Using Predictive Analytics to Address School Violence: Creating Safe Campuses for Students

August 1, 2018

1876 Bureau Drive
Fayetteville, NC 28312
www.BlueLightLLC.com

ABSTRACT: Most solutions focused on school violence are focused on reflexive or responsive measures i.e. physical security, active shooter training, exercises, social media analysis. While these measures are critical, they are only beneficial when a violent event is pending or ongoing. To date, there has been minimal attempts to leverage the vast stores of data and information available from school systems, law enforcement, open source, social media and darkweb data to conduct predictive analytics to mitigate school violence. The use of predictive analytics applied to existing data sources can assist in the identification and intervention of violence before it happens.

Suggested Citation: Parkman, Bruce J: *Using Predictive Analytics to Address School Violence: Creating Safer Campuses for Students* (2018); The Safe Campus, a Blue Light Project

1876 Bureau Drive
Fayetteville, NC 28312
www.BlueLightLLC.com

INTRODUCTION: Blue Light, a leading provider of predictive analytic solutions to industry, law enforcement and the military, and its school violence prevention project, The Safe Campus, are honored to outline this concept detailing the critical need to deploy proven analytical solutions to address the critical issue of violence in American schools. With over 14 years of experience and expertise in creating innovative solutions to address counter-threat financing, anti-terrorism, asymmetrical warfare, fraud and criminal activity, the author feels that the issue of school violence could be more successfully countered if technologies, platforms and analytics proven to predict behavior or acts were to be used.

PROBLEM: School violence is one the most pressing issues facing the American educational system today. The lethal nature of these attacks, combined with the continued inability to determine the actors or the methods of attack to be employed heighten the public's pressure on school systems, law enforcement and emergency responders to improve and if possible deter these attacks.

DISCUSSION:

Current situation: Currently school violence remains at the forefront of priorities for law enforcement, the educational system and parents due to its impact on society, families and innocent citizens[i]. Attempts by schools to address school violence have increased but are largely confined to briefings, threat assessments, presentations and training seminars until after 2015 when technologies such as social media platforms, anonymous texting platforms started to be used. While a critical concern, school violence remains random in nature and largely unpredictable hence the inability of authorities to get ahead of it. Across the U.S., addressing school violence continues to be reflexive or responsive in nature and largely relies on physical security approaches and planning vice technical methodologies and analytics. The application of technologies such as data analytics, social media analytics and integration of critical data sets such as school, hospital and law enforcement data are very limited, if even used, to address the possibility of predicting school attacks.

1876 Bureau Drive
Fayetteville, NC 28312
www.BlueLightLLC.com

Overview of School Violence Issues

School Violence Causes: There has been significant discussion regarding the cause of school violence in schools in America. Blame has been made on everything from the lack of 2-parent families, to the use of social media, increase in bullying and economic uncertainty[ii]. The range of backgrounds and supposed causes of school violence indicate that there is minimal common ground concerning the cause of violence on American campuses.

School Violence Types: Besides the most devastating form of school violence, school shootings, violence on educational campuses takes many and varied forms from targeted violence by students, parents or caregivers, rampage violence or domestic terror.[iii] Despite the numerous forms of violence, there is one, bullying, that seems to be the most common denominator in extreme school violence, i.e. school shootings.[iv]

Current Approaches to School Violence

Responsive Approaches: Most law enforcement and school districts historically tend to address school violence with the perception of responding to an attack to minimalized damage. These approaches tend to focus on "active shooter" scenarios, lockdowns (usually done simultaneously) and training law enforcement in the techniques, tactics and procedures (TTPs) to intervene and remove active shooters on campus. Other programs focused on physical security and relied on security audits to identify gaps in physical security measures and make recommendations to mitigate them. Hence, there has been a significant increase in certain aspects of school physical security to include metal detectors, electronic locks, surveillance cameras and other physical and technical means. While an important aspect of school security and critical to limiting the access and/or range of an active shooter, these aspects of security have minimal value in the prediction and intervention of school violence. As a matter of fact, most papers released on school violence by FEI[v], FWG[vi], the Constitutional Rights Foundation[vii] and even the Secret Service[viii] still focus on responsive, physical methods and planning through threat assessments and exercises and not the inclusion of technology to get ahead of violent events.

Institutional Coordination: There has also been a marked improvement in the coordination and planning between school administrations and law enforcement. Due to the societal impacts of school violence, the perception that these acts are a law enforcement problem and not the school's has

changed to a point where schools are much more actively involved in the planning for violent attacks. Thus, coordination with law enforcement, as well as the entire public sector to include hospitals, transportation, fire etc. is critical to ensure that an understanding is reached regarding the myriad of issues that must be addressed such as communications, student movements, incident response, medical treatment, counseling etc., that occur during a violent event. Some examples of this include exercise drills with local law enforcement, planning exercises, improved communications etc. all designed to better identify and respond to school violence attacks.

Increased use of Technology: There has also been an increased acceptance of technologies to assist school authorities in addressing school violence. However, recent programs to train faculty and students to recognize some of the indicators of school violence and the use of social media analysis and texting platforms for texting problematic students or persons have been integrated into school violence planning and do to some degree, allow schools to be more able to identify problematic individuals to reach out and intervene prior to a violent act being carried out. These are critical steps in the right direction to leverage existing means of communication to be able to take advantage of the student populations affinity for technology to be able to collect vital data on potential school violence. Schools, now, more than ever are looking to technology and understand that the ability to leverage that technology to identify potential school violence persons. This change from a reflexive approach based on enhanced physical and technical security to one based more on technology will be critical in being able to collect the information adequate to better predict violent attacks.

Impact of these changes: These and other solutions that have been applied to school security undoubtedly have stemmed the amount of and/or prevented at least some attacks as they do limit key factors that contribute to a successful school attack such as open access, limited or no sensors, recording devices or emergency devices, or the inability to recognize and report potential violent persons. This success cannot be overlooked and the continued improvement of physical, personnel and technical security must be a fundamental base of any approach to school violence.

However, it can be stated that while some school violence has been stopped, that these approaches support a responsive, reflexive response to school violence, vice a predictive one focused on intervention. While both perspectives are important, it is the latter one based on predictive analytics that can have the greatest impact on school violence by getting “left of boom” (military jargon for predicting and intervening on violent actors, thus preventing the event or “boom”) and identifying

potentially violent offenders and developing mitigation strategies to intervene prior to escalation. This perspective to school violence, discussed later, has been proven repeatedly to work in identifying and preventing violence or attacks by law enforcement and military since the early 2000s

Issues Impacting School Violence Solutions:

Lack of Integration: While efforts to address and prevent school violence are numerous there is minimal integration of the data, technologies and security improvements that would go far to give school and law enforcement authorities the means to become more predictive, or even better situationally aware of potential violent acts. Most improvements in school security are "one and done" programs that are funded in a variety of means; grants, donations, bonds but are not integrated with past and/or future endeavors inhibiting their effectiveness. Many, if not all schools do not have a forward-looking plan, other than maybe a security audit and it will be critical that any, and all, measures taken follow a plan to ensure that new ones

Expense: Many solutions offered school districts seem expensive when offered to school districts with limited funds or budget. Some of the technological and especially manpower-based solutions can overwhelm school districts with their cost and the fact that they are a part of a solution, rather than a solution unto itself.

Impact on IT architecture: Schools are anxious about any impact on their IT architecture. Given the sensitivity of data, the numerous data security and compliance issues they face (PCI, HIPAA, FERPA etc.), and the complexity of multi-tenant school systems, schools are not willing to take on solutions that require major data moves such as single data base storage or moving from a physical location to a cloud based IT architecture that require extensive Extract, Translate and Load (ETL) requirements.

Customization: Many educational institutions have been exposed to shameless contracts and highly customized technological solutions that hold them in servitude to the vendor for years. As solutions should be required to integrate with existing security measures, schools are not keen on customized solutions that are reliant on vendors due to customization, or that they do not own.

Sensitivity of Data and Privacy: Due to the personal nature of school data it is usually classified as Personally Identifiable Information (PII) or Personal Healthcare Information (PHI) and comes with onerous regulations under the HIPAA and FERPA act or oversight by privacy groups who feel that the information should remain private. Schools are loath to look at solutions touching their data that are not in compliance with the law, or that could expose that data to publicity.

Changing Approach to School Violence

With its societal impact and the fact that school violence has not diminished given the various approaches and monies spent to mitigate it, society itself finds its attitude towards school violence evolving. Where before only the affected community was devastated, recent school attacks are provoking responses from communities around the U.S and that is having a significant effect on how schools are looking at mitigating violence within them. For years, solutions such as armed guards, metal detectors, social media monitoring, student searches, expulsion etc. were all considered too severe or a deprivation of privacy and student rights. However, current discussion regarding school violence finds that these and other approaches, once considered overbearing and/or insensitive are now being supported by greater numbers of parents, students and teachers. The recent national reaction to the Lakeland Park event shows that every level of society is tired of school violence and is willing to discuss and accept more stringent and escalated solutions to prevent it. Schools are also adapting background checks on employees and hiring School Resource Officers or SROs to assist with monitoring students while other schools have on-duty police patrols in parking lots.

Why Predictive Analytics Can Help: The changes in school attitudes have schools and educational facilities of all sizes searching for solutions that can better assist in school violence. As stated, most of this focus has been on physical security and other responsive venues towards violent events. Given the costs and time to get these solutions on site, there is a definite case for more technical solutions that can leverage existing school assets and make them work for the school to increase security.

Untapped Data Sources: The key here, and to all predictive solutions is data: schools and their local environments and the internet are full of data that is related to potential violent acts and to date, hardly any solutions focused on school violence are leveraging the vast stores of relevant on-site data and integrating that with other data sources to conduct predictive analytics. If we want to actually

get “left of boom” and be predictive regarding school violence, this data must be integrated and used in a proven, non-invasive manner to protect our students and loved ones. Since the 1990’s schools have spent billions of dollars on integrating and updating technology and estimates are that the education technology market size is around $8B per year.[ix] While a lot of this budget is spent on improving the use of technology in learning, it also has been used to digitize most of the data used by schools to include administration data, student data, teacher/employee data, counseling data, website and social media data etc. All these data sources are maintained by schools and thus are available to be analyzed. Additionally, there are vast amounts of data that could be relevant to violent events on the internet, social media, and the darkweb not to mention in public databases, law enforcement and healthcare databases.

Warning Signs of School Violence: Recent reports indicate that most shootings had some form of warning prior to the event.[x] The forms of these warnings range from telling friends, to social media posts, to arrests or mental health care treatment. It is these data points that become increasingly important in the drive to become more predictive in our approach to school violence.

Predictive Analytics: A Proven Methodology: Predictive analytics as a methodology has had a significant impact on information analysis for decades. While it’s hard to identify exactly when, some folks point back as far as the 1940s, when Monte Carlo calculations first were used by the U.S. Government[xi]. What is evident in most discussions of predictive analytics is that as technologies and connectivity continued to expand, the inclusion of those technologies and ability to mine them through increasingly complex algorithms and tools for insight is what keeps predictive analytics amongst one of the continuously sought areas of expertise in the market. The reason: every customer wants to know, as best possible, what the future holds, and predictive analytics is a proven means to determine that.

Since 9/11 there has been a rapid increase in the integration of tools and technologies into the predictive analytic environment. While information analysis was usually limited to papers, charts, diagrams and other more conventional products, now it includes social media, cell phone, identity extraction, data searching and mining, web crawling and even video analytics databases and sources that really were not previously used, at least by military and law enforcement.

During that time, there has been a rapid increase in the effectiveness of predictive analytics primarily due to the amount of new data that is available and that effectiveness has been proven time and

time again in the ability of predictive analytic solutions to identify and resolve not only violence related issues like criminal activity and counter-insurgency, but data driven problems such as insurance, healthcare and retail fraud and cybersecurity[xii].

An Overview of the Predictive Analytic Model: To the novice, predictive analytics works as a cycle of flowing information or data that an analyst uses to identify problematic personnel, entities, situations and to validate the accuracy of that information to then determine which entities reflect an actual threat and to work with established authorities and rules to create mitigation strategies. Whether it's a criminal network, financial fraud, or counter-insurgency campaign, the basic premises and methodologies are the same. Depending on the use case, the process may differ in the types of data, tools used, collection methodologies etc., but remains virtually the same for any use case regarding the use of violence. For any predictive analytics model the foundation is usually called the intelligence cycle by most intelligence analysts and that concept has been around for decades and has seen some shifts in its application such as the F3EAD (Find, Fix, Finish, Exploit, Assess, Disseminate) model used by Special Operations. The model proposed here is based on that common analytical foundation.

To some analysts there is no difference between the intelligence cycle or predictive modeling as the use of the intelligence cycle has utilized many of the tools applicable to the predictive analytics as its integrated more and more technologies and the fact that the steps are similar. However, in an analysis of the intelligence cycle, it is evident that the cycle is intended to get to an end-state and support a decision to react to an analyst's findings. While predictive analytics could be used in getting to that decision point, once the decision is made, a new cycle begins to support a new event and there is no continuous monitoring of data for follow on operations, i.e. battle won, or case closed.

Our posture here is that, in the case of predicting violent behavior, predictive analytics is more of a continuous process that leverages data to identify potential patterns or anomalies leading to the identification of a potential offender and intervene as required or if necessary. In this model, the analyst would then conduct the continuous monitoring of the originating and additional data sources to be able to quickly ascertain when that person or a newly discovered entity may be prepared to act out. Once identified and information arises that would require a decision and subsequent action, the analyst would continue to monitor the data sources for additional information relevant to the case.

Predictive Analytics Model

As seen, there are some variations of the intelligence cycle when predictive analytics is used, especially in targeting violent people.

First, predictive analytics relies on data, and the more data the better since links and patterns become more evident when larger data sets are accessed. However, data should be aggregated in such a way to make it as easy to search as possible as continuously having to query individual data bases can be agonizing to the analyst. Thus, data aggregation, whether migrating data to a single server (painful) to being able to access data in place (preferred) is of significant interest to the analyst performing predictive analytics. The end-user should identify as many data bases as possible that are relevant to school violence, i.e. internal records, law enforcement records (if possible), open source searches, chatroom searches, darknet searches and especially, social media.

Second, using predictive analytics, data processing is more reliant on technology, than conventional analytics. To save time and resources, it is critical that all the data is processed, or translated in a way that results in a data storage model where the data is highly searchable by tools due to the

commonality of its structure. In a model where all the data has been migrated to a single server, this is still an issue, depending on the original data construct and whether the data has been translated to work with all other data on the server. The most successful models here use data connectors or ETL (extract, translate and load) technologies to make the data inter-relational and easy to query and then use schema and/or filters to organize data for predictive analysis.

Third, as stated, predictive analytics when applied to any violent target is a continuous process of data searching, monitoring and aggregation as usually they are focused on multiple entities or cases at once. Analysts should be on the lookout for additional sources of data relevant to their use case and continuously monitoring the ones that they have access to for any information indicating that an identified or new entity could be interested in a violent act. There has recently been a small explosion in the data sources available to analysts due to the proliferation of communication methods on the internet and easily identified sources of information. To be as "predictive" as possible, these sources should be searched daily and when possible, alerts set up to warn analysts of new and relevant information. In this model, analysis doesn't stop after reporting, but continues to monitor the relevant databases for actionable information.

Fourth, predictive analytics is part of a platform, not a solution in itself. For predictive analytics to show results it should be embedded as a solution that provides the school with the ability to access and monitor as much data as possible (records, sensor, internet, dark net, social media etc.), store that data in a manner that facilitates predictive analytics and comes with a reporting, decision making and incident response capability necessary to react to identified threats. While a school may have some of these features, it is key that they all be combined in one platform to ensure that not only is the school more successful in identifying potential violence, but also once identified is able to respond as required.

Predictive Modeling Systems Applications: it is critical that the approach to school violence using data analytics is one that allows integration of the model into the existing school security plan as well as their IT data security plan. But any use of data or predictive analytics would follow a standard project management plan to ensure that the system to be used was adequate for the scope of the engagement.

First the vendor as well as the stakeholders, school officials, security, law enforcement and others should ensure that a proper assessment of the school's data and architecture as well as an

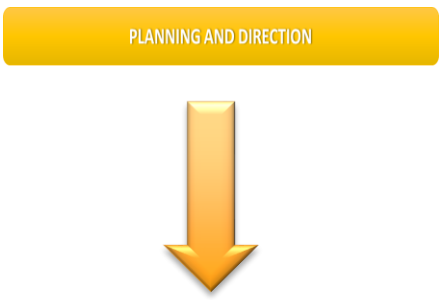
understanding of any system specific requirements should be used. Second, any required connectors for database, open source, social media platform, texting apps should be required as well as ensuring that the system is configured to accept the forms and/or types of data that the schools has. Third, the system should be installed according to an agreed upon timeline and in accordance with all school specific as well as Federally mandated compliance requirements. Fourth, the analysts, SROs or other individuals involved should be trained on the system. Finally, the system should be handed over to the school as their property and maintained or sustained according to the contract.

Configurations of predictive analytic systems for schools can vary from single systems used by a SRO or Law Enforcement analyst to an incident response center to larger intelligence and response centers. Due to the technologies used in conducting these types of assessments, systems do not have to be on-site at the school, but can be remote, possibly tying many schools together in a single district. Depending on school requirements and/or budget, systems can be tied into incident response or command and control systems where during an event, local assets such as police, fire, and medical resources can be controlled.

Another factor in configuring these systems are relations with local authorities or internal police forces as well as medical networks. Due to the increased possibility that some actors will have had problems with local law enforcement or have sought health care for issues related to violence, the access to that data, not access to the data but from case by case response basis, could provide critical data that could identify a potential violent actor.

School Violence Application Example: The following depicts how a school would apply predictive modeling based on the Predictive Analysis model depicted above. We will use the Parkland school shooting as an example as it was Blue Light that was brought on to advise local Law Enforcement after the event. (any information here related to the shooting comes from open source docs)

Planning and Direction: This phase provides the school administration and assigned staff the priorities for conducing predictive analytics with sensitive data. During this process, the authorities determine what threats are oriented towards the school based on historical data, i.e. bully, bomb threats, harassment,



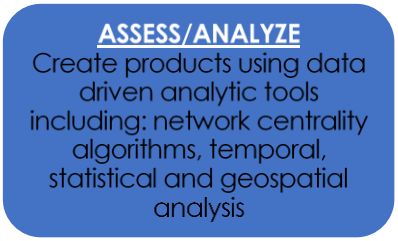
shootings etc. and prioritize them for the analyst. Consideration of data sources is also critical in creating the largest possible repository of data for analysis. Depending on the scope, schools should be looking at their own data, regardless of the type or form, and any other sources they would like to query, i.e. law enforcement, open source, dark web data etc. Attention should be placed on any limitations or compliance requirements to ensure that data is accessed in accordance to law or regulation. Regarding the Parkland shooting there are several data sources that, if available to an analyst, would have provided information regarding the shooter as he already had data and reports in the school's, law enforcement and local medical systems, as well as social media.

Collection/Monitor: During this phase, the analyst is initially querying the approved databases, texting platforms and social media alerts as well as law enforcement, state and federal databases if possible for relevant information regarding school violence. The information would be stored in an onsite database behind the firewall for processing and subsequent reporting. If information is found identifying an immediate threat, the school should have reporting processes to bring that to the attention of the authorities. Again, here the Parkland shooter may have been located as data relevant to him found in the collection phase was processed for analysis. It is quite possible that information from school records, law enforcement records and social media would have been processed during this phase for analysis and assessment. Monitoring of the data would have brought new data regarding arrests or social media posts into the analysis flow.

Process/Discovery: During this phase the school analyst takes the data from the earlier queries applies it to an existing or new use case and readies it for analysis by applying filters, algorithms, and schema to make the data inter-relational. Data determined to be irrelevant is dumped during this process. During this phase, data that drives other

cases can be discovered, and new cases begun on that data. Regarding the Parkland shooting, any information that is collected is formatted in a way to make tying a potential violent person to events and actions that would become increasingly evident in the next phase.

Assess/Analyze: Here the school analyst is applying more advanced tools and technologies to analyze data to create links between entities and events, add more relevant data to existing cases or to look for data that links a potential violent offender to an immediate threat. Analysis is continuous, meaning that on a daily basis new data is always being analyzed to value its connections to existing use cases. Threats that are identified are validated through data sharing or through vetting with authorities prior to submission as a report. It is here that the Parkland shooter could have been identified as it would be difficult for anyone to overlook the data that the shooter had on him in the resources that are available to schools and law enforcement using the tools that a predictive analyst uses. Using link analysis, temporal analyses, identity extraction tools an analyst would be able to identify numerous events that would indicate that an individual needs intervention.



Publish and Report: The final phase is when the analyst prepares the report to submit to the authorities for validation and action. The report can come in any format desire but should contain the information necessary to support the analyst's claim that action is necessary. If required, supporting documentation can be provided from the use case assigned to the individual.

Key Features of Predictive Analytical Solutions for Schools:

A review of technical systems that have been used to provide predictive analytics for use cases outside of school violence identifies key considerations that would add value to a school violence prevention platform based on predictive analytics. Such an approach would need to address several critical issues to be effective:

Affordable: Given the budgetary woes facing numerous school districts, as well as parents, it is critical that any solution should have a minimal impact on a school budget, not only in the original monetary outlay required to pay for it, but also over time.

Proven: Any solution should be required to be proven effective to predict violence and effective in identifying potential offenders prior to the execution of an attack. A solution should be beneficial to the end user, not only in the short term, but based on proven technologies so that it can be utilized for decades, with updates on technologies, training, technical support. Reliance on "out of the box" solutions, vice customized ones is also key as it provides the school districts the authority to look elsewhere for support when vender relations become frayed.

Forward Looking: Many of the security solutions offered to the school are based on measures that historically have been successful in combating violence. A case in point is the use of Resource Security Officers as becoming a continuous presence around the school to deter violence or improving security through remote controlled locking mechanisms and cameras. However, many of these solutions are based on decades old technologies and communications and do not yet integrate some of the newer technologies and analytic approaches to combating school violence. A school violence platform should be able to leverage and integrate with newer technologies or datasets as they emerge.

Scalable: Any solution offered should show the ability to scale with the size of the dataset or use case that it is applied to. The ability to scale to the growth of a school district, or vast increases in data available to better conduct predictive analytics will be key.

Able to Integrate with existing school and law enforcement databases or feeds: Schools should not see any predictive solution as being an overwhelming IT challenge or a customized approach

1876 Bureau Drive
Fayetteville, NC 28312
www.BlueLightLLC.com

Functional and Learnable: Most technology systems that focus on predictive analytics appear to be highly complex and require advanced technical skills or degrees. While some systems fall in that area, there are systems that anyone with a modicum of comfort with technology can learn and apply with confidence.

Compliant: Given the sensitivity of school and health care data and the potential for integration with Law Enforcement data, compliance with Federal and industry data security standards is critical. Some of the compliance standards that school violence solutions could encounter are the Heath Information Portability and Accountability Act or HIPAA, Payment Card Industry Data Security Standard or PCI-DSS, Criminal Justice Information System or CJIS and Federal Educational Rights and Privacy Act or FERPA. While seemingly overwhelming, if care is taken during the planning stage, these requirements can be easily met.

Limits Liability: As always, schools are under enormous pressure from everything from privacy groups to educational advocacy groups to student organizations to ensure that they are always acting in the student's best interest. Any school violence prevention solution, physical, technical or administrative goes far to help to limit liability in the occurrence of an unfortunate event.

Challenges for School Violence Oriented Date Analytics

There are several challenges that may have to be overcome when a school wants to integrate a predictive or data analytics package. A lot will depend on the interaction and relations between schools and local authorities to ensure that sensitive issues are addressed in the name of school and student safety.

Data Sensitivity: For example, some of the data being accessed is considered sensitive in nature, such as student health records, especially mental health records, or counseling records. While some privacy advocates would strongly recommend schools not using that data, conversations around ensuring that sharing only the data indicating potential violent acts will have to happen. It is foreseen that more and more parents and students are going to opt for more transparent access to data in the future. It is also possible that existing communication and data transfer processes that are in place will suffice for more short term solutions vice providing complete data access or integrating multiple data sources of sensitive data at once.

Budget cycle/approval: Most schools require permission to purchase and install significant or sizable purchases for their facilities. Also, schools work on an annual budget or with some, budget cycles that are 2-3 years long. Getting approval for the purchase of a predictive analytics system will have to be worked on and innovative approaches to funding may be needed. For example, in most major cities there are business supported non-profits that have monies to be used for projects like school violence prevention. There are also grants and currently a bill is going through the United States Senate called the STOP School Violence Act that will provide $1.2B in funding that can be accessed for systems like these.

Employee Qualifications: Due to the access to critical or sensitive data, any analyst that is hired or tasked with supporting analytics must be screened to prevent personnel with undesirable tendencies to have access to the data. Depending on the configuration, the analyst may have access to public records, law enforcement data and school student data. These positions need to be designated as "Public Trust" positions and the same standards applied to them as other similar ones.

Ability for Authorities to Act: There are numerous examples, such as the Lakeland shooting, where authorities, regulations, privacy concerns and other issues prevented proper action to intervene. To be effective, predictive analytics can provide the direction, but it is up to the community to put the processes and authorities in place to respond once information is provided to support intervention. In some communities, these are not in place and this can affect the value of this model.

Conclusion:

School violence is the most pressing concern facing schools and parents across the country and a comprehensive, analytical approach is required to take schools from a responsive mode to a predictive one. It is critical that the data that exists on the internet, social media and within schools is aggregated and analyzed to identify any potential violent offenders as early as possible with the intent of intervening before a situation gets out of hand. Predictive Analytics are one of the few solutions that can harvest all the data available to schools to ensure that a more comprehensive picture is created of the school's population and any threats against them. Armed with this information, school and law enforcement authorities can make informed decisions relevant to the threat and can be more effective in halting the unfortunate issue of school violence.

1876 Bureau Drive
Fayetteville, NC 28312
www.BlueLightLLC.com

About the Author: Bruce Parkman is the CEO of Blue Light LLC, a premier provider of data analytics solutions integrating analytic capabilities into solutions addressing some of today's toughest law enforcement, military and commercial challenges. He is the founder of The Safe Campus, a project that uses the methodologies here to address school violence issues. More information can be found at www.bluelightllc.com or at www.thesafecampus.com .

---

[i] https://everytownresearch.org/gunfire-in-school/#
[ii] https://teens.lovetoknow.com/cause-effect-school-violence
[iii] Buerger, M.E., Levin, B.H., and Schafer, J.A.(2018). Examining school violence: A consideration of select future avenues. Futures Working Group, Society of Police Futurists International.
[iv] https://www2.ed.gov/admins/lead/safety/preventingattacksreport.pdf
[v]https://www.feinet.com/sites/default/files/news/attachments/School%20Violence%20Prevention_FEI_2012_0.pdf
[vi] Buerger, M.E., Levin, B.H., and Schafer, J.A.(2018). Examining school violence: A consideration of select future avenues. Futures Working Group, Society of Police Futurists International.
[vii] http://www.crf-usa.org/school-violence/school-violence-prevention-strategy.html
[viii]https://www.secretservice.gov/data/protection/ntac/USSS_NTAC_Enhancing_School_Safety_Guide_7.11.18.pdf
[ix] https://www.edweek.org/ew/issues/technology-in-education/index.html
[x] https://www.wusa9.com/article/news/local/next/a-look-at-every-school-shooting-and-the-warnings-signs-before-they-happened/73-531119651
[xi] http://www.fico.com/en/latest-thinking/infographic/the-analytics-big-bang
[xii]https://pdfs.semanticscholar.org/presentation/90db/fd5ce371ac8cbc319c59d049bb374cdbe2e1.pdf

1876 Bureau Drive
Fayetteville, NC 28312
www.BlueLightLLC.com