

Best's Insurance Law Podcast

[How to Assess Security and Safety in Schools K-12: The Product War Continues - Episode #229](#)

Posted: Tues., July 8, 2025



Hosted by: John Czuba, Managing Editor

Guest Expert: Joe Hendry from [Cosecure Enterprise Risk Solution](#).

Qualified Member in *Best's Insurance Professional Resources* since: 2025



John Czuba: Welcome to Best's Insurance Law Podcast, the broadcast about timely and important legal issues affecting the insurance industry. I'm John Czuba, manager of *Best's Insurance Professional Resources*.

We're very pleased to have with us today Joe Hendry from qualified member expert service provider, Cosecure Enterprise Risk Solutions. Joe is an expert in civilian law enforcement responses to active threats, designated by the Ohio Department of Homeland Security and the Ohio Attorney General's Office. He served six years in the US Marine Corps and spent 27 years with the Kent State Police Department.

Joe serves as an expert service provider in risk assessment, expert witness, and safety analysis for the insurance industry. He is board certified as a physical security professional by ASIS International and he also serves as the education co-chair for the International School Safety and Security Community.

Joe is among 50 international specialists working on the International School Safety Standard under ASIS International. He also serves on NFPA 3000 as a special expert. His company, Cosecure, was selected to provide subject matter expertise to the federal Cybersecurity and Infrastructure Agency's Schools Safety Task Force, and Joe Hendry is currently serving as an SME in this role.

Joe, we're very pleased to have you with us today.

Joe Hendry: Very happy to be here, John.

John: Today's discussion is how to assess security and safety in schools, kindergarten through 12. Joe, for our first question, why did school security market grow out of fear and not out of reality?

Joe: For many years, and I'll go back 40 years ago to when I graduated from high school, there wasn't any type of school security products in the field. Only training we ever did in schools was for fire, weather-related incidents like tornadoes or storms, but we weren't concerned about things like gunfire in schools, very little focus on things with mental health and any prevention type of steps.

Then Columbine changed all of that. There was an outgrowth beginning there with some of the security products and things we were seeing. Some training started to happen, recommendations for things like lockdown, things like multi-option response for active shooter. That accelerated a little bit.

Law enforcement changed their response several times between Columbine and Sandy Hook in that 13-year period from SWAT tactics at Columbine to small unit tactics after Virginia Tech. Then after Sandy Hook happened, there was this response to move to solo engagement almost exclusively now.

We can see a couple of agencies and incidents that happened over the years where the tactical response from law enforcement failed at places like Virginia Tech and Sandy Hook which created fear, and that fear became an outgrowth in the products that we started seeing in the field, everything from secondary locking devices on doors.

The very first thing that happened that was an outgrowth of not the reality of a situation was, immediate aftermath of Sandy Hook, there was a lot of information that happened that supposedly the gunman had breached the front door and we started seeing all these secure vestibules being installed in schools, almost to the exclusion of every other door that was in the facility.

Things like visitor management systems came out of the outgrowth of that, but there was very little done and very little information shared when they found out that the gunman didn't come through a door. That he had actually come through a window next to the front door.

I, back then, coined a phrase a little bit, and called it mullet security, where everything security-wise, it was business in the front, but in the back of the buildings, there was almost nothing. That complete focus was not based on the reality of the situation or what had happened or even the fact that the gunman had gotten into the building and what was happening inside the building.

Sandy Hook really wasn't the best response. They were using lockdown. There wasn't a lot of emphasis or study about that response and contact, and it started focusing on the physical end of things, with not recognizing the reality of the people being involved in the incident and what they could have done or changed to save their lives.

We had done that in fire response for decades, but for active shooter, we didn't use that response. We totally became almost product-focused on everything, John.

John: Joe, why is the overemphasis on lockdown wrong, and why did this occur?

Joe: When incidents started happening where gunfire started happening in schools and on school grounds, there was no response, and we're talking this is back to the early 1990s. The response there was for gunfire on campus had been developed in Southern California.

This National School Safety Center at the time was in California. They gathered law enforcement professionals and some school people that had plans to respond to gunfire on campus or in the surrounding areas, but most of that was based completely on drive-by shootings.

All of the tactics we see in traditional lockdown, the locking of doors, the turning off of lights, the hiding below window levels, things like that on the ground, gathering people in corners away from doors, pulling drapes, all of those tactics are based on drive-by shooting drills from Southern California.

There's an article back in "Ed Week" in 1993 where you can go back and see where this started becoming the standard for a response. It became the recommendation nationally after Columbine without recognizing that Columbine, number one, was a failed bombing attempt, that the suspects weren't outside of the building, they were on the school grounds.

Southern California has very different school grounds than where they developed these tactics for drive-by shootings, fencing around the property, motel-style schools. That wasn't what was happening at Columbine, and it failed to address the threat that was actually in contact with people, especially in the area of the library.

Interestingly, the population of Columbine students, when given the opportunity and having to make their own decisions, actually evacuated the school and didn't stay inside it. It became another incident where I said this happened at Sandy Hook, where there was no plan for contact with the threat.

The students in the library, even though there was an exit there, continued to follow a lockdown plan. Even though the suspects at one point were shooting them under tables, they continued to remain stationary, and it showed at the point that there was a problem with lockdown.

It wasn't until 2008 when the federal documents started coming out in 2009 and a release from the International Association of Chiefs of Police where actually contact with threats in education started becoming a topic, and the fact that we needed to potentially evacuate the scene.

Students in some schools aren't in classrooms 40 to 60 percent of the day, so having a tactic that's only applicable in one spot, and that may not even be applicable there if you're in contact, has actually increased casualties in many incidents.

We've seen two incidents now, St. Louis and the most recent incident in Austria, that the suspects are beginning to learn that they can shoot doors open by shooting the locks, and they've entered rooms now and killed people in both of those incidents.

In the past, there was a lot of hanging your hat on that lockdown and a locked door was the best way to handle things, and that's starting to prove not to be the case as the suspects learn more about these incidents, John.

John: Joe, why is spending money on products over conducting a risk assessment wasting money?

Joe: One of the important things to understand, and almost any document you look at, whether it's from NFPA or ASIS International or other security organizations, documents from the federal government when you're preparing for events, things in the federal school safety warehouse and those documents from CISA.

Every document almost spells out immediately that the first thing you're supposed to do is conduct a risk assessment.

A risk assessment is something that sets all of your priorities, whether it is deciding whether you need additional training, maybe you do need a product, or maybe you need integration of the current systems you already have and you don't need to purchase anything except having some type of integration.

A lot of what happens is people immediately go out and make purchases without conducting risk assessments. I've had incidents in the past where clients designed a building without conducting a risk assessment, so their infrastructure doesn't match what their even their emergency operation plans are.

One of the things I'm starting to see in education is a return to the 1970s-style buildings with open floor plans. Those are very dangerous considering the school climate we have right now, and the incident response plans we have with a lot of schools that want to try to lock down. It was at a school in Illinois that had done a complete rehab on a school that was built in the 1980s.

They're a complete lockdown school and all of their infrastructure was based on having large basically glass garage doors to their classrooms that they leave open to have this shared space inside the education system where students if they hear a lesson in another classroom and they want to go over there and see what's going on.

In an educational process, that may be a good thing or bad, but in a security process, it is only bad because there's no capability for those people to stay inside that building if something happens.

With all of the glass that's inside, they're all visible to any type of suspect that's inside the building. Their emergency operation plan didn't change. They were still planning on locking down and turning the lights out.

Having a conversation with them after they had spent millions of dollars without conducting the risk assessment and doing the risk assessment basically four or five years later after they had done this, they wanted us to come in there and solve the problem.

The only way to solve that problem is install walls and completely rehabilitate the building to match the infrastructure to their emergency operation plan because the only thing they could actually train was evacuation and do some training for contact if a threat entered that building.

It makes a huge difference. It saves you time, it saves you money, and it saves you aggravation when you conduct a risk assessment, but especially on the money end because it sets what your priority is. If you're not matching your emergency operation plans with your infrastructure and your training, you're going to have a big problem.

John: Joe, why are security product purchases making us more vulnerable to threats?

Joe: Part of this is the purchasing of products in the immediate aftermath of events. Perfect example of this is, we'll have clients that there'll be a shooting somewhere or a threat of a shooting or they may experience a threat on their campus.

Some people actually run out and they immediately make a purchase to make it look like they're doing something, a school board or superintendent, something based on a recommendation from a law enforcement officer, from something they saw at a conference.

I see purchases that are gunshot detection systems, schools putting shatter-resistant film that they actually think is bulletproof on their windows and we'll talk about that, secondary locking devices. These are all things that they may not need. We see the purchasing patterns in education going up and down based on incidents.

The important thing is to understand that gunfire on a campus, and we're not even talking about active shooter events, which are extremely rare, but even gunfire on campus is an extremely rare occurrence.

Making purchases based on feelings rather than what the actual risk is presented to a school is very expensive and you end up with products that you can't service, companies go out of business all the time in this field, and the realization that the amount of incidents that occur is extremely small.

Education Week, which is one of the primary information sources in K-12 as far as educational products and security, they keep a firearm-related school shooting database. The entire year that we have right now for full statistics for is 2024. They only tracked 39 incidents in the entire United States where there was a firearm-related injury or death somewhere in a school.

Now, 39 sounds like a lot, but in reality, it is only like .00034 percent of schools in the United States experience an incident. We're spending a lot of money on products that we may not necessarily need, but many times we ignore products that we do need, things like behavioral threat assessment systems, training in behavioral threat assessment.

Training based on, even the threat of a gunfire incident, what training are we giving people besides using lockdown? The three locations where most gunfire actually occurs in schools are during dismissal in the parking lane, during arrival in the parking lane, and in school cafeterias.

Those are all areas where things like lockdown don't apply, but yet, we don't train people in those areas. The focus on having a product purchase to make it look like we're doing something doesn't match the reality of what's actually happening on the ground, John.

John: Joe, why are schools' inability to support products increasing their liability?

Joe: This is what happens with a lot of these purchases. The amount of cameras and alarms, school vestibule systems, emergency applications for communications, all of those system purchases aren't necessarily bad. You may need something, but one of the problems is schools aren't setting aside monies to support things, and we'll go basic here with a camera system.

Right now, camera systems replacement, because of technology increases in servicing by camera companies of cameras and technology improvements, cameras need to be replaced every five to six years. Schools are not setting aside money, number one, to do that, and they're making a lot of purchases without purchasing the service agreements for the cameras.

Who's cleaning them? Who's servicing them? What is the time between notification that a camera's down and that it's being repaired? I was just in a school district in Massachusetts. They've had cameras down. We're not even talking weeks. We've had some cameras that are down for months. Having security cameras down for a period of months is unacceptable.

If the maintenance or IT can't fix the camera, there's no agreement with the contract service with the camera provider or the installer to come in and fix those cameras, even clean them. I've seen cameras on the outside of buildings that are completely covered with bird excrement that haven't been serviced in probably years.

The important thing is we have to look at service agreements to service these things. If there's an assault, a sex assault, sexual assault, a fight, bullying, all of these things, that's the reason why the cameras are there.

If those cameras aren't accessible and aren't recording and they're inoperable, schools increase their liability because they're not able to prove anything that happened during the incident and they're not able to prove that they've been handling it correctly.

In fact, when systems are down for long periods of time, whether their communication systems go down, everything goes down that has some type of electronic component, when those systems are down for an extended period of time, it actually makes the school increase their liability because it makes them look like they're incompetent in front of a jury.

When they're in front of a jury looking incompetent, that makes it very easy for defense attorneys to argue the fact that not only are they incompetent in this area, but they're incompetent with how they're handling everything else. It creates a very high liability situation for them, John.

John: Joe, who should be making decisions on what schools should purchase? Should it be the vendors, IT, school administrators, law enforcement, or security professionals?

Joe: This is a very interesting field because you'll see a lot of legislatures, especially at the state level, talking about working with your local police in order to make purchases and decisions and conduct risk assessments and all of that.

I can tell you, from a law enforcement perspective, and I was a law enforcement officer for 27 years, when I moved from law enforcement into the security profession, I had had already some bleed-over working as a contractor. I thought I knew a lot about the security functions of K-12, and I worked at a university, and I thought I knew the security functions there.

What I didn't understand is how all of those systems worked together, and how decisions were made. One of the interesting things at the university I worked at, we had two different key systems, one for academic buildings and one for residence halls. I, at the time, thought that was OK. I didn't understand why we had two keys, but the key systems worked, and it was fine.

When I got into the private sector, the realization of how expensive that decision was to go with two different key systems, which meant two different vendors, two different sets of locks having to be installed, two different sets of locks having to be serviced, I didn't understand that piece at all.

I didn't understand how cameras, alarms, communication systems, all of those systems had to be integrated, how repeaters got set up. That was one of the big things. Law enforcement officers come on into buildings and our radios don't work, but how do you fix that? How do you get your communication systems to be able to communicate inside with people?

I didn't understand that, yeah, the phones go down, but that also means our phones went down, so if our radios didn't work inside a building and our phones didn't work inside a building, we had major communication issues that could end up causing casualties in an incident that we could be saving or at least know about where we're going to go, where a suspect is, all of those things.

Those are all purchase decisions that we don't practice making. I wasn't trained as a law enforcement officer to make those decisions and I can tell you from dealing with hundreds of schools and districts that IT departments in schools, school administrators, they don't understand those processes either.

There's some good vendors out in the field, but the integration of products and vendors are trying to sell things and get their product in the field knowing what's good and what's not good, what's appropriate for a university system that may not be appropriate for an education system that may not be appropriate for a healthcare system, what is the best system?

Who are the companies that work in those fields have their products set for those fields so that they work the best in those facilities? Sometimes you have a company that's really good at a university and they're trying to break into other fields. Those products may not be totally appropriate for the field they're walking into.

There's a lot of guns, gates, and guards-type thought process where integration of security products doesn't happen, or vendors' products don't work with other products. That takes a security professional looking at those.

A security professional, by doing the risk assessment in the beginning and deciding what you need, can set up how you conduct your RFPs, what you're asking for in your RFPs, how all the systems have to integrate, and security professionals know which systems integrate better with other products.

I work for a company and we're part of a law firm. We are vendor-agnostic, but I know what vendors are out in the field, what vendors are good to work within K-12, and which vendors aren't good to work within K-12 because that's not what the vendors built around. What people are good to work with, how system integration and products go.

That's not something a local law enforcement officer is going to know, and we need to front-load what our thought process is going to be rather than thinking about immediately spending money on things. That's pretty much how things work, John, the best.

John: Joe, one final question today. Why is free in the school safety marketplace a huge red flag for liability?

Joe: I always remember my grandfather saying when I was growing up, he was an electrician. I remember him telling me as a kid that if you got something for free, it's usually worth exactly what you paid for it, and that stands true, especially in K-12 education with security products.

One of the things I've seen, and I've seen this for years now, a company will come out and they'll say they'll give them a free security assessment. It sounds really good, but one of the problems with a free security assessment is if it's given to you by a company, I can almost guarantee you the company is going to recommend a product that matches what they sell in their assessment.

A lot of times, these assessments, all they are is checkboxes. People can download them right off the Internet from different states. There's some federal checkboxes. Those checkboxes give you a general idea of what you need but there's no specificity to them.

There's a saying in our field in K-12, if you've seen one school, you've seen one school. Every school is different. Every product doesn't fit in every school. Every product doesn't need every product in the field.

If you have an inner city school, they may need protective film on their windows because they experience break-ins or because of what's going on in the neighborhood, but we'll see people trying to sell schools ballistic film which doesn't even exist, and they'll try to use gunshot.

There was a huge article in the "Wall Street Journal" about this a few months ago where people are gaming the system on what they're showing schools and telling them they're selling bullet-resistant or bulletproof film for windows and it doesn't exist, but they'll do free assessment for you.

People in school education, superintendents, school boards, administrators, IT in schools, even law enforcement, they don't have the background to know what's happening in the field. 3M, who's the largest maker of film, makes shatter-resistant film which might be great for a school if they have problems, or even in schools that have housed students that have mental health problems.

You don't want them cutting themselves on glass in quiet rooms and things like that, but you don't need to purchase a ton of this in order to remain safe. These free assessments that are recommending cameras or alarms or film, those are products that schools may not even need, and then when they do spend their money, it doesn't benefit them to anything.

Now they have this product, and like I said earlier, you're talking well less than one percent chance of gunfire happening at any one school in the United States.

When you have over 115,000 schools in the United States and there's only been 34 incidents for the entire year of 2024, but the amount of products sold to those schools is way out of whack with what the actual incident risk is, that's money that can be better spent elsewhere.

When you see things like behavioral threat assessments fail or schools getting sued for bullying and not addressing it, those are the real issues that we're experiencing in education. It is not massive incidents of gunfire. It is how do we stop the small problems before they become huge problems? That's, John, where people need to start thinking.

Like I said, any time something's free, it probably needs to be looked at again before you make a decision to buy or have somebody come into your buildings.

John: Joe, thanks so much for joining us today.

Joe: Thank you, John. I appreciated being here.

John: You just listened to Joe Hendry from qualified member expert service provider, [Cosecure Enterprise Risk Solutions](#), and special thanks to today's producer, Frank Vowinkel. Thank you all for joining us for Best's Insurance Law podcast.

Thank you all for joining us for "Best's Insurance Law Podcast." To subscribe to this audio program, go to our web page, www.ambest.com/professionalresources. If you have any suggestions for a future topic regarding an insurance law case or issue, please email us at lawpodcast@ambest.com.

I'm John Czuba, and now this message.

Transcription by CastingWords

To find out more about becoming a Qualified Member in *Best's Insurance Professional Resources*, contact professionalresources@ambest.com or visit our [Learn More](#) page to start the application process.

Copyright © 2025 A.M. Best Company, Inc. and/or its affiliates. All rights reserved. No portion of the content may be reproduced, distributed, or stored in a database or retrieval system, or transmitted, or uploaded into any external applications, algorithms, bots or websites, including those using artificial intelligence or machine learning technologies such as large language models (LLM), generative AI (Gen-AI) or retrieval-augmented generation (RAG) in any form or by any means without the prior written permission of AM Best. AM Best does not warrant the accuracy, completeness, or timeliness of the AM Best content. While the content was obtained from sources believed to be reliable, its accuracy is not guaranteed. You specifically acknowledge that neither AM Best nor the content gives any investment, financial, tax, insurance, or legal advice. You are solely responsible for seeking competent professional advice before making any investment, financial, tax or insurance decision. For additional details, refer to our Terms of Use available at the AM Best website: <https://web.ambest.com/about/terms-of-use>.