Date of Hearing: May 5, 2020

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 2320 (Chau) – As Introduced February 14, 2020

**SUBJECT**: Personal information: contractors: cyber insurance

**SUMMARY**: This bill would require contractors doing business with a state agency to maintain cyber insurance to cover all losses resulting from potential unlawful access to or disclosure of personal information, as specified. Specifically, **this bill would**:

1) Require in any contract that contemplates, in the course of doing business with an agency, that a contractor will receive or have access to records containing personal information (PI) protected under the Information Practices Act of 1977 (IPA), the contract shall require the contractor to carry cyber insurance sufficient to cover all losses resulting from potential unlawful access to or disclosure of PI, in an amount determined by the contracting agency.

2) Define "agency," "PI," and "record" to have the same meanings as found in the IPA.

**EXISTING LAW**:

1) Provides, under the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const. art. I, Sec. 1.)

2) Sets forth, IPA, the right of an individual who is the subject of information maintained in state or local agency records to have access to that information. (Civ. Code Sec. 1798 et seq.)

3) Requires any agency, person, or business that owns or licenses computerized data that includes PI to disclose a breach of the security of the system to any California resident whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. (Civ. Code Secs. 1798.29(a) and (c); 1798.82(a) and (c).)

4) Requires any agency, person, or business that maintains computerized data that includes PI that the agency, person, or business does not own to notify the owner or licensee of the information of any security breach immediately following discovery if the PI was, or is reasonably believed to have been, acquired by an unauthorized person. (Civ. Code Secs. 1798.29(b), 1798.82(b).)

5) Defines "PI," for purposes of the provisions above, to include either a user name or email address, in combination with a password or security question and answer that would permit access to an online account, or the individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted: social security number; driver's license number or California identification card number; passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; account number, credit or debit card number, in

combination with any required security code, access code, or password that would permit access to an individual's financial account; medical information; unique biometric data, as specified; or health insurance information. "PI" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Civ. Code Secs. 1798.29(g) and (h); 1798.82(h) and (i).)

6) Authorizes any consumer whose nonencrypted or nonredacted PI is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information to institute a civil action. (Civ. Code Sec. 1798.150.)

7) Establishes CDT within the Government Operations Agency, under the supervision of the Director of Technology, also known as the State Chief Information Officer. (Gov. Code Sec. 11545(a).) Establishes OIS within CDT to ensure the confidentiality, integrity, and availability of state systems and applications. OIS must develop an information security program and establish policies, standards, and procedures directing state agencies to effectively manage security and risk. (Gov. Code Sec. 11549 et seq.)

8) Requires all state agencies defined in Section 11546.1 to implement the policies and procedures issued by the office, including, but not limited to, performing both of the following duties:

   - Comply with the information security and privacy policies, standards, and procedures issued pursuant to this chapter by the office.

   - Comply with filing requirements and incident notification by providing timely information and reports as required by the office. (Gov. Code Sec. 11549.3(b).)

**FISCAL EFFECT**: Unknown

**COMMENTS**:

1) **Purpose of the bill**: This bill seeks to ensure that businesses contracting with the state of California are insured to cover any loss as a result of a data breach or other cyberattack. This bill is author-sponsored.

2) **Author's Statement of Criticality**: In response to the unique constraints the COVID-19 crisis has placed on the legislative process, the Committee elected to focus attention this session on bills that address only the most urgent issues and issues critical for an efficient recovery from the pandemic. In order to prioritize bills that require immediate attention, the Committee asked the author of each bill to provide a Statement of Criticality explaining the applicability of one or more of the following criteria to that bill:

   - the bill addresses a problem that was created by, or has been significantly exacerbated by, the ongoing public health crisis due to COVID-19, or the response thereto;

   - the bill addresses an urgent problem that presents a threat to the safety and security of Californians and must be resolved immediately; or

- the bill makes a technical change to an existing program or function that must be immediately adopted to preserve the utility of that program or function.

In response, the Author writes:

> We expect to see an increase in the need for government contracting to help deal with the crisis of COVID-19, especially dealing with sensitive health information. Additionally, a denial of service attack would be particularly costly during a developing crisis since the effect of lack of access to critical health data is amplified. Cyber insurance is a product designed to assist an organization with mitigating risk exposure by offsetting costs involved with recovery after a cybersecurity breach. These breaches are often cyberattacks designed to disrupt an organization's business and come in a variety of forms, including malware, ransomware, DDoS attacks, and other methods used to compromise networks and sensitive data.
>
> Hospitals have already been hit with cyberattacks like ransomware or DDoS and other types of cybersecurity breaches. These breaches are also affecting labs involved in testing for COVID-19 by locking out staff from inputting data and/or stealing patients' personal information. Cyberattacks slow down medical staff who are rendered unable to access patient information, this delay in care could lead to the inability to diagnose or test, or even to the death of a patient. *The Hill* reported that cyberattacks have increased over 600% in a move to infect computers and hold critical information ransom. These attacks have impeded the critical work frontline medical staff are doing to end COVID-19, and some health organizations have elected to pay the ransom to prevent such delays.
>
> Microsoft, Inc. reported to U.S. federal agencies and hospitals that cybercriminals have been exploiting the crisis to steal personal information. On their blog site, they alerted those within their networks and worked with federal agencies to bolster cybersecurity; however, the attacks continue. Even if the attacks are not directly targeting hospital computer systems, they can still find ways in through an individual's email. Cybercriminals have also taken to targeting individuals by sending emails with a subject line about COVID-19 resources, false advertisements to purchase medical equipment, etc. in an attempt to profit off the reasonable fears of our anxious nation.

The Committee agrees that the issues addressed by this bill are timely and critical under the current circumstances. The number of contractors the State relies on in the performance of its obligations to the residents of California is vast. The State's response to the ongoing pandemic requires that increasingly more services are delivered entirely online. At the same time, many state critical services like hospitals and their medical professionals are stretched thin. Requiring state vendors to procure cyber insurance will help protect the businesses who contract with the State and residents of California alike by ensuring that the businesses are financially prepared to cope with and quickly recover after a cyberattack.

3) **California's response to the increasing threat of cyberattack**: Cybersecurity is not a new concern. Unfortunately, cyber-crime, data breaches, theft of proprietary information, hacking, and malware incidents are now routine. Notably, the skyrocketing number of mobile devices has spawned new threats. Downloadable applications can render individuals vulnerable to fraud, theft, and other privacy concerns, and mobile devices that are constantly connected to the internet or local Wi-Fi networks create nearly constant security issues.

California has been at the forefront of responding to these persistent threats. Effective 2003, California became the first state in the nation to require businesses and government agencies to notify residents of security breaches if PI was, or was reasonably believed to have been, stolen. (SB 1386 (Peace, Ch. 915, Stats. 2002).) Until January 1, 2017, this law did not apply to "encrypted" information, which created an incentive for businesses and government agencies to encrypt personal data and thereby avoid the notice requirement. AB 2828 (Chau, Ch. 337, Stats. 2016) required agencies, persons, and businesses to also disclose a breach of a security of a system containing *encrypted* PI when the encryption key or security credential that could render that PI readable or useable was also compromised in the breach.

After the Equifax breach in 2017, California began requiring any consumer credit reporting agency to begin "patching" their computer systems with reasonably known vulnerabilities in a timely manner, as specified. (SB 1859 (Chau, Ch. 532, Stats. 2018).) California residents also have a limited private right of action now their nonencrypted or nonredacted PI is breached as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PI. (SB 1121 (Dodd et al., Ch. 735, Stats. 2018).) Finally, all state contracts involving information technology are subject to approval by the California Department of Technology, and there are numerous standards and obligations required in every state contract, typically outlined in the Public Contract Code and the State Administrative Manual (SAM). This bill would amend the Public Contract Code to additionally require cyber insurance for any business whose contract with the state involves access to records containing PI.

4) **State contracts already cover loss in the event of a data breach**: The Department of General Services oversees state contracts generally, and the California Department of Technology (CDT) has negotiating authority over all state information technology contracts, as specified. (Pub. Con. Code Sec. 12100 et seq.) Requirements for these contracts are generally provided for by statute and the SAM. While cyber insurance does not appear to be expressly required under state law, there are arguably many provisions of law which would allow CDT to require cyber insurance if warranted by the particular contract and vendor. For example, the Public Contract Code requires state agencies to consider and potentially incorporate performance-based or share-in-savings contract terms to manage risks and create incentives for successful contract performance. This includes contract terms that structure the contract to minimize risk to the state by sharing risk with the private sector. (Pub. Con. Code Sec. 12101.5(d).) The SAM additionally requires each state entity shall ensure agreements with state and non-state entities include provisions which protect and minimize risk to the state. Agreements shall include, at a minimum, provisions which cover the following, among other things:

   - Appropriate levels of security (confidentiality, integrity and availability) for the data based on data categorization and classification.

   - Standards for transmission and storage of the data, including encryption and destruction, if applicable.

   - Agreements to comply with statewide policies and laws regarding the use and protection of information resources and data.

- Agreements to apply security patches and upgrades, and keep virus software up-to-date on all systems on which data may be used.

- Agreements that the ***data custodian*** shall be responsible ***for all costs incurred by the data owner due to security incident*** resulting from the data custodian's failure to perform or negligent acts of its personnel, and ***resulting in an unauthorized disclosure, release, access, review, or destruction; or loss, theft or misuse of an information asset***. If the contractor experiences a loss or breach of data, the contractor shall immediately report the loss or breach to the data owner. If the data owner determines that notice to the individuals whose data has been lost or breached is appropriate, ***the contractor will bear any and all costs associated with the notice or any mitigation selected by the data owner***. These costs include, but are not limited to, staff time, material costs, postage, media announcements, and other identifiable costs associated with the breach or loss of data. (emphasis added) (SAM Sec. 5305.8.)

Most vendors purchase insurance to cover losses that their business may reasonably anticipate. Given the requirements outlined for all state contracts above, insurance, whether classified as cyber insurance or under a more general term, is likely required by the state in contracts to cover losses associated with information assets. Accordingly, this bill arguably represents a clarification in law that is consistent with existing practice.

On this same point, a coalition of industry groups representing organizations from the technology sector, building trades, and medical technology argue that businesses contracting with government agencies are already required to carry insurance loss coverage and that this bill will "create additional financial burdens for contractors who must carry higher liability and loss coverages. In turn, this will disadvantage California because it is less likely to receive the best available technology to support state and local governmental agencies." The coalition further contends that the language is overly expansive. The coalition writes:

> AB 2320 requires a contractor to carry "cyber insurance sufficient to cover ***all*** losses resulting from ***potential*** unlawful access to or disclosure of personal information, in an amount determined by the contracting agency." (emphasis added). This language is extremely problematic because "potential" unlawful access or disclosure does not require measurable harm and "all" losses could include losses that are not the result of the contractor's breach of the agreement.

The cyber insurance requirements of this bill appear to be designed to achieve two important public policy goals. First, the requirement that contractors carry cyber insurance should result in a closer look at the cybersecurity practices of vendors, and hopefully result in increased cyber hygiene, so that those businesses contracting with the state are less likely to fall victim to data breach and other cyberattack. Second, this bill is intended to ensure that businesses contracting with the state have adequate resources to make victims whole and provide the services required under the law (like identity theft mitigation services) to the individuals whose information has been unlawfully accessed.

To the extent that the language of the bill would require duplicative coverage from contractors or otherwise require them to maintain coverage in excess of what would be needed to cover losses in the event of a cyberattack, the author may wish to narrow this bill

to eliminate any obligations outside of his intent as this bill moves through the legislative process.

5) **Cyber insurance coverage should reflect the unique risk associated with each contract**: Cyberattacks can come in a variety of forms. Malware and hacking breaches are caused by intentional intrusions into computer systems by unauthorized users. Physical breaches result from theft or loss of unencrypted data stored on laptops, computers, hard drives, or flash drives. Error breaches are the unintentional exposure of PI to unauthorized individuals by insider employees or service providers, and misuse breaches stem from trust insiders intentionally misusing privileges in an unauthorized manner. At the same time, there are many different types of contractors providing services to state agencies. Indeed, just looking at the sheer number of services the state provides -- law enforcement, hospitals, education, insurance, and pension funds, to name a few – gives insight into the different types of vendors and the PI they handle.

   To this point, the coalition argues in opposition that a one-size-fits-all approach to state contracts is not appropriate, and any requirement for cyber insurance should be handled during the request for proposal (RFP) process. The coalition writes:

   > The requirement of cyber insurance should be negotiated during the request for proposal (RFP) process rather than be legislatively mandated. Departments and agencies should procure technology through a "best overall value" approach, which emphasizes technical fit and flexibility. This approach gives an agency the opportunity to procure goods and services that best meet their needs. It is critical that California supports further development of technology. The state should not mandate additional one-size-fits-all requirements that unnecessarily increase costs for vendors and, ultimately, the state.
   >
   > Thus, government agencies should be allowed reasonable latitude in choosing contracting vehicles, so long as they are compatible with state laws regarding contracting and cooperative purchasing. By doing so, agencies will have greater choice and better overall competition from the private sector, as well as value and flexibility to seek solutions that work best for the state's needs and budget, rather than seeking to shoehorn a solution into an already established standard.

   On its face, nothing in the bill requires all state contracts with vendors to carry cyber insurance. Only those contracts that contemplate, in the course of doing business with the agency, that a contractor will have access to records containing PI are required to obtain cyber insurance. This would cover vendors tasked with storing and processing PI, such as vendors that process debit and credit card payments or vendors who hold medical records or financial information. This requirement may also extend to vendors that only have access to the PI of their own employees, which is arguably beyond the intent of the author.

   That being said, staff notes that the bill arguably does not create a "one-size-fits-all" requirement that all state vendors carry the same amount or even type of cyber insurance coverage. If one vendor stores medical records for three million people, that vendor would have different cybersecurity insurance needs than a vendor who processes late fees for a rural county library system. This bill anticipates that vendors will have different needs, and allows the amount of cyber insurance coverage to be determined by the contracting agency,

consistent with the requirements of the Public Contract Code and SAM, discussed in Comment 4, above.

6) **Prior legislation**: AB 1130 (Levine, Ch. 750, Stats. 2019) added government-issued identification numbers and biometric data, as defined, to the definition of PI in the data breach notification law.

   SB 1859 (Chau, Ch. 532, Stats. 2018) *See* Comment 3.

   SB 1121 (Dodd et al, Ch. 735, Stats. 2018) *See* Comment 3.

   AB 2828 (Chau, Ch. 337, Stats. 2016) *See* Comment 3.

   AB 1710 (Dickinson, Ch. 855, Stats. 2014) enacted various changes to the DBNL including requiring the source of the breach to offer appropriate identity theft prevention and mitigation services to consumers at no cost.

   AB 1950 (Wiggins, Ch. 877, Stats. 2004) required a business that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure. AB 1950 also required a business that discloses personal information to a nonaffiliated third party, to require by contract that those entities maintain reasonable security procedures.

   SB 1386 (Peace, Ch. 915, Stats. 2002) *See* Comment 3.

**REGISTERED SUPPORT / OPPOSITION**:

**Support**

None on file

**Opposition**

Advanced Medical Technology Association (AdvaMed)
California Building Industry Association
California Chamber of Commerce
Computing Technology Industry Association (CompTIA)
Information Technology Industry Council (ITI)
Insights Association
Internet Coalition
State Privacy & Security Coalition
TechNet

**Analysis Prepared by**: Nichole Rapier Rocha / P. & C.P. / (916) 319-2200