

BEHAVIOURAL & DIGITAL THREAT ASSESSMENT (BDTA) MANAGEMENT GUIDE



SAFER
SCHOOLS
TOGETHER



International Center for
Digital Threat Assessment



EXPECT RESPECT &
A SAFE EDUCATION

BEHAVIOURAL AND DIGITAL THREAT ASSESSMENT GUIDE



SAFER
SCHOOLS
TOGETHER



International Center for
Digital Threat Assessment

Copyright © 2024 Safer Schools Together. The reproduction of this material is strictly prohibited without the written permission of the copyright owners. All rights reserved. Disclaimer: Given the rapidly evolving nature of technology and social media applications, this information (especially social media platform related) is current as of the date of publication. This threat assessment (TA) process does not predict future violence nor is it a foolproof method of assessing individuals or groups' risk of harm to others. This TA process is not a checklist that can be quantified. It is a guide to assist in the inquiry/investigation of potential danger and identify circumstances that may increase risk in potential youth aggression. The goal of this guide is to assist school districts in the development of a threat management plan, furthermore, as circumstances change, so too does risk potential. Therefore, if you are reviewing these TA documents at a date after assessment completion, be mindful of supervision, intervention, and passage of time.

INTRODUCTION

The goal of the Expect Respect and a Safe Education (*erase*) Strategy is to ensure that every child in British Columbia feels safe, accepted, and respected regardless of their gender, gender identity, race, culture, religion, and sexual orientation. It is important for schools to be inclusive and have safe spaces for all students. Being SOGI-inclusive means: speaking about SOGI in a way that makes every student feel like they belong; not limiting a person's potential based on their biological sex and how they understand or express their gender and welcoming everyone without discrimination, regardless of their sexual orientation or gender identity.

Erase is about personalizing services and supports for students building on effective programs already in place in BC schools striving to ensure consistent policies and practices backed by strong community partnerships. Schools focus on developing a positive school climate and culture and enhancing school connectedness. The collaborative partnerships between schools, community partners, parents, and students help ensure positive educational and life outcomes.

The creation of the **Behavioural and Digital Threat Assessment (BDTA)** Guide creates a natural integration of the best practice from current North American evidence-based threat assessment models and Safer Schools Together's Digital Threat Assessment® (DTA).

Digital Threat Assessment® (DTA) was developed in 2015 by Safer Schools Together to keep pace with how evolving technology and digital platforms can negatively impact school and public safety today. Most violent school attacks have had vital information leaked online through social media posts. Knowing where, how, and when to look for this information is critically important to the threat assessment process and successful intervention planning.

“An overall assessment of risk cannot be determined without looking at social media and online activity. DTA® provides immediate risk reducing interventions to take place lowering the initial level of risk. It is imperative to understand the tools and methods available to identify online threat-related behaviour.”

Theresa Campbell, Founder & CEO
Safer Schools Together and The International Center for Digital Threat Assessment®

ACKNOWLEDGEMENTS

Safer Schools Together would like to acknowledge the BC Ministry of Education and Childcare for its commitment to preventing bullying and ensuring safe and caring school communities by initiating the Expect Respect and a Safe Education (*erase*) Strategy to help prevent, identify, and stop harmful behaviours by children and adults - whether they occur online, at school, or in the community.

SST would also like to acknowledge the following international threat assessment experts who have shared their passion and evidence-based threat management procedures. National Threat Assessment Center – US Secret Service (NTAC), Dr. Melissa Reeves, Safer Schools Together (SST), The International Center for Digital Threat Assessment® (ICDTA), North American Centre for Threat Assessment and Trauma Response (NACTATR) Kevin Cameron, United States Secret Service, United States Department of Education.

Theresa Campbell, M.A.

Theresa Campbell is the Founder, Founder & CEO of Safer Schools Together (SST), established in 2008 in British Columbia, Canada, and recognized internationally for its leadership, innovation, and evidence-informed strategies to ensure safe, caring, and trauma-informed school communities. SST's team of highly skilled professionals provide expertise, consultation and support to educators, law enforcement and other service providers across North America and internationally, in addressing student, school, and community student safety-related concerns. SST helps school communities minimize and manage risks of student violence with reliable, professional training.

SST is committed to ending school violence by encouraging school districts to create positive, safe, and caring learning environments for every student, staff, and parent. By providing school districts, school resource officers, and community partners comprehensive violence prevention and intervention strategies through training and services, SST provides threat assessment and school safety teams with the tools they need to build capacity and sustainability.

After a decade of successful work in Canada, Safer Schools Together (SST) Theresa recognized the need for her services in the USA and incorporated SST USA Inc. in 2018. She opened a US office in Washington State and has been conducting business for the past six years. SST USA Inc. is a Washington incorporated company registered in multiple states.

In this short time, SST USA Inc. has delivered core services including Worrysome Online Behaviour™ (WOB™) reports, Digital Threat Assessment® (DTA®) training, and 24/7 Case Consultation support for clients throughout North America.

Theresa serves as CEO of both SST USA Inc. and Safer Schools Together (SST) organizations that focus on violence prevention and intervention and promoting safety in all schools by working with them to improve their school's climate and culture. SST provides training opportunities for extensive professional development in these areas.

Theresa serves as the Subject Matter Expert in the areas of violence prevention, threat assessment and trauma response for the Government of British Columbia. She is an internationally recognized authority and thought leader on the future of Violence Prevention, Threat Assessment, Digital Threat Assessment® and Managing Traumatic Aftermath. She is a trusted resource to numerous schools and districts, law enforcement, public safety agencies, governments, and corporations that reach out to her and her team for case consultations.

Theresa and her team developed and implemented "Training for Justice System Personnel on Cyberbullying" for the Department of Justice in Canada. In Chicago, she was awarded the prestigious Frederic Milton Thrasher Award for superior service in gang prevention. With over 30 years of experience working with educators, law enforcement and corporations, Theresa brings a wealth of experience and genuine passion to this subject.

In 2012, SST was awarded the contract for the British Columbia provincial ERASE Bullying Prevention Training Strategy for which Theresa was the lead contributing author. In addition to hosting training symposiums, SST has authored the Safe & Caring School Tool to measure the climate and culture of a

school, as well as ensure best practices are followed and B.C. Ministry of Education mandates regarding school/student safety are met. Recommendations from each assessment are aimed at ensuring positive programs and proactive measures to address bullying, drugs and fighting are implemented and to help students, staff and parents feel safe and comfortable in their schools.

Theresa was responsible for the conceptualization, development and implementation of many successful and comprehensive, evidence-based prevention and intervention programs, initiatives, and resource materials aimed at enhancing student and staff safety. Many of these unique and innovative projects have also been recognized and implemented worldwide.

Theresa is the CEO of the newly incorporated International Center for Digital Threat Assessment® (ICDTA), offering Threat Assessment teams the tools and training needed to prevent tragedy and intervene at the first sign of worrisome behaviour. The training addresses these challenges and stays current with the ever-evolving social media landscape. ICDTA® aims to give all attendees a stronger understanding of the current social media; to proactively identify student safety concerns; and provide strategies to deal with online situations as they arise.

In 2008, Theresa developed PSSTWorld (Promoting Safer Schools Together), the first online student anonymous reporting tool to promote responsible reporting of worrisome behaviour observed by students, both in person and online. “See Something, Say Something, We Will Do Something.”

Theresa is an executive board member of the Odd Squad, a charitable organization dedicated to drug and gang prevention education for youth, comprised of serving and retired Vancouver Police Department officers. Theresa is the executive producer of five award-winning substance use and gang prevention documentaries.

Contributing Authors:

Theresa Campbell, Dr. Melissa Reeves, Dr. Greg Gerber, Sherri Mohoruk, Scott Rothermel and Colton Easton.

TABLE OF CONTENTS

PURPOSE 1

COMMUNITY THREAT ASSESSMENT PROTOCOL DEVELOPMENT..... 1

ESTABLISHING A MULTIDISCIPLINARY/MULTIAGENCY THREAT ASSESSMENT TEAM 3

**THE BEHAVIOURAL AND DIGITAL THREAT MANAGEMENT PLAN INCORPORATES THE FOLLOWING
EVIDENCE-BASED RESEARCH 3**

3 STEP THREAT ASSESSMENT RESPONSE PLAN 5

KEY CONSIDERATIONS..... 5

ISSUES REQUIRING RESPONSE 6

RESPONSIBLE SHARING OF INFORMATION 10

NOTIFICATIONS..... 11

SUPPORT FOR VICTIMS..... 12

ASSESSING THREATS 13

THE IMPACT OF MOVIES, MEDIA, AND VIDEO GAMES 21

ASSESSING VIOLENCE AND THREATS 22

INTERVIEWS..... 22

THREAT ASSESSMENT: INTERVENTION AND MANAGEMENT 25

SCHOOL AND LAW ENFORCEMENT INVESTIGATIONS 26

BUILDING A BEHAVIOURAL AND DIGITAL THREAT MANAGEMENT PLAN..... 32

CONCLUSION 42

PURPOSE

In British Columbia, school districts, independent schools, band schools and community partners are committed to making our schools safe for students, staff, volunteers, and visitors. All education and community partners have a shared obligation to actively take steps to address safety concerns through a behavioural and digital threat assessment process.

The strength of community partnership lies in a multidisciplinary/multiagency threat assessment response. In situations where facts suggest a child, youth, or adult may pose a significant risk to themselves and/or others, Community Threat Assessment partners agree to work together for the common goal of violence prevention, threat management, and safety planning by sharing information, advice, and support that assists in the reduction of risk in the following ways:

- Build collaborative working relationships based on mutual respect and trust.
- Work in ways that promote safe, caring, and restorative practices for schools, threat assessment partners, and the community as a whole....
- Provide coordinated and integrated supports and services for subjects of concern (SOC) and, as appropriate, for their families.
- Involve families in planning for services and supports for children and youth.
- Recognize the unique strengths of each SOC when developing interventions, supports, and services.
- Ensure Fair Notice is provided to all community threat assessment partners, students, parent(s)/guardian(s), and school staff.

*Excerpt from North American Center for Threat Assessment & Trauma Response (NACTATR)

Along with early intervention measures, the effective implementation of a Community Threat Assessment Protocol supports collaborative planning to prevent traumatic events and reflects safe, caring, and restorative approaches. Timely sharing of information about individuals at risk for violence towards themselves and/or others can ensure that supportive plans are put in place.

COMMUNITY THREAT ASSESSMENT PROTOCOL DEVELOPMENT

Community Threat Assessment Committee

Establishing a Community Threat Assessment Committee with leaders from community agencies involved in signing this protocol will help bind their organizations together in this multi-agency initiative. It is suggested that the school district or Independent School Authority will lead this group. Ideally, the Committee will meet on an annual basis to ensure the protocol is up to date and current best practices are implemented. Having some consistent permanent members is highly recommended. Consider including the following members (not an exhaustive list):

- Superintendent of Public Schools
- Head of Independent School Authority
- Law Enforcement Chief/Detachment Commander/OIC

- Probation/Parole Director/CEO
- Child Protection Director/CEO
- Mental Health Director/CEO
- Head of Band Schools
- University/College President
- Hospital and/or Health Region Lead

The Community Threat Assessment Committee as signatory parties will agree to:

- A multidisciplinary, collaborative approach to identify, investigate, and respond to worrisome, concerning and threat-related behaviours.
- Share information that they have the lawful authority to disclose under their respective legislative regimes.
- Exchange appropriate information without delay while respecting the individuals' rights to privacy.
- Follow the process set out in the Community Protocol in undertaking a behavioural and digital threat assessment to determine if the SOC poses a risk.
- The Board of Education, Independent School Authorities and their community partners will commit to ongoing professional development in threat assessment training and program review.

It is recommended that every agency participating as a formal protocol partner have members of their agencies receive up to date threat assessment training provided through the provincial erase strategy.

Sub-Committee

A Sub-Committee is organized with members who act on behalf of the organizational leads and have received threat assessment training. Ideally, the Sub-Committee would meet a minimum of two times per year.

Examples of Sub-Committee members could include some of the following members:

- Safe School Coordinator
- Director/Manager of Student Support Services
- Director/Manager of Special Education
- Supervisor of Community Clinical Services
- Mental Health Clinician
- MCFD Team Leader
- Child Protection Worker
- School Liaison Officer
- Officer in Charge
- Probation Officer

- Psychiatrist
- Psychologist
- Emergency Room Doctor/Nurse
- Local Independent School Authorities and/or Principals
- Local Band School Principals

The responsibilities of the Sub-Committee include:

- Reviewing and updating the protocol to ensure it is current and responsive to ever-changing needs (this should be done annually).
- Developing and maintaining a current list of all employees and volunteers within protocol agencies.
- Developing and maintaining a current list of a lead(s) for each protocol partner.
- Reviewing threat assessment practice by having one or two cases presented to the Sub-Committee that highlight successes, challenges, and lessons learned.
- Developing an annual report to be shared with the Threat Assessment Committee.
- Determining when additional training is required.

ESTABLISHING A MULTIDISCIPLINARY/MULTIAGENCY THREAT ASSESSMENT TEAM

Multidisciplinary threat assessment brings together groups of professionals from diverse disciplines to provide comprehensive assessment data and contextual variables. This allows you to determine an accurate level of risk and appropriate intervention strategy.

A school-based Threat Assessment Team should include the principal/designate, individuals with expertise in counselling (e.g., a school counsellor, school psychologist) and law enforcement (e.g., School Resource Officer).

Other school staff (or community agencies) may serve as regular members on the team or be consulted during the threat assessment process if there is evidence of an intent to harm themselves or others.

THE BEHAVIOURAL AND DIGITAL THREAT MANAGEMENT PLAN INCORPORATES THE FOLLOWING EVIDENCE-BASED RESEARCH

The Six Principles of Threat Assessment (Fein, et al., 2002)

1. Targeted violence is the end of an understandable process of thinking and behaviour.
2. Targeted violence stems from an interaction between the individual, the situation, the setting, and the target.

3. An investigative, skeptical, inquisitive mindset is needed.
4. Effective threat assessment is based on facts, rather than characteristics or “traits”.
5. An “integrated systems approach” is best.
6. Investigate whether a student poses a threat, not whether a student has made a threat.

MyEducation (MyEd) BC Threat Assessment Field

The Province of BC has identified a process for supporting students where threats of violence against self, others or school communities may be of concern. MyEd BC provides specific security roles and fields allowing authorized users to identify students for threat assessment.

The Province of BC has a clear process for supporting students where threats of violence against self, others or school community may be of concern. Districts appoint a Threat Assessment team leader to oversee the activation of the community protocol. Each school should have a Threat Assessment team.

MyEd BC is used by most school districts in BC. This system allows students to move seamlessly from one school district to another with their educational information intact. MyEd BC has the capacity to notify a receiving school/school district that a new student has been identified as moderate to high-risk through the threat assessment process.

Standards for use of the threat assessment field protects individual privacy while ensuring school administrators and Safe School Coordinators are notified that an incoming student has been deemed as moderate to high-risk through the threat assessment process. The purpose of the threat assessment field is to indicate to a principal that they should contact the previous school administrator or school/school district Safe School Coordinator for details of the threat assessment, to support the incoming student and ensure that appropriate supports and safety plans are in place. The threat assessment field will remain at a security level that does not allow classroom teachers and other school staff to access the information. The threat assessment field is not to be added as an inclusion on the permanent student record.

Limit Access: A threat assessment field should only be visible to Principals, Vice Principals, Superintendents, Safe Schools Coordinators and Team Leaders. This is enforced through security level profiles within MyEd BC.

Alert Only: No documents or plans should be uploaded to the MyEd BC application. The threat assessment field information will not be part of any inclusions to the Permanent Student Record.

Date Only: No information will be entered in the field except the school district number and the date the threat assessment was activated: SDxx-Jan2024. Independent Schools are to enter their Facility Number and the date the threat assessment was activated: FNxxxxxxxxx-Jan2024.

Moderate to High-Risk Threat Assessment:

The threat assessment field will only be entered in MyEd BC after the Step 2: Comprehensive Multidisciplinary Data Collection and Assessment is completed, and the Threat Assessment team deems the individual to be moderate to high-risk.

Ministry Consultation to Delete:

The threat assessment field can only be cleared at the discretion of the school district, following discussion and consultation with the Ministry of Education or their designated appointee. This process is in place to ensure that the field is not unintentionally cleared - the Ministry of Education does not hold the authority to clear the threat assessment field. The field information will remain on the student profile until removed through this process.

3 STEP THREAT ASSESSMENT RESPONSE PLAN

STEP 1: SCREENING (Identify)

- Conduct Screening
- If data reported indicates imminent intent to harm, follow *Initial Safety Considerations for Immediate Risk Reducing Interventions* (on next page) and then complete Step 2: Comprehensive Multidisciplinary BDTA
- If no intent to harm, then complete Step 1: Screening documentation only

STEP 2: COMPREHENSIVE MULTIDISCIPLINARY BDTA (Assess)

- Conduct BDTA
- Consider community multidisciplinary involvement
- Identify risk and protective factors in the Six Domains
- If risk is identified, complete Step 3: Threat Intervention & Management Plan

STEP 3: THREAT INTERVENTION & MANAGEMENT PLAN (Manage)

- Complete the Threat Intervention & Management Plan utilizing the data gathered in Step 2
- Review the Threat Intervention & Management Plan as per the agreed upon progress monitoring plan

KEY CONSIDERATIONS

Threat Assessment

Threat assessment is the process of determining if a SOC poses a risk to the target or targets, they have threatened. The goal is to prevent targeted violence to self, and/or others. Good news is that many individuals engage in threat related behaviour, but few pose actually pose a risk.

Unidimensional Assessments

A unidimensional assessment can occur when a professional such as mental health, policing or school administration decide to interview a SOC without validating crucial interview data and without considering

the SOC's past occurrences regarding worrisome, concerning and threat-related behaviour. A unidimensional assessment is conducted in a brief one-to-one interview that is based on the in-the-moment relationship with the SOC or relying on a single source of data for assessment of the initial level of risk. This type of assessment does not provide an accurate and comprehensive understanding of the potential level of risk.

Multidisciplinary Assessments

Multidisciplinary assessments are required to determine accurate levels of risk and appropriate intervention. By including data from various sources, they provide a comprehensive and inclusive understanding of all risk and protective factors. A multidisciplinary assessment brings together groups of professionals from diverse disciplines to provide comprehensive assessment data and contextual variables. This allows you to determine an accurate level of risk and appropriate intervention strategy.

Awareness of Cultural Bias

Members of some cultural groups may experience multiple stressors such as poverty, racism, discrimination, and language barriers. These factors, along with possible distrust for authority figures, may increase the level of perceived or actual risk. Every effort will be made to take into consideration the ethnic or cultural identity of the student or family.

When conducting a threat assessment, team members should be aware of cultural bias resulting from:

- The behaviours being assessed (individuals from one cultural group may present differently from individuals who belong to a different cultural group).
- The content and phrasing of questions (language and culture may influence interpretation by either the interviewer or the respondent).
- Team members should consider the ethnic and cultural identities of students and families, and where necessary request additional assistance to facilitate effective and sensitive communications.

ISSUES REQUIRING RESPONSE

Issues that raise safety concerns in schools may require a range of responses, whether involving threat assessment, law enforcement or other activity.

Immediate Risk Situations

These situations include armed (e.g., gun, knife, explosives, or other device/weapon capable of causing serious injury or death) intruders inside the building or on the periphery who may pose a risk to a target or targets (i.e., active shooter scenarios). When the immediate risk is identified, lockdown plans should be activated, followed by a call to 911. In these cases, a threat is unfolding, and the matter is one of immediate law enforcement intervention and protective school safety response.

*When an immediate risk is identified, call 911 and immediately activate the school safety plan. The Threat Assessment team will **not** initiate a formal threat assessment until the situation has been stabilized.*

Worrisome Behaviours

Worrisome behaviours are those that cause concern for members of the school and/or law enforcement agencies because of their violent content. They may be an early warning sign of more serious high-risk behaviours. Worrisome behaviours are specific to the individual and may include drawing pictures, writing stories, or making vague statements that do not necessarily constitute "uttering threats" as defined by law but cause concern for some members of the school, family, or community. Following up on worrisome behaviours results in effective early intervention measures. Most often, if there is no intent to harm, worrisome behaviours can be managed through problem solving, restorative practice or strengthening existing supports.

School principals should ensure that teachers, support staff and other members of the school community understand what constitutes worrisome behaviour and the importance of reporting signs of worrisome behaviour.

Threat Related Behaviours

A variety of situations call for schools to initiate a threat assessment and request law enforcement participation. Although not an exhaustive list, situations such as the following will lead to a threat assessment. Schools should ensure the participation of law enforcement in an immediate response to the situation and in follow-up threat assessment processes.

Examples of threat-related behaviours that require activation of a threat assessment include, but are not limited to:

- Serious violence or violence with intent to harm or kill.
- Indicators of suicidal ideation as it relates to fluidity (both homicidal and suicidal).
**Suicide risk-assessment may be required.*
- Verbal/written and direct threats to kill others ("clear, direct and plausible").
- The use of technology (social media posts) or writings that suggest that the SOC has engaged in threat-related behaviours or has demonstrated unusual interest in other instances of mass casualty attacks, radicalization, incels, and /or other content that encourages targeted violence.
- Possession of weapons (including replicas).
- Bomb threats (making and/or detonating explosive devices).
- Fire setting (contextual).
- Sexual intimidation, extortion, or assault.

- Ongoing issues with bullying behaviours and/or harassment.
- Gang-related intimidation and violence.
- Targeted hate incidents motivated by factors including, but not limited to; race, culture, religion, and/or sexual orientation.

Incidents that meet the above criteria are reported to the Threat Assessment Leads who in turn contact the remaining team members.

It is the Threat Assessment Team's responsibility to collect as much data as possible to determine risk as it relates specifically to the SOC. Baseline behaviour is the single most important variable in the field of threat assessment. It is incorrect to assume there is a "profile" or "checklist" that can conclusively identify a violent offender. It takes thoughtful data collection and evaluation to determine level of risk and intervene accordingly.

An accurate assessment of risk cannot be done without also establishing an individual's digital behavioural baseline (e.g., social media posts).

- *Does this behaviour represent a significant change from the individual's baseline behaviour?*
- *Does the behaviour represent a clear, direct, and plausible threat?*
- *Has the counsellor conducted a confidential inquiry with the student's teachers?*
- *Has the student's parent(s)/guardian(s) been contacted regarding current worrisome behaviour?*

Note: If you have reason to believe that a child or youth needs protection under Section 13 of the Child, Family and Community Service Act you must promptly report the matter to a child welfare worker.

Please visit the following website for more information:

<https://www2.gov.bc.ca/gov/content/safety/public-safety/protecting-children/reporting-child-abuse>

Student Suspension

Threat assessment overrides suspension of a student as it may increase the risk that they will finalize a plan to act on homicidal or suicidal thoughts.

The school principal should initiate the threat assessment process **before removing a student from the school environment** unless the student poses an imminent safety risk. The principal should ensure that a trusted adult at the school maintains contact with the suspended student if it is not safe for the student to be at the school.

A poorly timed out-of-school suspension is high-risk, as this period is often viewed by a high-risk student as the "last straw". It is in this stage that many SOCs decide to finalize a plan to terrorize their school or attack a specific target. The plan can include homicidal or suicidal acts. The suspension does not cause the violence to occur but creates the necessary context for a high-risk student who is already struggling with suicidal and/or homicidal ideation to take the final step from planning to action.

1. Consultation with the Threat Assessment team should be a precursor to any suspension.
2. The issues of when and where to suspend must be considered.
3. Steps need to be taken to ensure that the student stays connected to healthy support systems.

Outside of School Hours Cases

Many evening or weekend incidents continue into school the next day. Open communication from law enforcement to the school-based Threat Assessment team helps identify and respond to these incidents. This has proven especially useful in youth gang-related cases.

Schools should call law enforcement when they receive information regarding serious violence, weapons possession, a threat, or any other immediate risk situation during non-school hours.

The Threat Assessment team should initiate Step 2 Comprehensive Multidisciplinary BDTA assessment if the situation has the potential for ongoing risk to members of the school community.

Criminal Charges

Law enforcement will take the lead in any threat assessment involving a criminal investigation. Team members will continue to support the police investigation. Team members may continue to collect data related to the threat assessment if their activities do not interfere with the law enforcement investigation. They should maintain independence from the law enforcement investigation so that they are not considered “agents of law enforcement.” Any relevant information should be reported to the law enforcement.

Occurrences Involving Students with Diversabilities

Individualized planning for students with diversabilities requires school teams to compile information and assessments related to the student’s educational needs. This information can be helpful in assessing shifts in baseline behaviour that may require activating the threat assessment process. The same dynamics that can increase the risk of violence in the general student population can also contribute to the potential violence of students with diversabilities, independent of their diagnosis.

Some students with diversabilities may engage in threat related or aggressive behaviours that are typical to their baseline behaviour and can be managed by strengthening existing supports.

The Threat Assessment team should call on staff members from the school and district level who have responsibility for program planning and service delivery to students with diversabilities. They can act as consultants and expert advisors in the threat assessment process.

RESPONSIBLE SHARING OF INFORMATION

If there is imminent danger, laws allow the disclosure of personal information without consent.

Increasingly, government, schools, law enforcement and other service providers are working collaboratively to share pertinent information about an individual who may pose a risk of harm to themselves or others. Collaborative multi-disciplinary teams can help ensure public safety, timely intervention and support.

If there is imminent danger to an individual's health or safety, federal and provincial laws allow disclosure of personal information to law enforcement, next of kin, school officials, health care workers and others. The information can be disclosed **without consent**.

If information has been disclosed without consent, the individual must be advised with whom the information was shared, as required by law, except in circumstances where notification would compromise an ongoing criminal investigation.

As part of their obligation to maintain safety in schools, the school or school district may share information with law enforcement about students who pose a threat of violence. However, they should identify the purpose for the disclosure and limit the disclosure to what is necessary to deal with the safety issues.

A school or school district can share personal information about a student with law enforcement when they are part of a threat assessment, if the purpose for sharing the information is to assess the risk of a threat of violence involving the student.

Information can also be shared with law enforcement if the school or school district determines that compelling circumstances exist affecting any person's health or safety, including both threats of self-harm or harm others. In such a case, notice of the disclosure must be sent to the parent/guardian or legal guardian of a threat maker as well as to the parent(s)/guardian(s) of the target of a threat, provided disclosure does not jeopardize a law enforcement investigation.

If law enforcement is conducting an investigation, disclosure of relevant information to them is authorized under legislation.

Schools should ensure that principals, teachers, and staff know they have the right, and in some cases the obligation, to share information responsibly to assess and avoid a risk of violence.

When disclosing personal information, school personnel should limit disclosure to what is necessary to deal with the safety issues and identify the purpose for the disclosure.

Subject to law enforcement investigation requirements, school personnel should give notice of the disclosure to the student and their parent(s)/guardian(s) that their personal information has been shared and why.

Schools should consult legal counsel if there is a question as to whether authority to disclose information exists, except in cases of imminent danger.

NOTIFICATIONS

Parent/Guardian of SOC

Parent/guardian notification is meant to help parent(s)/guardian(s) and school officials work together to more fully assess a SOC and plan for intervention. It is very important that parent(s)/guardian(s) understand this is not a disciplinary process but a way of possibly identifying additional supports that their child may need.

- Questions for parent(s)/guardian(s) should focus on the student's behavioural baseline and specifically any known behaviours that may be attack related.
- The student's interest in weapons should be explored, as well as their access to the means.
- Parent(s)/guardian(s) should be encouraged to explore all methods of their child's communication including social media platforms such as Snapchat, Tik Tok, Instagram, Twitter, WhatsApp, Telegram, etc.
- A parent/guardian of the SOC should be notified at the earliest opportunity by the agency considered most appropriate in the circumstances, except as noted in the **Delay of Notification** section below.
- Notification should occur after the threat assessment process has confirmed a threat or violent incident has occurred and has determined the potential for violence.

Delay of Notification – Child Protection Concerns

If the student discloses child abuse during the threat assessment process, consultation with child protection workers with the Ministry of Children and Family Development (MCFD) will help determine the appropriate time to notify a parent/guardian. MCFD may opt to notify a parent/guardian themselves as part of their child protection investigation.

If the student discloses child abuse during the threat assessment process, the Threat Assessment team should delay notification until the Ministry of Children and Family Development has determined an appropriate response.

Potential Victim/Target Notification

If a threat of violence has been made or is suspected, law enforcement should be informed as soon as possible. Law enforcement will consider notifying the intended target and their family as part of their investigation.

Law enforcement should lead any criminal investigation, including threats of violence. In relation to threats and as part of an investigation, law enforcement will determine when to notify the intended target and their family what steps are being taken, including any safety measures being considered. If there is no

criminal investigation it is still a priority to notify target and parent/guardian. This notification may also include information relating to support, counselling, and other support services available. The information may be distressing, and emotional support may be necessary to support the potential target and family respond in a healthy and productive way. You should consider interviewing the victim/target as part of your threat assessment process to acquire additional information about the SOC and any known grievances.

Post-Secondary Institutions Notification

When a Threat Assessment team expects that a student of high-risk will leave the school to attend a post-secondary institution, the team may share information about potential risks of threatening behaviour to help the institution prepare and respond to the risk. The *Freedom of Information and Protection of Privacy Act*, Section 25, requires that personal information regarding a risk of significant harm to the public or a group or people be disclosed to the public or an affected group of people.

Many post-secondary institutions have teams trained in the threat assessment process and may be able to continue interventions to support the student and reduce the risk of harm.

SUPPORT FOR VICTIMS

Threat Assessment team members need to have authority to offer or recommend supportive services for victims of violence or targets of a threat of violence. Support services and interventions should be culturally appropriate and accessible to the victims.

- Law enforcement-based victim services provide services to victims of crimes.
- Community-based victim services provide services to victims of family and sexual violence.
- Community-based victim services can be accessed without an incident report to law enforcement.
- Clinicians on the Threat Assessment team (e.g., psychologists, therapists, or counsellors) should ensure that victims of violence and recipients of threats are provided with appropriate support and services. These may include either law enforcement-based or community-based victim services.
- The clinician should consider, within the limitations of the community, supportive services and interventions are culturally appropriate and accessible.

Fair Notice

**Acknowledgment:* North American Centre for Threat Assessment and Trauma Response (NACTATR)

Staff, students, and parent(s)/guardian(s) must be aware that a school uses a threat assessment process to reduce the risk of violence in the school. When they know that the process exists and how to report concerns, they can contribute information that would otherwise be missed. They should also understand that no action will be taken against a person who reports a concern in good faith. However, there may be consequences for malicious reporting. Giving fair notice of the threat assessment process and its justification also protects the legitimate privacy rights of individuals.

At the beginning of the school year, the school should give students, staff, and parent(s)/guardian(s) “fair notice” that the school will use a process to collect and assess information about threats of violence, including:

- Notice that violence or threats of violence will not be tolerated.
- General messaging about the threat assessment process.
- Notice that the threat assessment process is used provincially.

The school should advise students, staff, and parent(s)/guardian(s) to promptly report high-risk or threat-related behaviour to the school principal, a school designate or law enforcement.

ASSESSING THREATS

Threat: an expression of intent to do harm or to act out violently against someone or something.

Can be spoken, written or symbolic.

Threat assessment: is the process of determining if a threat-maker poses a risk to a target or targets they have threatened. Many individuals engage in threat-making behaviour, but few pose a risk to others or themselves.

Motivation: Knowledge of the motives of a SOC is very helpful to evaluate the intent and potential risk for violence. Understanding the circumstances or perceived grievances that may have prompted the SOC to consider violence towards others is very helpful in the intervention and management planning for this situation.

The following are concepts and definitions that will help the Threat Assessment team assess the motivation and emotional state of a threat-maker.

Types of Threats

Direct: A threat that identifies a specific act against a specific target and is delivered in a straightforward, clear, and explicit manner. “I am going to stab Jason in the cafeteria at lunch.”

Indirect: A threat that tends to be vague, unclear, and ambiguous. “I could kill you; I could kill everyone in this school.”

Veiled: A threat that strongly implies, but does not explicitly threaten, violence. “My life would be better if you weren’t around anymore.”

Conditional: A threat that warns a violent act will happen unless certain demands or terms are met. “If you don’t give me the money you owe me, I am going to shoot you.”

*Excerpt from: *Federal Bureau of Investigation (FBI): "The School Shooter: A Threat Assessment Perspective"*

All threats are NOT created equal. However, all threats should be assessed in a timely manner and decisions regarding how they are handled must be done quickly.

To effectively evaluate a threat, the team must have as many details about the threat as possible. The Step 1-Screening provides a framework for collecting and analyzing these details.

If the threat is “clear, direct and plausible” the threat assessment process is activated. Specific details can indicate the amount of thought and planning that has gone into carrying out a threat. A lack of specific details may indicate that little thought has gone into the threat and the threat-maker is just venting frustration or trying to frighten people.

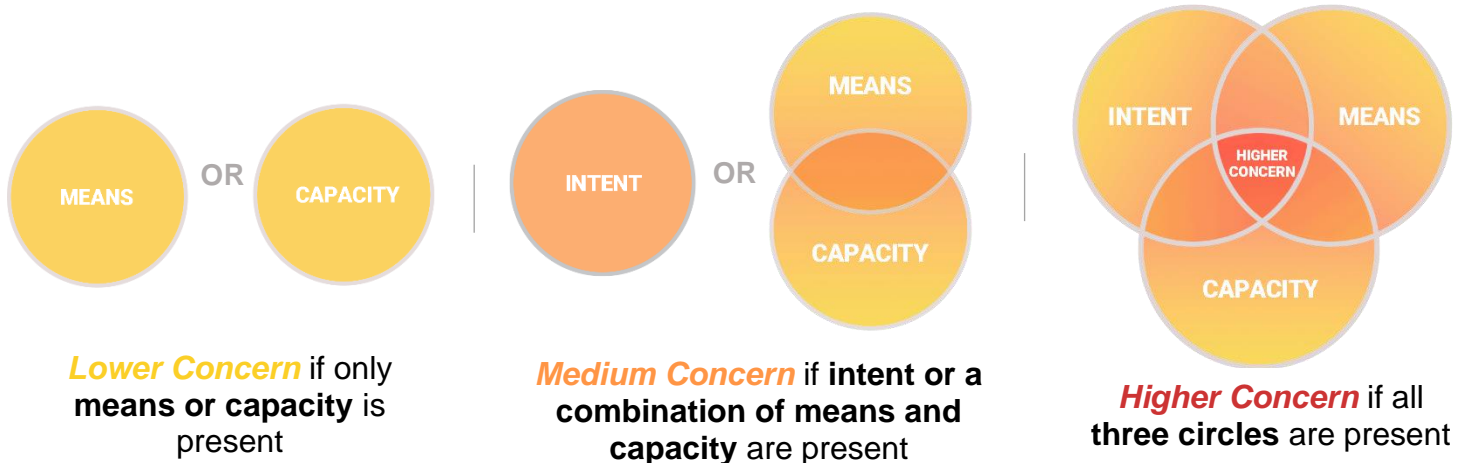
LEVEL OF CONCERN

Determined during the Comprehensive Multidisciplinary BDTA process and guides how intensive and directive the intervention and management plan both need to be to mitigate concern.

Means = access to weapons

Capacity = physical and cognitive capacity and physical proximity to carry out attack

Intent = motivation and desire to carry out attack



LOWER CONCERN

MEDIUM CONCERN

HIGHER CONCERN

Concern level:	Concern Rating Grid
LOWER	There was no true threat (no evidence was found that a threat was made), and/or behaviours were taken out of context, and/or threat is vague, indirect, inconsistent, implausible, and/or SOC lacks developmental understanding or intent. The student can be managed through existing resources and programming, but the individual should be observed for changes that could increase their risk level. Supports and resources may be recommended.
MEDIUM	Threat is plausible but lacks specificity or intent. No clear indication that the student has taken preparatory steps. Has the capacity and means to carry out an act of violence if stressors/contributing factors cannot be mitigated. Some grievances and/or indications of a potential plan but does not view situation as hopeless, helpless, and/or desperate; willing to consider non-violent alternatives and some protective factors present. An intervention and management plan must be developed with increased monitoring, supervision, and interventions established. Progress monitoring and ongoing team reviews are to occur.
HIGHER	Has intent, means, and capacity. A highly directive and intensive intervention and management plan must be developed. Student may not be at school in the short term in order to receive interventions and supports. All risk reducing interventions, monitoring, and supports must be explored and closely monitored with frequent progress monitoring and team reviews. A return-to school plan may also need to be developed.
IMMINENT	Risk is very serious. Immediate containment is needed from law enforcement (i.e., taken into custody) or an emergency mental health hold is necessary to assure safety.

We work from the leading premise that most threats are a **cry for help**.

A threat that contains specific details about targets, weapons, locations, motivation, and perceived grievances is much more likely to be carried out. The more detail contained in a threat, the more thought that has gone into the planning.

Complete Step 1 Screening BEFORE Suspension (i.e., we want to know if they have access to the means that we need to address prior to suspension).

Suspension or Expulsion can provide further justification/grievance to the SOC and can inadvertently increase the current level of risk and inadvertently make the school or administrator a justifiable target. We are not saying there is no suspension rather slow the process down and ensure you complete Step 1 Screening first.

Assessment of Anonymous Threatening Communications

**Excerpt from: International Handbook of Threat Assessment, Simons, A. & Tunkel, R. (2021)*

Anonymous threatening communications have evolved considerably over the years to evade identification. The lack of ownership or authorship of the threat generally denotes a lack of commitment. However, it is important to:

- Assess the anonymous threatening communications.
- Attempt to identify the SOC.

- Avoid or minimize the crisis/trauma response.

Threat Assessment teams should consider the following in determining the initial level of risk based on the current data (i.e., the language of the threat.)

- Amount of detail, such as location, target(s), date, and time the violence is to occur, justifications or other specifics.
- Threatened to do what and to whom (i.e., kill, murder, ruin your lives, shank, shoot etc.)
- Method of delivery of the threat. Who found/ received the threat, when and where was the threat received, and who else knows about the threat?
- Is the threat ***clear, direct, and plausible?***

Depending on the severity of the threat, some or all staff members may be asked to assist in analyzing the anonymous threatening communications.

Depending on the severity of the threat, some students may be asked to give their opinion regarding the origin and authorship of the threat.

Verbal or Telephonic Threats

- SOC typically telephonically contacts a targeted person, organization, or institution to verbalize a threat.

Written Threats (Letter, Email, Text, Social Media)

- Most common type of anonymous threatening communications that has a wide variety of options for delivery (i.e., handwritten or typed hard copy mailed or left in a specific location, delivered via handheld electronic devices, smart phones, and social media.

Prank or Hoax Threats

- SOC's main goal is to generate amusement and entertainment through intimidation and disruption. Some prank threats can be harmless while others fall under the category of swatting by calling law enforcement to falsely report a crisis. situation. Swatting necessitates a tactical response which may result in harmful outcomes.

Bathroom Wall Threats

- This type of anonymous threatening communications is most commonly found in schools and places of education.
- The scrawled threats are generally brief and designed to promote fear and panic. This

anonymous threatening communication relies on discovery and reaction from others and rarely correlates with a subsequent act of violence.

Poison Pen or Third-Party Victimization

- SOC sends an anonymous threatening communication to draw the unwanted attention of an authority figure (e.g., school principal) to target a third-party.

Cyber-Based Extortions

- Anonymous threatening communications range from simple ransomware to elaborate data theft extortions that can be devastating to an organization.

Hitman Extortion

- This type of anonymous threatening communication is an extortionate threat of future violence or fatal attack that can be cancelled if payment is made.
- Almost always a scam they can include references to the target's family and provoke fear and intimidation.

Blackmail and Sextortion

- SOC claims to possess personally embarrassing and often sexually explicit information and demands payment from the target in exchange for silence.
- A failure to comply will result in the sharing of embarrassing behaviour with the target's family, friends and others often accessed through the target's contact list.

Self-Victimization

- Anonymous threatening communications may be generated by the victims themselves and staged for discovery. The victim may be seeking sympathy and attention or the inability to navigate through a stressful situation in a healthy prosocial manner.

Threatwaves

- Threatwaves often emerge during supercharged political or social issue conflicts. Having to assess the credibility of multiple and often disparate threats from different individuals but revolving around similar themes and targets.

Evidence of planning has evolved in terms of digital leakage and is why Digital Threat Assessment® is such an integral component of threat assessment.

Virtual Pairing:

The advent of the Internet has allowed cyberspace to become an increasingly popular means of pairing. Social networking sites provide potential attackers with the opportunity to pair with others. Proximity is no longer a requirement in pairing (*See Finland School Shooter, Nov. 2007*).

Leakage:

“Leakage in the context of threat assessment is the communication to a third party of an intent to do harm to a target. Third parties are usually other people, but the means of communication vary...”

Meloy & O’Toole

Leakage occurs when a student intentionally or unintentionally reveals clues to feelings, thoughts, fantasies, attitudes, or intentions that may signal an impending violent act. These clues can take the form of subtle threats, boasts, innuendos, predictions, or ultimatums. They may be spoken or conveyed in stories, diary entries, essays, poems, letters, songs, drawings, doodles, tattoos, or videos.

Another form of leakage involves efforts to get unwitting friends or classmates to help with preparations for a violent act, at times through deception. For example, the student asks a friend to obtain ammunition for him because he is going hunting.

Leakage can be a **cry for help**, a sign of inner conflict or boasts that may look empty but that express a serious threat. **Leakage is one of the most important clues** that may precede an adolescent’s violent act.

Examples of leakage:

- Recurring preoccupation with themes of violence, hopelessness, despair, hatred, isolation, loneliness, or an end-of-the-world philosophy. The themes may be expressed in conversation or jokes, or in seemingly offhand comments to friends, teachers, other school employees, parent(s)/guardian(s), or siblings. Statements may be subtle or immediately minimized by comments such as, “I was just joking,” or “I didn’t really mean that.”
- Recurring themes of destruction or violence appearing in a student’s artwork. The themes may involve hatred, prejudice, death, dehumanization, dismemberment, mutilation of self or others, bleeding, use of excessively destructive weapons, homicide, or suicide.

Many adolescents are fascinated with violence and the macabre, and writings and drawings on these themes can be a reflection of a harmless but rich and creative fantasy life. Some adolescents, however, seem so obsessed with these themes that they emerge no matter what the subject matter, the conversation, the assignment, or the joke.

Anonymous Reporting Tool - erase|Report It

The BC Ministry of Education and Childcare erase|Report It is an online reporting tool where students can anonymously report anything they find worrisome or concerning, directly to their school district’s Safe School Coordinators. The reporting tool can be accessed by erase.gov.bc.ca or directly via

erasereportit.gov.bc.ca

The erase |Report It tool is powerful, effective and gives students the opportunity to have their voice heard. This tool will help reinforce the idea that we want students who see something, to say something and we'll do something!

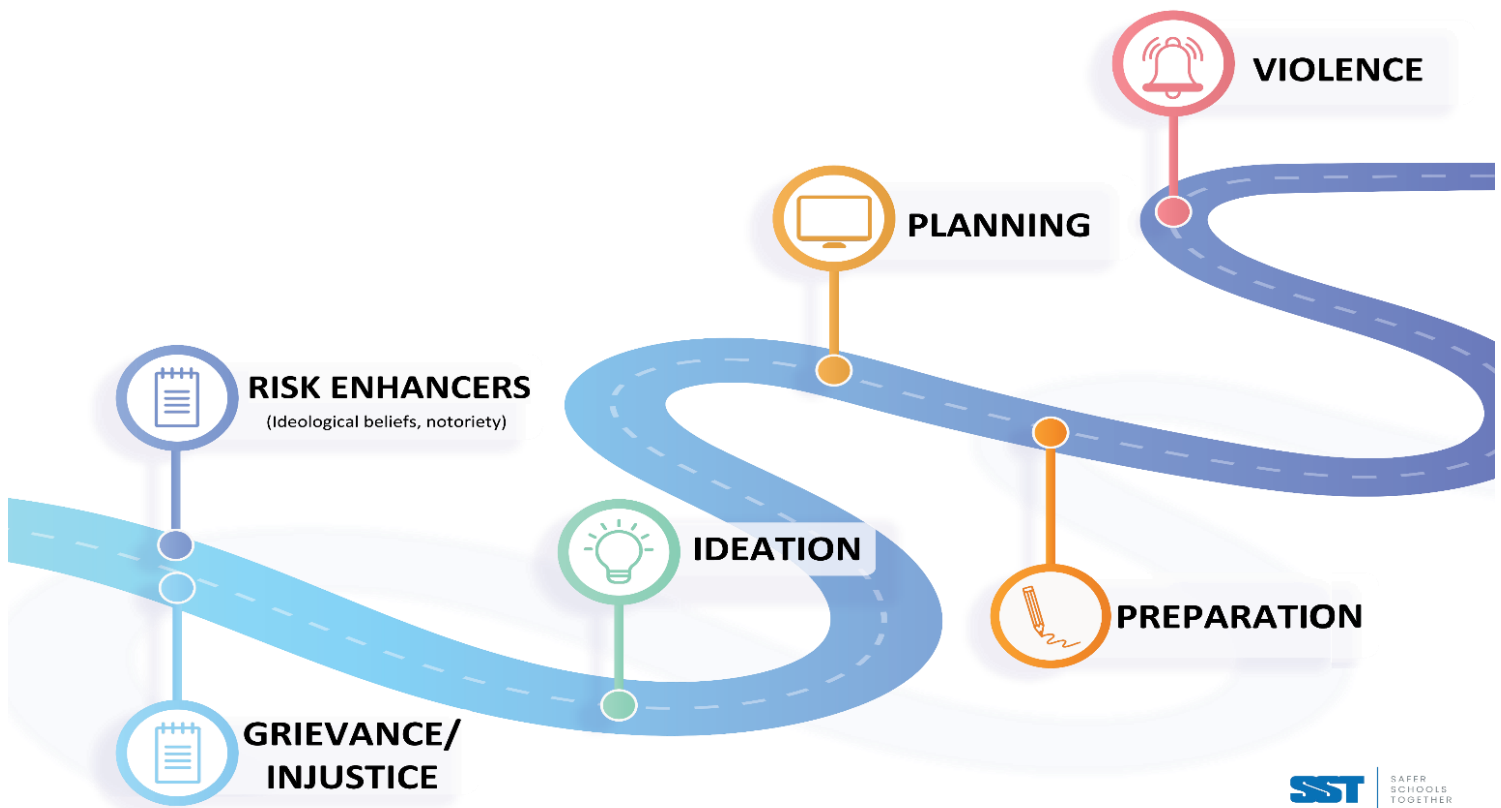
It is important that the service is easy for students to use and has all the features and security factors necessary to safeguard student identity and satisfy school staff and community concerns. Students should be made aware of the site and should have constant reinforcement regarding and how to use it.

Evolutionary Process

“One of the most important concepts in threat assessment is the idea that serious violence is an evolutionary process.” (J. Kevin Cameron)

An individual who engages in serious violence does not suddenly decide to harm someone. Their perceived grievances, behaviours and thoughts play a role in planning and preparation to complete an act of violence.

Pathway to Violence



This graphic is critical in making the distinction between making a threat (no pathway behaviours are evident) and carrying out a threat or act of violence. The goal of BDTA is to identify individuals who might be on the pathway to violence, where are they on the pathway and how do we redirect them off the pathway with successful data driven intervention and management plans.

Many pathway graphics begin with a *grievance or injustice* before ideation. We do not want Threat Assessment teams to assume that if an apparent injustice or grievance is not expressed, an individual is not capable of entering the pathway to violence. An individual can still enter onto the pathway without a grievance or expressed injustice.

Ideation is when the person begins to think about conducting an act of violence.

Planning is when they start to put together ideas of how to carry out the act of violence.

Preparation/acquisition is when the person begins to acquire the means (9mmgun, molotov cocktail bombs) and method they will use to carry out the act and figures out the best opportunity that allows them to get in close proximity to their intended targets. This could also include rehearsal behaviour.

Implementation is when the person executes their plan.

With early identification, Threat Assessment teams can successfully intervene and redirect individuals off the pathway to violence.

A series of sequential steps – from its beginning with a felt grievance, to violent ideation, research and planning, specific preparations for violence, critical breaches of security or other boundaries, to a concluding attack –indicating that an individual is progressing towards an act of targeted violence (Calhoun & Weston, 2003; Fein et al., 2002).

Grievance/Justification

An individual uses their perceived justification or grievance for carrying out a threat to rationalize the purpose and intent of committing a violent act.

Commitment

Commitment refers to one's determination to carry out an act of violence. Often pre-incident signs (e.g., leakage) indicate an individual's commitment level and provides an opportunity for intervention.

Behavioural and Digital Baseline

Determining an individual's behavioural and digital baseline is important. If the behaviour is not typical for the individual, you need to consider it to be an increase in worrisome, concerning or threat-related behaviour.

Dehumanization/Desensitization

Dehumanization or desensitization is the process of making others seem less than human and not worthy of human treatment. The SOC views other people as non-persons or objects to be thwarted. This attitude may appear in the SOC's writings and artwork, in interactions with others or in comments during conversation.

When a change in baseline behaviour occurs, it is important to pay careful attention to the increase of the **frequency, intensity and recency** of the threat-related behaviours that denote the risk is increasing.

THE IMPACT OF MOVIES, MEDIA, AND VIDEO GAMES

Consider development of hypotheses regarding the impact of movies, media, and video games:

Does a student's interest in, and involvement with, violent media play a role in the justification process? Justification is the process through which the student seeks or is given the means to justify the intended violence. We need to determine if the viewing of, or interacting with, violent media allows a student to feel justified acting out in violent ways that they have come to think of as *normal* or *acceptable*—or at the very least, *justifiable*.

The integration of violence into our value system has been heightened by technology. We have all become immune to certain levels of violence, and this is a cause for concern. Technology has proven to have a great impact on threat-making behaviours and the potential for violence. It can affect socialization, as viewing of violence in all areas of the media can create desensitization. Violent video game exposure has been linked to reduced P300 amplitudes in the brain, which is associated with desensitization to violence and an increase in aggressive behaviour.

Violent video games teach youth that violence is an acceptable conflict-solving strategy and an appropriate way to achieve one's goals. A 2009 study found that youth who play violent video games have a lower belief in the use of non-violent strategies and are less forgiving than players of non-violent video games.

Often propaganda is seen as real and affects what students view as acceptable behaviour. The effect of these views on schools and communities is significant.

Gender involvement is also significant. Female engagement with violent media is now equivalent to that of males. Classroom teachers are reporting increasing numbers of students who seem too often disengaged. Instead of being aware of the news and what is going on in the real world, students are hooked into technology. Regular viewing of violence seems to be creating lower levels of empathy and higher levels of detachment. Students who lack empathy show an inability to understand the feelings of others and appear unconcerned regarding the feelings of others.

Risk factors are emerging in relation to technology. Television, movies, video games, radio and music all have effects on the development of youth.

Before youth have established their own value systems and are able to make moral judgments, the media promotes drugs and violence as an acceptable lifestyle. This can create a sense of moral panic both in youth and the adults who are witnessing the outcomes.

Gaming disorder has been added to the World Health Organization's 11th Revision of the International Classification of Diseases (ICD-11).

Gaming disorder is defined as *a pattern of gaming behaviour (“digital-gaming” or “video-gaming”) characterized by impaired control over gaming, increasing priority given to gaming over other activities to the extent that gaming takes precedence over other interests and daily activities, and continuation or escalation of gaming despite the occurrence of negative consequences.*”

“For gaming disorder to be diagnosed, the behaviour pattern must be of sufficient severity to result in significant impairment in personal, family, social, educational, occupational or other important areas of functioning and would normally have been evident.”

ASSESSING VIOLENCE AND THREATS

Data Collection Adapted from Threat Assessment in Schools: US Secret Service and US Department of Education

The safety of the school, students, staff and community is our priority. The SOC(s) and any known targets should be immediately and safely contained under supervision with digital devices removed if possible until the threat assessment process and safety procedures have been activated.

INTERVIEWS

Threat assessment procedures should include practices for maintaining documentation, identifying sources of information, reviewing records, and conducting interviews using open-ended questions. When possible, interviews should be conducted with the SOC(s), target(s), witnesses, peer groups and parent(s)/caregiver(s).

Key considerations when you are preparing for an interview:

The Interviewer:

“An investigative, skeptical, inquisitive mindset is critical to successful threat assessment.”

Fein, V., Pollack, B., & Modzeleski, R. Threat Assessment in Schools Guide, 2002

- An investigative mindset is central to successful application of the threat assessment process.
- Thoughtful probing, viewing information with healthy skepticism and paying attention to key points regarding pre-attack behaviour are all required.
- Authorities who carry out threat assessments should strive to be accurate and fair.
- Information and data collection should be questioned continuously.
- Credible verification or corroboration of the essential facts is critical whenever possible.

Good common sense must be applied. The interviewer should step back from the situation occasionally and ask whether the information gathered makes sense and supports the hypothesis formed.

The Interviewed:

The following individuals should be interviewed when a formal threat assessment is activated: teachers and other school staff, students, target(s), SOC(s), parent(s)/guardian(s) and others.

Prior to conducting a series of interviews, beyond that of the reporter, the team should ask the following questions:

1. The first question to be asked is an overriding one: “How much time do we have?” When threats are clear, detailed and denote a specific time that is imminent, action will need to be taken to ensure the safety of possible targets. For example, a student reports after lunch that his friend said at 2:15 p.m. today, “they are going to finally bring a gun to school and blow away the freaks in math class”. In these situations, law enforcement involvement is critical and lockdown procedures may need to be implemented. When the threat is not imminent, circumstance will help the team determine who and when to engage in the strategic interviewing process. In some instances, the SOC may be among the last people to be interviewed.

Most threat assessment cases are opened as soon as the behaviours listed in the protocol come to the attention of any Threat Assessment team member.

2. The second question to be asked is, “Who will be interviewed?” It is understood that those selected for the initial interview often provide information that results in further interviews being conducted with more individuals. Threat Assessment team members need to decide who the most credible and best-informed individuals are and focus on them first.
3. The third question to be asked is, “In what order will we interview them?” If the threat is not imminent, the Threat Assessment team has the flexibility based on circumstance to decide in what order to interview. The SOC may be one of the last individuals to be interviewed if initial data suggests that the risk is low. For example, the team may want to look at credible collateral information first by talking with some of the threat maker’s teachers before interviewing the threat maker.
4. The fourth question to be asked is, “Who will interview whom?” The answer to this question will depend on circumstance and relationships between the team members and those to be interviewed. Some individuals may be interviewed one-on-one whereas the team may decide that two members should be present while interviewing others.

Depending on the severity of the case, one Threat Assessment team member may serve as the primary interviewer to ensure continuity of data collection and interviewing technique. The higher the level of potential risk, the more appropriate it is to use a primary interviewer to lead the process. When criminal charges are likely, law enforcement members of the Threat Assessment may take the lead. When mental health issues appear to be the dominant concern, the clinical member of the Threat Assessment team may take the lead.

Collateral school interviews: Both Students and Adults who know the SOC should be interviewed.

Remember they don't know what we know and always ask open ended questions. The focus of

interviews should be open-ended and factual.

Witnesses:

Below are a few open-ended questions to ask any witnesses who may have seen and/or heard the incident or worrisome behaviour:

- *What was said? To Whom? What did they say?*
- *What was written/posted? Who was it directed too?*
- *When and where did this occur? Who else was there and what did they say? If posted online, where was it posted and who else was there when it was posted?*
- *Did the SOC say why they acted as they did?*

Other Individuals that know the SOC:

- *How would you describe them?*
- *What makes them happy?*
- *What does it look like when they are mad or angry?*
- *How would you describe their life?*

Current living/home situation:

- *Describe their current living or home situation?*
- *Describe recent changes in their current living/home situation?*
- *What's it like when you hang out at their place?*
- *Can you describe any recent losses they've experienced?*

Trusted Relationships with healthy mature adults:

- *What adults do they have a health trusted relationship within our community and out of community?*
- *Who do they have current conflict/grievances with and why?*

- *Do they believe they are being treated fairly by friends, family, school, sports team, or any other groups identified?*
- *Can you tell me about any recent losses or changes in their relationships?*
- *What adult(s) do you think have a connection to them? (Coaches, certain teachers etc.)*
- *How do you feel when you're around them?*
- *What do they do in their spare time? (What are they filling themselves up with?)*
- *How would you describe the nature of the quality of their relationships overall? Supportive etc.*

THREAT ASSESSMENT: INTERVENTION AND MANAGEMENT

Threat Assessment teams should use the data from the threat assessment to design and develop a management plan to mitigate risk and provide a successful intervention strategy and supports.

The intervention/management plan may include but is not limited to:

- Monitoring of the student within the school (identified needs)
- Locker, backpack, and digital dynamics
- Participation in the local diversion programs and restorative practices
- Local law enforcement agency involvement
- Maintaining connections with identified staff
- Other community agency involvement
- No contact agreements

Guidelines for Re-Entry into School

When data suggests that a student poses a threat to others, they may be suspended from school until a more comprehensive threat assessment can be conducted. Threat Assessment teams guide the process from screening to planning interventions to decrease risk, to planning for re-entry into a school when a suspension has occurred. This is best accomplished when Threat Assessment teams outline in writing, steps the student, family, school, and others need to follow to ensure appropriate assessment is conducted prior to re-entry into the school. Following the completion of necessary assessments, the initial Threat Assessment team members may work with the student and parent(s)/guardian(s) to develop a plan for re-entry that becomes a signed contract by all participants, including the student and parent(s)/guardian(s), if circumstances warrant.

Supportive Services

Each of the Threat Assessment team members need to have the authority within their own organization to make immediate decisions about supportive services. For example, it may be necessary to provide secure residential treatment, psychiatric hospitalization, or increased supervision in the school setting. It is also important to ensure that the support services and interventions extended to the student and family are culturally appropriate and/or accessible within the context of the limitations of the community. Recommending services that are not readily available or accessible can add to the level of anxiety and risk inherent in the family structure.

Supporting Targeted or Victimized Students or Staff

The Threat Assessment clinician—psychologist, therapist, or counsellor—should be responsible to ensure that the recipients or targets of the SOC’s threats/behaviours are assessed and that services are provided as necessary. As the threat may be directed towards one or more students, an entire class, or the school population in general, the circumstances will dictate how far-reaching an intervention may be. The Threat Assessment clinician (e.g., counsellor) and the school administrator should determine if crisis counselling or a crisis response team is needed to re-establish calm.

Key Point: There may be cases where the recipient of a threat has been engaged in high-risk behaviours that lead to the threat(s) in the first instance. In those situations, the recipient of the threat(s) may need to be assessed for high-risk behaviour as well.

To learn effectively, students need to feel secure and accepted. And staff members, too, have the right to feel safe and secure as they carry out their professional responsibilities

Baldwin, J.D., & Baldwin, J.I., 1986

SCHOOL AND LAW ENFORCEMENT INVESTIGATIONS

Law enforcement Involvement in Student Interviews

Unnecessary publicity regarding threats of violence can hamper an investigation and cause emotional distress for targets or witnesses. It can also frustrate attempts to intervene and de-escalate a threat, and lead to inaccurate or harmful information circulating in the community.

When being interviewed by law enforcement, a student who is a SOC, a target or a witness may request that an adult be present, although this may not always be possible.

In situations when interviews by law enforcement take place at the school, the school will strive to maintain low- profile interactions between students and law enforcement. The principal should ensure that an appropriate setting is available. Investigations involving law enforcement interviews with students require special sensitivity.

Law enforcement interviews on school premises should observe the following guidelines:

SOC

- A parent/guardian of an SOC must be notified, except in situations that would compromise safety and the integrity of an investigation.

Target or witness

- Parent(s)/guardian(s) of targets or witnesses should be notified, as soon as practical, that their child has been interviewed in connection with a threat assessment.
- At law enforcement discretion, and with the student's consent, school personnel may be present for the interview to provide support to a student who is a target or witness.

Search and Seizure

Remember:



Laws give both schools and law enforcement authority for search and seizure in certain circumstances. The School Regulation, section 5 (7), provides that the principal is responsible for administering and supervising the school, including the general conduct of students and the discipline of students. This section of the school regulation provides authority for searching a student's locker and desk, both for gathering evidence for use in the prosecution of a criminal charge and for ensuring the safety of the school, students, and staff.

Common law, statute law and the Charter of Rights and Freedoms provide law enforcement with authority for search and seizure. The protection against unreasonable search and seizure depends on assessing all the circumstances, including the Charter. In general, the validity of a search or seizure takes into consideration the following:

- The expectation of privacy
- Whether the conduct amounted to a search and/or seizure
- Whether the search and/or seizure was reasonable

Locker and Bedroom Dynamics Need to Include Digital Devices

Evidence of planning has been found in either the SOC's locker or computer at school, their bedroom and digital devices. Where there are reasonable grounds to suspect that a student is planning to compromise the safety of other students, the school, or the staff, school administration can search a locker, backpack etc. for evidence of pre-planning, or the means to carry out the threat. It is the responsibility of the principal to advise students that desks and lockers are school property and that, in certain circumstances, a search of that property may be performed by the school administration. Law enforcement can search a person incidental to arrest or detention for safety but would require a warrant for a locker search.

Evidence of planning may also be found in desks, textbooks, student vehicles, etc. The more committed an individual is to carry out an offense without being caught, the more likely they may hide weapons, journals of justifications, maps, floor plans, etc., elsewhere in the home and surrounding property as part of what is referred to as attack-related behaviours.

Search of Vehicles on School Property

Items that raise a concern in a vehicle on school property might come to the notice of school personnel. In such a case, they should contact law enforcement. There may be legal issues regarding the right to search and seizure a vehicle unless an imminent threat is apparent.

If school personnel view items that raise concerns in a vehicle, they should contact law enforcement. If there is no imminent threat, they should attempt to monitor the situation until law enforcement provide further direction.

Social Media Evidence and Digital Data Searches

Evidence and data are often found on digital devices. Schools can request searches of student digital devices, but students can refuse to comply. Schools and school districts can only undertake the collection of digital information in compliance with privacy laws. It is important to preserve and protect evidence by ensuring steps are taken to deactivate remote erase capabilities of devices. Screenshots of images or posts of publicly available online data with time and date stamp embedded are always preferable.

There is no expectation of privacy regarding content that has been posted publicly on social media with no user privacy settings restricting view. The evaluation of publicly posted digital data and data on devices may be essential to an assessment of risk. Information collected as part of a threat assessment should be provided to law enforcement agencies. Law enforcement agencies employ technological crime experts who can assist. Forensic searches of devices may be necessary, but they can take time.

School personnel should report to law enforcement any threat-related information that they find on digital devices as part of a threat assessment.

School personnel should take steps to preserve and protect evidence found on digital devices. Whenever feasible, they should save screenshots of images or posts of publicly available online data with time and date stamp embedded.

Preservation Orders and Production Orders

Law enforcement can obtain preservation orders to require private companies to preserve and retain data that is related to an investigation.

Production orders are used when law enforcement may be required to gather evidence of subscriber data from social media providers, such as files involving statements made on Facebook. A production order is a type of search warrant that can compel a social media provider to produce documentation to a specified law enforcement officer, at a specified time and place. There must be reasonable grounds to believe an offence has been, or is suspected to have been, committed and the document or data will afford evidence of the offence.

Digital Searches in Exigent Circumstances

Exigent circumstances exist when there is a threat of imminent bodily harm or death to a person, or imminent

loss or destruction of evidence. Investigating officers are permitted to intervene, and search and seize without a warrant, in exigent circumstances.

Exigent circumstances can also exist when assessing online threats or dangerous situations. Investigating officers must decide if an imminent threat exists. For example, exigent circumstances may justify a digital search and seizure if a student makes an online threat with a Facebook photo showing a gun and a threat to use it that day.

Law enforcement investigators can use the power authorized in exigent circumstances to search, seize and preserve digital evidence without a warrant when required.

In an investigation that involves digital evidence, law enforcement investigators should consider obtaining a preservation order requiring social media companies to preserve digital information relating to an offence.

Report to Crown Counsel

If law enforcement decides to recommend a charge against an accused, the officer will complete a detailed Report to Crown Counsel (RTCC). Law enforcement may need statements by school staff to complete the RTCC.

Crown Counsel will review the RTCC and will decide whether to lay charges. Crown Counsel may also decide to refer the matter to extrajudicial alternate measures for non-violent offences under the Youth Criminal Justice Act, such as a caution or a referral to a specialized program.

Law enforcement agencies should liaise with the Threat Assessment team and school staff to investigate the circumstances of a threat, to assess possible charges, and to consider whether a recommendation for alternate measures would be in the best interests of the school community and the SOC.

Some Common Criminal Code Offences Involving Young People, Among Others, Include:

- Uttering Threats – Criminal Code (R.S.C., 1985, c. C-46) S 264.1
- Conspiracy to Commit Murder – Criminal Code (R.S.C., 1985, c. C-46) S 465
- Possession of Weapons – Criminal Code (R.S.C., 1985, c. C-46) S 92 (1) & (2)
- Counselling Indictable Offence that is not committed - Criminal Code (R.S.C., 1985, c. C-46) S 464(a)
- Assault with a Weapon or Causing Bodily Harm - Criminal Code (R.S.C., 1985, c. C-46) S 267

Youth Criminal Justice Act

Youths may be arrested by law enforcement for more serious offences. The rights expressed in the Canadian Charter of Rights and Freedoms apply to youths and adults.

“Youths and adults have the right to obtain immediate legal counsel of their own choice upon arrest or detention. The youth offender also has the right to have his or her parent(s)/guardian(s) present during questioning. Upon arrest or detainment, these rights must be explained in clear and understandable language. If law enforcement have violated the above rights, the charges may be dismissed by a judge, or any statements

made to law enforcement may be ruled inadmissible by the judge in court.”

Disclosure of Information Regarding a Young Person

Although records of a young person are protected, s. 125 (YCJA) indicates some situations when disclosure may be applicable and the means in which this is accomplished. Namely, the disclosure by peace officer during investigation whereby in s. 125(1) “A peace officer may disclose to any person any information in a record kept under section 114 (court records) or 115 (law enforcement records) that it is necessary to disclose in the conduct of the investigation of an offence.”

Further, in reference to disclosure of information to those person(s) listed in s. 125(6) *“The provincial director, a youth worker, the Attorney General, a peace officer or any other person engaged in the provision of services to young persons may disclose to any professional or other person engaged in the supervision or care of a young person—including a representative of any school board or school or any other educational or training institution—any information contained in a record kept under sections 114 to 116 if the disclosure is necessary”*

- a) to ensure compliance by the young person with an authorization under section 91 or an order of the youth justice court.
- b) to ensure the safety of staff, students, or other persons; or
- c) to facilitate the rehabilitation of the young person

Youth Court Record vs. Law Enforcement Records

A record of proceedings under the *Youth Criminal Justice Act* can be kept by both the courts and law enforcement.

Law enforcement can keep the following records:

- a) A record of any offence alleged to have been committed by a young person, and
- b) A record of any extrajudicial measure used to deal with a young person. Youth records are kept as follows:
 - i. **Canadian Law Enforcement Information Centre (CPIC):** the only national offender database which records data from within the formal justice system.
 - ii. **Justin:** a provincial (BC) offender database which records data from within the formal provincial justice system.
 - iii. **Prime:** a national offender database which records data from law enforcement contact.

The YCJA has strict control over the keeping and use of information pertaining to a young person and has set strict rules to ensure that the privacy of a young person is protected while at the same time balancing the need for access to information to ensure an effective and efficient youth justice system. There is a general prohibition for anyone to access records kept. The exceptions to this rule are set out in s. 119 YCJA and include but are not limited to the Attorney General and any peace officer for law enforcement purposes. There are also rules relating to the length of time that access is permitted – generally, the more serious the offence, the longer the period of access. Once the access period has expired, the Youth Court record is

sealed. There are limited circumstances in which information may be accessed even after the record is sealed.

Prime records remain visible to law enforcement even after the offender becomes an adult. There are, however, restrictions on the use of this information.

Peace Bond

A judge can issue a peace bond, also known as a Section 810 recognizance, requiring a person to keep the peace and be of good behaviour. The peace bond can prohibit the person named from contact with certain individuals and from carrying weapons. A peace bond can be valuable when investigating a threat or intervening with a SOC.

Usually, law enforcement recommends a charge for a substantive offence. The Crown may request that a judge issue a peace bond. In rare circumstances, law enforcement may request a peace bond directly.

When recommending a charge for an offence, law enforcement should consider recommending that Crown apply for a peace bond if they believe that it would be useful in dealing with a SOC.

Additional Sources

Provinces and states have legislation that permits information sharing under circumstances where there is imminent danger. It is important to review relevant legislation in your own province or state to ensure adherence while providing for workplace, school, and community safety.

Release

A person in custody can be released with or without conditions. An appropriate set of release conditions can help reduce risks to the school community. Law enforcement can recommend conditions in the Report to Crown Counsel for the Crown to present to the judge or justice.

If a SOC is in custody, law enforcement should consider making a recommendation to Crown Counsel regarding release conditions to reduce risks to the school community.

Threat Assessment Documentation and Record Keeping

Documentation of Threat Assessments, in addition to individually administered aptitude tests, confidential reports, and other sensitive materials, are personal information subject to the Freedom of Information and Protection of Privacy Act and the Personal Information Protection Act. They may also be evidence in legal proceedings. As such, they should be maintained in a secure and confidential folder.

The Threat Assessment team should place all reports and other sensitive material or documents in a folder under supervision of the school principal or designate of the superintendent. The school or school district should retain the records in accordance with its records management policies.

BUILDING A BEHAVIOURAL AND DIGITAL THREAT MANAGEMENT PLAN

Creating a Comprehensive Violence Prevention Plan

The National Threat Assessment Center – US Secret Service and the US Department of Homeland Security identify.

8 steps of a comprehensive school-based violence prevention plan that are addressed in the Behavioural and Digital Threat Assessment Management (BDTAM).

1. Establish a multidisciplinary Threat Assessment team.
2. Define behaviours.
3. Establish and provide training on a central reporting system.
4. Determine the threshold for law enforcement.
5. Establish threat assessment procedures.
6. Develop risk management options.
7. Create and promote a safe school climate.
8. Provide training for all stakeholders.

Secret Service/NTAC Investigative Themes

**Excerpt from: Dr. Melissa A. Louvar Reeves (2021). Adapted from Fein et al (2004).*

A threat assessment inquiry should seek to answer the key questions below identified by the Secret Service. BTAM teams need to examine all evidence for behaviours and conditions that suggest the individual of concern POSES a threat by planning and preparing for an act of violence or to cause harm to self or others.

1. What are the subject's motive(s) and goals?/What first brought him/her to someone's attention?

- Does the subject have a major grievance or grudge? Against whom?
- Does the situation or circumstance that led to these statements or actions still exist?
- What efforts have been made to resolve the problem and what has been the result?
- Does the subject feel that any part of the problem is resolved or see any alternatives?
- Has the subject previously come to someone's attention or raised concern in a way that suggested he or she needs intervention or supportive services?

2. Have there been any communications suggesting ideas, intent, planning, or preparation for violence?

- What, if anything, has the subject communicated to someone else (targets, friends, co-workers, others) or written in a diary, journal, email, or Web site concerning his or her grievances, ideas

and/or intentions?

- Do the communications provide insight about ideation, planning, preparation, timing, grievances, etc.?
- Has anyone been alerted or “warned away”?

3. Has the subject shown any inappropriate interest in, fascination, and/or identification with other incidents of mass or targeted violence (e.g., terrorism, rampage violence, school/workplace shootings, mass murderers)?

- Previous perpetrators of targeted violence
- Grievances of perpetrators
- Weapons/tactics of perpetrators
- Effect or notoriety of perpetrators

4. Has the student engaged in attack-related behaviours?

- Developing an attack idea and plan
- Making efforts to acquire or practice with weapons
- Investigating possible sites
- Rehearsal

5. Does the subject have (or are they developing) the capacity to carry out an act of targeted violence? Does the SOC have access or is trying to get access to weapons, explosives, and incendiary devices?

- How organized is the subject’s thinking and behaviour?
- Does the subject have the means (e.g., access to a weapon) to carry out an attack?
- Are they trying to get the means to carry out an attack?
- Have they developed the will and ability to cause harm?
- Are they practicing or rehearsing for the violence?
- What is the “intensity of effort” expended in attempting to develop the capability?

6. Is the subject experiencing hopelessness, desperation, and/or despair?

- Is there information to suggest that the subject is feeling desperation and/or despair?
- Has the subject experienced a recent failure, loss and/or loss of status?
- Is the subject having significant difficulty coping with a stressful event?
- Has the subject engaged in behaviour that suggests that he or she has considered ending their life?

7. Does the subject have a positive, trusting, sustained relationship with at least one responsible person?

- Does the subject have at least one friend, colleague, family member, or other person that he or she

trusts and can rely upon for support, guidance, or assistance?

- Is that trusted person someone that would work collaboratively with the team for the well-being of the SOC?
- Is the subject emotionally connected to other people or becoming more socially isolated?

8. Does the subject see violence as an acceptable, desirable – or the only – way to solve a problem?

- Does the subject identify alternatives to violence to address their grievances?
- Does the setting around the subject (friends, colleagues, family members, others) explicitly or implicitly support or endorse violence as a way of resolving problems or disputes?
- Has the subject been “dared” by others to engage in an act of violence?
- Has the subject expressed sentiments of finality or desperation to address grievances?

9. Are the subject’s conversation and “story” consistent with their actions?

- Does information from collateral interviews and from the subject’s own behaviour confirm or dispute what the subject says is going on and how they are dealing with it?
- Is there corroboration across sources or are the subject’s statements at odds with their actions?

10. Are other people concerned about the subject’s potential for violence?

- Are those who know the subject concerned that he or she might take action based on violent ideas or plans?
- Are those who know the subject concerned about a specific target?
- Are persons around the subject engaging in protective actions (e.g., distancing, avoiding, minimizing conflict, etc.)?

11. What circumstances/stressors might affect the likelihood of an escalation to violent behaviour? Does the SOC have an emotional and/or developmental issue that may impact behaviour or decision making?

- What events or situations in the subject’s life (currently or in the near future) may increase or decrease the likelihood that the subject will engage in violent behaviour?
- Are threat assessment team interventions escalating, de-escalating, or having no effect on movement toward violence?
- What is the response of others who know about the subject’s ideas or plans?
- Actively discourage subject from acting violently,
- Encourage the subject to attack
- Deny the possibility of violence, and/or
- Passively collude with an attack, etc.?

FBI 4-Prong Model

The following is based on the Federal Bureau of Investigations *“The School Shooter: A Threat Assessment*

Perspective.”

Behavioural and Digital Threat Assessment Management is designed to assess an individual who has made a threat and to evaluate the likelihood that the threat will actually be carried out. Anyone can deliver a spoken or written message that sounds sinister but evaluating the threat alone will not establish whether the person making it has the intention, the ability or the means to act on the threat.

To make that determination, conducting a multi-disciplinary Threat Assessment is vital.

This section lists certain types of behaviour, personality traits and circumstances in the family, school and community environment. These should be regarded as warning signs if all or most of them—in all four categories—seem to fit a student who has made a threat.

It should be strongly emphasized that this list is not intended as a checklist to predict future violent behaviour by a student who has not acted violently or threatened violence. The list should be considered *only* after a student has made some type of threat.

No one or two traits or characteristics should be considered in isolation or given more weight than the others. Any of these traits, or several of these traits, can be seen in students who are not contemplating a school shooting or other act of violence.

Behaviour is an expression of personality. One bad day may not reflect an individual’s real personality or usual behaviour pattern. Accurately evaluating someone’s behaviour requires establishing a baseline of how he or she typically behaves most of the time. Those responsible for assessing a student should seek information from those who have known the student over a period of time and who have been able to observe the individual in varying situations and with a variety of people.

Many of the behaviours and traits listed below are seen in depressed adolescents with narcissistic personality characteristics and other mental health problems. Signs of serious mental illness and/or substance abuse disorders can significantly elevate the risk for violence and should be evaluated by a mental health professional.

This model provides a framework for evaluating the SOC to determine if he or she has the motivation, means and intent to carry out the stated threat.

The assessment is based on the totality of what is known about the student in four major areas:

Prong One: Personality of the student

Prong Two: Family dynamics

Prong Three: School dynamics and the student’s role in those dynamics

Prong Four: Social dynamics

In the data collection stage of Threat Assessment, the team quickly collects as much information as is available in the four categories.

The following section outlines factors to be considered in each of the four prongs:

Prong One: Personality of the Student

Personality shapes how people consistently view the world and themselves and how they interact with others.

Forming an accurate impression of someone's personality requires observing their behaviour over a period of time and in a wide variety of situations.

Clues to a student's personality come from observing behaviour when the student is:

- Coping with conflicts, disappointments, failures, insults, or other stresses encountered in everyday life.
- Expressing anger or rage, frustration, disappointment, humiliation, sadness, or similar feelings.
- Demonstrating or failing to demonstrate resiliency after a setback, a failure, real or perceived criticism, disappointment, or other negative experiences.
- Demonstrating how the student feels about himself, what kind of person the student imagines himself or herself to be, and how the student believes he or she appears to others.
- Responding to rules, instruction, or authority figures.
- demonstrating and expressing a desire or need for control, attention, respect, admiration, confrontation, or other needs.
- Demonstrating or failing to demonstrate empathy with the feelings and experiences of others.
- Demonstrating his or her attitude toward others—for example, does the student view others as inferior or with disrespect? Assessors who have not been able to observe a student firsthand should seek information from those who knew the student before they made a threat.

Behavioural characteristics and traits to be aware of:

Low Tolerance for Frustration: The student is easily bruised, insulted, angered, and hurt by real or perceived injustices done to him/her by others and has great difficulty tolerating frustration.

Poor Coping Skills: The student consistently shows little, if any, ability to deal with frustration, criticism, disappointment, failure, rejection, or humiliation. Their response is typically inappropriate, exaggerated, immature or disproportionate.

Lack of Resiliency: The student lacks resiliency and is unable to bounce back even when some time has elapsed since a frustrating or disappointing experience, a setback or putdown.

Failed Love Relationship: The student may feel rejected or humiliated after the end of a love relationship and cannot accept or come to terms with the rejection.

Injustice Collector: The student nurse's resentment over real or perceived injustices. No matter how much time has passed, the *injustice collector* will not forget or forgive those wrongs or the people he or she believes are responsible. The student may keep a hit list with the names of people the student feels have wronged him/her.

Signs of Depression: The student shows features of depression such as lethargy, physical fatigue, a morose or dark outlook on life, a sense of malaise and loss of interest in activities that they once enjoyed.

Adolescents may show different signs than those normally associated with depression. Some depressed adolescents may display unpredictable and uncontrolled outbursts of anger, a generalized and excessive hatred toward everyone else and feelings of hopelessness about the future. Other behaviours might include psychomotor agitation, restlessness, inattention, sleep and eating disorders and a markedly diminished interest in almost all activities that previously occupied and interested them. The student may have difficulty articulating these extreme feelings.

Narcissism: The student is self-centered, lacks insight into other's needs and/or feelings and blames others for failures and disappointments. The narcissistic student may embrace the role of a victim to elicit sympathy and to feel temporarily superior to others. They display signs of paranoia and assumes an attitude of self-importance or grandiosity that masks feelings of unworthiness (Malmquist, 1996). A narcissistic student may be either very thin-skinned or very thick-skinned in responding to criticism.

Alienation: The student consistently behaves as though they feel different or estranged from others. This sense of separateness is more than just being a loner. It can involve feelings of isolation, sadness, loneliness, not belonging and not fitting in.

Dehumanizes Others: The student consistently fails to see others as fellow human beings. The student characteristically views other people as non-persons or objects to be thwarted. This attitude may appear in the student's writings and artwork, in interactions with others or in comments during conversation.

Lack of Empathy: The student shows an inability to understand the feelings of others and appears unconcerned about anyone else's feelings. When others show emotion, the student may ridicule them as weak or stupid.

Exaggerated Sense of Entitlement: The student constantly expects special treatment and consideration and reacts negatively if not receiving the treatment they feel entitled to.

Attitude of Superiority: The student has a sense of being superior and presents himself/herself as smarter, more creative, more talented, more experienced, and more worldly than others.

Exaggerated or Pathological Need for Attention: The student shows an exaggerated, even pathological need for attention, whether positive or negative, no matter what the circumstances.

Externalizes Blame: The student consistently refuses to take responsibility for his/her own actions and typically faults other people, events or situations for any failings or shortcomings. In placing blame, the student frequently seems impervious to rational argument and common sense.

Masks Low Self-Esteem: Though the student may display an arrogant, self-glorifying attitude, conduct often appears to veil an underlying low self-esteem. The student avoids high visibility or involvement in school activities, and other students may consider him/her a non-entity.

Anger Management Problems: Rather than expressing anger in appropriate ways and in appropriate circumstances, the student consistently tends to burst out in temper tantrums or melodramatic displays or to brood in sulky, seething silence. The anger may be noticeably out of proportion to the cause or may be

redirected toward people who have nothing to do with the original incident. The anger may come in unpredictable and uncontrollable outbursts and may be accompanied by expressions of unfounded prejudice, dislike or even hatred toward individuals or groups.

Intolerance: The student often expresses racial or religious prejudice through intolerant attitudes toward minorities. Slogans or symbols of intolerance may be displayed through such things as tattoos, jewelry, clothing, bumper stickers, or book covers.

Inappropriate Humor: The student's humor is consistently inappropriate. Jokes or humorous comments tend to be macabre, insulting, belittling or mean.

Seeks to Manipulate Others: The student consistently attempts to con and manipulate others and win their trust so they will rationalize any signs of aberrant or threatening behaviour.

Change of Behaviour: The student's behaviour changes dramatically. Academic performance may decline, or reckless disregard for school rules, schedules, dress codes and other regulations may appear.

Unusual Interest in Sensational Violence: The student demonstrates an unusual interest in school shootings and other heavily publicized acts of violence. They may declare admiration for those who committed the acts or may criticize them for incompetence or failing to kill enough people. The student may explicitly express a desire to carry out a similar act in his own school, possibly as an act of justice.

Fascination with Violence-Filled Entertainment: The student demonstrates an unusual fascination with movies, TV shows, computer games, music videos or printed material that focus intensively on themes of violence, hatred, control, power, death, and destruction. They may incessantly watch one movie or read and reread one book with violent content, perhaps involving school violence. Themes of hatred, violence, weapons, and mass destruction recur in virtually all activities, hobbies and pastimes.

The student spends inordinate amounts of time playing video games with violent themes and seems more interested in the violent images than in the game itself.

The student regularly searches for websites involving violence, weapons, and other disturbing subjects. There is evidence the student has downloaded and kept material from these sites.

Negative Role Models: The student may be drawn to negative and inappropriate role models such as Hitler, Satan or others associated with violence and destruction.

Behaviour Appears Relevant to Carrying Out a Threat: The student appears to be increasingly occupied in activities that could be related to carrying out a threat. For example, the student may spend unusual amounts of time practicing with firearms or on various violent websites. The time spent in these activities has noticeably begun to exclude normal everyday pursuits such as homework, attending classes, going to work and spending time with friends.

Prong Two: Family Dynamics

Family dynamics are patterns of behaviour, thinking, beliefs, traditions, roles, customs, and values that exist in a family.

When a student has made a threat, knowledge of the dynamics within the student’s family, and the way those dynamics are perceived by both the student and the parent(s)/guardian(s), is a key factor. It is essential to understand the circumstances and stresses in the student’s life that could play a role in any decision to carry out the threat.

Assessors need to be aware of, and take into consideration the following:

Turbulent Parent/Guardian-Child Relationship: The student’s relationship with parent(s)/guardian(s) is particularly difficult or turbulent. This difficulty or turbulence can be uniquely evident following a variety of factors including recent or multiple moves, loss of a parent/guardian, addition of a stepparent and other factors. The student expresses contempt for his/her parent(s)/guardian(s) and dismisses or rejects his or her role. There is evidence of violence occurring within the student’s home.

Acceptance of Pathological Behaviour: Parent(s)/guardian(s) do not react to behaviour that most parent(s)/guardian(s) would find very disturbing or abnormal. They appear unable to recognize or acknowledge problems with their child and respond quite defensively to any real or perceived criticism of their child. If contacted by school officials or staff about the child’s troubling behaviour, the parent(s)/guardian(s) appear unconcerned, minimize the problem, or reject the reports altogether, even if the child’s misconduct is obvious and significant.

Access to Weapons: The family keeps guns or other weapons or explosive materials in the home, and these items are accessible to the child. More important, weapons are treated carelessly, without normal safety precautions. For example, guns are not locked away and are left loaded. Parent(s)/guardian(s) or a significant role model may handle weapons casually or recklessly and, in doing so, may convey to the child that a weapon can be a useful and normal means of intimidating someone else or settling a dispute.

Lack of Intimacy: The family appears to lack intimacy and closeness. The family has moved frequently and/or recently.

Student Rules the Roost: The parent(s)/guardian(s) set few or no limits on the child’s conduct and regularly give in to his/her demands. The child insists on an inordinate degree of privacy, and parent(s)/guardian(s) have little information about his/her activities, school life, friends, or other relationships.

The parent(s)/guardian(s) seem intimidated by the child. They may fear the child will attack them physically if they confront or frustrate him/her. They may be unwilling to face an emotional outburst, or they may be afraid that upsetting the child will spark an emotional crisis. Traditional family roles are reversed. For example, the child acts as if they were the authority figure while the parent(s)/guardian(s) act as if they were the children.

No Limits or Monitoring of TV and Internet: Parent(s)/guardian(s) do not supervise, limit, or monitor the child’s television watching or use of the Internet. The child may have a TV in his/her own room or is otherwise free to spend as much time as desired watching violent or otherwise inappropriate shows. The child spends a great deal of time watching television rather than involved in activities with family or friends.

Similarly, parent(s)/guardian(s) do not monitor computer use or Internet access. The child may know much more about computers than the parent(s)/guardian(s) do, and the computer may be considered off limits to the

parent(s)/guardian(s). The student may be secretive about computer use, which may involve violent games or Internet research on violence, weapons, or other disturbing subjects.

Prong Three: School Dynamics

School dynamics are patterns of behaviour, thinking, beliefs, customs, traditions, roles, and values that exist in a school's culture. Some of these patterns can be obvious and others subtle.

The relationship between school dynamics and threat assessment has not been empirically established. Its level of significance can either increase or decrease depending upon additional research into these relationships.

While it may be difficult for educators/assessors to critique their own school, it is necessary to have some level of understanding of the dynamics in the school. The school ultimately can become the scene of the crime.

Identifying those behaviours, which are formally or informally valued and rewarded in a school, helps explain why some students get more approval and attention from school authorities and have more prestige among their fellow students. It can also explain the role a particular student is given by the school's culture and the way the student may see himself/herself fitting in or failing to fit in with the school's value system.

Students and staff may have very different perceptions of the culture, customs, and values in their school. Assessors need to be aware of how a school's dynamics are seen by students. A big discrepancy between the students' perceptions and the administration's perceptions can be a significant piece of information for the assessor.

Assessors need to be aware of, and take into consideration the following:

Student's Attachment to School: Student appears to be *detached* from school, including other students, teachers, and school activities.

Tolerance for Disrespectful Behaviour: The school does little to prevent or punish disrespectful behaviour between individual students or groups of students. Bullying is part of the school culture and school authorities seem oblivious to it, seldom or never intervening, or doing so only selectively. Students frequently act in the roles of bully, victim, or bystander. Sometimes the same student plays different roles in different circumstances. The school atmosphere promotes racial or class divisions or allows them to remain unchallenged.

Inequitable Discipline: The use of discipline is inequitably applied or has the perception of being inequitably applied by students and/or staff.

Inflexible Culture: The school's culture, official and unofficial patterns of behaviour, values and relationships among students, teachers, staff, and administrators is static, unyielding, and insensitive to changes in society and the changing needs of newer students and staff.

Pecking Order among Students: Certain groups of students are officially or unofficially given more prestige and respect than others. Both school officials and the student body treat those in the high prestige groups as though they are more important or more valuable to the school than other students.

Code of Silence: A code of silence prevails among students. Few feel they can safely tell teachers or administrators if they are concerned about another student's behaviour or attitudes. Little trust exists between students and staff.

Unsupervised Computer Access: Access to computers and the Internet is unsupervised and unmonitored. Students can use the school's computers to play violent computer games or to explore inappropriate websites, such as those that promote violent hate groups or give instructions for bomb making.

Parental/Guardian Denial: Parent/guardian firmly believes there are NO issues with their child and perceives the schools and other agencies are picking on him/her.

Prong Four: Social Dynamics

Social dynamics are patterns of behaviour, thinking, beliefs, customs, traditions, and roles that exist in the larger community where students live. These patterns impact the students' behaviours, feelings about themselves, outlook on life, attitudes, perceived options, and lifestyle practices.

An adolescent's beliefs and opinions, choices of friends, activities, entertainment and reading material, and attitudes toward such things as drugs, alcohol, and weapons, will all reflect in some fashion the social dynamics of the community where they live and goes to school.

Within the larger community, an adolescent's peer group plays an especially crucial role in influencing attitudes and behaviour. Information about a student's choice of friends and relationships with peers can provide valuable clues to his/her attitudes, sense of identity and possible decisions about acting or not acting on a threat.

Assessors need to be aware of the following influences:

Media, Entertainment and Technology: The student has easy and unmonitored access to movies, television shows, computer games and Internet sites with themes and images of extreme violence.

Peer Groups: The student is intensely and exclusively involved with a group who share a fascination with violence or extremist beliefs. The group excludes other who do not share its interests or ideas. As a result, the student spends little or no time with anyone who thinks differently and is shielded from the *reality check* that might come from hearing other views or perceptions.

Drugs and Alcohol: Knowledge of a student's use of drug and alcohol and attitude toward these substances can be important. Any changes in behaviour involving these substances can also be important.

Outside Interests: A student's interests outside of school are important to note, as they can mitigate the school's concern when evaluating a threat or can increase the level of concern.

The Copycat Effect (Imitator rather than Innovator): School shootings and other violent incidents that receive intense media attention can generate threats or copycat violence elsewhere. Copycat behaviour is very common. Anecdotal evidence strongly indicates that threats increase in schools nationwide after a shooting has occurred anywhere in North America. Students, teachers, school administrators and law enforcement officials should be more vigilant in noting disturbing student behaviour in the days and weeks or even several

months following a heavily publicized incident elsewhere in the country.

CONCLUSION

Behavioural and Digital Threat Assessment (BDTA) incorporates best practices in the international field of Threat Assessment. BDTA includes a Three-Step Threat Assessment Response Plan to ensure all worrisome, concerning, and threat-related behaviours are responded to in an initial assessment, a comprehensive multidisciplinary data collection and assessment if there is an intent to harm and an intervention and management plan, including follow-up and review.

Violence prevention, multidisciplinary/multiagency threat assessment and ensuring a safe and caring school climate and culture are integral components of BDTA. In particular, understanding what constitutes worrisome, concerning, and threat-related behaviours help school staff and others pay attention to subtle signs and indicators that a SOC may be at risk of harming themselves or others.

Most threat assessment cases involve technology, such as Facebook, the Internet, YouTube, TikTok, texting or other channels in some way. We want to be proactive in intervening in worrisome, concerning and threat-related behaviours before they escalate to violence or suicide. Good collaboration between school, parent(s)/guardian(s), and law enforcement is essential in addressing issues that may seem unconnected but are part of an ongoing situation that occurs in person, online or in the community. Parent(s)/guardian(s) and professionals need to understand that some issues start at school and finish in the community. They also need to realize that many issues, including inappropriate internet use and texting, may begin at home and end at school.

Ensuring safe and caring schools requires far more than just threat assessment procedures. It requires evidence-based, preventative safe school culture/climate initiatives, connectedness, commitment to restorative practice, ongoing training, and refinement of all policies, procedures and protocols that promote socially responsible behaviour.