CYBERSECURITY FOR SCHOOL DISTRICTS IN SANTA BARBARA COUNTY

The Need for Centralized Authority

SUMMARY

Santa Barbara County school districts are regularly targeted by cybersecurity threats, placing students and teachers directly in harm's way. If the response to the COVID pandemic has underscored anything, it is that the resiliency of the U.S. public education system is integral to the national economy and the well-being of communities, whether rural, suburban, or urban across the nation. Serving over 20 public school districts with approximately 70,000 students, the Santa Barbara County public education sector is an enormous albeit highly decentralized entity.

This report analyzing cybersecurity programs in Santa Barbara County's school districts follows last year's (2021) Grand Jury report entitled "Cybersecurity for Special Districts and County Service Areas in Santa Barbara County," which focused on all special districts within Santa Barbara County. This report centers directly on the status and effectiveness of cybersecurity programs in County schools.

County school districts have not mandated the use of multi-factor authentication (MFA)[1] nor formal cybersecurity training for teachers or students, both of which are well-

[1] Multi-factor authentication is an umbrella term for verifying the identity of end-users with a password and at least one other form of authentication.

recognized "best practices" for combatting cyber-attacks. County school districts operate independently and without significant support or oversight from the Santa Barbara County Education Office (SBCEO) in instituting MFA or formal training. Most small, rural districts lack sufficient resources to address the best practices standards recognized by federal and state governments. Even the larger, financially equipped districts have struggled with mandating MFA and formal training. These efforts can and should be centralized within the authority of the SBCEO to formalize policies and procedures in a more cost-effective manner, thereby placing all County school districts on equal footing.

INTRODUCTION

County school districts' Information Technology (IT) members are committed to their mission to ensure that the technology offered in the schools best supports their students and teachers. However, they are often faced with inadequate and underfunded resources, particularly the smaller districts. Some smaller districts rely entirely on independent contractors who work offsite and are often unable to immediately respond to urgent security breaches. The SBCEO also operates with a limited IT budget. The question here is whether expenses associated with cybersecurity should be given higher priority.

Significant sources of K-12 cyber data threats and breaches derive from the actions of school district staff, who, whether from a lack of training or lax cybersecurity controls, inadvertently share the personal information of students and staff in the course of their duties. The other group of individuals commonly responsible for school data breaches is the students themselves. These threats are often facilitated by weak school district password policies and a lack of multi-factor authentication.

METHODOLOGY

The Jury interviewed IT staff members within several school districts and SBCEO. The Jury also interviewed independent IT contractors working for school districts that are too small to have an IT person on staff. Cybersecurity experts were also interviewed about the necessities for a successful cybersecurity program. Finally, the Jury reviewed current Federal and California statutes and public and private publications relating to the administration of cybersecurity within K-12 school districts.

OBSERVATIONS

In January 2023, the U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) authored a report,[2] which outlined the urgent need for the K–12 communities to prevent and mitigate cyber-attacks.[3] CISA recommended that K–12 schools begin with a small number of prioritized investments including deploying MFA and implementing a strong cybersecurity training program.

Santa Barbara County Education Office's Role in Supporting Cybersecurity

SBCEO supports 20 public school districts, students, and families within Santa Barbara County. The largest district in the County has an enrollment of 17,000 students, whereas the smallest school district has only 51 students enrolled.[4]

SBCEO's website defines its role as providing the schools with managed antivirus protection, file storage and file sharing, backup services, and purchasing, installing, configuring, and troubleshooting computer hardware and software. SBCEO recognizes

---

[2] Protecting Our Future, Partnering to Safeguard K-12 Organizations from Cybersecurity Threats

[3] See, https://www.cisa.gov/protecting-our-future-cybersecurity-k-12 March 2023.

[4] See SBCEO.org May 17, 2023.

that it supports local school districts by providing services that can be delivered more efficiently and economically at the County level. These include implementing new standards, staff development, and training programs.[5]

Despite SBCEO's numerous cybersecurity responsibilities outlined above, it has provided minimal formal cybersecurity training to its school districts. SBCEO's IT Department is short staffed at present. SBCEO's IT Department primarily manages all school districts' financial systems, which is a complex undertaking for such a large school community.

Threats to Santa Barbara County School Districts

School personnel and people outside the school districts, share a responsibility to address the threats. They include:

- Teachers, administrators, and school board members who might lack the training and knowledge necessary to avoid the errant sharing of personal data and credentials;
- Tech-savvy students, who-in the absence of mentoring and adult guidance, might attempt to circumvent existing cybersecurity controls and/or be lured into using their legitimate access to school IT systems to disrupt, cheat, or even cause harm to others;
- School suppliers and vendors, whose security practices might not be adequately considered during school district procurement decisions and product/service implementation; and
- Online criminals, some based in the U.S., but many based overseas, who seek to profit from weak school district cybersecurity controls by stealing or extorting money from school districts, their employees, and vendors, or via credit and tax fraud enabled by stealing personally identifiable information from school districts.

[5] See SBCEO.org

School IT personnel regularly encounter and block cyberbullying in district emails, online searches for inappropriate content, and students playing online games. Most of the County's schools have reported repeated phishing attempts inadvertently transferred to school networks from outside vendors every week, many of which have successfully been blocked by filter software.[6]

In early 2020, SolarWinds, a major software company based in Tulsa, Oklahoma, which provided system management tools for network and infrastructure monitoring, was hacked by nation-state criminals who gained access to the networks of thousands of SolarWinds customers throughout the country. The hack compromised the networks and systems of more than 30,000 public and private organizations, including local, state, and federal agencies – one of which was the Lompoc Unified School System.

On July 2, 2021, a ransomware hacker group based in Russia, exploited vulnerability in the Santa Ynez Valley Union High School District's (SYVUHSD) remote access software, called "Kaseya", and initiated an attack that spread to all Kaseya servers, including one used by SYVUHSD. The ransomware attack encrypted 19 school staff's personal computers, three student laptops, and three servers in addition to about one million systems world-wide.[7] The hackers demanded $44,999 per machine to decrypt each machine. The SYVUHSD did not pay the ransom and immediately wiped and restored all its files from the backup software. No data was compromised because of the incident.

---

[6] Phishing schemes often use spoofing techniques to lure you in and get you to take the bait. These scams are designed to trick you into giving information to criminals that they shouldn't have access to. https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing

[7] Encryption converts (information or data) into a cipher or code to prevent the school's access to its network.

However, the impact could have been greater because regular school was not in session, - it was the last day of summer school, with very few teachers and students on campus.

In December 2021, a criminal enterprise hacked a district vendor's email. Using a purchase order found in the email, the hackers ordered computers shipped to Nigeria. Without the intervention of the Department of Homeland Security stopping the shipment, the school district and/or SBCEO were in danger of being billed for those computers.

To test students' compliance, staff sent fake emails to students to identify improper uses of the network. Several students opened links that could have infected the network with viruses and malware.

Although damage from these threats may seem unremarkable at present, efforts must be undertaken to limit the predictable increase in future cyber-attacks. According to the cybersecurity expert and IT staff the Jury interviewed, all internet users must begin instituting sound cybersecurity programs as soon as possible to stem the tide of an imminent threat posed by cybercriminals. To that end, the expert and IT staff recommend that the Districts centralize the training, use MFA, and purchase software and cyber insurance through the SBCEO. By placing the control in the hands of the schools' headquarters, the SBCEO would reap the benefits of lower costs because of bulk purchases and a central authority who could issue mandates for all districts in an equal and fair manner.

Zero Trust Architecture

The National Institute of Standards and Technology (NIST), and the expert the Jury interviewed, have recommended the use of Zero Trust Architecture (Zero).[8] Zero assumes there is no implicit trust granted to:

[8] See, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420 May 17, 2023.

- Assets (devices, infrastructure components, applications, virtual and cloud components);
- User accounts based solely on their physical or network location (i.e., local area networks versus the internet); or
- Based on asset ownership (enterprise or personally owned).

Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. The entire network is not considered an implicit trust zone. All assets should always act as if an attacker is present on the network, and communication should be done in the most secure manner available. This entails actions such as authenticating all connections and encrypting all traffic. Every asset must have its security posture evaluated before a request is granted to an enterprise-owned resource.

Obstacles to Training and Multifactor Authentication

In addition to inadequate IT funding, other problems are standing in the way of achieving the necessary fixes. The Jury learned that most of the County's school IT departments work independently and rarely interact with each other about decision-making. In addition, the Jury learned that some of the Districts want to maintain local control.

Most of the districts have instituted a written agreement between students, parents, and the schools, typically executed at the beginning of the school year. The agreement is distributed in simple, accessible language among parents, students, and school personnel, and outlines the terms of responsible use and consequences for misuse of hardware. Parents are expected to acknowledge that their child(ren) will follow basic guidelines, and students agree to the standards laid out in the policy. Multilingual versions of the agreements are made available. However, either execution of these agreements has not been required or school officials are not enforcing them. The Jury learned that many families cannot, or will not, sign the agreements.

The inconvenience inherent in the use of multi-factor authentication, which some interviewees described as daunting to busy teachers, must be overcome for the good of the school communities' safety from cyber threats.

Costs of Formal Cyber Training and Multi-Factor Authentication are Minimal When Compared to the Potential Consequences

Although the costs of the recommended cyber programs may initially result in necessary cost-cutting elsewhere, the need for IT training and MFA significantly outweigh the harm caused by ransomware, network interference, and emotional distress resulting from hacking, cyberbullying, phishing, and criminal acquisition of personal data.

Cyber training is offered free-of-charge by the Federal and State governments, and other non-profit organizations.

A study performed in 2019 revealed that 84 percent of parents worldwide were worried about their children's online safety, according to a survey commissioned by Kaspersky and conducted by the market research company Savanta.[9]

CONCLUSION

Santa Barbara County schools are at great risk if immediate action is not implemented. Cyber threats are targeting our education system and increased cybersecurity demands add strain to school districts. IT personnel provided extensive information for this report. Cybersecurity programs need resources and prioritization.

[9] See, https://www.kaspersky.com/about/press-releases/2019_parents-are-worried-about-their-childs-online-safety Date last viewed May 17, 2023.

Collaboration Amongst IT Staff, More Robust Threat Reporting, and Written IT Policies

IT personnel need more opportunities to coordinate with other districts' IT staff and to share reported cyber threats, recommended updates to software and hardware, damage done because of hacking, and potential fixes.

Reporting of cyber-attacks must be a part of cybersecurity. Currently, very few schools report such instances to the SBCEO, which results in the lack of transparency needed to foresee and fix problems. The Jury learned that most threat attempts have not been reported because those efforts were blocked by network filters. If asked to provide such reports currently, IT staff would spend additional time searching through their data and compiling information.

Smaller school districts within the County do not have a technology handbook, manual, or policies and procedures regarding the use of hardware and software. A newly hired employee cannot learn proper cyber procedures without accessible guidelines. While poor outcomes from data threats remain manageable in County schools, most cybersecurity professionals, and much of the public, realize that current threat attempts are merely the tip of the iceberg and that such threats, and potential damage to the school population, will significantly increase with time. As many school districts throughout the country have already learned, it is best to tackle the problem before, not after, the damage has been done.

FINDINGS AND RECOMMENDATIONS

Finding 1

Santa Barbara County school districts have not mandated formal cybersecurity training for school administrators, teachers, staff, and students.

Recommendation 1

That the Santa Barbara County Education Office require all school administrators, teachers, staff, and students who use district networks and computers (including laptops, iPads, and any other electronic media) receive formalized cybersecurity training at least once per year.

Finding 2

Santa Barbara County school districts have not required the use of multi-factor authentication.

Recommendation 2

That the Santa Barbara County Education Office require multi-factor authentication for anyone logging onto the districts' networks.

Finding 3

That some Santa Barbara County school districts are not adequately insured for losses arising from cybersecurity incidents, not insured for cybersecurity or lack sufficient coverage limits.

Recommendation 3 a

That the Santa Barbara County Education Office purchase cyber insurance that will provide limits of between $1-2 million for each district.

Recommendation 3b

That the Santa Barbara County Education Office require contribution of funds from all districts.

Finding 4

That the districts fail to report cyber-attacks.

Recommendation 4

That the Santa Barbara County Education Office require districts to report cyber-attacks.

Finding 5

Although some district IT members meet from time to time to discuss recent cyber updates, problems, and problem resolution, attendance is voluntary and many rarely attend.

Recommendation 5a

That the Santa Barbara County Education Office issue a written policy requiring collaboration amongst school district IT staff.

Recommendation 5b

That the Santa Barbara County Education Office issue a written policy requiring IT staff to attend regularly scheduled meetings at least four times per year.

REQUEST FOR RESPONSE

Pursuant to *California Penal Code Section 933 and 933.05*, the Santa Barbara County Grand Jury requests each entity or individual named below to respond to the enumerated findings and recommendations within the specified statutory time limit:

Responses to Findings shall be either:

- Agree
- Disagree wholly
- Disagree partially with an explanation

Responses to Recommendations shall be one of the following:

- Has been implemented, with a summary of implementation actions taken
- Will be implemented, with an implementation schedule
- Requires further analysis, with an analysis completion date of no more than six months after the issuance of the report
- Will not be implemented, with an explanation of why

Santa Barbara County Education Office - 90 days

Findings 1, 2, 3, 4, and 5

Recommendations 1, 2, 3a, 3b, 4, 5a, and 5b

Recipients of Informational Copies – No Response Required

Ballard School District

Blochman Union School District

Buellton Union School District

Carpinteria Unified School District

Cold Spring School District

College School District

Cuyama Joint Unified School District

Goleta Union School District

Guadalupe Union School District

Hope Elementary School District

Lompoc Unified School District

Los Olivos School District

Montecito Union School District

Orcutt Union School District

Santa Barbara Unified School District

Santa Maria-Bonita School District

Santa Maria Joint Union High School District

Santa Ynez Valley Union High School District

Solvang School District

Vista del Mar Union School District