Cybersecurity

Collaborative Training Better Defense Against Cyberattacks than Punitive Rules

- There is more than one way in which the state can increase data protections.
- The state is increasingly vulnerable to cybersecurity attacks in a post-COVID world. The California Department of Finance just suffered a cyberattack in December 2022.
- The responsibility to prepare and defend against such attacks falls on all: government, business and individuals.
- There is no silver bullet solution when it comes to cybersecurity and increasing restrictions or passing increasingly punitive laws upon businesses cannot change that. Moreover, humans are the weakest link in our cybersecurity preparedness and defense.
- Other states have incorporated interesting concepts such as cyber ranges to help educate and train their current/future workforce. California has made great strides in cybersecurity preparedness, particularly by partnering with experts across government, academia and the private sector. But more needs to be done to improve the cyber awareness, hygiene and skills of not only current and future information technology (IT) staff, but also ordinary citizens.

BACKGROUND

Data protection laws share an underlying goal: to prevent the misuse and/or unauthorized access and use of private or otherwise confidential data.

There is a tendency to associate the concept of "data protections" with data privacy laws regulating the collection, use, retention and dissemination of personal data by an industry or industries, particularly in the post-General Data Protection Regulation (GDPR), post-California Consumer Privacy Act (CCPA) world. Such laws commonly entail:

• Transparency requirements, such as disclosures around data practices in privacy policies to help empower consumers to make informed decisions;

• Limitations around the permissible data practices of businesses based on the business purpose, commercial purpose, or other purposes for which the data may be used; and

• Granting consumers rights that enable them to exert control or make choices limiting how their personal data is collected, used, retained and/or otherwise disseminated, such as by way of giving them the ability to delete data, the ability to correct data, and/or the right to restrict (that is, opt out of or opt in to) certain transfers or disclosures of their data.

But those laws are not the end-all, be-all when it comes to data protection.

In reality, data protection can come in many different forms,

CalChamber

Creating A More Affordable California

2023 Business Issues and Legislative Guide

See the entire CalChamber 2023 Business Issues and Legislative Guide at www.calchamber.com/businessissues
Free PDF or epub available to download.

Special Thanks to the Sponsor
Of the 2023 Business Issues and Legislative Guide

Major

AUTOMOBILE CLUB • SOUTHERN CALIFORNIA • AAA

including data breach or cybersecurity laws aimed at protecting against and responding to the unauthorized access and use of data such as by way of cyberattacks, cybercrimes, or other "hacks." (*See*, for example, California's Data Breach Notification Law, Civil Code Section 1798.82.) Such laws can, for example, include mandated security standards and procedures to help protect against attacks, set the obligations of an entity that is breached or attacked, and can seek create deterrents by way of criminalizing the activities.

Our social compact presumes that if reasonable care is taken, negative outcomes can (largely) be prevented; that compliance with safety regulations ensures safety. In the realm of cybersecurity, however, there is widespread recognition that failure is inevitable. An entity — be it a private or government entity — could undertake every reasonable precaution, properly/adequately train its employees on a regular basis, use the most secure technologies available, and follow best practices — and still fall victim to some form of data breach or hack. Stated another way: ***when it comes to cybersecurity, there is no silver bullet solution that can guarantee protection***. As Ivan Novikov, CEO of the prominent data security firm Walleye stated: "After spending $157 billion over the last two years on data security … it is unclear what needs to be protected from (whom)." (*"Why Is There No Silver Bullet In Cybersecurity?" Forbes Technology Council, August 4, 2017*)

Another commonly understood reality? ***Humans are cybersecurity's weakest link***.

That is not to suggest that it is pointless to try to protect against attacks. It is only to say that the problem goes much deeper than businesses "taking more care" or "not taking enough care."

Accepting these realities and knowing that new vulnerabilities are being found constantly calls into question whether we do enough as a *society* to prevent attacks. Is the best use of societal resources imposing new data privacy restrictions on businesses or mandating increasing statutory or civil damages, if the goal of these laws and regulations is to ensure data protection? If humans pose our weakest link, then it is with our behavior where we have the most room for improving or bolstering our cybersecurity defenses.

CALIFORNIA CYBERSECURITY ENTITIES

It is worth noting that in the last 10 years, California has taken significant steps in recognizing the gravity of the threat posed by cyberattacks, both by creating the California Cybersecurity Task Force and establishing the California Cybersecurity Integration Center (Cal-CSIC). Officially a statewide partnership comprising key stakeholders, subject matter experts, and cybersecurity professionals from California's public sector, private industry, academia and law enforcement, the task force advises senior administrative officials in cybersecurity matters. Cal-CSIC, which was created initially by way of Executive Order B-34-15 in 2015, exists within the Governor's Office of Emergency Services (CalOES) and has the primary mission of reducing the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in our state. Cal-CSIC also is responsible for coordinating with federal and state partners to provide warnings of cyberattacks, develop a statewide cybersecurity strategy, and establish a Cyber Incident Response Team to serve as California's primary unit to lead cyber threat detection, reporting, and response.

At the same time, there are more opportunities for bad actors through phishing, ransomware or other cyberattacks, given the state's increasing and massive reliance on virtual/online tools for everything from shopping for groceries to work meetings, to providing access for education and health care.

To be clear, these threats exist in both the private and public realms. In such an environment, it becomes even more critical that the people, businesses, and state work collaboratively to proactively enhance the tools we have at our disposal to thwart such attacks. Shortages in IT staff are nothing new and neither are the vulnerabilities posed by human error as attacks become more sophisticated and harder to identify.

CYBER RANGES

We should consider new, innovative ways to approach the issue of cyberattacks. For example, five other states in the United States currently operate a "cyber range": Virginia, Michigan, Arizona, Georgia and Florida. Such ranges function like shooting or kinetic ranges, facilitating training in weapons, operations or tactics, where people can train, develop and test cyber range technologies to ensure consistent operations and readiness for real-world deployment. Others have described these ranges as a lab environment or a "secure sandbox" that provides a flexible and secure environment for cybersecurity education, training exercises and software testing wherein the workforce can be trained to defend their digital assets.

Instead of passing laws that heap restrictions upon businesses, the state should increase its efforts to identify new ways

in which we can collectively shape a society where children and future workers are equipped with better cyber awareness, hygiene and skills.

CALCHAMBER POSITION

The California Chamber of Commerce has significant concerns regarding new proposals that would be overly restrictive or punitive toward businesses that fall victim to cyberattacks, despite taking reasonable efforts, and which would create less flexibility in developing future technologies. Although businesses can and must do their part, cybersecurity is a multi-faceted issue that requires action from many different fronts. The CalChamber would support new proposals that would better equip California and its workforce to meet the challenges ahead.

Staff Contact
Ronak Daylami
Policy Advocate

ronak.daylami@calchamber.com
January 2023