From: Brian Katz <brian@saferschoolsolutions.com>
Subject: Follow-up From 11/23/21 Discussion - Poudre School District
To: Kingsley, Brian <bkingsley@psdschools.org>
Cc: Phillip Dunn <phillip@saferschoolsolutions.com>; Bob Robertruncie.Com <bob@robertruncie.com>; Montoya, Dave - SSC <davem@psdschools.org>; Hooten, Lauren - SSC <lhooten@psdschools.org>; Nielsen, Scott - SSC <snielsen@psdschools.org>
Sent: November 29, 2021 3:25 PM (UTC+00:00)
Attached: S3 Data Flow.pdf, Case Study September 2021-1.pdf

Superintendent Kingsley & Team,

Thank you again for taking the time to meet with us last Tuesday to discuss the opportunity for your district to participate in this Chiefs for Change cohort grant opportunity to help make K12 districts safer. Even on the eve of a long weekend I think the discussion was productive, which shows your district's focus on safety and security.

Attached to this email is the referenced case study "A Tale of 3 Attacks: A public school district's resilience in an age of bad actors and a global pandemic" for your team's review and information. It is the response to those events which has informed the development of this product. We have also attached a Safer School Solutions (S3) Data Flow infographic to help articulate how our product fits into the physical and cyber safety and security ecosystem.

Implementation Models

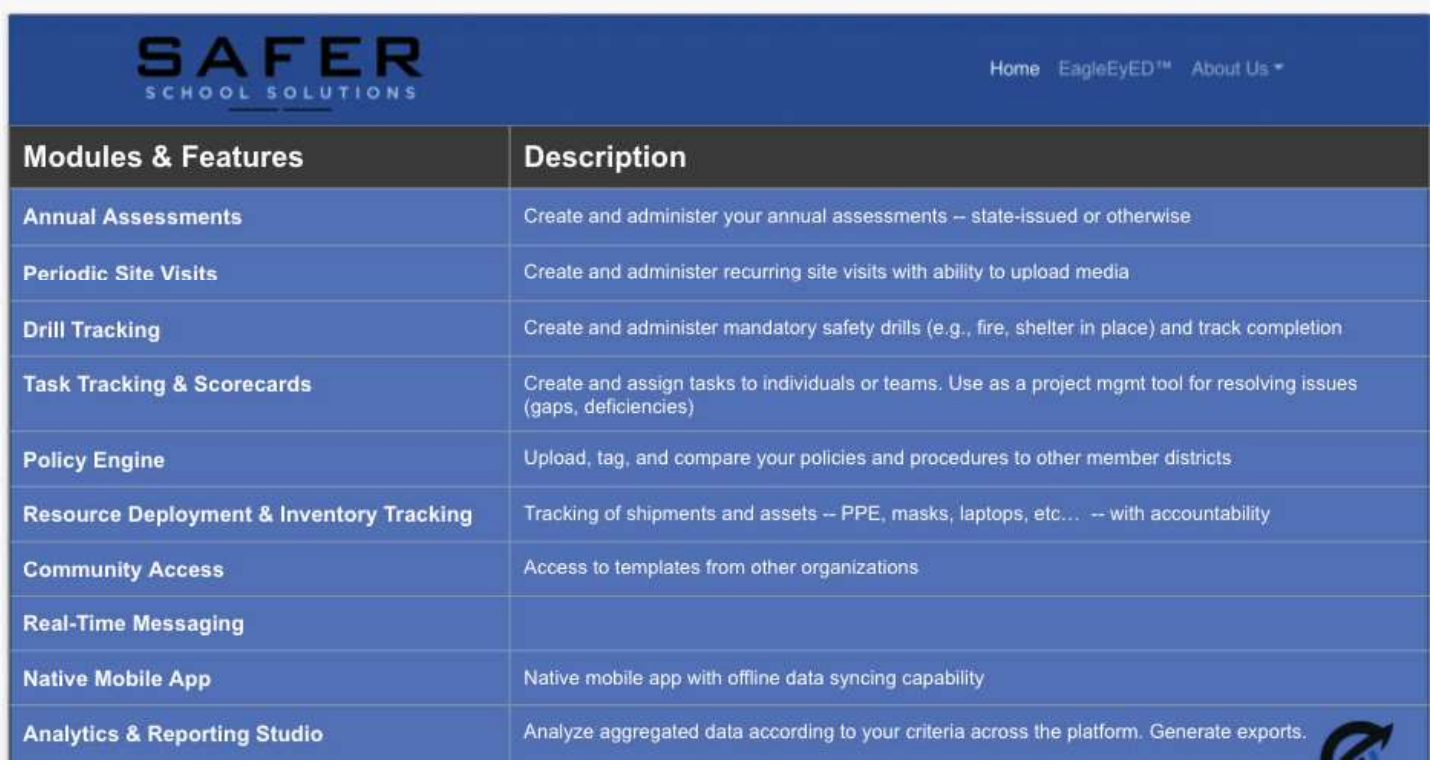
As far as your district's usage (userbase) you can start with as many or as few stakeholders and then expand as you see appropriate. We recommend that you begin implementation with your senior staff and principals. For some districts, their goal is to utilize EagleEyED™ with school-based administrators, district safety/security, and IT staff to track district-level visits and share feedback with their schools. Most districts we have talked to intend to deploy EagleEyED™ for district staff assessments, drill tracking, resource deployment and task/deficiency tracking. For other districts, they are thinking of implementing it for all of their safety and security staff so that they can have school-based sites "self-evaluating" their status, and then the district staff validating those findings during their periodic visits. They want facilities department staff as users to help track progress of issue resolution and they want to start to flow all relevant data including policies and procedures through this new system.

We can customize to your needs throughout the implementation phase.

As we discussed, we want to fit your current workflows now and then if you want to modify those flows or interactions over time we can help you with the change management process to increase your success.

Chiefs For Change Funding

As far as the cohort expectations, Chiefs for Change will be funding the implementation fees, which are typically $3000 per school, so that the district's responsibility will only be the software licensing fee at $1000 per school/per year for the full suite of modules and features including:



Timeline

Once we have contract commitments from the cohort districts, we will kick off the implementation phase which we expect to begin after the new year. This will involve collaboration between Safer School Solutions and the cohort districts to review each district's policies and procedures in the physical and cyber security space so that we can provide initial drafts of helpful assessments you can utilize (typically a 90-day process). The district counterparts will be able to share their templates (in addition to the initial ones we provide), questions and best practices to learn from each other and to work toward potential common understandings.

We will also work with you on your user permissions and hierarchy, site data and other elements throughout the implementation to ensure you're able to drill down into data you collect and provision as many or as little of your staff to be successful (just district staff, include principals, include other relevant departments for tracking follow-ups, etc.).

While timing will depend on the start of the initial cohort and finalization of contracts and funding, we anticipate having your instance of the software up and running, implemented for your district (and relevant staff trained), during your 4th academic quarter. As discussed, we can also take your current safety assessment data and help you aggregate and analyze that data to help inform your future assessments and priorities and help track future follow-ups.

As a deliverable for this project and Chiefs for Change, we will work with this cohort of districts to publish artifacts and report(s) to share insights, strategies, and best practices as a national model for managing enterprise school safety and cybersecurity risks.

For cohort members, we will lock in your licensing price at the current rate for this 3 year contract period and for the next contract renewal period. Any additional modules we develop will be included in this license in addition to training on those new items for as long as you maintain your licenses.

If you have any questions please feel free to contact me. We plan to work with Chiefs for Change to identify the eligible districts (from the interested districts) over the next week, so please let us know as soon as possible if you are committed to participating and wish to be considered.

Thank you,

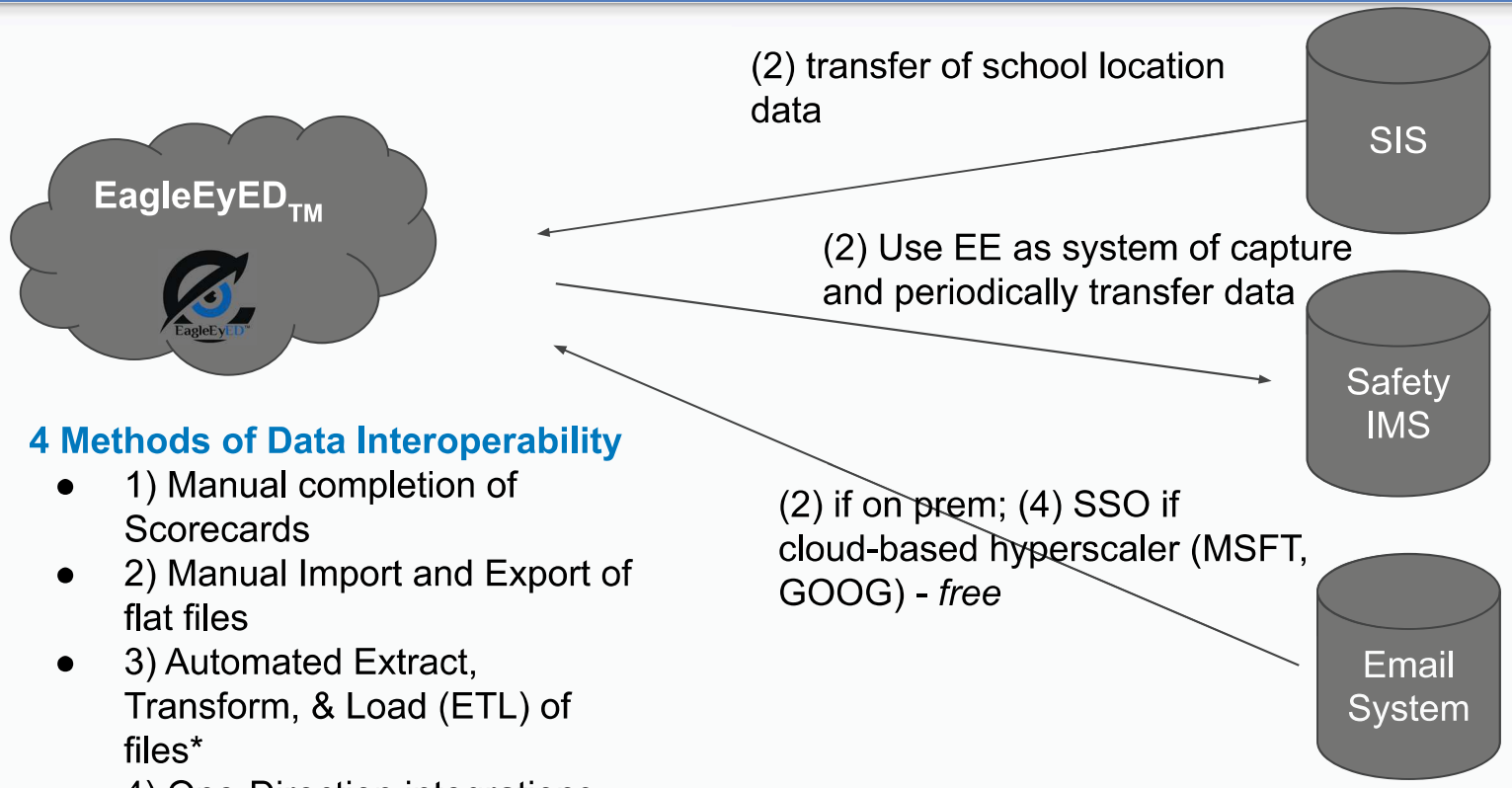
Brian Katz

--
Brian Katz
CEO, Safer School Solutions, LLC

EagleEyED$_{TM}$ Data Flow

November 2021

EagleEyED Data Schematic

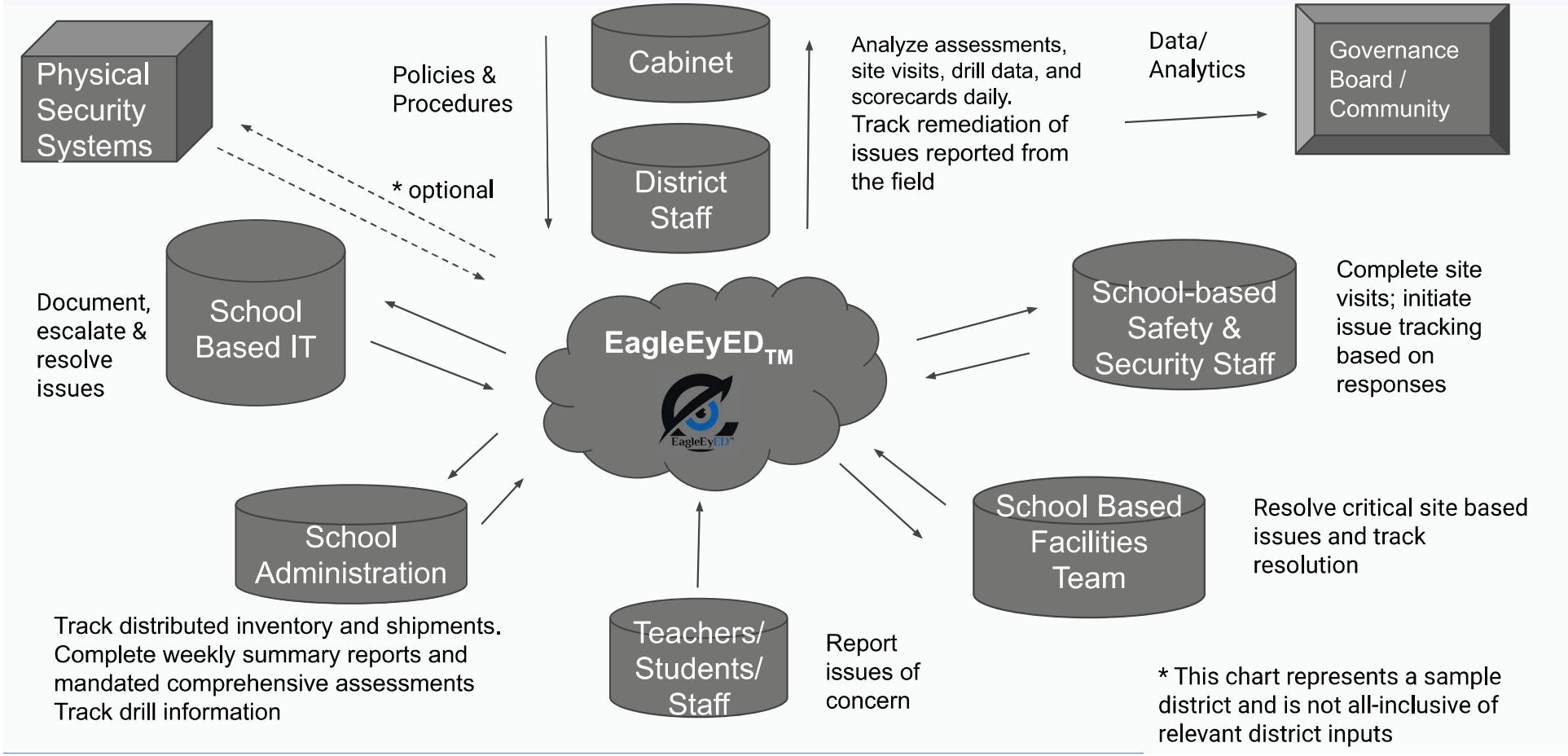


4 Methods of Data Interoperability

- 1) Manual completion of Scorecards
- 2) Manual Import and Export of flat files
- 3) Automated Extract, Transform, & Load (ETL) of files*
- 4) One-Direction integrations through public APIs*

** = custom integrations requiring a small additional fee*

Sample EagleEyED Overview of Usage, by Stakeholder Group



SAFER
SCHOOL SOLUTIONS

September 2021

A Tale of 3 Attacks: A public school district's resilience in an age of bad actors and a global pandemic

---

Introduction

Broward County Public Schools (the "District") suffered three massive attacks within three years, including one of the worst school mass shootings in US history, a potentially crippling ransomware attack, and a global pandemic. The massive impact of these events was further complicated by the complex interaction of federal, state and local politics. Few times before has one district faced such complex logistical and recovery efforts, while simultaneously meeting extensive documentary and jurisdiction requests to aid in the quest for accountability. In many ways the District can be viewed as a cautionary tale regarding school safety and security, the need to think holistically across the physical and virtual domains (enterprise risk management), and the encroachment of our society's political tensions on public education systems. School board meetings nationwide have now become ground zero for some of America's nastiest political brawls. Even more chastening is the growing cry to hold school leaders accountable — often with great personal stakes at risk.

Throughout these events, one thing was consistent — post incident, the District was asked to "show its work" and demonstrate the steps of preparedness and readiness prior to the events, as well as the plans for response and recovery being used to "return to normal" as soon as possible. Throughout all these crises, emails and documents were scoured to provide evidence to federal and state law enforcement, the Marjory Stoneman Douglas Public Safety Commission, the state-wide grand jury and local governance entities. The onus was on the District to demonstrate that even with "best practices" employed, tragedy may not be avoided entirely, but at best mitigated, contained and responded to in a measured and effective manner.

In 2018, following the tragedy at Marjory Stoneman Douglas High School (MSD), the District initiated an independent review by school safety experts at the non-profit organization Safe Havens International to identify opportunities to improve school safety protocols, as well as areas where Broward county may have been well ahead of contemporary school safety standards. These gaps and acknowledged strengths would years later become the standard for national expectations around school hardening and safety and security accountability, as well as threat assessment strategies for students needing mental health support.

Act I: Valentine's Day, 2018 and Marjory Stoneman Douglas High School

The April 24, 2018 Miami NewTimes story titled "After Parkland, Broward Schools Superintendent Robert Runcie Battles the NRA and Local Critics" led with the following:

As the white Chevy Tahoe hurtled toward Marjory Stoneman Douglas High, Broward schools Superintendent Robert Runcie jammed an iPhone to his ear. Between a never-ending stream of calls from reporters and school staffers and politicians asking questions he couldn't yet answer, he dialed Sheriff Scott Israel.

Just a few hours earlier on that sun-baked Valentine's Day, the slim, six-foot-four educator with closely cropped hair and a whisper of a mustache had beamed as he handed keys to a new car to the District's teacher of the year. He had grinned as Tammy Freeman ran to the bow-topped red Camry outside Monarch High, where students waved banners and silvery pompoms. Now he was rushing to another school, where students — two or six or maybe more; the numbers kept changing, kept getting worse — had been shot to death in their classrooms. It was hard to comprehend.

The shooting lasted six short minutes. In the aftermath, 14 students and 3 staff were dead, and 17 more were injured. The deadliest high school shooting in U.S. history. In the immediate hours following the tragedy at MSD, District administrators found themselves face-to-face with federal agents and local law enforcement officers demanding all originals and copies of the video surveillance footage for the school. Administrators explained that the data they were looking for existed on servers with other critical District data including payroll and life safety systems. One administrator recounted that the agents didn't care and were prepared to go to the District's network operations center and seize all servers. Agents said no copies could exist outside of law enforcement hands to avoid them being leaked to the press or shared without the consent of the investigating agencies. Even with this, photos and video of the massacre were ultimately released, but not by the school district.

To this day District personnel - including the District's law enforcement agency - have not had access to the video footage to conduct their own investigation. For years to come, elements of the footage will be referenced and used to identify gaps, mistakes and lapses without District staff having the opportunity to review the video. The most comprehensive recount of what occurred that fateful day is contained in the Marjory Stoneman Douglas Public Safety Commission report published in December 2018, the result of a commission appointed by then Governor Rick Scott (R) to investigate the events that occurred in the only solidly Democratic voting county in the state. The make-up of the commission with the inclusion of several of the parents of victims raised questions about its independence and objectivity, and ultimately led to

the publication of over 450 pages of critiques and recommendations, closely followed by the empanelment of a state-wide grand jury to investigate "school safety issues."

In the absence of the video surveillance footage and with the crime scene under lock-and-key by the county sheriff's office, the building remains on the campus as a daily reminder of the tragedy. Mental health and crisis professionals advocated for its immediate demolition, but the state attorney's office maintains the crime scene and intends to use it as part of the trial for the murders over the coming years. A fence was erected and windscreens with trees were fastened to try to block the view from staff and students, but the building stands tall over this fence with its windows still boarded from where the killer attempted to shoot additional victims from an upper floor.

Safe Havens International, conducted a risk assessment of the District's more than 240 schools, as well as the District's entire safety and security practices. Safe Havens made 121 detailed recommendations for improvement. The Safe Havens report drafts were produced prior to the draft MSD commission report and the District began to implement the highest priority recommendations from both draft reports.

Simultaneously, the school District launched a public campaign to increase school safety funding allocated from the state legislature for school districts, which had been stagnant for years. In addition to that effort, in August 2018 the school board passed a local tax-payer ballot initiative to fund teacher pay increases, additional safety and security staffing and mental health resources. Later that fall the State also increased the Safe Schools Allocation for the first time in over a decade (that allocation would immediately decline again the following year).

While parts of the community came together to support the staff and students during a time when the focus should have been on recovery, the politics of this crisis shifted the focus to a state-wide commission collecting thousands of pages of documents and evidence:

When was the last active assailant (or Code Red) drill conducted at MSD? What did that training consist of? Who conducted it? Who attended? When did the last training session on how to respond to such an event take place? Were these specific people in attendance? How many hand-held radios did that school have? How many school resource officers were at the school? How many unarmed district security staff were present? When was the last time the school intercom was tested? Had the fire alarms been recently tested? Were the gates typically locked at that time of day? Were they locked on that day? Were the classroom doors supposed to be locked? Were they locked that day? Was the video surveillance system working? Did law enforcement have real-time access to that video? Was there a way for law enforcement to easily access the campus and classrooms?

District staff scrambled to gather this information in the days following the attack while witnesses were interviewed by law enforcement to put together the full accounting not only of what occurred that day, but also what occurred on a typical day at MSD as well as across the other schools in the District. Like most large school districts, Broward County followed a decentralized model where district administrators provided guidance to principals regarding safety and security expectations and yearly refresher training to be passed on to staff. The District's strained Special Investigative Unit, made up of about a dozen law enforcement detectives whose primarily role was to conduct administrative employee investigations, was suddenly being tasked to provide safety training, serve as "safe school officers -- a term adopted by the Florida Legislature in the "MSD Public Safety Act," requiring a qualified armed officer, at every school district site during instructional hours (The District, like many others, has had contracts with local law enforcement agencies, including the Broward Sheriff's Office, to provide armed school resource officers at its schools which included MSD on the day of the tragedy). Along with this came requirements related to i) conducting threat assessments for students exhibiting potentially threatening behavior, ii) the specific make-up of that team at each school site, iii) advertisement of a state-wide anonymous reporting platform (beyond what the District already provided to students, staff and the public) and iv) a number of other responsibilities. Additionally, there were new District requirements to mark "safer spaces" in each eligible classroom, reiterating to all staff the expectations that they any employee can notify others of a suspected active assailant on campus, to lock or man all exterior gates throughout the school day and to keep classroom doors locked during instructional time.

There was simply not enough staff, resources, infrastructure or time. Moreover, there were debates on whether some recommendations would actually improve school safety.

With the slew of new requirements, the District was under the microscope as "ground zero" for implementing them. For any new rule - funded or unfunded - the District regularly had to show evidence of its compliance, even for the public charter schools, over which it had minimal oversight mechanisms to enforce anything … this by legislative design. The state enacted yearly comprehensive risk assessments requirements and a state-funded tool to complete these assessments, which among other things required each first-responder agency to conduct campus tours with administrators to identify areas for improvement and make recommendations. The state also hired "monitors" to make unannounced visits to schools across the state every day to ensure that they were in compliance with the laws and to note any perceived derivation from "best practices" as determined by the MSD Commission. Even items not in statute, including locking of classroom doors, designating "hard corners," securing single points of entry and providing window coverings to be deployed in the event of an active assailant event are noted on these visit reports. These visits don't focus on safety and security holistically, they focus almost entirely on the high impact/low likelihood active assailant event, and more specifically, the exact type of event that occurred on February 14, 2018. The actions

do little to prepare for other more likely events and/or for slightly different attack vectors which could one day occur.

In its comprehensive report, most of which was published for the public to review, Safe Havens made two significant recommendations to District leadership:

1. The centralization of all safety and security functions for the District under a new Cabinet-level position; and
2. Implementation of an Enterprise Risk Management (ERM) model.

At the time, the ERM model was unheard of in the K12 space, although the Council of the Great City Schools (CGCS) advocated for this approach in a spring 2016 report (link). The model pushes districts to look beyond traditional risk management (typically employed for insurance risk) to establish a governance and review cycle for evaluating all district related risks/threats, prioritizing those risks and deploying resources accordingly in a continuous cycle. In response, the District made significant investments in technology, personnel and infrastructure to include accelerating the completion of Single Points of Entry for all school campuses (which began prior to MSD and was completed ahead of schedule), increasing the number and type of video surveillance cameras at schools, improving the intercoms at the high schools and the District's technical colleges for better communication reach to common areas, increasing the onsite unarmed security staff at each school (doubling the number of school safety and security staff from prior to Feb 2018), improving the radio communications system and building out a new Safety, Security & Emergency Preparedness division.

All the while, the District continued to engage with Safe Havens International for validation of the strategy and implementation details of these various projects. District staff presented at national conferences on the improvements and enhancements made by the District to help inform discussions taking place at districts across the country, including the new ERM model and strategy, as well as how to conduct safety and security drills in a productive and age-appropriate manner.

ACT II: Should we be worrying about this COVID-19?

In March 2020 a phone rang at District headquarters, *"Have you heard about this virus going around? It is called COVID-19 and our hospitals are starting to get overwhelmed by patients."*

The call was from an administrator at one of the area's largest hospitals - Broward Health. The question that day wasn't whether the schools would be a vector for passing the virus (that would come later) but instead whether the in-school transmissions would impact vulnerable populations in students' homes and whether those transmissions would quickly exceed health care capacity. The District acted ahead of most others to quickly transition all staff and students to virtual learning and remote work for what was expected to be the length of spring break vacation.

As we now know, in reality the time frame was much longer: through the end of the school year, the summer and beyond -- a global pandemic continues to be an ongoing crisis throughout the world at the time of this writing.

Broward County Schools successfully leaned on its existing online learning management systems and contracts for video conferencing to stand up one of the most effective online learning systems in the nation, with the fewest number of days of education missed during transition. The IT infrastructure deployed more than 100,000 laptops and mobile internet hot-spots for students and educators. It increased licensing for online tools to account for the volume and capacity, while providing remote education and engagement to its students with minimal disruption.

As case numbers began to decline in September 2020, the District began its summer planning for what the return to "modified in-person" classes would look like at its 240 schools for those students who needed it most. It deployed signage and floor stickers indicating proper physical distancing expectations and personal hygiene, ordered and installed plexiglass dividers to high traffic areas, procured e-misters, hired and implemented deep cleaning services, converted water fountains to bottle filling stations, outfitted school nurses with up-to-date and accurate thermometers and distributed a range of Personal Protective Equipment (PPE) to all schools in anticipation of staff and student return in October. The Enterprise Risk Management structure, established a year prior, sprang into action, dividing the response into work streams with almost weekly reporting to the community and the school board about the plans and progress of implementing those plans. More than 60 hours of meetings were conducted at workshops where parents, community members and staff raised questions and concerns and provided feedback, while the daily work consumed District personnel and stretched financial capacity. Funding would eventually come from the federal government, until then the District was forced to spend millions of dollars on preparation. Additionally, the District updated, revised and

re-published its existing pandemic response plan in real time to deal with this unprecedented public health crisis.

But there was something new, something different.

The infrastructure built for Safety, Security & Emergency Preparedness proved to be more than just "active assailant response" or "hurricane preparedness" ready and was able to help drive a cohesive and agile response throughout the crisis. District safety administrators called Area Security Managers (ASMs) visited schools daily to make sure that the precautions and resources authorized by the School Board and pushed out by District staff arrived at schools and were implemented with fidelity. They tracked this information in a homegrown mobile application along with their everyday safety and security observations so that district staff could understand real-time what was completed and what was still pending long before students arrived back on campus. The ability to pull this information into dashboards, allowed administrators to monitor the deployment of electronic devices, the distribution of much-needed food to our most vulnerable community members, delivery of resources to school buildings and allowed the District to "show its work" regarding the progress it made - something missing at the time of the MSD tragedy. It also gave the District the opportunity to demonstrate its value as a lifeline of critical resources for the community.

Even though the tracking application was rudimentary, it made it possible to understand the true "state of the district" more fully as it related to the holistic safety and security picture at schools. Newly created oversight measures allow resources (staff and technology) to be deployed and redeployed as needed.

Act III: Cyber Warfare Comes to School

Another year later, early on a Sunday morning in March of 2021, District staff raced to join a need-to-know meeting on Microsoft Teams. While almost 250,000 students were engaged in remote learning as their exclusive means of attending school, technology system logs showed a rapidly spreading piece of malware that was disabling servers, locking access to student and staff devices, and disabling the District's capability to provide internet access on school premises. This malware would later be attributed to the international ransomware group known as "Conti," and communications with federal and local law enforcement, showed there was very little that the District could do to stop this threat.

The stakes were enormous. Teachers throughout Broward County relied on the availability of technology systems to broadcast instruction from District facilities to students at home under lockdown orders. In parallel, the District's very theory of action for its previous investments in safety and security systems was predicated on working technology. For any large enterprise organization like the District there is an expectation that having a technology-leveraged strategy greatly reduces security personnel costs and improves efficiency and effectiveness. This allows for many layers of safety and security to be employed from out in the community all the way to the classroom. By installing thousands of machine-learning surveillance cameras, digital radios, network-dependent safety appliances, and sophisticated visitor management systems, among other things, the District continued to improve student safety at minimal personnel costs. With this strategy, however, the District's educational and student and staff safety functions were now relying on the efficient and reliable functioning of technology — and at this moment, nothing that relied on the District's network was working.

In that Sunday morning meeting, after triaging the situation with its woefully underfunded and understaffed IT resources, administrators decided to focus on educational continuity before containing the spread of and remediating the malware. School had to open virtually the next day with minimal disruption to an already tenuous learning environment. The strategy focused on three things:

1. The restoration of the District's Internet controllers so that teachers could teach virtually;
2. The safeguarding of the District's enterprise resource planning (ERP) system — which performed budget and payroll functions; and
3. The security of the District's learning management system that more than 200,000 students used daily to access virtual instruction.

Where other districts took many weeks to recover, teams of Broward staff worked tirelessly over the next 10 days, with some working 48-hour shifts, to ensure that these three efforts were successful. The collateral damage rendered 2,000 servers inoperable and locked more than 150,000 student and staff laptops and desktops behind a threat actor's demand for ransom.

Fortune favored Broward. The District had distributed more than 130,000 laptops to students to use during the COVID lockdowns and those devices were not impacted by the malware. A first-day-of-school crash of the learning management system in August 2020 ended up proving fortuitous, resulting in the team working with the vendor to re-architect how the application was hosted, which made it more scalable and resilient in the process. The District had also made massive investments in backup servers during the prior school year, which aided in restoring more than 100,000 laptops and thousands of servers within just two weeks. Those used for education and financial purposes were prioritized first, with other systems restored later. The timing of the attack could not have been better: with one week left until spring break, District staff knew it had to maintain a sense of normalcy for a short time before intensive remediation efforts could occur. Unlike other school districts that were later revealed to have suffered cyber-attacks, Broward was able to address this crisis with minimal impact to students and teachers and no disruption to school continuity. In fact, by the time the crisis made the national press two months later, nearly all issues had been resolved with no ransom paid to the attackers and relatively minimal impact to the District. Many within the Broward community had no idea of the scope and scale of the attack until myriad public records requests and voluminous press coverage shed light on just how serious it had been.

What should have been heralded as an industry-leading response to cyber threats, and a modern playbook for school districts, quickly became politicized. Although law enforcement privately applauded the response, the District was unable to tell its side of the story because of the sensitive interests involved. Citizens were shocked to see that the threat actors initially demanded more than $60M to unlock District systems. At the advice of law enforcement, the District made offers to the cyber-criminals, for ransoms it never intended to pay, as part of a coherent strategy to keep the threat actors engaged in dialogue in hopes of buying more time to catch them and contain the threat. These bad faith offers, used as bait, later became the subject of great controversy in the community. Many citizens did not understand why a district would negotiate with threat actors, and the District was not at liberty to shed light on its strategy because of the active criminal investigation underway by multiple law enforcement agencies.

The District again found itself in the position of trying to do the work to secure students and staff, while being subject to criticism by those who didn't have all the facts or information.

Conclusion

Crisis is unavoidable, and during times of crisis there is no such thing as perfection. The primary mission of school districts is to educate students in as safe of an environment as possible. Knee-jerk reactions to emergency events often result in overspending on technology and quick "solutions" along with overcorrection through policy and procedures. When the dust settles, however, — and there is an opportunity to go back to review these events — the obvious areas of improvement always exist: communication, preparedness and accountability. The ability for the district to "show its work" to help stakeholders both internally and externally to understand the challenges and complexities of everyday operations of a school district is critical. Simply believing that it won't happen in your district or that if it did you are just better prepared is rarely the model for the success. Putting in place strategies to understand, categorize, rank and deploy resources to address your most vulnerable and highest impact gaps may help you turn tragedy into resilience.

Discussion - How Does Your District Answer the Following?

1) How many safety & security related policies and procedures have you pushed out to staff at all levels of your district (policies, memos, emails)? Do you even know? Do you track when you shared this info and with whom?

2) Great, so you've pushed it out, how do you know it is being implemented with fidelity? Onsite leads (principals)? District staff (site visits)? 3rd party assessments?

3) How do you track those visits?

4) What if items are identified for resolution or gaps (how do you rank their severity) or prioritize the work?

5) How do you track resolution? Is this all done on paper? Excel sheets? Through email exchanges?

6) When COVID hit and you deployed PPE, plexiglass, posters, stickers, e-misters and other items, how did you track their deployment and then also verify they were delivered and installed correctly?

7) Does all this data get aggregated so you can allocate resources (money, people, time, repairs) in an appropriate order or defend why things haven't been resolved?

8) If an auditor asked you for that 5 years from now, would you have that information in an easy to access location? How about after a major event?

9) Do your safety and life-saving systems rely upon the successful functioning of the internet (e.g., internet-connected panic buttons; video surveillance; speaker systems)?

10) Do you know the key best practices that can best mitigate your risk of a cybersecurity event?

About

Safer School Solutions provides comprehensive enterprise risk management support to school districts to improve the implementation and accountability of their safety and security policies and programs.

Services

- Evaluation of safety & security and IT/cyber organizational structures
- Review policies, procedures and practices for effectiveness in mitigating physical safety and security and cyber-related threats
- Comprehensive independent school district risk assessments including individual school site assessments

Proprietary EagleEyED Software Solution

- Single location for compliance tracking of safety, physical security, and cyber security-related items
- Resource allocation tracking including deployment of COVID-19 supplies and initiatives
- Consolidated dashboard to understand gaps, prioritize investments, and access data to support security related grant opportunities
- Snapshot comparison of schools and benchmark against other districts
- Incorporates best practices and recommendations from a variety of sources
- Customized to the local district's policies and procedures
- Reminders and push notifications based on district priorities
- Data analytics to maximize transparency and management of enterprise risks
- Real-time capture and retention of communications between field staff and district administrative staff in one easy to access location for audit and compliance requirements
- Tracking of action items and projects for follow-up and resolution
- Emergency drill tracking (fire, tornado, active assailant, etc.)
- Works within your district's technology environment and on mobile devices so data can be captured in the field at any location, at any time
- EagleEyeED works online and offline, syncing to the cloud with internet connectivity

The authors of this case study and the contacts for product and services related questions, invitations for speaking engagements and consultation are:

Brian Katz (brian@saferschoolsolutions.com), CEO Safer School Solutions
Phillip Dunn (phillip@saferschoolsolutions.com), President Safer School Solutions
Robert Runcie (bob@robertruncie.com), Former Superintendent of
Broward County Public Schools, 2011-2021