecution under any other law.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: yes.

The people of the State of California do enact as follows:

SECTION 1. Section 502 of the Penal Code is amended to read:

502. (a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created ~~computer data and computer systems.~~ *computers, computer systems, computer networks, and data.* The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, *computer networks,* and ~~computer~~ data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, *computer networks,* and data.

(b) For the purposes of this section, the following terms have the following meanings:

(1) “Access” means to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

(2) “Computer network” means any system that provides communications between one or more computer systems and input/output devices, including, but not limited to, display terminals, remote systems, mobile devices, and printers connected by telecommunication facilities.

(3) “Computer program or software” means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(4) “Computer services” includes, but is not limited to, computer time, data processing, or storage functions, Internet services,

electronic mail services, electronic message services, or other uses of a computer, computer system, or computer network.

(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer ~~programs,~~ *programs or software,* electronic instructions, input data, and output data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(6) "Government computer system" means any computer system, or part thereof, that is owned, operated, or used by any federal, state, or local governmental entity.

(7) "Public safety infrastructure computer system" means any computer system, or part thereof, that is necessary for the health and safety of the public including computer systems owned, operated, or used by drinking water and wastewater treatment facilities, hospitals, emergency service providers, telecommunication companies, and gas and electric utility companies.

(8) "Data" means a representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

(9) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.

(10) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program.

(11) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data

was or was not altered, deleted, damaged, or destroyed by the access.

(12) "Computer contaminant" means any set of computer instructions *or data* that are designed to modify, damage, destroy, *render inaccessible,* record, or transmit ~~information~~ *data* within a computer, computer system, or computer network without the intent or permission of the owner of the ~~information.~~ *data.* They include, but are not limited to, a group of computer instructions commonly called viruses or worms, ~~that~~ *which* are self-replicating or self-propagating and are designed to contaminate *data or* other computer programs ~~or computer data,~~ *or software,* consume computer resources, ~~modify, destroy, record, or transmit data, or in some other fashion~~ *or otherwise* usurp the normal operation of the computer, computer system, or computer network.

(13) "Internet domain name" means a globally unique, hierarchical reference to an Internet host or service, assigned through centralized Internet naming authorities, comprising a series of character strings separated by periods, with the rightmost character string specifying the top of the hierarchy.

(14) "Electronic mail" means an electronic message or computer file that is transmitted between two or more telecommunications devices; computers; computer networks, regardless of whether the network is a local, regional, or global network; or electronic devices capable of receiving electronic messages, regardless of whether the message is converted to hard copy format after receipt, viewed upon transmission, or stored for later retrieval.

(15) "Profile" means either of the following:

(A) A configuration of user data required by a computer so that the user may access programs or services and have the desired functionality on that computer.

(B) An Internet Web site user's personal page or section of a page that is made up of data, in text or graphical form, that displays significant, unique, or identifying information, including, but not limited to, listing acquaintances, interests, associations, activities, or personal statements.

(16) (A) "Ransomware" means a computer ~~or data~~ contaminant or lock placed ~~in~~ or introduced *without authorization* into a ~~computer system, computer or data in a computer system, or computer~~ *computer, computer system, or computer network* that restricts access ~~to the system, computer, or data in some way, and~~

by an authorized person to the computer, computer system, computer network, or any data therein under circumstances in which the person responsible for the *placement or introduction of the* ransomware demands payment of money or other consideration to remove the *computer* contaminant, ~~unlock the computer system or computer, or repair the injury done to the computer system, computer, or data by the~~ *restore access to the computer, computer system, computer network, or data, or otherwise remediate the impact of the computer* contaminant or lock.

(B) A person is responsible for placing or introducing ~~a contaminant or lock into a computer system, computer or data on a computer system, or computer~~ *ransomware into a computer, computer system, or computer network* if the person directly places or introduces the ~~contaminant or lock, directs another to do so, or~~ *ransomware or directs or* induces another person do so, with the intent of demanding payment or other consideration to remove the ~~contaminant, unlock the computer system or computer, or repair the computer system, computer or data on the computer system, or computer.~~ *ransomware, restore access, or otherwise remediate the impact of the ransomware.*

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of

computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network.

(10) Knowingly and without permission disrupts or causes the disruption of government computer services or denies or causes the denial of government computer services to an authorized user of a government computer, computer system, or computer network.

(11) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a public safety infrastructure computer system computer, computer system, or computer network.

(12) Knowingly and without permission disrupts or causes the disruption of public safety infrastructure computer system computer services or denies or causes the denial of computer services to an authorized user of a public safety infrastructure computer system computer, computer system, or computer network.

(13) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or public safety infrastructure computer system computer, computer system, or computer network in violation of this section.

(14) Knowingly introduces any computer contaminant into any public safety infrastructure computer system computer, computer system, or computer network.

(15) Knowingly introduces ransomware into any computer, computer system, or computer network.

(d) (1) Any person who violates any of the provisions of paragraph (1), (2), (4), (5), (10), (11), or (12) of subdivision (c) is guilty of a felony, punishable by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years and a fine not exceeding ten thousand dollars ($10,000), or a misdemeanor, punishable by imprisonment in a county jail not exceeding one year, by a fine not exceeding five thousand dollars ($5,000), or by both that fine and imprisonment.

(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:

(A) For the first violation that does not result in injury, and where the value of the computer services used does not exceed nine hundred fifty dollars ($950), by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000) or in an injury, or if the value of the computer services used exceeds nine hundred fifty dollars ($950), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(3) Any person who violates paragraph (6), (7), or (13) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000).

(B) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(4) Any person who violates paragraph (8) or (14) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, a misdemeanor punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in a county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both that fine and imprisonment.

(5) Any person who violates paragraph (9) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000).

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(6) Any person who violates paragraph (15) of subdivision (c) is guilty of a felony, punishable by imprisonment pursuant to subdivision (h) of Section 1170 for two, three, or four years and a fine not exceeding ten thousand dollars ($10,000). Prosecution under this paragraph does not prohibit or limit prosecution under any other law.

(e) (1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.

(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees.

(3) A community college, state university, or academic institution accredited in this state is required to include computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a resolution to that effect.

(4) In any action brought pursuant to this subdivision for a willful violation of the provisions of subdivision (c), where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud, or malice as defined in subdivision (c) of Section 3294 of the Civil Code, the court may additionally award punitive or exemplary damages.

(5) No action may be brought pursuant to this subdivision unless it is initiated within three years of the date of the act complained of, or the date of the discovery of the damage, whichever is later.

(f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

(g) Any computer, computer system, computer network, or any software or data, owned by the defendant, that is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture, as specified in Section 502.01.

(h) (1) Subdivision (c) does not apply to punish any acts which are committed by a person within the scope of his or her lawful employment. For purposes of this section, a person acts within the scope of his or her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment.

(2) Paragraph (3) of subdivision (c) does not apply to penalize any acts committed by a person acting outside of his or her lawful employment, provided that the employee's activities do not cause

an injury, to the employer or another, or provided that the value of supplies or computer services which are used does not exceed an accumulated total of two hundred fifty dollars ($250).

(i) No activity exempted from prosecution under paragraph (2) of subdivision (h) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

(j) For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

(k) In determining the terms and conditions applicable to a person convicted of a violation of this section the court shall consider the following:

(1) The court shall consider prohibitions on access to and use of computers.

(2) Except as otherwise required by law, the court shall consider alternate sentencing, including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.

SEC. 2. No reimbursement is required by this act pursuant to Section 6 of Article XIII B of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution.

O