School Safety Newsletter

Volume 5, Issue 12 July 2018

Department of Education Advises that Schools Can Comply with the Clear and Present Danger Reporting Requirements of the Firearm Concealed Carry Act without Violating FERPA

Franczek Radelet Attorneys & Counselors, June 11, 2018

https://www.jdsupra.com/legalnews/department-of-education-advises-that-25616/

The Firearm Concealed Carry Act (CCA) went into effect in 2013. One of its provisions requires a principal or designee to make a report to the Illinois Department of State Police (ISP) "when a student is determined to pose a clear and present danger to himself, herself, or to others." The purpose of the provision is to prevent individuals from obtaining a Firearm Owner's Identification (FOID) Card if they pose a such a danger. When the law was enacted, administrators questioned whether reporting this information to the ISP may conflict with the Family Educational Rights and Privacy Act (FERPA) and the Illinois School Student Records Act (ISSRA). ISP subsequently addressed this issue in its implementing regulations, adopted in December 2013, by appearing to acknowledge that such a report may be made pursuant to the "health and safety" exception under FERPA, stating that "clear and present danger reporting shall be made consistent with [FERPA] to assist the Department with protecting the health and safety of the public by denying persons who present a clear and present danger from having lawful access to weapons." In response to a November 2013 inquiry sent by the Illinois Association of School Boards, the Department of Education recently confirmed that schools can make such reports without violating FERPA.

According to the Department of Education's opinion, one way that a school can make the required report to the ISP and comply with FERPA is if the report is a law enforcement unit record. Law enforcement unit records must be created by a law enforcement unit, created for a law enforcement purpose, and be maintained by the law enforcement unit. Law enforcement unit records are not considered educational records and may be disclosed without consent from parents or eligible students. Accordingly, the principal may designate a member of the law enforcement unit, such as its school resource officer, to create, send, and maintain the report required by the CCA. If the report includes directory information (and the parent has not opted out) and the observations of the law enforcement unit, then the report can qualify as a law enforcement unit record. However, if personally identifiable information from the student's educational records is shared with the law enforcement unit (as school officials) and included in the report, that information would remain subject to FERPA.

If the report is not created by the school's law enforcement unit or includes information from the student's educational records and is therefore subject to FERPA, the Department of Education also affirmed that it can still be provided to the ISP under FERPA's health and safety emergency exception. The emergency exception allows schools to disclose, without prior written consent, educational records and personally identifiable information "in connection with an emergency [to] appropriate persons if the knowledge of such information is necessary to protect the health and safety of the student or other persons." Under this exception, the school must include in the student's educational records an explanation that the report was made to the ISP and the ISP's legitimate interest in the report. Further, under ISSRA, when a student record is disclosed under the emergency exception, the school must notify the parent on the following day of the information released, to whom it was released, and the purpose of the release.

The Department of Education's response provides a detailed analysis of how the requirements of the CAA relate to the requirements and exceptions of FERPA. Schools with questions regarding clear and present danger reporting and student records are encouraged to seek guidance from legal counsel.

Note: The Clear and Present Danger Form is used by law enforcement officials and school administrators to report individuals determined to pose a clear and present danger within 24 hours of the determination to the Illinois State Police Firearms Services Bureau. Instructions can be found at: http://directives.chicagopolice.org/forms/ISP%202-649.pdf

Clear and Present Danger form can be found at: https://www.isp.state.il.us/docs/2-649.pdf

Protecting our future through information sharing

In This Issue

- Department of Education Advises that Schools Can Comply with the Clear and Present Danger Reporting Requirements of the Firearm Concealed Carry Act without Violating FERPA
- Lessons Learned from Averted Acts of School Violence
- Next Monthly Webinar - September TBD, 2018
- Online Only: Is Your School Board Increasing Your District's Cyber Risk?
- Chicago Public School Breach Exposes Private Student Data
- FBI Begins Investigation of Ransomware Attack at Roseburg Public Schools
- How to Get Help For Someone Who Might Be Suicidal

Lessons Learned from Averted Acts of School Violence

Campus Safety, July 2, 2018

https://www.campussafetymagazine.com/safety/averted-school-violence/?utm_source=CS_trends&utm_medium=email&utm_campaign=content&eid=350362379&bid=2163856

Every year across the nation, acts of violence are prevented on school and college campuses by students, parents, teachers, staff, administrators, school resource officers, campus police and security officers. What have we learned from these averted acts of school violence, and how can those lessons help other schools protect our children and their staff?

The Police Foundation — a national non-profit, non-partisan organization dedicated to improving policing through innovation and science — has initiated a project, with funding from the U.S. Department of Justice, Office of Community Oriented Policing Services and the National Institute of Justice, to study "averted acts of school violence."

The project is based on the concept of a "near miss," which has been used to inform the business practices in the aviation, fire and medical professions. The near miss concept holds that for every incident that occurs, there are significantly more averted incidents. These averted incidents contain invaluable information regarding the strengths or potential weaknesses of current policies, procedures, training and methods.

The Police Foundation has built a national database to record incidents of averted and/or completed acts of school violence (ASV). The national database collects and analyzes data regarding averted incidents to identify best, and more importantly, "next" practices to prevent and respond to acts of violence in our schools and on our college campuses.

Definition of Averted School Violence

The Police Foundation defines an averted school violence incident as a violent attack planned with or without the use of a firearm that was prevented either before or after the potential perpetrator arrived on school grounds and before any injury or loss of life occurred. The Police Foundation collects incidents that occurred in the United States after the Columbine tragedy in 1999.

Lessons Learned from 51 Averted Attacks

So far, Police Foundation subject matter experts have reviewed approximately 51 incident reports that have been entered into the averted school violence database. These averted incidents were identified primarily from open source news stories and court documents, however, there has also been an increase in the number of incidents reported by individuals who are aware of averted incidents.

The Police Foundation also develops incident reports on completed acts of school violence and is currently working with subject matter experts to review these reports and provide lessons learned before entry into the database. The Police Foundation has conducted preliminary analysis on the 51 averted school violence incident reports.

To date, the team has identified the following lessons learned:

- Schools and law enforcement must have a strong, pre-established relationship and open lines of communication before an attack occurs.
- Students who hear threats of violence from other students should take them seriously and report them to school or other authorities immediately. Based on our preliminary study, in over half of the open source incidents we studied, students were the first to discover another student's plans for school violence. (See figure to the right)
- Students should be trained not only to recognize threats of violence but also to recognize signs of suicide or depression.
- Parents should monitor their child's social media accounts and remain aware of their general Internet use for any concerning searches or violent material.
- Potential perpetrators of violence frequently make direct threats or openly discuss their violent plans with others. In some instances, they use social media platforms such as Facebook, Instagram, and even Snapchat to share violent plans or thoughts, or to express disdain for a school/situation. (See figure next page)

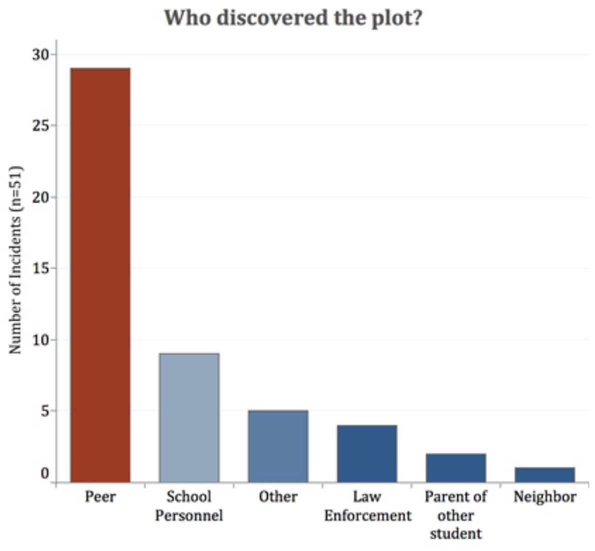


Figure 1: A student peer initially discovered the attack plan in 29 incidents.

Monthly Webinars!

First Wednesday of Every Month

at 10 am

(Except January, July, and August).

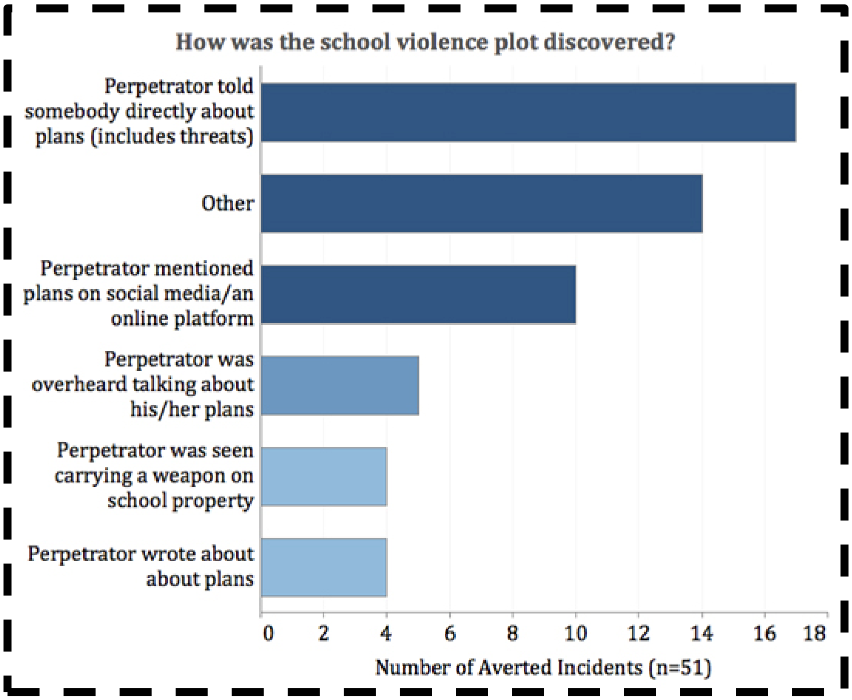
Next Webinars

Wednesday, September TBD, 2018

Each webinar has a round table discussion at the end. Questions are always welcome!

To participate, you must be a vetted member. For more information please email schoolsafety@isp.state.il.us

Lessons Learned from Averted Acts of School Violence (Continued)



- Parents should take their children's threats of violence seriously and seek assistance from law enforcement, mental health professionals and other service providers.

- Parents should keep all guns in a locked and secure location if they are in the home.

- School personnel, school resource officers, campus police and security officers should strive to develop and maintain rapport with students so they are aware of students who are bullied, feel excluded, depressed or challenged in other ways so they can connect them to services.

- Schools must continuously update and practice their emergency communication systems and response plans.

- Schools should have a plan in place for timely communication of incidents to parents.

- Schools, particularly universities and higher education campus, should be aware that financial distress can be a trigger for violence.

- Schools should notify all staff when a student is suspended or expelled. That student should not be allowed back on campus the same day of the suspension or expulsion.

- Schools should direct concerns through a "safety team" for review and to design an appropriate course of action.

- Schools must be vigilant at entrance locations and have sufficient staff to process and observe individuals entering the school.

Online Only: Is Your School Board Increasing Your District's Cyber Risk?

National School Boards Associations, April 2018

https://www.nsba.org/newsroom/american-school-board-journal/asbj-april-2018/online-only-your-school-board-increasing-your

Insights from the 2018 National School Boards Association (NSBA) Cyber Risk Report, School Board Communication at Risk

Today every business and organization faces risks from cyber-attacks. Schools hold a special appeal for hackers as a school database often contains highly sensitive information on students which fetch high prices on the black market as identify theft from children is far less likely to be discovered, sometimes for many years. Unfortunately, school board communications can be used by cyber criminals as a gateway to access the sensitive information held by our schools. To assess the current state of cyber security among America's school districts, in July 2017 the NSBA conducted a nationwide survey; there were 482 respondents with a representative distribution both geographically and among district size.

The findings clearly demonstrate that school boards must take additional steps to protect their board communications from cyber-attack. And, while there are no fool proof methods to stop cybercrime, there are a number of easy to implement practices that can significantly reduce risk. This report summarizes the key findings from the survey, provides observations on the significance of the findings and includes some suggested action steps for school boards to improve communication practices.

Should Cybersecurity be a Concern for School Boards?

The term "cybercrime" might conjure up images of a shadowy group of 'hacktivists' attacking those in power, both to showcase their hacking prowess as well as making a political statement. But cybercrime these days tends to be far more mundane: focusing on easy targets whose cybersecurity defenses are the weakest, and who are the most likely to pay ransom in BitCoin, the value of which has exploded in recent years.

The survey suggests school officials are less prepared for cyberattack than private-sector companies, though both face formidable threats. The NSBA survey parallels a report called "The Price of Convenience," a survey of 381 directors of U.S. companies, completed in early 2017 by NYSE Governance Services and Diligent, which showed private company boards to be similarly underprepared. The threat, however, extends beyond the private sector. According to Dottie Schindlinger, vice president and Governance Technology Evangelist, who collaborated on the "Price of Convenience" report, "At the end of the day, organizations with leaders that don't have at least a good foundational understanding of cybersecurity are the most at risk. An easy way to gage a school's preparedness to handle a cyberattack is to look at their board minutes to see if the topic has come up – if it's never on the board's agenda, it likely indicates cybersecurity isn't a high priority for the school, and they are at greater risk."

Cybercrime is big business, with ransomware alone generating over $5 billion in damages last year, according to CSO Online – the leading magazine covering cybersecurity issues. It's true that many criminals target high-level executives of big companies, such as former US Secretary of State and Salesforce board member, Colin Powell, whose personal email account was hacked and a document containing the company's M&A strategy was leaked to the Wall Street Journal, negatively impacting share price. Yet, many hacking attempts are far more random – according to Symantec's 2017 Internet Security Threat Report, one in every 131 emails is malicious, and masses of ransomware-laden emails are blanketing organizations and individuals with the least cybersecurity prowess. The ransom demand is often a relatively small amount averaging about $1,000 (CSO Online), and smaller organizations are more likely to pay to make the nuisance go away. But paying the ransom only makes the victim more vulnerable to future attacks – partly because once their systems are infected, they are likely to remain so until they are professionally scrubbed or replaced entirely. With cybercrime damages on pace to hit $6 trillion annually by 2021 (CSO Online), clearly this problem isn't going away anytime soon.

What Is Ransomware, Anyway?

According to CSO Online, "Ransomware is a form of malicious software (or malware) that, once it's taken over your computer, threatens you with harm, usually by denying you access to your data. The attacker demands a ransom from the victim, promising — not always truthfully — to restore access to the data upon payment."

Are Schools Really at Risk of Cybercrime?

In October 2017, the US Department of Education warned that cybercriminals were extorting schools for ransom to avoid making stolen student records public. In the foreseeable future, such attacks could cost not only the ransom payers or the victims of identity theft, but also the district's leaders themselves – including school board members. Recent EU legislation (General Data Protection Regulation, or GDPR) holds financially and legally responsible any entity that compromises the privacy of EU citizen data with fines of €20 million, or 4% of annual revenue – whichever is greater. This includes potential direct legal action against directors and officers of these entities. GDPR is considered a high-water mark for data protection legislation, and is actively being considered for replication in the US. Similar rules now exist in a few US jurisdictions, including recent rulings in New York State by the Department of Financial Services (NYDFS) holding financial service directors (and the vendors who provide services to them) liable for cybersecurity breaches. Meanwhile, rules taking effect in other states including Virginia and Georgia now include mandatory breach notification in as little as one week after an event is first discovered. Considering the severity and frequency of the hacks that took place in 2017, additional legislation targeting organizational leadership is expected.

Schools need cyber-protection every bit as much as their for-profit peers. Small budgets and an educational mission offer no protection. Rather, the schools that are the least prepared are the most likely to become prime targets precisely because of the ease of breaching their defenses.

The survey sought to determine school boards' level of preparedness and awareness to handle these challenges. Below, are the key findings along with observations on the significance of the data and suggested action items for school boards' consideration.

In September 2017, NSBA – with sponsorship by BoardDocs – surveyed over 480 public school board members to determine how, in this digital age, boards see to the safeguarding of their communications, all the while ensuring a high level of effectiveness. Below are some of the key findings from the report.

Communication Methods

- 79% of board members report regularly using email as the primary communication method for board business, making it the second most common method of communication behind face-to-face meetings (81%).

- Half of the respondents (50%) reported using board portals regularly, with an additional 11% who say they occasionally do so as well.

Effectiveness

- Since the move to digital, 81% of board members maintain they receive the right mix of summary highlights and accompanying detail from administration.

- 38% of directors acknowledged it is common practice to download board books or company documents onto personal computers and devices, and 20% reported storing these materials onto personal or external drives.

Awareness and Control

- 47% claimed being unaware of any security audit having been conducted on their board's communications practices.

- Two-thirds (62%) of board members reported not being required to undergo cybersecurity training.

- 35% of the board members agreed the move to digital file sharing has increased the risk of improper handling of sensitive information.

To vie the full School Board Communication at Risk by the NSBA report, visit: https://cdn-files.nsba.org/s3fs-public/NSBA_Cyber_Survey.PDF

Chicago Public School Breach Exposes Private Student Data

Chicago Suntimes, June 16, 2018

https://chicago.suntimes.com/news/cps-data-breach-exposes-private-student-data/

Chicago Public Schools (CPS) apologized Friday evening for a mass email accidentally linking to the private data of thousands of students and families.

CPS apologized for the "unacceptable breach of both student information and your trust" and asked recipients of the email to delete the sensitive information, Executive Director Tony Howard wrote in an email to families that received the private data. The data includes children's names, home and cellphone numbers, emails and ID numbers.

Families were sent an email Friday evening from CPS's Office of Access and Enrollment inviting them to submit supplemental applications to selective enrollment schools. Attached at the bottom of the email was a link to a spreadsheet with the private data of over 3,700 students and families.

The link to the private data was active for several hours after CPS noticed and apologized for the breach. The link was eliminated by Saturday morning.

The employee responsible for sending the link was going to be removed from their position, Howard said.

This isn't the first time CPS exposed the private data of students. Students' medical conditions and dates of birth were shared by CPS in a spreadsheet February of last year. In 2016, a CPS employee improperly leaked student names, addresses and current schools to the Noble Network of Charter Schools.

FBI Begins Investigation of Ransomware Attack at Roseburg Public Schools

KCBY Coos Bay Oregon, May 15, 2018

http://kcby.com/news/local/fbi-begins-investigation-of-ransomware-attack-at-roseburg-public-schools

ROSEBURG, Ore. -- The superintendent of Roseburg Public Schools has issued an update regarding the recent ransomware attack on the district's computers. Superintendent Gerry Washburn says the district continues to recover from the attack and is making progress on restoring the systems. The FBI has begun an investigation into the attack, Washburn said in his statement. "The FBI reports that these types of attacks are occurring at increasingly frequent rates, targeting schools, businesses and government entities," Washburn said. "While the FBI discourages payment of sought-after ransoms, entities must make their own decisions based on cost-effectiveness and the level of damage resulting from attacks." He says they hope to have the district website functioning by the end of the week.

I would like to thank all of our Roseburg Public Schools staff, students, and parents for their patience during this difficult time as we continue to recover from the recent ransomware attack on our computer systems.

Below is the full statement from RPS Superintendent Washburn:

We continue to make progress on restoring our systems and hope to bring this to an end soon.

> *Our IT staff hope to have a new platform for email functioning by the end of the week. Initially we will only be able to send and receive new emails. Email history will be available to staff on the computer they normally used to send and receive email. Once the system is up and running, IT staff will have to scan email histories to ensure they can be safely uploaded to the new email platform.*
>
> *We also hope to have our website functioning again by the end of the week.*
>
> *We expect to receive an update from Navigant, the company assisting with data recovery, on Thursday regarding the current status of our servers.*
>
> *The FBI has begun its investigation into the attack and believes that those responsible are most likely located outside of the country. It is believed that the attack occurred through a complex method using remote desktop protocols, rather than through malware attached to a particular email sent to someone within the district.*
>
> *The FBI reports that these types of attacks are occurring at increasingly frequent rates, targeting schools, businesses and government entities. While the FBI discourages payment of sought-after ransoms, entities must make their own decisions based on cost-effectiveness and the level of damage resulting from attacks.*
>
> *At this time, we are not releasing specifics on how this attack is being resolved; however, a full report of the recovery process will be forthcoming.*
>
> *We are grateful for the support we are receiving through the district's insurance company as well as other agencies assisting with the data recovery process.*
>
> *We will be releasing additional updates as progress is made.*

How to Get Help For Someone Who Might Be Suicidal

CNN, July 9, 2018

https://www.cnn.com/2018/06/06/health/iyw-suicide-how-to-help/index.html

The recent deaths of celebrity chef Anthony Bourdain and fashion designer Kate Spade spotlights the importance of recognizing potential warning signs when someone intends to end their life.

The attention is needed, especially now.

When a high-profile person dies by suicide, the "celebrity-suicide effect" can lead to a rise in copycat deaths. In the four months after Robin William's took his own life in 2014, there was a 10% increase -- almost 2,000 additional suicides -- recorded.

There is already a rise in suicide rates in the US, increasing more than 25% since 1999. Suicide was the 10th leading cause of death in 2015, according to the US Centers for Disease Control and Prevention.

Suicide rates are also rising worldwide, with some one million people dying annually from suicide. The World Health Organization estimates a global suicide rate of one death every 40 seconds, which by 2020 they predict will increase to one every 20 seconds.

If you or someone you know might be at risk of suicide, here are ways to help:

Call 1-800-273-8255 to reach the National Suicide Prevention Lifeline. It provides free and confidential support 24 hours a day, seven days a week for people in suicidal crisis or distress. You can learn more about its services here, including its guide on what to do if you see suicidal language on social media. You can also call 1-800-273-8255 to talk to someone about how you can help a person in crisis. For crisis support in Spanish, call 1-888-628-9454.

For the TrevorLifeline, a suicide prevention counseling service for the LGBTQ community, call 1-866-488-7386.

Text HOME to 741741 to have a confidential text conversation with a trained crisis counselor from Crisis Text Line. Counselors are available 24/7. You can learn more about how the texting service works at https://www.crisistextline.org/texting-in/

The American Foundation for Suicide Prevention aims to improve awareness by hosting conferences and community walks for survivors and their families.

For online chat, the National Suicide Prevention Lifeline provides a confidential chat window, with counselors available 24/7 at https://suicidepreventionlifeline.org/chat/

Boys Town also provides counselors for youth-specific online chat at http://www.yourlifeyourvoice.org/Pages/ways-to-get-help.aspx It is available every Monday through Friday between 6 p.m. and midnight in the Central time zone. They also have a 24/7 phone number (1-800-448-3000), text for young adults from 11 am to 1 am CST (Text VOICE to 20121), and email available at the website listed for chat.

If you suspect someone may be suicidal:

1. Do not leave the person alone.
2. Remove any firearms, alcohol, drugs or sharp objects that could be used in a suicide attempt.
3. Call the U.S. National Suicide Prevention Lifeline at 1-800-273-TALK (8255).
4. Take the person to an emergency room or seek help from a medical or mental health professional.

Source: American Foundation for Suicide Prevention. For more tips and warning signs, visit: https://afsp.org/about-suicide/risk-factors-and-warning-signs/

School Safety Newsletter

Statewide Terrorism &
Intelligence Center
2200 S. Dirksen Parkway
Springfield, IL 62703
Phone: 217-558-2661
E-Mail:
Schoolsafety @isp.state.il.us

Mia Ray Langheim

School Intelligence

Officer