

NOV 18 2024

By: T. Cutts, Deputy

CYBERSECURITY IN SAN DIEGO SCHOOL DISTRICTS

SUMMARY

Cyberattacks on computing systems are a daily occurrence, impacting government, private industry, and education organizations. In San Diego County multiple school districts have been the targets of such attacks, resulting in disruption of education services, loss of private information, and money spent to restore services.

San Diego County has 42 school districts, ranging in size from almost 100,000 students to less than 100. The San Diego County Office of Education (SDCOE) provides a wide variety of services to help districts in their cybersecurity preparations. However, each school district operates independently and is ultimately responsible for its cybersecurity preparedness.

There are many established best practices for school districts to guard against and recover from cyberattacks. The Grand Jury interviewed seven San Diego County school districts. Surveys and interviews with this subset of county school districts show varying degrees of implementation of these best practices, from mature to nascent.

The Grand Jury recommends that all interviewed school districts implement at least a basic set of preparedness measures, including annual training, multi-factor authentication, and maintaining cyber insurance. Further, the Grand Jury recommends that the interviewed school districts improve their understanding of cybersecurity threats and preparations to counter them, and recommends that the SDCOE support school districts in this effort. The Grand Jury also encourages all other San Diego County school districts to implement similar practices.

BACKGROUND

News stories appear almost daily detailing successful cyberattacks against U.S. corporate, government, education, and healthcare institutions. While cyberattacks are now in the public's awareness due to these stories, the threat from malicious actors trying to steal information or extort money from computer users is almost as old as the personal computer industry.¹ Since the first ransomware attack in 1989, there has been a steady struggle between defensive measures designed to protect computer systems, and new attack methods designed to get around those measures.

The U.S. Department of Education, Office of Educational Technology published a report on K-12 digital infrastructure, which documented 1,619 cybersecurity-related incidents from 2016–2022, with an untold number of additional attacks that were never publicized.² In the last few years, several of these cyberattacks have struck targets in San Diego County, including three school districts: San Diego Unified, Sweetwater Union, and San Dieguito Union. These attacks included a ransomware attack and the successful theft of private information. These attacks have had direct financial impacts on school districts, have negatively affected instruction to students, and have placed community members' private information at risk.

With cyberattacks posing an immediate threat to school districts, the Grand Jury investigated the readiness of school districts to defend against cyberattacks and to respond in the event of a successful attack. Each of the 42 school districts in San Diego County operates as an

independent entity, so the Grand Jury elected to investigate a subset of all districts to determine trends and best practices that can subsequently be shared across all the districts.

METHODOLOGY

The Grand Jury interviewed individuals from several school districts on the state of their cybersecurity readiness, using a structured template to assess the district’s cybersecurity readiness. The districts selected represent a cross-section of San Diego County’s 42 public school districts: urban, suburban, and rural; elementary, high school, and unified; smallest to largest. The individuals interviewed varied in job titles from Network Analyst to Superintendent. Table 1 lists the school districts and their student and total staff (certificated and classified).

District	# Students	# Staff
Borrego Springs Unified School District	<400	75
Cajon Valley Union Elementary School District	17,500	2,600
Grossmont Union High School District	21,000	2,000
San Diego Unified School District	90,000	13,000–14,000
San Dieguito Union High School District	12,500	1,250
Santee Elementary School District	6,900	1,500
Sweetwater Union High School District	35,000–38,000	4,500–5,000

Table 1. Interviewed School Districts

The decision to select a sample of school districts for interviews, rather than attempting to interview all 42 districts, was based on the time constraints of the Grand Jury. For the districts interviewed, the average elapsed time between request and interview was almost four months. Three other districts did not respond to repeated requests.

The Grand Jury also interviewed representatives of the SDCOE and a cybersecurity expert with experience in academia and industry. The Grand Jury reviewed several cybersecurity frameworks and research reports published by government and private organizations. The Grand Jury also reviewed data the SDCOE, and several school districts provided regarding specific cybersecurity readiness programs and their details.

DISCUSSION

Introduction

Cybersecurity is well-known to the public. A recent survey by the Chicago Council on Global Affairs showed that almost three-quarters of Americans view cyberattacks as a critical threat.³ However, a survey by the Pew Research Center found that, when asked 13 questions on

cybersecurity issues and concepts, the typical respondent answered only five questions correctly.⁴ This lack of practical knowledge creates opportunities for successful cyberattacks. Understanding the various threats and how to recognize and counter these threats will reduce the risk of a successful attack. This report will describe some of the most important measures that an enterprise (public or private) can take to reduce those threats, and then apply that understanding in the context of San Diego County's school districts.

Any discussion of cybersecurity can become highly technical, with sets of terms and concepts that may be beyond the understanding of a common computer user. A few critical concepts are described below.

Cyberattack Concepts

Attacks on an enterprise may come in a variety of forms, from a variety of sources, with a variety of impacts. Some key concepts include:

- Threat actor: an individual, group, organization, or government that conducts detrimental activities, i.e., the “bad guys.” In school districts, students can be a threat actor.
- Attack vector: a way for attackers to enter a network or system. Examples include:
 - Phishing: tricking a user into revealing sensitive information (like a password) by using an email that appears legitimate on cursory inspection.
 - Email attachments that contain malicious code.
 - Taking over an account using stolen credentials, and
 - Exploiting vulnerabilities in the computing environment, such as exploiting a security vulnerability in a network or software product.
- Types of cyberattacks: the actions that a threat actor can take that will harm a computer user. Examples include:
 - Ransomware: blocking access to a computer system until a sum of money is paid.
 - Data breach: removing (stealing/exfiltrating) sensitive information (e.g., Social Security Number) from a computer system.
 - Data destruction: deleting or damaging information so it is no longer readable or usable, and
 - Distributed Denial of Service (DDOS): a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

The lists above are just an abbreviated listing of the types and methods of attack. Threat actors are constantly adapting their techniques and developing new ones to keep ahead of cybersecurity vendors, such as the growing use of artificial intelligence to create highly personalized phishing emails.⁵

Cybersecurity Frameworks

Faced with all the possible types and means of attack, an individual responsible for cybersecurity could be overwhelmed. A cybersecurity framework is a mechanism for organizing and simplifying the way an entity prepares its defenses, providing a prioritized list of steps to be taken. Some common frameworks include:

- U. S. Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency’s (CISA) Cross-Sector Cybersecurity Performance Goals.⁶
- Center for Internet Security (CIS) Critical Security Controls,⁷ a set of 154 controls organized into three implementation groups by priority.
- The U.S. Department of Justice and the U.S. Department of Health and Human Services jointly released a one-page set of Cybersecurity Action Steps for the K-12 Community, shown in the Appendix.⁸ In brief, this document lists four steps to reduce cybersecurity risk:
 - Enable multi-factor authentication (MFA).
 - Use strong passwords.
 - Recognize and report phishing, and
 - Update system software.

This report groups the set of defensive measures into three categories: human measures, technical measures, and organizational measures.

Human Measures

Human behavior is the weakest link in cybersecurity. A major tool to influence human behavior is training: risk awareness, the methods used to exploit weaknesses, and the role that individuals have in preventing successful attacks. Two additional measures to help strengthen a user’s behavior are multi-factor authentication (MFA) and password management.

MFA is generally acknowledged as one of the most valuable preparedness measures an organization can take.⁹ With MFA, users need to provide a second factor (after the username and password) that positively confirms their identity. This second factor is often delivered as a code via a text message to the user’s mobile phone or a notification on a smartphone app.

Password management includes policies, procedures, and technology to ensure robust and secure passwords. Password management applications can enforce an organization's rules on password strength and non-reuse, and auto-fill online passwords to eliminate users' need to remember long, complex passwords.

Technical Measures

Technical measures are steps a school district can take to harden its computing environment, to make it more resistant to a cyberattack and more resilient in response to a successful intrusion. The list below is a subset of the technical readiness steps that apply to almost any organization that uses information technology (IT) to run or support their business.

- **Cloud Computing**
Moving software applications “into the cloud” frees an organization from many of the administrative tasks described below, as the cloud service provider manages these activities.
- **Patch Management**
Security defects are constantly discovered in software systems, and vendors (hopefully) respond by issuing security patches. Best practices call for organizations to stay current with patches, applying them no more than one month after the patch release.

- **Backups and Disaster Recovery**
In a ransomware attack, the intruder encrypts the organization's files, making them unreadable. Having a backup of applications and data will allow an organization to restart operations by restoring from the backup. If the event causes more significant damage to a data center, a disaster recovery site is a geographically separate data center that can be used in the event of a disaster.
- **Distributed Denial of Service (DDOS) Protection**
Internet Service Providers may provide DDOS protection as part of their connectivity offering.
- **Vulnerability Scanning**
Certain organizations offer vulnerability scanning services, where the scanner will look for weaknesses in an organization's IT systems. For example, CISA offers a Vulnerability Scanning service at no cost.

The set of technical best practices evolves constantly, as threat actors change tactics and new technologies (such as artificial intelligence) become more widely available.

Organizational Measures

Organizational measures for a K-12 school district start with an understanding that the district's mission to deliver educational services can be threatened if it does not secure its IT environment. Best practices that enable a school district to harden itself against cyberattacks, and to recover in the event of a successful attack include:

- **Clear Technical Leadership:** an identified person responsible for “establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected”,¹⁰
- **Informed Executive Leadership:** a School Board and Superintendent who understands the critical role of cybersecurity in protecting the ability of the district to deliver on its mission.
- **Cyber insurance:** helps a district recover from a successful cyberattack.

San Diego County Office of Education

For the scope of this Grand Jury's investigation, the San Diego County Office of Education (SDCOE) has two distinct roles: as a formal oversight body of county school districts for state-mandated functions such as annual reports, and as a provider of technical services and tools that individual school districts can use at their option.

The SDCOE has limits on the level of oversight of county school districts, generally related to financial matters. The SDCOE has no authority to require a district to take any specific action on cybersecurity readiness. However, the SDCOE can influence individual school districts to take appropriate actions. It exerts this influence by providing a broad set of products and services to districts to help them improve their cybersecurity readiness.

Technology Services

The scope of the technology services offered by the SDCOE is very broad.¹¹ They have a special focus on cybersecurity and offer a wide variety of cybersecurity services to the County's school districts:

- Vulnerability assessment, penetration testing, and remediation services that help detect, identify, and analyze current network, server, and/or endpoint vulnerabilities and threats.
- Cybersecurity framework implementation.
- Setup and configuration guidance for firewalls, secure networks, and domain management.
- Security policy review and recommendations (board policies, administrative regulations, internal guidelines, etc.), and
- Post-incident Services: Cyber incident response and digital forensics.¹²

The SDCOE also offers the Red Herring software solution to provide phishing awareness training for school district employees and is offered free of charge to San Diego County school districts.

In addition to the technology, training, and consulting service described above, the SDCOE sponsors a Risk Management Joint Powers Authority (JPA) that offers risk management and insurance products to member school districts. In particular, the JPA offerings include cyber insurance from a commercial underwriter.

While San Diego County school districts are not required to use any of these products and services, many of the San Diego County districts use at least some of these offerings. Based on information provided by the SDCOE:

- 28% of districts have received educational services from SDCOE since 2017.
- 67% of districts are using or evaluating Red Herring for phishing awareness.
- 81% of districts receive internet service with DDOS protection through the SDCOE and the Corporation for Education Network Initiatives in California (CENIC) backbone.
- 76% of districts have cyber insurance provided through the JPA.

The Grand Jury commends the SDCOE for providing a comprehensive set of cybersecurity products and services to the County’s school districts and for the leadership they have demonstrated on local and national stages.

School District Cybersecurity Readiness

The Grand Jury interviewed personnel from seven San Diego County school districts to assess their district’s cybersecurity readiness. Rather than focus on specific weaknesses of individual districts—which could direct threat actors to target new attacks—the Grand Jury presents a summary of cybersecurity readiness factors.

Human Readiness

As previously discussed, humans are the weakest link in ensuring the cybersecurity of an organization. One way to exploit this weakness is by phishing—enticing an employee to click a link in a legitimate-looking email. The best defense against phishing and other cyberattacks is to train users on cybersecurity and their role in helping protect their school district against attack.

Best practices call for such cybersecurity training to be done annually, as part of the district’s other annual training. Furthermore, such training should apply to all staff who use computer systems. The Grand Jury found that the training delivered by the interviewed districts varied widely. Most provided some form of cybersecurity training to all teachers and staff annually, although there were exceptions. One interviewed district was just beginning a pilot training

program for their classified staff only and did not have a firm plan to expand to include teachers. Another interviewed district provides only a briefing on IT “acceptable use” policies for new hires, which falls far short of even the most rudimentary level of cybersecurity readiness.

Training for students is much less common, beyond the basic “acceptable use” training that accompanies district-provided laptops for students. There were two notable exceptions: Cajon Valley Union and San Dieguito Union provide a “Digital Citizenship” class for their students, and San Dieguito Union also has a special training focus on 7th-grade students. While student computers are less of a threat vector since they are typically walled off from district IT systems that contain sensitive data, such digital citizenship training will bring benefits to students beyond their K-12 education.

In addition to formal annual training, most interviewed districts also implement an anti-phishing solution to provide continuous reinforcement of the need to maintain awareness. The Red Herring solution provided by SDCOE was most cited. Several interviewed districts also had a tool in their email platforms that allowed individual users to flag a message as “suspect,” which triggered an investigative process by IT to determine if the suspect email was legitimate.

The Grand Jury recommends annual cybersecurity training for all school district staff and students, with a particular focus on new-hire training for staff. Training material is not one size fits all; the curriculum should be appropriate for the role (staff) or age/grade (student) receiving the training. The Grand Jury also recommends that districts implement a phishing awareness solution as well.

The Grand Jury Recommendations include a target implementation date at the beginning of the 2026-2027 school year. This gives districts two full years to implement these solutions, which should allow sufficient time to roll out these programs to all users.

Technical Readiness

The Grand Jury queried school districts on several specific technical readiness factors: MFA and password management, patch management procedures, backup management procedures and disaster recovery, DDOS protection, and vulnerability scanning. Almost all interviewed districts have adequate solutions in place for these protection measures; the notable exception was that three out of seven interviewed school districts had not completely implemented MFA for all staff. Given that MFA is one of the most critical tools in defending against cyberattacks, anything less than full implementation is concerning. The Grand Jury recommends that all interviewed school districts implement MFA for all staff members (not students), by the start of the 2026-2027 school year. The Grand Jury also encourages all other San Diego County school districts to implement MFA for all staff members.

The details of why districts had not implemented a full MFA solution varied.

- One district was in the process of implementing MFA, with final deployment scheduled for the next school year.
- Multiple districts noted difficulties working with unions to get an agreement to deploy MFA, as it would require changes to work rules that would require negotiation.
- Some Districts noted concerns about the use of cell phones to receive the second factor, and whether this would be a personal (employee-owned) or district-owned device.

- Other districts have deployed MFA to only a subset of staff; in one case only to users with access to privileged information (<2% of all staff).

The Grand Jury observed that several school districts have implemented MFA with all staff, including unionized staff, and have reported little or no pushback from users after the initial implementation period. This suggests that a well-run change management program can help work through obstacles (people, process, technology) that may be encountered. To assist with a district's change management efforts, the SDCOE offers a complete set of consulting services to support districts deploying MFA, such as an MFA Workbook that helps districts structure an MFA deployment project.¹³

The Grand Jury also received testimony from an industry expert on two best practices related to MFA and password management. The first concerns the method of delivering the second factor in an MFA scheme. Most people have experience with delivery of the second factor via a text message on their mobile phone. While easy to use, this method is considered less secure than delivery of the second factor via a phone-based app (better) or a hardware token (best). The other best practice is the use of an enterprise password management application to secure the user's passwords and to enforce guidelines on password complexity and non-reuse. The Grand Jury views these as more aspirational steps and does not make specific recommendations at this time.

Finally, it should be noted that the set of technical best practices is not static. Threat actors are constantly changing and adapting their attack methods to work around the latest defenses, and school districts will need to adapt their defensive measures accordingly.

Organizational Readiness: Technical Leadership

The Grand Jury interviewed representatives of seven school districts involved with cybersecurity who had a wide variety of technical expertise, from extensive training and experience to only a high-level understanding of technology issues. These variations are natural based on the vast differences in district size, from 400 to 90,000 students.

While there is no one-size-fits-all prescription for staffing and operating a cybersecurity readiness function in a school district, one best practice is clear: There should be one individual who is responsible and accountable for cybersecurity readiness in the district. This Cybersecurity Lead position should be the point person for (a) organizing the district's readiness efforts, and (b) communicating to the overall district leadership on the status of the district's readiness. This Cybersecurity Lead need not be a new hire in the district; ideally, it would be a formal role designation for an existing employee.

Organizational Readiness: Organizational Leadership

The Grand Jury asked individuals about the attitude of their district's organizational leadership (i.e., Superintendent and School Board) on cybersecurity, and the support the technical organization has from leadership in implementing cybersecurity readiness measures. The responses indicated a variety of attitudes, from actively engaged to effectively disengaged. The level of engagement of senior leadership did not correlate with district size; it appears to be based on the specific individuals in leadership roles. These examples illustrate the diversity of leadership engagement and the impacts it has on the district's readiness. In one interviewed school district, the school board mandated that all staff take annual cybersecurity training, which

they made happen. In another interviewed district the senior leadership did not support the technology team's efforts to implement MFA, complaining it was too difficult.

A cybersecurity expert cited the recent Securities and Exchange Commission (SEC) final rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure final rule.¹⁴ The rule includes a requirement to disclose annually information regarding cybersecurity risk management, strategy, and governance, including a description of the board of directors' oversight of risks from cybersecurity threats. This rule helps potential investors evaluate the risk exposure of public companies before making investment decisions.

Although school districts are not public companies, they are just as susceptible to cyberattacks. By analogy to the SEC rule, the Grand Jury recommends that the Cybersecurity Lead deliver an annual report to the school district leadership on the district's cybersecurity readiness. This report would make district leadership more informed on the readiness of their district and help inform future readiness plans and actions. A copy of this report should also be sent to the SDCOE to enable the development of a county-wide view of cybersecurity readiness and provide feedback to the school district where appropriate.

To provide a level of rigor and consistency in these reports, the Grand Jury also recommends that the SDCOE take a lead role in preparing materials (templates, guides, training, etc.) that will support this reporting requirement. Further, the content of the report should be updated annually to reflect changes in the threat landscape and best practices for cybersecurity readiness.

Organizational Readiness: Cyber Insurance

A final element of organizational readiness is cyber insurance. Cyber insurance is part of an overall approach to risk management for a school district; it helps a school district recover from a successful cyberattack. Cyber insurance also will help a district prepare against a possible attack; the underwriting criteria require a school district to have a minimum set of readiness standards (such as MFA) in place to qualify for insurance.

Almost all interviewed districts reported having cyber insurance in place obtained through the Risk Management Joint Powers Authority (JPA). One district directly contracts for cyber insurance. Not all San Diego County school districts receive cyber insurance through the JPA. The Grand Jury was unable to determine whether these districts are covered by a policy outside the JPA. Given the value of cyber insurance to help a district both prepare for and recover from a cyberattack, all school districts should have cyber insurance coverage.

SSNs and Cybersecurity

Social Security Numbers (SSNs) are a highly desired target, as valid SSNs can be used for identity theft. In the K-12 school context, student SSNs are particularly valuable: A threat actor may use the student's SSN for identity theft, and the impact of that theft (e.g., fraudulent credit cards) may not be noticed until the student reaches adulthood and attempts to open their first credit card.

Although school districts are required to store and use SSNs for staff for legitimate purposes such as W-2 reporting, California Education Code § 49076.7(b)¹⁵ specifically prohibits a school district from collecting SSNs from students or parents unless there is a specific requirement. In practice, programs that require some form of identity verification only use the last four digits of a

parent's or a guardian's SSN, so there is no known circumstance that a district should be requesting or storing the SSN of a student or a parent.

Recent newspaper articles and school district notices have stated that personal information, possibly including SSNs, was stolen from certain school districts.^{16,17} The articles did not specify whether the stolen SSNs belonged to students, parents, or staff, which left the impression that students' or parents' SSNs might have been compromised, in apparent violation of state law.

The Grand Jury found that none of the interviewed school districts request or receive SSNs for students or parents. One interviewed district has such data on its servers, but they stated they are "in the process of purging" such data. The known instances of SSN thefts were restricted to staff SSNs only. Without minimizing the impact that any SSN theft can have on the individuals involved, the Grand Jury is pleased that parents and students were not subject to that attack.

Scope of Findings and Recommendations

The Grand Jury's investigation shows that the level of cybersecurity preparedness in San Diego County school districts varies widely, from best-in-class to needing significant improvement. Furthermore, the level of preparedness across the three dimensions of Human, Technical, and Organizational readiness is uneven, with one interviewed district having excellent technical preparedness almost despite the lack of organizational preparedness. The Grand Jury's Findings summarize key aspects of cybersecurity readiness, and the Grand Jury Recommendations identify steps for school districts to achieve a moderate level of cybersecurity readiness.

The Grand Jury identifies two sets of school districts for responses: those that are required to respond according to the Grand Jury report per California Penal Code §933(c), and those that are invited to respond. This Grand Jury *requires* responses from the school districts that were investigated and *invites* (but does not require) responses from the remainder of the County's 42 public school districts. (See the Require Responding Agency and Invited Responding Agency tables starting on page 13.)

FINDINGS

- F1.** The San Diego County Office of Education provides high-quality cybersecurity readiness tools and services to county school districts at no or very low cost.
- F2.** The best practice for cybersecurity training in school districts is annual training for all staff and students.
- F3.** Preventable human behavior is the main cause of successful cyberattacks.
- F4.** Multi-factor authentication is the most effective cybersecurity technical measure to reduce successful cyberattacks.
- F5.** Successful organizations often have a role or position that is identified as responsible and accountable for the planning, resourcing, and execution of cybersecurity activities.
- F6.** A school district leadership's knowledge of cybersecurity issues can positively influence a district's cybersecurity readiness.
- F7.** Obtaining cyber insurance helps a school district to both prepare defenses against and recover from cyber-attacks.

RECOMMENDATIONS

- R1. School districts provide cybersecurity training to all staff members, at least annually, by the beginning of the 2026-2027 school year.
- R2. School districts provide cybersecurity training to all students, at least annually, by the beginning of the 2026-2027 school year.
- R3. School districts implement a phishing awareness training solution for all staff members by the beginning of the 2026-2027 school year.
- R4. School districts implement multi-factor authentication for all staff members by the beginning of the 2026-2027 school year.
- R5. School districts designate a single individual as Cybersecurity Lead responsible for cybersecurity readiness in the district by the beginning of the 2025-2026 school year.
- R6. School districts require the Cybersecurity Lead to provide an annual report to the school board and the SDCOE on the state of cybersecurity readiness by the beginning of the 2025-2026 school year.
- R7. School districts acquire and maintain cyber insurance coverage by the beginning of the 2025-2026 school year.
- R8. SDCOE creates a methodology, training, and report template to support a school district's Cybersecurity Lead, updated annually to reflect the changing threat landscape by the beginning of the 2025-2026 school year.
- R9. SDCOE receives and reviews school district annual reports on the state of cybersecurity.

¹ Dudley, Renee, and Daniel Golden. "The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from Cybercrime." Farrar, Straus and Giroux. 2022.

² Office of Educational Technology, "K-12 Digital Infrastructure Brief: Defensible & Resilient" (February 8, 2023). https://tech.ed.gov/files/2023/08/DOEd-Report_20230804_-508c.pdf p6.

³ The Chicago Council on Global Affairs. "Americans Recognize Cyber Threats, but Are Divided on Best Response" (June 7, 2022) <https://globalaffairs.org/commentary-and-analysis/blogs/americans-recognize-cyber-threats-are-divided-best-response>

⁴ Pew Research Center. "What the Public Knows About Cybersecurity" (March 22, 2017). <https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/>

⁵ Fast Company. "The growing threat of AI in social engineering: How business can mitigate risks" (April 8, 2024) <https://www.fastcompany.com/91088574/the-growing-threat-of-ai-in-social-engineering-how-business-can-mitigate-risks>

⁶ Cybersecurity & Infrastructure Security Agency. "Cross-Sector Cybersecurity Performance Goals". <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>

⁷ Center for Internet Security. "CIS Critical Security Controls" <https://www.cisecurity.org/controls>

⁸ SchoolSafety.gov, "Cybersecurity Action Steps for the K-12 Community" (October 2022). [https://www.schoolsafety.gov/sites/default/files/2022-10/Cybersecurity Action Steps for the K-12 Community SchoolSafety.gov Infographic October 2022.pdf](https://www.schoolsafety.gov/sites/default/files/2022-10/Cybersecurity%20Action%20Steps%20for%20the%20K-12%20Community%20SchoolSafety.gov%20Infographic%20October%202022.pdf)

⁹ See notes 6, 7, and 8.

¹⁰ Wikipedia. "Chief Information Security Officer." https://en.wikipedia.org/wiki/Chief_information_security_officer

¹¹ San Diego County Office of Education, Technology Services. <https://www.sdcoe.net/administrative-services/technology>

-
- ¹² San Diego County Office of Education. <https://www.sdcoe.net/administrative-services/technology/cybersecurity>
- ¹³ San Diego County Office of Education, Cybersecurity. “Multi-Factor Authentication Workbook” (October 2022). <https://resources.finalsite.net/images/v1666803502/sdcoenet/vhozlhoh3k1bzhksf0aa/MFAWorkbookOct2022.pdf>
- ¹⁴ 17 CFR §229.106 Cybersecurity (2023). [https://www.ecfr.gov/current/title-17/chapter-II/part-229/subpart-229.100/section-229.106#p-229.106\(b\)](https://www.ecfr.gov/current/title-17/chapter-II/part-229/subpart-229.100/section-229.106#p-229.106(b))
- ¹⁵ California State Education Code § 49076.7 (1976). https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=49076.7&lawCode=EDC
- ¹⁶ Schroeder, Lauryn. “San Diego Unified students’ medical data compromised in October cybersecurity breach, school district says.” San Diego Union-Tribune. (May 19, 2023). <https://www.sandiegouniontribune.com/news/education/story/2023-05-19/student-medical-data-compromised-san-diego-unified-cybersecurity-breach>
- ¹⁷ Sweetwater Union High School District, Data Security Notice. Accessed April 16, 2024. <https://www.sweetwaterschools.org/data-security/>

REQUIREMENTS AND INSTRUCTIONS

The California Penal Code §933(c) requires any public agency which the Grand Jury has reviewed, and about which it has issued a final report, to comment to the Presiding Judge of the Superior Court on the findings and recommendations pertaining to matters under the control of the agency. Such comment shall be made no later than 90 days after the Grand Jury publishes its report (filed with the Clerk of the Court); except that in the case of a report containing findings and recommendations pertaining to a department or agency headed by an elected County official (e.g. District Attorney, Sheriff, etc.), such comment shall be made within 60 days to the Presiding Judge with an information copy sent to the Board of Supervisors.

Furthermore, California Penal Code §933.05(a), (b), (c), details, as follows, the manner in which such comment(s) are to be made:

- (a) As to each grand jury finding, the responding person or entity shall indicate one of the following:
 - (1) The respondent agrees with the finding
 - (2) The respondent disagrees wholly or partially with the finding; in which case the response shall specify the portion of the finding that is disputed and shall include an explanation of the reasons therefor.
- (b) As to each grand jury recommendation, the responding person or entity shall report one of the following actions:
 - (1) The recommendation has been implemented, with a summary regarding the implemented action.
 - (2) The recommendation has not yet been implemented but will be implemented in the future, with a time frame for implementation.
 - (3) The recommendation requires further analysis, with an explanation and the scope and parameters of an analysis or study, and a time frame for the matter to be prepared for discussion by the officer or head of the agency or department being investigated or reviewed, including the governing body of the public agency when applicable. This

time frame shall not exceed six months from the date of publication of the grand jury report.

(4) The recommendation will not be implemented because it is not warranted or is not reasonable, with an explanation therefor.

(c) If a finding or recommendation of the grand jury addresses budgetary or personnel matters of a county agency or department headed by an elected officer, both the agency or department head and the Board of Supervisors shall respond if requested by the grand jury, but the response of the Board of Supervisors shall address only those budgetary or personnel matters over which it has some decision-making authority. The response of the elected agency or department head shall address all aspects of the findings or recommendations affecting his or her agency or department.

Comments to the Presiding Judge of the Superior Court in compliance with the Penal Code 933.05 are required from the:

Required Responding Agency	Findings	Recommendations
Borrego Springs Unified School District	F1 through F7	R1, R2, R3, R4, R5, R6
Cajon Valley Union School District	F1 through F7	R5, R6
Grossmont Union High School District	F1 through F7	R1, R2, R4, R5, R6
San Diego Unified School District	F1 through F7	R1, R2, R5, R6
San Dieguito Union High School District	F1 through F7	R5, R6
Santee School District	F1 through F7	R3, R4, R5, R6
Sweetwater Union High School District	F1 through F7	R2, R3, R5, R6
San Diego County Office of Education	F2 through F7	R8, R9

Comments to the Presiding Judge of the Superior Court in compliance with the Penal Code 933.05 are invited from the:

Invited Responding Agency	Findings	Recommendations
Alpine Union School District	F1 through F7	R1 through R7
Bonsall Unified School District	F1 through F7	R1 through R7
Cardiff School District	F1 through F7	R1 through R7
Carlsbad Unified School District	F1 through F7	R1 through R7
Chula Vista Elementary School District	F1 through F7	R1 through R7
Coronado Unified School District	F1 through F7	R1 through R7
Dehesa School District	F1 through F7	R1 through R7
Del Mar Union School District	F1 through F7	R1 through R7

Encinitas Union School District	F1 through F7	R1 through R7
Escondido Union School District	F1 through F7	R1 through R7
Escondido Union High School District	F1 through F7	R1 through R7
Fallbrook Union Elementary School District	F1 through F7	R1 through R7
Fallbrook Union High School District	F1 through F7	R1 through R7
Jamul-Dulzura Union School District	F1 through F7	R1 through R7
Julian Union School District	F1 through F7	R1 through R7
Julian Union High School District	F1 through F7	R1 through R7
La Mesa-Spring Valley School District	F1 through F7	R1 through R7
Lakeside Union School District	F1 through F7	R1 through R7
Lemon Grove School District	F1 through F7	R1 through R7
Mountain Empire Unified School District	F1 through F7	R1 through R7
National School District	F1 through F7	R1 through R7
Oceanside Unified School District	F1 through F7	R1 through R7
Poway Unified School District	F1 through F7	R1 through R7
Ramona City Unified School District	F1 through F7	R1 through R7
Rancho Santa Fe School District	F1 through F7	R1 through R7
San Marcos Unified School District	F1 through F7	R1 through R7
San Pasqual Union School District	F1 through F7	R1 through R7
San Ysidro School District	F1 through F7	R1 through R7
Solana Beach School District	F1 through F7	R1 through R7
South Bay Union School District	F1 through F7	R1 through R7
Spencer Valley School District	F1 through F7	R1 through R7
Vallecitos School District	F1 through F7	R1 through R7
Valley Center-Pauma Unified School District	F1 through F7	R1 through R7
Vista Unified School District	F1 through F7	R1 through R7
Warner Unified School District	F1 through F7	R1 through R7

October 2022

SCHOOLSAFETY.GOV


Cybersecurity Action Steps for the K-12 Community


Take proactive steps to defend against cybersecurity threats to your school.


Our growing dependence on technology systems – coupled with emerging, evolving, and increasingly deceptive cyber threats – demands enhanced awareness and vigilance when it comes to our online world. All educational institutions are at risk of falling victim to a cyberattack, and in recent years, K-12 schools have been an increasingly frequent target. These attacks can impact a school’s ability to carry out its educational obligations, protect sensitive student and staff data, and provide a safe and secure learning environment for our nation’s youth.


Defending against cyber threats takes teamwork, and every individual in the school setting, no matter their role, can play a part. Students, educators, administrators, and school personnel should “see themselves in cyber” by taking simple, proactive steps to better protect themselves and their school systems online.

School communities can take four simple action steps to reduce their cybersecurity risk posture.

- 

Enable Multi-Factor Authentication
Adversaries are increasingly capable of phishing or harvesting passwords to gain unauthorized access to information systems. Multi-factor authentication (MFA) is a layered approach to securing online accounts and the data they contain that requires users to provide two or more authenticators to verify their identity. Users who enable MFA are significantly less likely to be hacked because even if a password is compromised, unauthorized users will not be able to meet the second authentication requirement, stopping them from gaining access to online systems and data.
- 

Use Strong Passwords
Passwords are the most common means of authentication, and many systems have been successfully breached because of non-secure and inadequate passwords. Tips for creating a strong password include applying a combination of varying character types; avoiding common words, numerical patterns, and personal information; and using the longest password or passphrase permissible. School staff can also consider using a password manager program, which stores randomly generated passwords across multiple accounts and is only accessible with a master password.
- 

Recognize and Report Phishing
Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. Common signs of a phishing attempt include suspicious sender addresses, generic greetings and signatures, spoofed hyperlinks and websites, misspellings, poor grammar and sentence structure, and suspicious attachments. Schools can reduce the risk of phishing emails by enabling strong spam filters and implementing a cybersecurity awareness and training program to educate students and staff on the ways to recognize and report suspicious activity.
- 



Update Your Software
Outdated software can contain vulnerabilities that can be exploited by threat actors. When vendors become aware of vulnerabilities in their products, they often issue patches. Schools and districts should install updates as soon as possible to protect their systems, as well as enable automatic software updates whenever possible.

Sources: cisa.gov/ | schoolsafety.gov/cybersecurity/

SchoolSafety.gov Disclaimer

The U.S. Department of Homeland Security (DHS), U.S. Department of Education (ED), U.S. Department of Justice (DOJ), and U.S. Department of Health and Human Services (HHS) do not endorse any individual, enterprise, product, or service. DHS, ED, DOJ, and HHS do not mandate or prescribe practices, models, or other activities described in this communication. DHS, ED, DOJ, and HHS do not control or guarantee the accuracy, relevance, timeliness, or completeness of any information outside of those respective Departments, and the opinions expressed in any of these materials do not necessarily reflect the positions or policies of DHS, ED, DOJ, and HHS.



 Follow  Sign up

