GAVIN NEWSOM
GOVERNOR

NANCY WARD
DIRECTOR

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

March 13, 2024

The Honorable Gavin Newsom
Governor of California
1021 O Street, Suite 9000
Sacramento, CA 95814

The Honorable Bill Dodd
Chair, Senate Committee on
Governmental Organization
1020 N Street, Room 584
Sacramento, CA 95814

The Honorable Freddie
Rodriguez
Chair, Assembly Committee
on Emergency Management
1020 N Street, Room 360B
Sacramento, CA 95814

Mr. Gabriel Petek, Legislative
Analyst
Legislative Analyst's Office
925 L Street, Suite 1000
Sacramento, CA 95814

Subject: Report to California Legislature Summarizing Cyberattacks and Data Breaches Impacting Local Educational Agencies

Dear Senators, Assemblymembers, and Legislative Analyst:

The California Cybersecurity Integration Center (Cal-CSIC) is providing this report pursuant to California Education Code Section 35266. This report summarizes the types and number of cyberattacks on local educational agencies, the types and number of data breaches affecting local educational agencies that have been reported to the Attorney General, any activities provided by the Cal-CSIC to prevent cyberattacks or data breaches of a local educational agency, and support provided by the Center following a cyberattack or data breach.

Should you have any questions, please contact Legislative and External Affairs Coordinator, Chris Hacker at (916) 845-8929 or chris.hacker@caloes.ca.gov.

Sincerely,

Nancy Ward

NANCY WARD
Director

cc: Ann Patterson, Cabinet Secretary, Office of the Governor

EMAP Accredited
EMERGENCY MANAGEMENT ACCREDITATION PROGRAM

3650 SCHRIEVER AVENUE, MATHER, CA 95655
(916) 845-8506 TELEPHONE (916) 845-8511 FAX
www.CalOES.ca.gov

REPORT TO CALIFORNIA LEGISLATURE

REGARDING CYBERSECURITY REPORTING REQUIRED BY AB-2355

SUMMARY OF LOCAL EDUCATIONAL AGENCY CYBERATTACK AND DATA BREACH REPORTING TO THE CAL-CSIC

January 1, 2024

Contents

1. EXECUTIVE SUMMARY

This report is being provided pursuant to California Education Code Section 35266. The California Cybersecurity Integration Center (Cal-CSIC) is required to establish a database that tracks reports of cyberattacks submitted by local educational agencies and submit annually, by January 1, a report to the Governor and the relevant policy committees of the Legislature summarizing, among other requirements, cyberattacks and data breaches affecting local educational agencies.

AB 2355 added Section 35265 of the Education Code which defined two terms central to this report:

> (b) "Cyberattack" means either of the following:
>
> > (1) Any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by unauthorized access.
> >
> > (2) The unauthorized denial of access to legitimate users of a computer system, computer network, computer program, or data.

(c) "Local educational agency" means a school district, county office of education, or charter school.

AB 2355 further clarified the threshold for reporting such cyberattacks to the Cal-CSIC:

EDC Code Section 35266. (a) A local educational agency shall report any cyberattack impacting more than 500 pupils or personnel to the California Cybersecurity Integration Center.

Consistent with the requirements of Education Code Section 35266, this report:

1. Summarizes the types and number of cyberattacks on local educational agencies,
2. Summarizes the types and number of data breaches affecting local educational agencies that have been reported to the Attorney General pursuant to Sections 1798.29 and 1798.82 of the Civil Code, and,
3. Summarizes any activities provided by the Cal-CSIC to prevent cyberattacks or data breaches of a local educational agency, and,
4. Support provided by the Cal-CSIC following a cyberattack or data breach of a local educational agency.

The reporting dates used in this report cover the period November 2022 to October 2023.

2. CYBERATTACKS ON LOCAL EDUCATIONAL AGENCIES

Cybersecurity Incidents[1] Involving Local Educational Agencies

Category By Count of Impacted Individuals	Count of Incidents
500 or more pupils or personnel	16
Less than 500 pupils or personnel	1
Unknown (information not provided by reporting party)	21
Total	**38**

Cyberattacks by Educational Agency Type

Cyberattack Type	School District	Charter School	County Office of Education	Total
Ransomware	5	3	3	11
Malware/Scareware/Virus	2	0	1	3
Total	7	3	4	**14**

In its initial version of its tracking database, the Cal CSIC has collected 38 reports of cybersecurity incidents affecting local educational agencies during the reporting period.

Due to the low numbers of local educational agencies reporting under AB 2355, the Cal-CSIC had to rely on open-source intelligence and vendor-provided proprietary cyber threat intelligence to get a more complete perspective of incidents impacting local educational agencies. Open-sources often included only limited incident information, therefore, the Cal-CSIC classified the incident based on the information that was available.

[1] A cybersecurity incident is an occurrence that: (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

3. DATA BREACHES AFFECTING LOCAL EDUCATIONAL AGENCIES

Data Breaches by Educational Agency Type

Incident Type	School District	Charter School	County Office of Education	Total
Data Breach	11	2	0	13
Data Breach and Ransomware	2	1	1	4
Total	13	3	1	**17**

Due to the nature of cybersecurity incidents, ransomware events often include data breaches and are not mutually exclusive. There is a difference between the total of 17 in this table and the total of 14 in the cyberattacks table because not all cyberattacks include data breaches, and not all data breaches include cyberattacks.

4. ACTIVITIES OR SUPPORT PROVIDED TO LOCAL EDUCATIONAL AGENCIES BY THE CAL-CSIC

SUPPORT PROVIDED BY THE CAL-CSIC FOLLOWING A CYBERATTACK OR DATA BREACH OF A LOCAL EDUCATIONAL AGENCY

Of the incidents listed above affecting local educational agencies and meeting AB 2355 criteria, the Cal-CSIC provided the following response services:

	Count	Types of Services or Outreach Provided (Summary)
Cyberattacks		
School District	7	The Cal-CSIC conducted outreach to four of the seven school districts impacted. Services were not provided to three of the four school districts due to the school district not being responsive, declining services or invoking cyber insurance. Of the four, one school district received Cal-CSIC Incident Response services which consist of: Quarantine, Vulnerability Scanning/Vulnerability Analysis, NetFlow Analysis, Dark Web Analysis/Dark Web Monitoring, Hard Disk Forensics, Memory Forensics, Network Forensics, Malware Analysis. No outreach was performed with the remaining three school districts due to the lack of direct and/or timely reporting to the Cal-CSIC.
Charter School	3	The Cal-CSIC conducted outreach to one of the three charter schools impacted but the charter school declined services. No outreach was performed with the remaining two charter schools due to the lack of direct and/or timely reporting to the Cal-CSIC.
County Office of Education	4	The Cal-CSIC conducted outreach to three of the four County Offices of Education impacted. Services were not provided to three of the County Offices of Education due to the office not being responsive, declining services or invoking cyber insurance. No outreach was performed with the one remaining County Office of Education due to the lack of direct and/or timely reporting to the Cal-CSIC.

Data Breaches		
School District	11	The Cal-CSIC conducted outreach to five of the eleven school districts impacted. All five received some services such as threat notification, mitigation recommendations and support from the Cal-CSIC. Of the five, one school district received Cal-CSIC Incident Response services which consist of: Quarantine, Vulnerability Scanning/Vulnerability Analysis, NetFlow Analysis, Dark Web Analysis/Dark Web Monitoring, Hard Disk Forensics, Memory Forensics, Network Forensics, Malware Analysis. No outreach was performed with the remaining six school districts due to the lack of direct and/or timely reporting to the Cal-CSIC.
Charter School	2	No outreach was performed for any of the two charter schools due to the lack of direct and/or timely reporting to the Cal-CSIC.
County Office of Education	0	

ACTIVITIES PROVIDED BY THE CAL-CSIC TO PREVENT CYBERATTACKS OR DATA BREACHES OF LOCAL EDUCATIONAL AGENCIES

Notification Type	School District	Charter School	County Office of Education	Total
Credential Leak	21	0	0	21
Malicious Activity	3	0	5	8
Vulnerability	3	0	7	10
Total	27	0	12	**39**

The Cal-CSIC provides additional proactive support to local educational agencies in efforts to prevent a potential cyberattack. This includes 39 instances

of: notifying entities of vulnerabilities in their network, malicious activity observed in their network, and credential leaks observed on the dark web. These notifications provide indicators of possible incidents but are not confirmed incidents and require additional analysis and follow-up to validate. The 39 notifications here is different from the total of 38 incidents because some of these notifications do not involve confirmed incidents, and not all incidents involved proactive notification services.

Additionally, the Cal-CSIC provides products such as threat briefs and bulletins on critical sectors such as the Education sector to inform the sector audience of threats and vulnerabilities to improve their cybersecurity posture. During the reporting period, the Cal-CSIC distributed 112 cyber threat intelligence products to a large distribution list which includes a number of local educational agencies. This included one bulletin specifically about cyberthreats to the education sector.

5. AB 2355 CYBERATTACK REPORTING DATABASE DESCRIPTION

To avoid excluding any relevant reporting, the Cal-CSIC began by tracking all incidents which appear to affect local educational institutions (more broadly defined)[2] from all sources normally used to monitor cybersecurity incidents. This means that the tracking database includes incidents reported directly to the Cal-CSIC as AB 2355 incidents, reports discovered on the Attorney General's Office data breach reporting public website, and incidents which may or may not meet AB 2355 criteria discovered through other intelligence sources Cal-CSIC uses in its cybersecurity mission.

As part of its normal operations, the Cal-CSIC generally focuses on tracking cybersecurity "incidents" which is a broader category of event than the more narrowly defined "cyberattack." Incidents meeting the definition of cyberattack

[2] California Government Code Section 8586.5 requires the Cal-CSIC to coordinate cyber threat information sharing including that "received from utilities, *academic institutions*, private companies, and other appropriate sources." As a result, as part of Cal-CSIC's regular operations it tracks threat information related to public and private institutions in K-12, colleges, and universities. Reporting required by California Education Code Section 35266 is a subset of this data.

in AB 2355 are generally more limited in number and require further analysis and information to confirm.

The Cal-CSIC follows the definition of an incident as defined by Federal law (see 44 U.S.C. § 3552(b)(2))[3] and guidelines from the National Institute of Standards and Technology (NIST)[4] which defines the term incident (in the context of cybersecurity) as:

> *(2) The term "incident" means an occurrence that-*
>
> *(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or*
>
> *(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.*

[3] 44 USC 3552: Definitions (house.gov)
[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf