School Safety Newsletter

Volume 4, Issue 4 November 2016

Bomb Incidents in Schools: An Analysis of 2015 - 2016 School Year October 2015 - January 2016 Edition

Researched and written by Dr. Amy Klinger and Amanda Klinger, Esq. The Educator's School Safety Network

https://static1.squarespace.com/static/55674542e4b074aad07152ba/t/56d65c5b0442629982c5f79c/1456888923883/Executive+summary+3pg.pdf

Overview and Summary –

This school year, school safety news has been overwhelmingly dominated by reports of bomb threats. At the Educator's School Safety Network, we think it is critical to move beyond mere speculation on this issue to an analysis of actual facts and data. The Educator's School Safety Network (ESSN), a national non-profit school safety organization, has compiled the most current information on bomb incidents in America's schools to determine the scope and severity of the bomb incident problem.

School administrators and law enforcement officials find themselves making critical decisions about bomb threat incidents with few established best practices, outdated protocols, and a complete lack of education-based training. More significantly, many school leaders do not understand the potentially catastrophic effects of a bomb incident or do not have the requisite skills to respond appropriately and effectively.

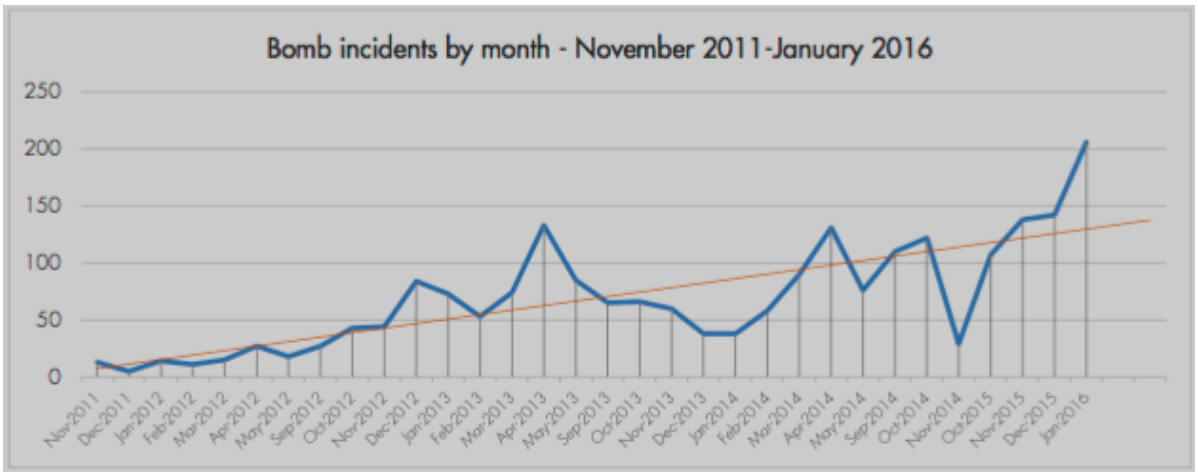
The full report has two important purposes:

1. To provide the educational and law enforcement communities with the most current data and analysis available on the rate, frequency, severity, scope, and nature of bomb incidents in the United States.

2. To provide school and law enforcement responders with an overview and understanding of the critical trends and warning signs that have emerged from our analysis of recent incidents.

Summary of Findings

Is There an Increase in the Number of Bomb Threats?



The most significant result of the report is the dramatic increase in school-based bomb threat incidents specifically during the 2015-2016 academic year. While incidents have been gradually increasing since 2012, so far this school year U.S. schools have experienced 745 bomb threats, an increase of 143% compared to that same time period in 2012-2013.

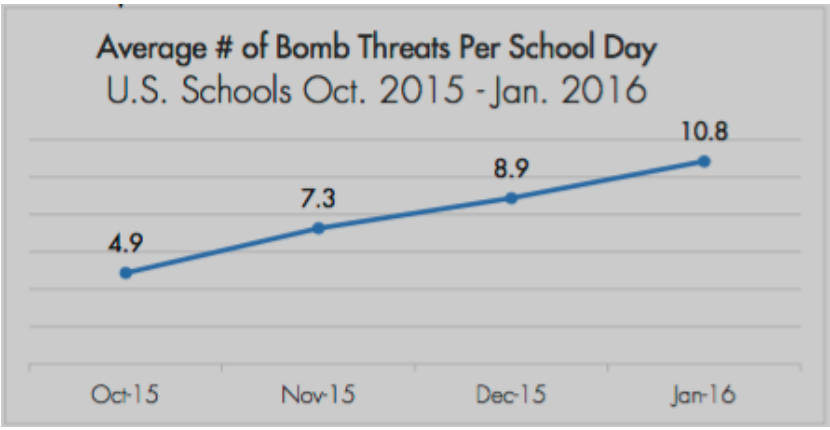
Protecting our future through information sharing

In This Issue

Bomb Incidents in Schools: An Analysis of 2015 - 2016 School Year October 2015 - January 2016 Edition (Continued)

How Many Bomb Threats Have Been Reported?

While there is clearly an increase in threats, rapid growth has occurred in the last four months. January of 2016 saw 206 school- based bomb threats, an average of more than 10 threats per school day- the highest number recorded to date.

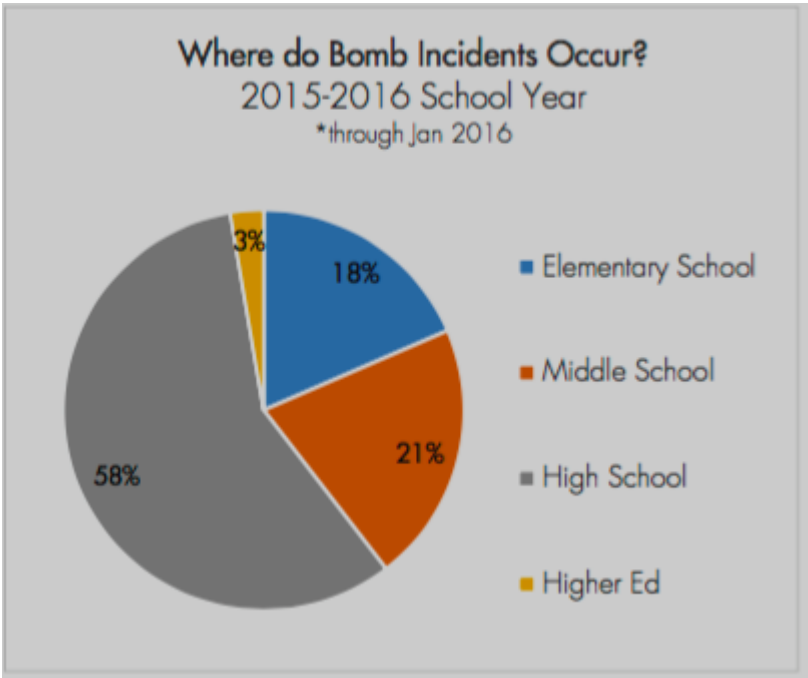


Which States Have the Most Threats?

Since 2011, California and Ohio reported the most bomb threats. Widespread instances of automated calling threats on the east coast in December and January altered this dynamic with Massachusetts, New Jersey, and Maryland now experiencing bomb threats most frequently. During the first half of the 2015-2016 school year, bomb threats occurred in 48 of the 50 states.

Where Do Bomb Threats Occur?

While 58% of this year's bomb threats have occurred in high schools, an almost equal number have taken place in settings with much younger students. These "non- traditional" targets of bomb threats contain extremely vulnerable populations and are often ill-equipped and trained to deal with crisis events.



In a secondary school setting, the perpetrator is often found to be a student who desires a disruption or notoriety. At the elementary level, the perpetrator is most often someone from the outside whose purposes are much more obscured – and potentially much more deadly.

Recommendations

School administrators need to develop the critical skills necessary to prepare, prevent, and respond to bomb incidents. All building and district administrators should:

- Have a functional understanding of explosive devices, sheltering distances, and the disruptive/destructive capabilities of explosive devices
- Have an understanding of the protocols and practices that will be employed by emergency responders
- Be able to appropriately assess the level and validity of threats and identify pre-attack indicators
- Have protocols in place to prevent future bomb threats and diminish copycat incidents

It is critical for educators and emergency responders to be equally involved in training, prevention, and response as it pertains to violence in schools – particularly in terms of bomb-related incidents. Educators must secure a prominent "seat at the table" and be active, equal partners in preventing and responding to bomb threat incidents.

To view the full report, visit: https://static1.squarespace.com/static/55674542e4b074aad07152ba/t/57a401e2ff7c508424d9b0a0/1470366180190/final+15-16+bomb+report+temporary+website.pdf

Monthly Webinars!

First Wednesday of Every Month at 10 am (Except January, July, and August).

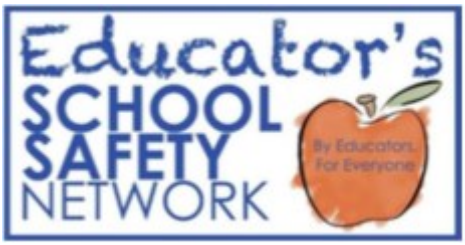
Next Webinar

Wednesday, December 7, 2016

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

Bomb Incidents in Schools: An Analysis of 2015 - 2016 School Year October 2015 - January 2016 Edition (Continued)



For additional information and training opportunities, go to:

www.eSchoolSafety.org

For the complete report, go to: www.eSchoolSafety.org/bir-2016/

Contact: Dr. Amy Klinger, Amy@eSchoolSafety.org

Amanda Klinger, Amanda@eSchoolSafety.org

Five Injured in Stabbing at Mountain View High School, Suspect in Custody

November 15, 2016 by Kurt Hanson, Daily Herald

http://www.heraldextra.com/news/local/central/orem/stabbing-at-mountain-view-high-school-leaves-multiple-victims-wounded/article_4346b7a8-705a-5272-af73-3e7d15736b1c.html

Five students were injured in a stabbing at Mountain View High School in Orem Tuesday morning. Orem police say that one suspect, a 16-year-old boy, was detained by the school resource officer and is now in custody. Five students were stabbed in the locker room at the high school just before 8 a.m. on November 15, 2016 as they were getting ready for a first-period PE class, according to Orem Police Chief Gary Giles.

The school resource officer was at the school at the time of the incident, preparing to teach a law enforcement class and as he arrived at the scene, staff members had cornered the suspect, a student at the school. "Staff had boxed the suspect into a bathroom area of the locker room," Giles said. "The suspect still had a knife at that point, so staff members did place themselves in harm's way to keep him from going after other students." At that point, the school resource officer used a Taser on the suspect and was able to get the knife from him to take him into custody.

According the Orem Police Department, all five victims were male, and received at least one stab wound to the neck or torso area. The suspect then stabbed himself with the three-inch knife. Conditions of the victims range from fair to critical. "All the other students are safe, we just have five student victims right now," Martinez said. According to a post from Orem City, none of the injuries appear to be life-threatening. Two of the victims were treated at Timpanogos Regional Hospital and were released Tuesday morning. "Had it not been for the quick reaction of the high school staff, school resource officer and the fire department, the situation certainly could have been much worse," Giles said. All area hospitals were notified and were asked to prepare to take victims.

The suspect was only described as being a white male and a new sophomore student at Mountain View High School. He was home-schooled previously. David Stephenson, administrator of public relations for Alpine School District, said the school was on lockdown earlier in the morning, but the lockdown was lifted mid-morning. School resumed for the day as normal as possible for students who wish to stay, and counselors are available at the school.

"[A] question that has come up recently is why did we keep the school in session," said Kimberly Bird, spokeswoman for Alpine School District. "Our answer in doing such is that the scene was secured by the police department so quickly. School is a safe place for students to be and that we have resources there for kids to use and utilize. Sometimes, when we push kids home, we don't know what's there and available for them." Stephenson said parents can come check out their children who want to leave for the day. Parents can pick up their kids in the parking lot between the auditorium and the seminary building, and Stephenson said parents should check their students out using a sign out sheet at the north end of the school by the auditorium. Bird said a majority of students were checked out of school.

Before seeing their students, parents were alarmed, not knowing if their child was involved. "We didn't know who it was or what was going on. I was definitely scared my son was involved because all we heard was there were stabbings around the school,"said Chantelle Lawrence, mother of a Mountain View High School student, Te Lawrence. "I'm relieved now; this is the first time I've seen his face all morning."

Students and teachers both on lockdown shared the anxiety as they had no idea what was happening in their school as they were on lockdown. "It was scary hearing that we were on a lockdown. It was like, oh, this is actually happening," Te Lawrence said. The Lawrences are just a few of the hundreds of students and parents who left the school this morning. Teacher Dani Macias said that her class was alerted that the school was on a lockdown by the school's vice principal. "Because I didn't know if this was a lockdown that involved a terrorist attack, I instructed students to grab something near them that they could use as a weapon," Macias said in a Facebook post. "They spread out around the room ready to distract and attack as we had been trained to do so earlier this year."

She said many of her students contacted parents via phone from her classroom. "One of my students suggested that we pray for the victims, and my sweet class, although from different religious affiliations, respectfully joined in a prayer for their peers," Macias said. "It was truly a tender moment. We are still on lockdown, but we are okay."

Mia Ray Langheim
School Intelligence Officer

Simple Cyber Security Steps Your Organization Should Implement Now

November 10, 2016, by Robin Hattersley Gray, CampusSafety

http://www.campussafetymagazine.com/article/simple_cyber_security_steps_your_organization_should_implement_now?utm_source=newsletter&utm_medium=email&utm_campaign=editorial&eid=350362379&bid=1584871#

For years now, *Campus Safety* has been warning our readers about the dangers of hacking, malware, ransomware and other cyber threats, and last month we were once again reminded of the vulnerabilities associated with devices connected to the internet.

On Oct. 21 there was a massive distributed denial of service (DDoS) attack that caused internet outages across America. Malware known as "Mirai" enslaved Internet of Things (IoT) devices — including about 10 percent of our nation's IP-enabled cameras, digital video recorders (DVRs), home networking gear and other connected devices — to form a massive connected network. The devices were then used to bombard websites with requests, overloading the sites and effectively taking them offline. Amazon, Spotify and Twitter were among the sites affected by the attack.

It turns out that the Mirai botnet malware that caused the attack used default admin passwords to exploit Telnet vulnerabilities. Video surveillance equipment as well as other devices that connect to the internet usually come with factory-installed default passwords, and according to Hikvision Sales Engineer Joe Coe, this presents significant vulnerabilities.

"Often people don't understand that when they put in '12345' or 'password' as a password, middle school children could figure those passwords out without any social engineering," he says.

Coe recommends that campus end users immediately change any default passwords that come pre-installed on devices that connect to the internet, including their security cameras. He also recommends that the passwords they create be strong and long.

"It's much easier to reset a password than reconstruct your security environment or have someone do forensics once someone has access to your environment," he warns. "[Setting strong, long passwords] isn't convenient, but once users get used to it, it becomes second nature."

Some device manufacturers, such as Hikvision, have avoided the default password and Telnet issues altogether by no longer delivering products that have Telnet access by default or have default passwords. Instead, a user-defined passcode must be created during device initialization. As a result, products from these manufacturers were not affected by the Oct. 21 DDoS attack.

Although some manufacturers are taking big steps to improve the cyber security profile of their products, end users can help to address this issue as well. Coe recommends campuses take the following steps with their security integrators to make their internet-connected security devices more cyber secure:

- Limit Authorization and Access to Appliances: "Only provide people with authorization for the things they need to do," he says. "For example, Bob the receptionist may need to look at live and recorded video, but he doesn't need to ensure the hard drives get formatted correctly."
- Have the Ability to Audit Activity: "If your appliances don't have the ability to provide a log entry for everything that takes place on that appliance, you are doing yourself a disservice. If you need to go back and do forensics, whether it's for a cyber security incident or it's just to fix something that's broken, having those log files can be very helpful."
- Regularly Update Your Firmware and Software: Outdated firmware makes cameras and other devices more vulnerable to hacking.
- Segment Your Network: Be certain security appliances are on a separate server. According to Dale Tesch, who is director of advanced security operations for NTT Security, "Many breaches originate in one segment of the network, where attackers find entry easiest, and then propagate to other unrelated segments of the network as the attack progresses."

Of course, no one can be completely certain that their internet-connected devices are 100 percent secure. Hacker methods and technologies continue to evolve.

"As soon as you plug in any device into the internet, regardless of what it is, it immediately becomes potentially vulnerable," Coe warns. That's why he believes it's so important for campuses to work with integrators and manufacturers who take cyber security seriously.

"Only work with vendors that have a passion for cyber security so that when you identify something that you believe is a potential risk, you can work with those folks to get it resolved quickly," he says. "If they find something that no one else has, they are actually working toward the betterment of everyone."

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