

Introduced by Senator HertzbergFebruary 18, 2016

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

LEGISLATIVE COUNSEL'S DIGEST

SB 1137, as introduced, 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 contaminant that restricts access to the infected computer and demands that the user pay a ransom to remove the restriction. 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 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:

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

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

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

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

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

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

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

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

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

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

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

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

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

25 (9) “Supporting documentation” includes, but is not limited to,
26 all information, in any form, pertaining to the design, construction,
27 classification, implementation, use, or modification of a computer,
28 computer system, computer network, computer program, or
29 computer software, which information is not generally available
30 to the public and is necessary for the operation of a computer,
31 computer system, computer network, computer program, or
32 computer software.

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

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

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

3 (12) “Computer contaminant” means any set of computer
4 instructions that are designed to modify, damage, destroy, record,
5 or transmit information within a computer, computer system, or
6 computer network without the intent or permission of the owner
7 of the information. They include, but are not limited to, a group
8 of computer instructions commonly called viruses or worms, that
9 are self-replicating or self-propagating and are designed to
10 contaminate other computer programs or computer data, consume
11 computer resources, modify, destroy, record, or transmit data, or
12 in some other fashion usurp the normal operation of the computer,
13 computer system, or computer network.

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

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

26 (15) “Profile” means either of the following:

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

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

35 (16) “Ransomware” means a computer contaminant that
36 restricts access to the infected computer system in some way and
37 demands that the user pay a ransom to the person responsible for
38 the computer contaminant to remove the restriction. Ransomware
39 may systematically encrypt files on the system’s hard drive, which
40 become difficult or impossible to decrypt without paying the

1 *ransom for the encryption key, or may simply lock the system and*
2 *display messages intended to coax the user into paying.*

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

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

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

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

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

21 (5) Knowingly and without permission disrupts or causes the
22 disruption of computer services or denies or causes the denial of
23 computer services to an authorized user of a computer, computer
24 system, or computer network.

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

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

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

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

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

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

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

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

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

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

20 (d) (1) Any person who violates any of the provisions of
21 paragraph (1), (2), (4), (5), (10), (11), or (12) of subdivision (c) is
22 guilty of a felony, punishable by imprisonment pursuant to
23 subdivision (h) of Section 1170 for 16 months, or two or three
24 years and a fine not exceeding ten thousand dollars (\$10,000), or
25 a misdemeanor, punishable by imprisonment in a county jail not
26 exceeding one year, by a fine not exceeding five thousand dollars
27 (\$5,000), or by both that fine and imprisonment.

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

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

35 (B) For any violation that results in a victim expenditure in an
36 amount greater than five thousand dollars (\$5,000) or in an injury,
37 or if the value of the computer services used exceeds nine hundred
38 fifty dollars (\$950), or for any second or subsequent violation, by
39 a fine not exceeding ten thousand dollars (\$10,000), or by
40 imprisonment pursuant to subdivision (h) of Section 1170 for 16

1 months, or two or three years, or by both that fine and
2 imprisonment, or by a fine not exceeding five thousand dollars
3 (\$5,000), or by imprisonment in a county jail not exceeding one
4 year, or by both that fine and imprisonment.

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

7 (A) For a first violation that does not result in injury, an
8 infraction punishable by a fine not exceeding one thousand dollars
9 (\$1,000).

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

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

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

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

29 (B) For any violation that results in injury, or for a second or
30 subsequent violation, by a fine not exceeding ten thousand dollars
31 (\$10,000), or by imprisonment in a county jail not exceeding one
32 year, or by imprisonment pursuant to subdivision (h) of Section
33 1170, or by both that fine and imprisonment.

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

36 (A) For a first violation that does not result in injury, an
37 infraction punishable by a fine not exceeding one thousand dollars
38 (\$1,000).

39 (B) For any violation that results in injury, or for a second or
40 subsequent violation, by a fine not exceeding five thousand dollars

1 (\$5,000), or by imprisonment in a county jail not exceeding one
2 year, or by both that fine and imprisonment.

3 (6) *Any person who violates paragraph (15) of subdivision (c)*
4 *is guilty of a felony, punishable by imprisonment pursuant to*
5 *subdivision (h) of Section 1170 for two, three, or four years and*
6 *a fine not exceeding ten thousand dollars (\$10,000).*

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

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

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

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

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

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

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

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

19 (2) Paragraph (3) of subdivision (c) does not apply to penalize
20 any acts committed by a person acting outside of his or her lawful
21 employment, provided that the employee's activities do not cause
22 an injury, to the employer or another, or provided that the value
23 of supplies or computer services which are used does not exceed
24 an accumulated total of two hundred fifty dollars (\$250).

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

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

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

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

39 (2) Except as otherwise required by law, the court shall consider
40 alternate sentencing, including community service, if the defendant

1 shows remorse and recognition of the wrongdoing, and an
2 inclination not to repeat the offense.

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