SENATE
CALIFORNIA LEGISLATURE

STATE CAPITOL
SACRAMENTO, CALIFORNIA
95814

INFORMATIONAL HEARING

Select Committee on Cybersecurity and Identity Theft Prevention

Exploring Data Breaches: What State, Local, and Private Institutions can do to Protect Themselves and the Public

Monday, November 8
1:30 PM
Room: 4203

Background Paper

Overview

There have been a record number of data breaches and threats to our cybersecurity in recent years and the problem is quickly becoming more pervasive. Cyberattacks present a fast-growing and technically complex problem for California state and local agencies, businesses, and individuals.

In a data breach, unauthorized individuals gain access to or control of data, such as personal information. Criminals who seek to profit from the information — such as by using it in identity theft schemes — generally carry out these cyberattacks. Between 2012 and 2016, the California Attorney General received reports of 657 data breaches affecting over 49 million records in California. Most data breaches in California occurred in the retail, financial, and healthcare sectors of the economy.[1]

Data breaches are an evolving threat that have a significant impact on the economy. Estimated global losses from cybercrime hit just under a record $1 trillion for 2020, as the rapid shift to remote operations during the COVID-19 pandemic presented hackers to target consumers and businesses.[2] Additionally, according to a recent report by IBM and the Ponemon Institute, the

[1] Legislative Analyst's Office. (2017, December 1). Letter to Attorney General Xavier Becerra regarding review of proposed statutory initiative (A.G. File No. 17-0039, Amendment #1): https://lao.ca.gov/BallotAnalysis/Initiative/2017-039.

[2] Riley, T. (2020, December 7). *Cybersecurity 202: Global losses from cybercrime skyrocketed to nearly $1 trillion in 2020, new report finds*. The Washington Post.

average cost of a data breach among companies surveyed reached $4.24 million per incident in 2021, the highest in 17 years. [3]The Identity Theft Resource Center, a nationally recognized nonprofit organization established to support victims of identity crime, released data this fall demonstrating the number of data breaches through September 30, 2021 has exceeded the total number of events in Full-Year 2020 by 17 percent (1,291 breaches in 2021 compared to 1,108 breaches in 2020).[4] These trends point to a record-breaking year for data compromises (the all-time high of 1,529 breaches was set in 2017).

Examples of Recent Data Breaches

Colonial Pipeline Ransomware Attack

On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that affected computerized equipment managing the pipeline. Colonial Pipeline, which operates the nation's largest fuel pipeline, was compromised by a hacking organization called DarkSide. The group stole nearly 100 gigabytes of data, threatening to release it to the internet unless a ransom was paid. As a result, U.S. gas prices rose and many gas stations faced shortages fueled by panic buying and supply disruptions.[5]

Accellion Data Breach

Accellion FTA is a file transfer application used to share files. A vulnerability in Accellion's FTA was first exploited by cybercriminals in December 2020 and then again in January 2021.[6] The data breach has impacted hundreds of companies, organizations, universities, and government agencies, including the University of California (UC), Stanford University, and other California based entities. In connection with the attack, certain UC data was accessed without authorization. Perpetrators gained access to information from students, faculty and alumni. The personal information of several UC community members has been released on the dark web, including email addresses, driver's license information and even social security numbers.

Aeries Breach

On April 27th, 2020, Aeries Software notified several hundred school districts that their system was breached. Many California school districts were impacted, including Inglewood Unified School District, Laguna Beach Unified School District, San Bernardino City Unified School District, Los Alamitos Unified School District, El Dorado County Office of Education, and Santa

https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020/.

[3] IBM Security. (2021, July). *Cost of a Data Breach Report 2021*. https://www.ibm.com/downloads/cas/OJDVQGRY.

[4] Identity Theft Resource Center. (2021, October 6). Press Release: *Identity Theft Resource Center to Share Latest Data Breach Analysis with U.S. Senate Commerce Committee; Number of Data Breaches In 2021 Surpasses All Of 2020.* https://www.idtheftcenter.org/identity-theft-resource-center-to-share-latest-data-breach-analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/.

[5] Blue Fin. (2021, September 9). *The Biggest Data Breaches of 2021 so far.*https://www.bluefin.com/bluefin-news/2021-biggest-data-breaches-so-far/

[6] Fireeye. (2021, March 1.) *Accellion, Inc. File Transfer Appliance (FTA) Security Assessment*. https://www.kiteworks.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf

Clara Unified School District. School districts use the Aeries Student Information System to provide students and their parents with online access to information regarding school events and schedules. In late November 2019, Aeries learned that an unauthorized individual exploited a vulnerability in the Aeries software that would allow access to student and parent information.[7] The compromised information included student ID numbers, student email addresses, parent email addresses and parent password hashes. A password hash is when a password is transformed into a scrambled version of itself as a form of security.

Considerations for State and Local Government

State Government

Managing Cyber Threats through Effective Governance: A Call to Action for Governors and State Legislatures, a recent report by the Center for Internet Security (CIS), discusses the risk cybersecurity threats pose to states and strategies for states to establish effective cybersecurity governance frameworks. The report notes that while every state has implemented cybersecurity programs, few have cybersecurity governance that effectively ensures that a state's risk is managed to a level and in ways that have been determined to be, through formalized governance processes, acceptable to the governor and legislature. CIS also suggests once established, cybersecurity governance must be agile, allowing cybersecurity programs to evolve as new threats that require adaptations in risk management strategies emerge.[8]

According to the National Conference to State Legislators (NCSL), states face several significant obstacles to sound cybersecurity practices. These include a lack of resources to meet the challenges of an ever-evolving cyber threat landscape, workforce and education issues, and development of sound resiliency practices to keep state systems safe and protect privacy.[9] A survey of top IT security officers across all 50 states identified three top issues affecting states' cybersecurity: budget, talent and increasing cyber threats.[10] A top priority of state legislatures in recent years has been improving cybersecurity practices within state governments and increasing resources and training to combat cyberthreats. For example, more states are now requiring agencies to have a statewide, comprehensive approach to security and security oversight. Often, chief information security officers are charged with creating statewide security policies and IT standards, establishing information security plans with annual

[7] San Bernardino City Unified School District breach notice letter. (2020, May 28). https://oag.ca.gov/system/files/2020-05-22%20-%20Aeries%20Breach.pdf.

[8] Gilligan, J, and Pardo, T. A. (2020, October). *Managing Cyber Threats through Effective Governance*. Center for Internet Security and the Center for Technology in Government at the University at Albany, State. University of New York (CTG UAlbany). https://www.ncsl.org/documents/taskforces/Managing-Cyber-Threats-through-Effective-Governance.pdf.

[9] Frederick, S., Greenberg, P., & Gruwekk, A. (2019, November). *State and federal efforts to enhance cybersecurity*. National Conference of State Legislatures. https://www.ncsl.org/research/telecommunications-and-information-technology/state-and-federal-efforts-to-enhance-cybersecurity.aspx.

[10] Greenberg, et al.

assessments or reporting, creating cyber incident response or readiness plans, and requiring security awareness training for employees.[11]

Local Government

A 2019 report by the National League of Cities (NLC) found that every hour, 26 percent of local governments report a cyberattack and that number rises to 66.7 percent over the duration of a year.[12] Despite the prevalence of cyberattacks on local government, NLC also found that a large number of local governments do not know how often they are attacked (27.6 percent), experience an incident (29.7 percent) or a breach (41.0 percent).[13] Local governments are in the midst of a significant change in their operations, as more basic government functions rely on technology. Many local governments typically have limited budgets for upgrading networks and security systems, may use outdated technology, and do not have dedicated IT staff to implement organizational safeguards.[14] Developing the practices and tools to protect our local governments from emerging cyber threats is vital to safety, data protection, and the security of the infrastructure.

Questions for Panelists

Panel I: Overview of Data Breaches, Response, and Prevention

- Generally, how have cybersecurity threats evolved in the last 5 years?
- In what ways has the pandemic changed the landscape of cyberattack prevention and response?
- What do you look for when evaluating the weaknesses of a private or public entity when it comes to cyberattack prevention?
- What factors are most crucial in the time immediately following a cyber-attack?
- What advantages do government bodies have when it comes to building sufficient cybersecurity policies versus private companies? Disadvantages?
- What types of entities are top targets for cyberattacks? Has this changed over time?
- What would you say are the "low-hanging fruit" of cybersecurity weaknesses that you frequently find in risk analytics?
- Do you have any suggestions for how California may be able to improve our cybersecurity preparedness and response?

[11] Greenberg, et al.
[12] National League of Cities. (2019, October). *Protecting Our Data: What Cities Should Know About Cybersecurity*. https://www.nlc.org/wp-content/uploads/2019/10/CS20Cybersecurity20Report20Final_0.pdf.
[13] National League of Cities.
[14] Lisa N. Thompson. *Cybersecurity Best Practices for Municipalities*. New Hampshire Municipal Association. https://www.nhmunicipal.org/town-city-article/cybersecurity-best-practices-municipalities.

- Are there any specific areas you think this committee and the legislature should focus on?

Panel II. State and Local Government Considerations

- What are some examples of legislation you have seen passed in other states that effectively prevent cybersecurity attacks on state entities?
- What factors play into successful cyberattack responses?
- What role does the state government play in preventing cyberattacks in the public and private space? What role does the federal government play?
- What federal resources are available to help states with cybersecurity preparedness?
- What, if any, emerging issues in cybersecurity do you predict playing a more significant role in the future?
- Several hundred local governments have been victims of cyberattacks in recent years.
    - What consequences comes after these attacks?
    - What weaknesses have these events exposed in how local governments respond to cyber-attacks?
- What role can and should the state government play in supporting local governments in attack prevention and response?
- What role, if any, do state and local agency employees play in helping prevent cyberattacks? How can we get them to buy into this responsibility?
- What are the greatest obstacles local governments face in building robust cyber-attack prevention and response policies?
- Do you have any suggestions for how California may be able to improve our cybersecurity preparedness and response?
- Are there any specific areas you think this committee and the legislature should focus on?