Unveiling Digital Traces: Understanding Leakage and Threats of Violence in K-12 Environments

by

Angi Meyer

A dissertation accepted and approved in partial fulfillment of the

requirements for the degree of

Doctor of Educational Leadership

in Educational Leadership

Dissertation Committee:

Dr. P. Shawn Irvin, Chair

Dr. Lina Shanley, Core Member

Dr. Jen Doty, Institutional Representative

University of Oregon

Spring 2025

DISSERTATION ABSTRACT

Angi Meyer

Doctor of Education in Educational Leadership

Title: Unveiling Digital Traces: Understanding Leakage and Threats of Violence in K-12 Environments

The increasing prevalence of school violence, particularly school shootings, presents a significant challenge for educational institutions and policymakers. This dissertation explored the potential of digital leakage—defined as the exposure of violent intentions through digital communications and social media—as an early warning system to prevent violent incidents in K-12 educational settings. This study aimed to quantify the connection between digital leakage and school violence. This research involved analyzing data from school districts to identify patterns and correlations between digital leakage and school violence. The study addressed gaps in current research, including integrating digital and behavioral data and the impact of evolving digital platforms on scanning and interpreting digital leakage. The findings provided insights for enhancing threat assessment protocols and intervention techniques, ultimately contributing to safer school environments. This research examines the theoretical frameworks of Routine Activity Theory, the General Aggression Model, and Social Cognitive Theory to analyze digital leakage as a predictor of school violence.

CURRICULUM VITAE

NAME OF AUTHOR: Angi Meyer

GRADUATE AND UNDERGRADUATE SCHOOLS ATTENDED:

University of Oregon, Eugene, Oregon
University of Notre Dame, South Bend, Indiana
University of Portland, Portland, Oregon

DEGREES AWARDED:

Doctor of Education, Educational Leadership, 2025, University of Oregon
Master of Educational Leadership, 2020, University of Notre Dame
Bachelor of Science, Secondary Education, 1995, University of Portland

AREAS OF SPECIAL INTEREST:

School Violence Prevention
Educational Leadership and School Culture

PROFESSIONAL EXPERIENCE:

Public Safety Manager, Beaverton School District, 2024-Present

Associate Director of Safety, Suicide, Risk and Asset Management, Eugene School District 4J, 2020-2023

PE Teacher, O'Hara Catholic School, 2013-2020

Middle School Teacher, Archdiocese of Portland, 1996-2002

ACKNOWLEDGMENTS

First and foremost, I extend my deepest gratitude to my husband, who has encouraged and supported me since I took the leap to apply to graduate school in 2018. Ed, your unwavering support, confidence, and encouragement have been my foundation. Without you, completing this dissertation would not have been possible.

To my parents, thank you for instilling in me a profound appreciation for education and exemplifying a lifelong dedication to public service. Your example has influenced my identity and guided my path throughout this journey.

A special thanks to my "work ride or die," Kari Skinner, whose consistent belief and trust in my capabilities have impacted my path. Kari, you recognized the passion and potential within me. Your faith has continually energized me, and I am incredibly grateful to have your support and friendship.

I am grateful to my advisor, Dr. P. Shawn Irvin, for your positive support, attentive ear, and invaluable guidance. Your direction has been instrumental in helping me cross this finish line, and your mentorship has enriched my experience beyond words.

I would also like to express my heartfelt appreciation to my committee members. Dr. Lina Shanley, thank you for your incredible statistical expertise, patience, and clarity in helping me navigate the complexities of my data analysis. Dr. Jen Doty, your thoughtful guidance, insightful feedback, and depth of content knowledge have significantly influenced and informed my research. I am grateful for your involvement.

Without each of you, this achievement would not be a reality. I am immensely thankful for you all.

DEDICATION

To my children, Maddie and Cole: This work is dedicated to you with all my love and hope for your futures. I want you to know that life is filled with endless opportunities to learn, grow, and reinvent yourselves. It is never too late to discover new passions or start down a new path, no matter where you are. Let curiosity guide you and keep your hearts open to the unexpected journeys that may come your way. Remember, you have one precious life—make the most of it. Pursue your dreams with courage, embrace challenges with resilience, and live fully and boldly, knowing that the journey is as meaningful as the destination. I love you both to the moon and back, now and always. May this dedication remind you of the power of perseverance, the value of learning, and your boundless potential.

Love,

Mom

TABLE OF CONTENTS

Chapter Page

Chapter Page

Chapter Page

LIST OF FIGURES

Figure Page

LIST OF TABLES

Table Page

CHAPTER I

INTRODUCTION

In recent years, there has been a growing concern surrounding the recurring incidents of school violence in K-12 educational institutions. This well-founded concern stems from an alarming trend revealed by statistics in 2022. Researchers in the *New England Journal of Medicine* reported that gun violence surpassed deaths by car accidents among youth, marking the first time in modern history that it became the leading cause of death (Lee et al., 2022). Additionally, in 2022, more school shootings occurred than any year since the tragic events at Columbine in 1999, and the 2023 school year surpassed that record (Cox et al., 2023). This surge in school-related violence has resulted in over 338,000 students, about half the population of Wyoming, experiencing gun violence at school. For comparison, Lee et al. (2022) found that the rate of firearm deaths in youth is five times higher than that of drowning.

The escalating prevalence of school violence, particularly school shootings, is a matter of increasing concern for educational stakeholders and the broader community. Data from the National Center for Education Statistics (NCES) indicates a significant increase in reported incidents of violence within K-12 educational institutions across the United States (NCES, 2023). This contrast highlights the complex relationship between school environments and the occurrence of violent incidents, suggesting that changes in instructional formats during the pandemic may have temporarily influenced these trends. Many schools operated remotely or in a hybrid format during the 2020-2021 school year due to the COVID-19 pandemic, resulting in fewer in-person violence opportunities. This shift in educational delivery likely contributed to the lower frequency of school shootings being recorded during that period. However, as schools returned to predominantly in-person learning in the 2021-2022 academic year, the frequency of

school shootings surged to 188, marking an increase of more than 50%. These statistics highlight that the transition back to brick-and-mortar education may have influenced the rise in incidents. Table 1 shows the number of school shootings in the United States from the 2000-2001 school year to the 2020-2022 based on the publicly available data from NCES (2023). These data show trends and patterns in the occurrence of school shootings over the past two decades.

Table 1

Number of School Shootings from 2000-01 to 2020-22

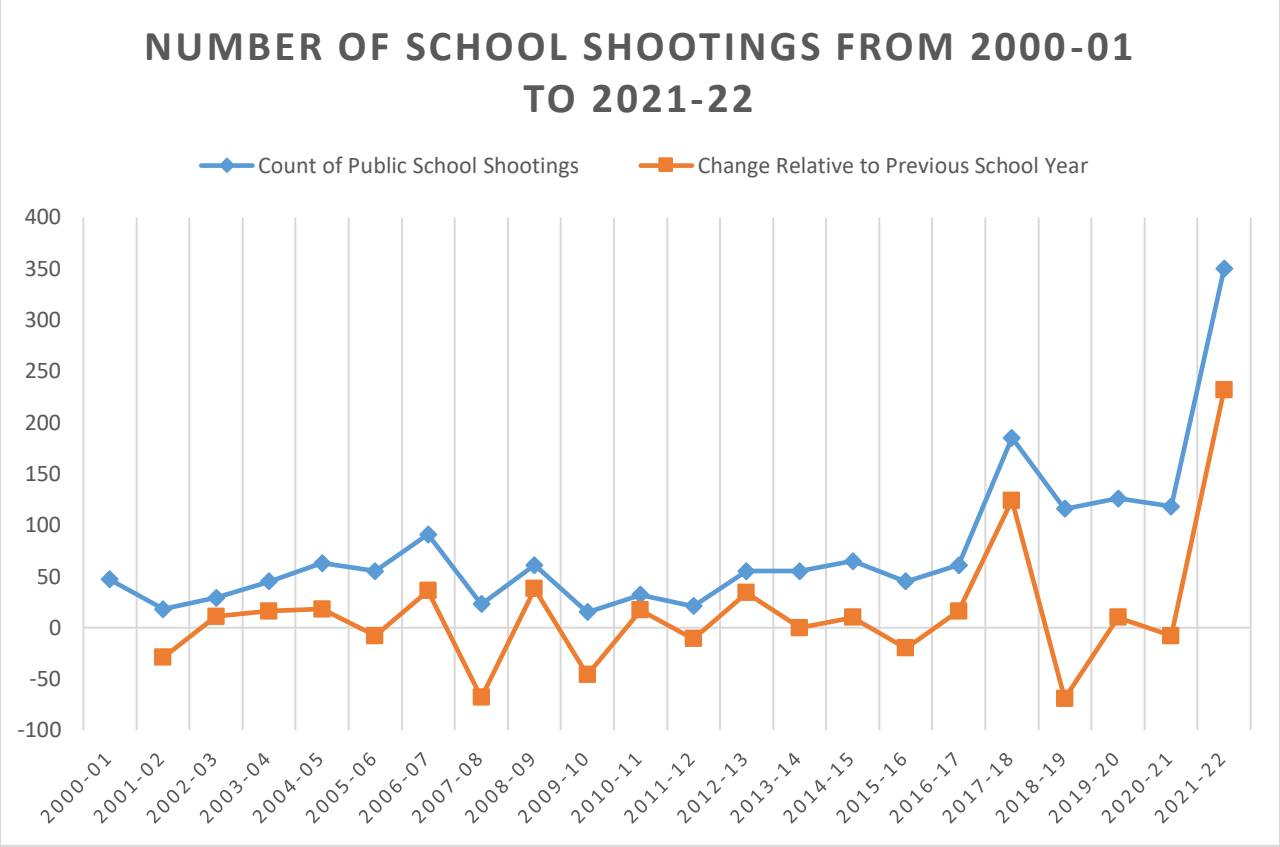
School Year	Number of Shootings	School Year	Number of Shootings
2000-2001	47	2011-2012	21
2001-2002	18	2012-2013	55
2002-2003	29	2013-2014	55
2003-2004	45	2014-2015	65
2004-2005	63	2015-2016	45
2005-2006	55	2016-2017	61
2006-2007	91	2017-2018	185
2007-2008	23	2018-2019	116
2008-2009	61	2019-2020	126
2009-2010	15	2020-2021	118
2010-2011	32	2021-2022	350

The number of school shootings between 2000 and 2017 displayed periodic fluctuations with an overall upward trend. Figure 1 shows these same NCES data graphically, with the

change in the number of reported shootings relative to the previous school year as a separate line from raw counts. In 2000-2001, there were 47 shootings, which dropped and then largely increased each year to 91 in 2006-2007. After this, although there were notable decreases in specific years, such as 15 in 2009-2010 and 21 in 2011-2012, these were followed by substantial increases in subsequent years. The 2017-2018 school year saw a significant spike with 185 shootings, more than tripling the number from the previous year (61). The number of shootings continued to rise, peaking dramatically at 350 in the 2021-2022 school year, a more than threefold increase compared to the previous year (118 in 2020-2021).

Figure 1

Number of School Shootings from 2000-01 to 2020-22



Despite efforts to implement preventative measures, NCES (2023) data revealed a lack of consistent decline in school shootings. Instead, they showed a pattern of high peaks, indicating persistent challenges in addressing school violence effectively (U.S. Department of Justice, 2018). These challenges could exist due to increased access to firearms, the impact of social media on communication and imitation, and potentially ineffective security measures (Cook & Ludwig, 2000; Patton et al., 2016; Peterson et al., 2023). The slight decrease from 2020 to 2021 is likely attributable to the COVID-19 pandemic, which led to prolonged school closures and remote learning, reducing opportunities for on-campus violence (Dorn et al., 2020). The subsequent spike to 350 shootings in 2021-2022 likely reflects a return to in-person learning combined with pandemic-related stressors and disruptions to normal school operations (UNESCO, 2020).

Given these troubling trends, the ubiquity of reporting on news outlets and social media platforms indicates that school violence is a daily concern for educators, parents, and community members. The prevailing concern permeates the minds of parents and educators, even though the statistical reality of school shootings is low (Speedy, 2023). Pervasive fear of violence within our culture disrupts the essential conditions of physical and psychological safety necessary for effective learning (NCES, 2021). Such disruption, where fear and actuality intersect, prompts districts to reevaluate their approaches to ensuring a culture of school safety.

Despite extensive research on school violence and threat assessment, significant gaps remain. There is insufficient understanding of the specific digital behaviors associated with predicting violent actions; digital and behavioral data integration is lacking. Digital and behavioral data continue to be viewed separately, as noted by Veijalainen et al. (2010), leading to a fragmented understanding of a perpetrator's profile and potential actions. This lack of

integration hampers the ability to predict violent behaviors, especially as evolving technology introduces new digital expression and interaction platforms, creating challenges for effective scanning and interpretation. Raitanen and Oksanen (2019) reinforce that this rapid emergence of new social media platforms and digital communication tools makes it difficult to establish comprehensive, longitudinal studies that adequately capture trends or shifts in online behaviors. This disconnect hinders the integration of digital and behavioral data, limiting the development of comprehensive threat assessment frameworks.

The effectiveness of current prevention and intervention strategies that utilize digital traces must be assessed to better understand the links between digital behavior and violent activity. Miller et al. (2017) found that studies fail to follow through on long-term outcomes and potential unintended consequences, such as impacts on privacy or community trust. This challenge exposes the need for adaptive research methodologies that can respond to the dynamic nature of digital ecosystems.

Given these challenges, exploring innovative approaches that integrate digital and behavioral data for a more comprehensive threat assessment is imperative. This integration could reveal early warning signs and provide a proactive framework for preventing school-related violent incidents. Recognizing the urgency of these concerns, this dissertation explored the potential of threat assessments as a proactive measure in preventing school-related violent incidents by analyzing digital leakage and its implications for school safety protocols. My goals for the dissertation were to:

1. Contribute to our understanding of how digital leakage—the exposure of intentions to commit violence through digital communications and social media platforms—could be identified, analyzed, and utilized to prevent violent incidents in schools.

2. Provide actionable insights and effective strategies for school districts to enhance their threat assessment protocols and intervention techniques by incorporating digital leakage of threats.
3. Strengthen schools' capacity to proactively identify and mitigate violence risks while expanding school personnel's knowledge and preparedness.

Key Terms

Prior to the literature synthesis in Chapter II, it is critical to understand the provided definitions for potentially unfamiliar key terms and explain how they are operationalized in this dissertation and the field of school violence prevention.

Digital Leakage - Digital leakage refers to disclosing harmful intent toward a target through various mediums, such as letters, diaries, blogs, videos, emails, images, voicemails, and social media platforms. This type of warning behavior often demonstrates an individual's fixation on the target, which may signal that they are engaging in research, planning, or preparation for an attack. Identifying digital leakage is critical in threat assessment as it can provide early warning signs of potential violence (Meloy & O'Toole, 2011).

Digital Platform - A digital platform is an online infrastructure or service that facilitates user interactions, communication, content sharing, or transactions. Examples include social media networks, learning management systems, e-commerce websites, and messaging applications. These platforms provide tools and spaces for users to create, share, and access information, fostering individual and collective engagement (Poell et al., 2019).

Threat Actor - A threat actor is an individual, group, or entity that poses a potential or actual risk of harm to a person, organization, or community. In contexts such as cybersecurity and physical security, this term describes someone or something that initiates or carries out actions with malicious intent, including violence, data breaches, or other harmful activities (Casey, 2011).

Threat Assessment - Threat assessment systematically evaluates a communicated or observed threats credibility, seriousness, and potential impact. It involves gathering and analyzing information to determine whether an individual or situation poses a risk of harm and to develop appropriate intervention or mitigation strategies. In educational settings, threat assessment focuses on preventing violence through early identification and support for individuals who may pose a risk (Cornell et al., 2020).

Threat Related Incidents **-** Incidents explicitly involving potential harm or violence (e.g., firearms, weapons, gang-associated behavior, physical violence, sexual assault). Communications that suggest an intent, potential, or preparation to cause harm, violence, or disruption toward specific individuals, groups, or the broader school community (Cornell et al., 2009).

Non-Threat Incidents **-** Incidents do not explicitly involve threats or intended harm towards others. Non-threat-related incidents include concerning behaviors or circumstances involving students who are experiencing emotional distress, mental health, self-harm ideation, interpersonal conflicts, or possession of prohibited items without explicit intent or planning to harm others (NASP, 2021; Reeves et al., 2008).

CHAPTER II

LITERATURE SYNTHESIS

This literature synthesis first details three theoretical frameworks and then synthesizes existing research on the relationship between digital leakage, violent behaviors, and intervention strategies in K-12 educational settings. Specifically, the chapter examines how digital leakage—defined as the exposure of intentions to commit violence through digital communications—was identified, analyzed, and utilized to prevent school violence. By examining theoretical frameworks (i.e., Routine Activity Theory, General Aggression Model, and Social Cognitive Theory) and evaluating empirical findings, gaps in the research were identified, the effectiveness of intervention strategies was assessed, and insights for enhancing school safety were provided.

Theoretical Frameworks

Three theoretical frameworks examined the relationship between digital leakage, violent behaviors, and intervention strategies in K-12 educational settings. The integration of Routine Activity Theory, the General Aggression Model, and Social Cognitive Theory allowed for a multidimensional analysis to capture the complexity of these phenomena.

Routine Activity Theory

Routine Activity Theory (RAT; Cohen & Felson, 1979) posits that crime occurs when three elements converge: a motivated offender, a suitable target, and the absence of capable guardianship. Figure 2 is adapted from Cohen and Felson (1979) and illustrates the convergence of RAT elements in the context of digital leakage and school violence. The researchers suggested that the three converging elements can reasonably manifest as the following:

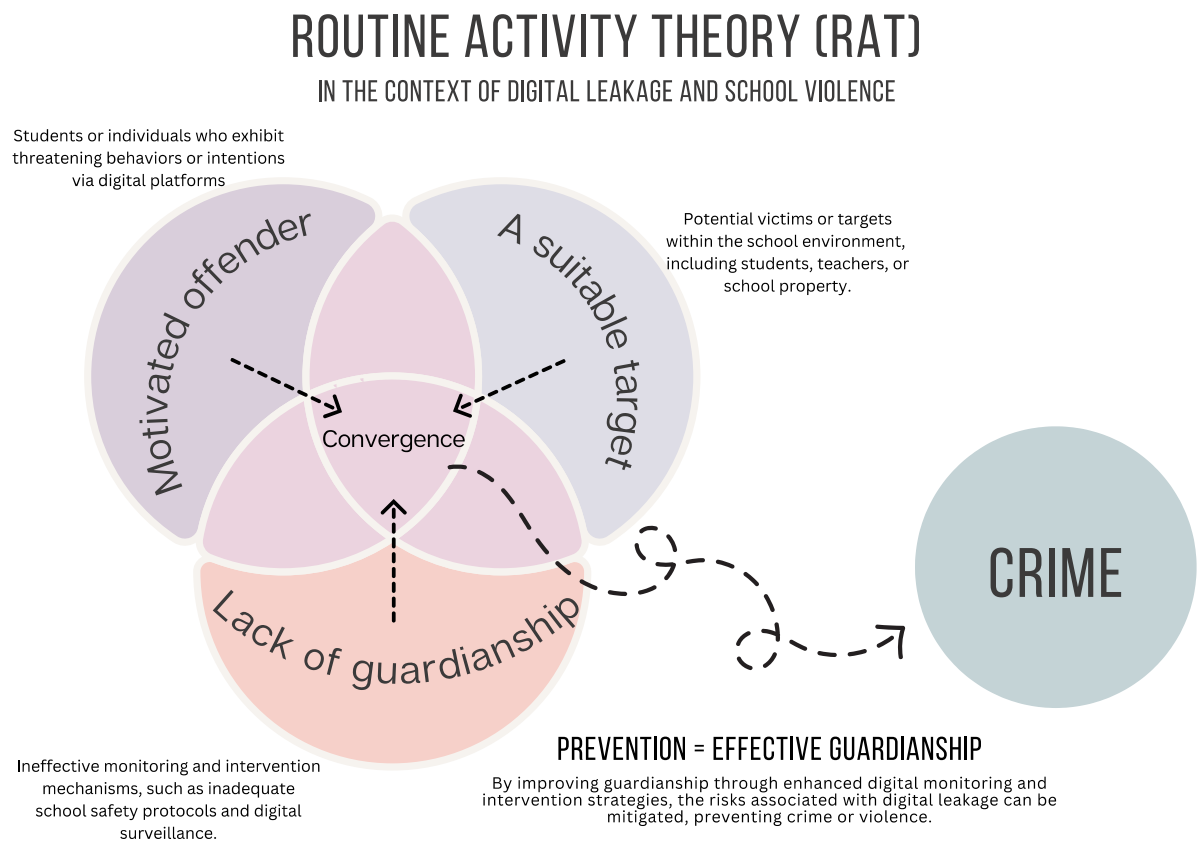
- ***Motivated Offender:*** Students or individuals who exhibited threatening behaviors or intentions via digital platforms.

- ***Suitable Target:*** Potential victims or targets within the school environment, including students, teachers, or school property.
- ***Lack of Guardianship:*** Ineffective scanning and intervention mechanisms, such as inadequate school safety protocols and digital assessment.

RAT emphasizes effective guardianship in preventing school violence and suggests that enhancing digital assessment and intervention may mitigate risks associated with digital leakage.

Figure 2

Routine Activity Theory



General Aggression Model

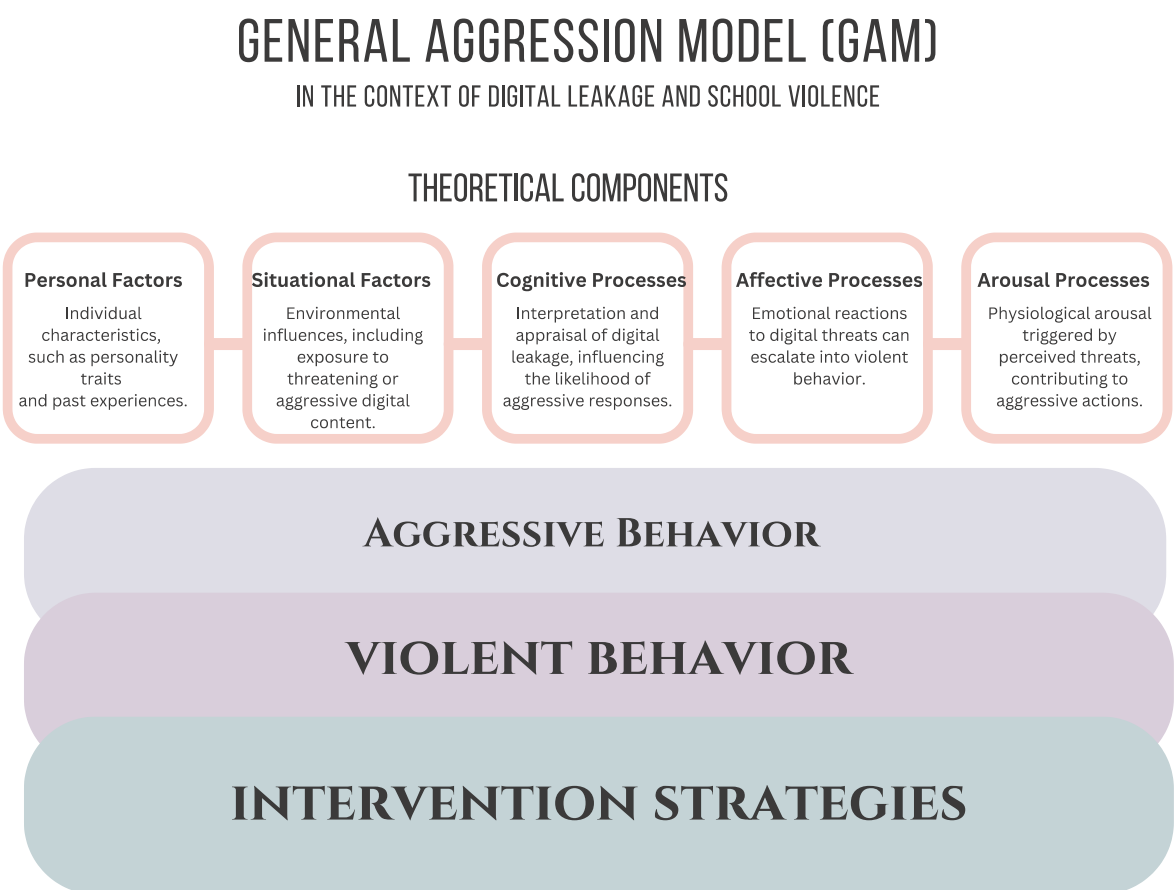
The General Aggression Model (GAM), developed by Anderson & Bushman (2002) and adapted as one of the three main frameworks for this study, integrates personal and situational factors contributing to aggressive behavior. Key components relevant to this study are shown in Figure 3 and include:

- ***Personal Factors:*** Individual person characteristics like personality traits and past experiences.
- ***Situational Factors:*** Environmental influences, including exposure to threatening or aggressive digital content.
- ***Cognitive Processes:*** Interpretation and appraisal of digital leakage, influencing the likelihood of aggressive responses.
- ***Affective Processes:*** Emotional reactions to digital threats escalate into violent behavior in individuals.
- ***Arousal Processes:*** Physiological arousal triggered by perceived threats contributes to aggressive actions.

GAM helps frame how exposure to digital leakage can lead to violent behaviors across various individuals and emphasizes the need for interventions that address personal and situational factors across the diversity of contexts.

Figure 3

General Aggression Model



Social Cognitive Theory

Social Cognitive Theory (SCT), an evolution of Bandura's Social Learning Theory (SLT; 1986), emphasizes the dynamic interplay between personal, behavioral, and environmental factors in shaping behavior. In the context of digital leakage and school violence, SCT provides a comprehensive framework for understanding how students' behaviors were influenced by their environments, including digital and social interactions. Three key concepts from SCT are particularly relevant, as shown in Figure 4:

- ***Observational Learning:*** Students observe behaviors from peers or digital media and consider their outcomes, learning through observation and anticipating consequences

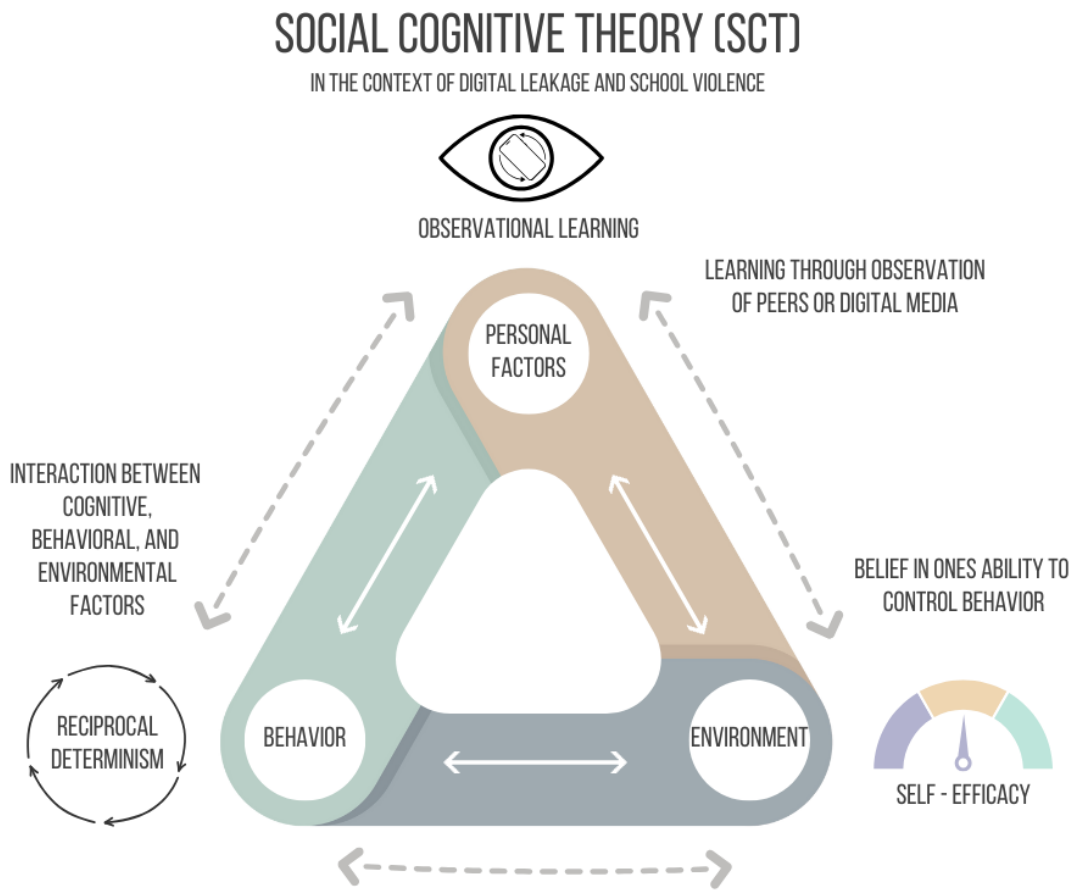
(Bandura, 2001). Digital platforms can amplify exposure to violent content, increasing the likelihood that students may emulate these behaviors (Anderson & Bushman, 2012). For example, this could foster a fascination and identification with an extremist group.

- ***Reciprocal Determinism:*** SCT highlights that behavior is shaped by a continuous interaction between cognitive, environmental, and behavioral factors (Bandura, 1989). In digital contexts, students' online behaviors—such as sharing threats or violent content—shape their online and offline social environments and are influenced by them, creating a reinforcement cycle (Valkenburg & Peter, 2013), often called an echo chamber.
- ***Self-Efficacy:*** Central to SCT is the belief in one's ability to control behavior (Bandura, 1997). Students who observe violent or threatening behaviors online might feel empowered to imitate them if they believe they can successfully replicate the behavior or if it appears socially rewarded (Anderson et al., 2017). For example, they might idolize former, well-known threat actors and attempt to emulate them.

Expanding on the foundational principles of SLT, SCT emphasizes the importance of developing interventions that address negative modeling and imitation and the broader social and cognitive processes that contribute to students' engagement with digital platforms and potentially harmful behaviors (Bandura, 2001).

Figure 4

Social Cognitive Theory



Integration of Theoretical Frameworks

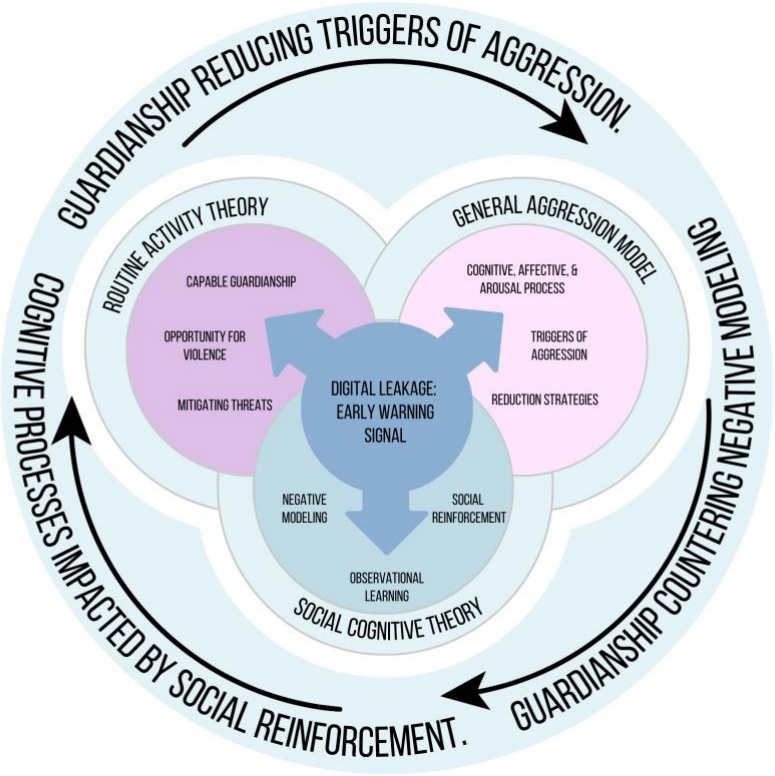
Integrating Routine Activity Theory (RAT), the General Aggression Model (GAM), and Social Cognitive Theory (SCT) offered a comprehensive approach to examining the relationship between digital leakage, violent behaviors, and intervention strategies. Each theory provided distinct insights and contributed to a multidimensional understanding of these phenomena. In short, digital leakage can serve as an early warning signal of potential threats (RAT). It could activate aggressive behavior by influencing the cognitive, affective, and arousal processes associated with aggression (GAM). Through observational learning (SCT), students who

observed violent content online or among their peers might have their (potentially) aggressive or violent behaviors socially reinforced or normalized.

Effective intervention strategies centered on capable guardianship, like school personnel or digital scanning tools, may mitigate the opportunity for violence (RAT). Addressing the cognitive, affective, and arousal mechanisms that foster aggression appears essential for reducing violence (GAM). Additionally, countering negative modeling, such as violent content or threats shared in digital spaces, by promoting positive behaviors and reducing exposure to harmful influences warrants exploration (SCT). Figure 5 shows how these frameworks capture the complexity of digital leakage, its implications for school violence, and potential intervention. Integrating distinct, though related, frameworks facilitated deeper analysis and a nuanced understanding of violence prevention, including behavioral safety threat assessment.

Figure 5

Integrated Theories



Threat Assessment

In 2002, a collaboration of educators, psychologists, and law enforcement professionals created a guide titled *Threat Assessment in Schools: A Guide to Managing Threatening Situations and Creating Safe School Climates*. Responding to the growing awareness of the need to address school violence, the and the U.S. Department of Education (2022) conducted a collaborative study through the Safe Schools Initiative, which aimed to provide strategies for identifying and managing potential threats within the school environment. The National Threat Assessment Center (NTAC) created a federal model known as SIGMA®, from which they developed a toolkit for K-12 schools (Mussington & Alathari, 2023). Currently, two predominate models straddle most schools in the United States: (a) Forensic psychologist Dewey Cornell's *Comprehensive Student Threat Assessment Guidelines* (CSTAG) and (b) school psychologist John Van Dreal's *Salem-Keizer Cascade* model (Cornell, 2003; Van Dreal, 2011).

Threat assessment seeks to evaluate and respond to concerns or behaviors that may indicate a risk of violence or harm within educational settings, with prevention and intervention as its primary purposes. O'Toole (2000) outlined procedures to identify individuals posing a danger to themselves or others, fulfill the responsibility of warning potential victims, and implement strategies to mitigate or eliminate identified risks. Overall, threat assessment aims to establish a safe and secure learning environment for all students, focusing on support and resources for threat actors rather than solely imposing punitive measures (Van Dreal et al., 2011). In 2019, the Oregon Department of Education (ODE) adopted the Salem-Keizer Cascade model and issued an unfunded mandate that schools adopt a threat assessment model by 2021. In 2021, ODE rebranded threat assessment as a Behavioral Safety Assessment (BSA) to enhance communication about how children are viewed and treated during an evaluation. The Bureau of

Justice Assistance (2022) awarded ODE a two-million-dollar grant to create an Oregon model of BSA based on John Van Dreal's Salem-Keizer Cascade Model (Bureau of Justice, 2023). The Oregon Model of Behavioral Safety Assessment (BSA) is evolving and improving. However, its rebranding efforts have not gained traction due to this being an unfunded mandate, the widespread national and international recognition, and the use of the term "threat assessment."

Implementing Threat Assessment in K-12 Schools

Operationalized in schools, the threat assessment process involves recognizing and reporting behaviors, statements, or actions that indicate a potential threat (Cornell, 2020). Students, teachers, parents, or other school community members can initiate the threat assessment process by communicating concerns to the school. Trained professionals, including school counselors, psychologists, and law enforcement personnel, assess the credibility and seriousness of the threat by examining factors such as the individual's history, motives, and access to lethal means for carrying out an act of violence.

Upon identifying a credible threat, the Student Threat Assessment Team (STAT), comprised of trained professionals such as administrators, counselors/psychologists, case workers, law enforcement, and/or social workers, formulate an intervention plan to address underlying issues and support the individual. Intervention can encompass counseling, mental health services, accommodations, and referrals to community resources (Van Dreal et al., 2022). Similar to models for measuring and tracking achievement progress, ongoing documentation and assessment are crucial for managing threat assessment and stabilizing the individual's behavior; follow-up assessments are conducted to measure progress and adjust intervention strategies.

Adopting threat assessment procedures in educational institutions represents a proactive and integrated approach to addressing school violence, aiming to prevent violent incidents,

support distressed students, and maintain a secure environment for students and staff (Cornell, 2020). In the wake of numerous tragic school shootings (see Table 1 and Figure 1), the implementation of threat assessment protocols has emerged as a critical component of school safety. When implemented with fidelity, these procedures offer a range of potential benefits, particularly in identifying and addressing potential threats before they escalate into acts of violence (Slemaker, 2023). Post-shooting analyses highlight a key lesson: Leakage, referring to the intentional or unintentional communication of violent intent, is often present, emphasizing the importance of early detection and intervention in threat assessment (O'Toole, 2000).

Leakage of Threatening Intent

Establishing threat assessment protocols cultivates a culture of safety within schools. Ideally, it encourages students and staff to remain vigilant, report concerns, and collaborate with professionals to address potential threats (Meloy & O'Toole, 2011). Through threat assessment, educational institutions can identify and assess potential threats in their early stages, thereby preventing them from escalating into more severe and harmful actions. For example, Kaati et al. (2020) found that recognizing leakage facilitated timely intervention in preventing potential school shootings, emphasizing that such early identification significantly improved the likelihood of averting violent incidents. Their research highlighted that proactive responses to digital warning behaviors could interrupt the pathway to violence, showcasing the critical role of leakage recognition in effective threat assessment protocols. The most significant advantage of threat assessment lies in its potential to prevent school violence and its devastating consequences. By recognizing and responding to leakage, schools were more likely to avert the tragedy of school shootings and protect the lives of students and staff (Page, 2016). Leakage often serves as a critical early indicator of intent, with research showing that up to 80% of school

shooters communicated their plans or exhibited warning behaviors prior to their attacks (Langman, 2015). Timely recognition and intervention can disrupt these pathways, as threat assessment teams leverage this information to identify concerning patterns, mobilize resources, and provide targeted support. Effective responses to leakage not only enhance safety but also underscore a school's commitment to its legal and ethical responsibility to act on credible threats, reinforcing a culture of care and prevention. This proactive approach minimizes harm, mitigates trauma, and strengthens community trust, emphasizing the lifesaving potential of behavioral safety protocols.

Threat assessment does not solely focus on punitive measures; instead, it emphasizes providing support, enhancing protective factors, and offering resources for emotional or psychological challenges and trauma that may foreshadow violence. When schools recognize leakage, they ideally connect threat actors with appropriate interventions and services and disrupt the pathway to violence (Cowan et al., 2022). In this manner, threat assessment procedures are aligned with legal and ethical obligations to protect students and staff from harm, demonstrating a school's commitment to its duty of care, a fundamental aspect of education (ODE, 2021).

Pathways to violence often remain unclear; however, recognizing effective disruption can yield paths to prevention and intervention. These "wins" offer hope and reveal lessons instrumental to shaping strategies for safeguarding students and staff. Investigating specific cases of acts of violence has provided valuable insights and revelations, offering hope in an otherwise grim context. Success stories often revolved around the timely recognition of warning signs and early intervention (Slemaker, 2023). Thus, successfully detecting and addressing potential threats before they escalated underscored the importance of maintaining open communication channels and fostering a collective commitment to safety. Effectively disrupting the pathway to violence

frequently results from seamless collaboration among educators, mental health professionals, law enforcement, and students (Van Dreal et al., 2022). These cases highlight the value of a holistic response considering all students' mental and emotional well-being.

Threat assessment is critical to enhancing approaches to identifying potential and preventing violence. Threat assessment underscores the significance of behavioral cues and patterns as essential tools for identifying potential threats, a fundamental aspect of analyzing digital leakage of violent intentions. The following section, grounded in threat assessment principles, details how *digital* communications emerged as pivotal indicators of violence. It explores how digital indicators can facilitate early detection of and timely response to potential violent acts and contribute to the preventive strategies employed by educational institutions.

Digital Leakage of Violent Threats

The significance of threat assessment as a foundational pillar in identifying potential harm was closely linked to the concept of warning behavior leakage within violence prevention frameworks (Kaati et al., 2020). Digital leakage refers to communicating intentions to harm a specific target through digital platforms, including social media posts, text messages, emails, or other online interactions. This form of leakage may involve direct threats, implicit warnings, or concerning behaviors shared within personal circles or publicly visible spaces in the digital realm. Meloy and O'Toole (2011) emphasized the prevalence of leakage in cases of targeted violence, encompassing a spectrum from school shootings to attacks on public figures. Safer Schools Together (SST; https://saferschoolstogether.com), recognized for improving community safety through innovative solutions and training for threat assessment teams, has compiled a timeline of tragic events with digital leakage. This timeline of tragic events highlights instances where individuals displayed clear warning signs digitally before violent incidents occurred.

Table 2

Timeline of Tragic Events

Date	Location	Incident	Digital Leakage
November 20, 2021	Oxford, MI	A 15-year-old boy fatally shoots four students and injures seven others.	Instagram posts revealing access to weapons and rehearsal behavior
May 14, 2022	Buffalo, NY	A racially motivated attack by gunman in a supermarket.	Discord messages showing evidence of attack planning.
May 24, 2022	Uvalde, TX	An 18-year-old enters Robb Elementary School, killing 19 students and two teachers.	Concerning comments about weapons on Instagram and Yubo
July 4, 2022	Highland Park, IL	Gunman opens fire at an Independence Day parade.	YouTube videos depicting mass shootings and rehearsal behaviors.
August 28, 2022	Bend, OR	Shooting at a Safeway grocery store.	Wattpad manifesto indicating access to weapons and target selection
February 17, 2023	Lansing, MI	A shooting at Michigan State University leaves three dead and five injured.	Facebook posts involving discussions of "spiritual warfare."
March 27, 2023	Nashville, TN	A targeted attack at the Covenant School.	An Instagram message was sent to a peer before the attack.
April 10, 2023	Louisville, KY	Mass shooting at a Louisville bank.	The attack was livestreamed on Instagram.
August 26, 2023	Jacksonville, FL	Racially motivated attack.	A TikTok video of perpetrator in tactical gear posted before the attack.
October 25, 2023	Lewiston, ME	A gunman kills 18 and injures 13 others across two locations	X (Twitter) activity engaging with conspiratorial content.
December 6, 2023	Las Vegas, NV	Shooting at the University of Nevada, Las Vegas.	YouTube following of conspiracy-related channels
December 21, 2023	Prague, Czech Rep.	A former student kills 14 people at Prague University.	Telegram posts revealing access to weapons and pleas for help.
January 4, 2024	Perry, IA	Perry High School attack by a 17-year-old.	Discord posts suggesting planning; TikTok video of suspect with a duffle bag; Instagram livestream of attack.

Note: Adapted from Safer Schools Together Timeline of Tragic Events (2024).

The timeline and events in Table 2 illustrate how, in each case, digital platforms contained clues, including direct threats, rehearsals, access to weapons, and ideological motives. Proper identification and reporting of these warning signals might have opened intervention opportunities to prevent tragedies. Online posts, messages, or other digital communications often convey distress, ideations of harm, or explicit threats. Had digital traces been identified, there could have been opportunities for timely support measures, possibly disrupting the individuals' pathways toward violence. Such intervention strategies might include mental health assessments, counseling, or engagement with school or community resources, underscoring the critical need for vigilant scanning and proactive response systems to address digital cues effectively. Acknowledging and identifying digital leakage emphasizes the potential for early intervention if signals are recognized and reported to the appropriate authorities accurately and promptly.

Violent Threats and Digital Manifestation

The nature of digital leakage, whether intentional or unintentional, often manifests as indirect, conditional, or direct threats to individuals associated with the intended target (O'Toole, 2000; Winch et al., 2024). As founding researchers in the field of behavioral threat assessment, Meloy and O'Toole (2011) emphasized the critical importance of leakage, stating that it is "one of the most important clues preceding an adolescent's act of violence" (p. 14). Their groundbreaking work laid the foundation for understanding leakage as a pivotal indicator in the early detection of potential violence, shaping current practices in identifying and mitigating threats within schools. This recognition highlights the essential role of educators and threat assessment teams in leveraging these insights to effectively disrupt pathways to violence.

This study indicated that threats rarely directly confronted the primary target, presenting a complex challenge in detection. In cases involving lone actors or individuals involved in

extremist activities, a substantial majority, around 86%, communicated their radical beliefs in some manner. In comparison, approximately 58% exhibited signs hinting at suspicious or potentially violent behaviors, as revealed in comprehensive analyses of both lone actor cases and school shooting incidents (Meloy & O'Toole, 2011). The frequent co-occurrence of leakage and violence stresses a need to explore the different types and predictive aspects of digital leakage to uncover early indicators and mitigate potential threats in violence prevention strategies.

The digital sphere increasingly served as a platform where individuals expressed intentions, frustrations, and grievances, some of which could advocate or escalate into violence. Social media, messaging apps, and online forums, for example, became spaces where individuals might inadvertently or intentionally leak information about their violent thoughts, tendencies, and obsessions. The relative anonymity of many online platforms often leads individuals to express thoughts and feelings they might not share in person. Studies demonstrated that anonymity fosters a disinhibition effect, reducing individuals' sense of accountability and leading them to reveal otherwise suppressed or harmful behaviors. For instance, Lapidot-Lefler et al. (2020) found that online anonymity allows individuals to express more aggressive or threatening behavior than in face-to-face interactions. Similarly, Pater et al. (2022) highlighted how anonymity on social media platforms encouraged individuals to experiment with violent ideas without fear of immediate consequences, often leading to the disclosure of threats that would remain concealed in other settings. This disinhibition effect, resulting from relative anonymity, can potentially reveal threats that might go unnoticed in non-digital environments.

To systematically understand these expressions, it is essential to categorize and describe the different types of threats. As shown in Table 3, O'Toole (2000) identified direct, indirect, veiled, or conditional—categories used by the Federal Bureau of Investigation (FBI) and threat

analysts today. Adapting the digital manifestations of these threat types provides a framework for analyzing online behaviors that may indicate potential violence as a basis for intervention.

Table 3

Threat Category Definitions and Digital Manifestation

Threat Type	Definition	Digital Manifestation
Direct	Explicit expressions of harm or violence toward a specific target.	Direct messages and images on social media or other online platforms stating an intention to cause harm.
Indirect	Vague, unclear, and ambiguous expressions that suggest harm without explicitly stating it.	Posts or messages that use ambiguous language, symbols, or metaphors require interpretation to discern potential harm.
Veiled	Strongly implies but does not explicitly threaten violence.	Online communication may involve cryptic messages or disguised language, which individuals familiar with the context can interpret.
Conditional	Threats upon specific conditions or events.	Statements online outline a potentially harmful action dependent on the occurrence of a specific circumstance.

In K-12 education settings, early identification of potential threats holds significant importance (Cowan et al., 2022). By investigating the digital realm to identify and categorize threats, educators gain perspective through the thoughts and expressions of individuals, allowing for timely intervention before any harm occurs. As outlined in the Salem-Kaiser Cascade model, scrutiny extends beyond merely spotting overt threats; it encompasses understanding the subtle nuances of indirect and veiled threats that might otherwise go unnoticed. Assessing the risk landscape became a comprehensive endeavor when accounting for the complex nature of digital threats. Recognizing the spectrum from direct to conditional threats equips educators and administrators with a nuanced understanding, enabling them to tailor interventions based on the specific nature and severity of the identified risks (Daniels et al., 2007). Analyzing digital expressions of violence provides insight into the backdrop against which threats might unfold.

This contextual understanding of threat types and warning behaviors is invaluable for assessing a situation's seriousness and formulating effective, proportionate responses.

Warning Behaviors Predictive of Violence

Adapted from Kaati et al. (2022), Table 4 defines the four types of warning behaviors and lists common examples within contexts relevant to school settings. Successful identification and intervention in cases of leakage were pivotal for preventing violence by addressing both the immediate risks and the underlying issues contributing to threatening behavior. By acting promptly, interventions have de-escalated potential threats and provided the individual with the necessary resources to manage their emotions and grievances healthily (Silva et al., 2021). Further, integrating mental health interventions into threat assessment processes has reduced the likelihood of violence (Jones et al., 2022). In addition to direct interventions, employing *situational prevention measures*—enhanced security protocols, access control, or environmental adjustments—reduced the opportunities for violent acts. Farrell et al. (2023) emphasized that modifying the environment where leakage was detected helped mitigate immediate risk and created a safer community atmosphere that contributed to violence prevention.

Metrics reflecting the success of these interventions included the number of detected leakage cases, the effectiveness of intervention strategies, and the reduction of violent outcomes. Schools that employed modern threat assessment models, such as those studied by Silva et al. (2021), reported reductions in threats escalating into violence and fewer overall incidents of harm. Successful identification and intervention in these cases, when focused on mental health and situational factors positively contribute to violence prevention statistics, reduced the likelihood of violent behavior by addressing root causes (Jones et al., 2022; Silva et al., 2021).

Table 4

Warning Behaviors and Examples

Warning Behavior	Definition	Example
Leakage	Communication of intent to harm a specific target, whether intentional or unintentional. It may involve written or verbal threats, often aimed at individuals associated with the target. Radical convictions are commonly communicated in cases of targeted violence.	• Written or verbal statements expressing harm. • Patterns of threats preceding attacks. • Communication of radical convictions. • Instances in school shootings.
Fixation	Pathological preoccupation with a person or cause is shown through perseveration, strong opinions, or negative characterizations. Extracting fixation from social media may need longitudinal data, but it is possible to detect fixation on an object with static data.	• Pathological preoccupation. • Increasing perseveration. • It may be challenging on social media without longitudinal data. • Detection of fixation on a specific object is possible even with static data.
Identification	Indicating a desire to be a "pseudo-commando," closely associating with weapons or identifying with previous attackers constitutes behavior. Subcategories encompass radical action or role model identification.	• Desire for a "pseudo-commando" identity. • Close association with weapons. • Identification with previous attackers. • Subcategories: Radical action and role model identification.
Affiliation	Acts motivated by shared Extreme Overvalued Beliefs within a cultural or subcultural group. Online forums can serve as subcultures. "Affiliation" measures the extent of association with a specific group.	• Motivated acts: terrorism, mass murders. • Online forums as subcultures. • Affiliation is measured by the extent of association with a group. Example: Incel (involuntary celibacy) online subculture.

Note. Adapted from Kaati et al. (2022).

Addressing instances of *digital leakage* involved immediate actions, including targeted interventions such as counseling, mental health support, and, if necessary, collaboration with law enforcement (Cowan et al., 2022). Additionally, tackling the underlying issues contributing to digital leakage involved implementing situational prevention measures. Successfully identifying

and intervening in cases of digital leakage positively impacted violence prevention statistics (Randazzo & Plumber, 2009). Metrics such as the number of detected cases, effectiveness of intervention strategies, and potential harm reduction reflected these outcomes.

Fixation, intense and persistent preoccupation or obsession with a particular idea, person, or goal, often to the exclusion of other thoughts or activities, necessitates customized interventions, frequently involving mental health professionals. L'Abate and Baggett (1997) found that redirecting fixation toward healthier expressions required collaboration among educators, counselors, and parents. Successful interventions for fixation were evident in statistics reflecting mental health support in educational settings, where reducing fixation-related behaviors led to a general decrease in potential threats (L'Abate & Baggett, 1997). More recent research by Meloy and Hoffmann (2021) further examined fixation concerning targeted violence. They identified fixation, characterized by an intense and unhealthy focus on an individual or cause, served as a warning sign in evaluating violence risk. Meloy and Hoffmann recommended customized interventions facilitated by a multidisciplinary team, including educators, mental health experts, and law enforcement, to help individuals avoid this detrimental fixation. They argued that reducing fixation is essential for preventing potential violent acts. For instance, fixation was often observed in individuals who displayed obsessive behaviors or recurring grievances. Recent case studies indicate that interventions, such as cognitive-behavioral therapy (CBT) or trauma-informed care, could help redirect these fixations toward healthier outlets, thereby decreasing the risk of violence (Meloy & Hoffmann, 2021).

Early *identification* of potential threats enabled a range of actions, including personalized counseling, increased supervision, and, in severe cases, involvement of law enforcement or other external agencies. Implementing educational programs on conflict resolution and mental health

awareness enhanced prevention efforts (Jackson & Viljoen, 2024). Successful identification of potential threats contributed to positive outcomes in violence prevention statistics. Meloy and O'Toole (2011) determined that metrics might include the number of cases identified, the types of interventions employed, and the effectiveness of these measures in mitigating risks.

Recognition of *affiliation* with risky groups or ideologies often led to targeted educational programs, counseling, or, in extreme cases, collaboration with law enforcement. Promoting a positive and inclusive school culture proved essential to counterbalancing negative affiliations. Horgan (2008) found that identifying and addressing affiliations contributed to improved statistics on the prevention of radicalization or involvement in violent activities. Metrics reflecting the success of prevention programs and reducing affiliations that posed a threat underscored positive outcomes, highlighting the importance of proactive assessment, intervention, and continuous scanning to foster safer educational environments. Prevention programs include the Salem-Keizer Cascade Threat Assessment Model, Virginia Student Threat Assessment Guidelines (VSTAG), Start with Hello (Sandy Hook Promise) program (NTAC, 2021), and SAMSA Safe Schools/Healthy Students program. Twemlow et al. (2020) emphasized that inclusive school cultures counterbalanced negative influences and affiliations. Creating environments where students felt a sense of belonging reduced the likelihood of them affiliating with harmful or violent ideologies. Schools that promoted inclusivity and fostered positive peer relationships observed significant declines in violent incidents and negative affiliations. At the 2024 Oregon School Resource Officers Conference, law professor Dr. Bernie James of Pepperdine University emphasized that school safety personnel "exist to intervene." James argued that while the nation's laws have not changed, societal shifts required adults in educational settings to intervene rather than remain complacent.

Unveiling Opportunities for Intervention in the Context of Digital Leakage

The surge in social isolation and heightened digital engagement addictions following the COVID-19 pandemic have made understanding and managing online threats in educational settings more important. As students increasingly turned to digital platforms for social communication and support, recognizing warning behaviors within these digital interactions became critical. Digital spaces frequently host cyberbullying and victimization (Kaati et al., 2022). Recognizing online harassment and supporting threat actors and victims helped prevent digital threats from escalating into real-world violence within educational environments (Sandeeshwara Kasturiratna & Hartanto, 2024). Individuals with high trait online disinhibition are significantly more likely to become cyberbullying perpetrators after being victimized. These findings underscored the importance of addressing online disinhibition tendencies to break the victim-bully cycle. They highlighted the need to develop features and guidelines that reduce factors, such as perceived anonymity, contributing to disinhibition on online platforms.

The digital landscape presented unique challenges for those studying and implementing threat assessment. School districts and personnel often struggled to keep pace with the changing digital platforms, which grew in number and complexity. Accessing and analyzing associated information to identify, categorize, and assess potentially concerning behaviors is a significant challenge. Therefore, it is essential to train students, staff, and the extended school community (e.g., parents, guardians, and other family members) on recognizing threat categories (Table 3) and warning behaviors (Table 4) as they manifest online. Such training facilitates timely and meaningful reporting and implementation of appropriate support when an individual is in crisis (Page, 2016). Stakeholders in school safety needed to stay attuned to the evolving dynamics of online interactions to navigate this multifaceted landscape effectively (Bartlett, 2023).

While the digital environment presents challenges in threat assessment, it also offers opportunities for proactive mental health interventions. Page (2016) suggested incorporating strategies that address students' psychological well-being as part of a comprehensive approach to violence prevention. Building a resilient and supportive school community involves fostering an environment where individuals feel empowered to seek help for mental health concerns. Evidence from Skeen et al. (2019) supports this approach, identifying three key components—interpersonal skills training, emotional regulation strategies, and education on alcohol and drug use—as particularly effective in promoting mental health and reducing risk behaviors among adolescents. These components not only tackle immediate mental health concerns but also enhance social support systems, equip students with tools to manage stress, and mitigate key risk factors such as substance use. Similarly, Cowen et al. (2022) found that recognizing the signs of emotional distress and providing accessible mental health resources could create a safety net beyond threat detection. These multidimensional interventions strengthen stakeholders' trust and confidence and align with cultivating a positive and nurturing educational environment.

Gaps in understanding relate to identifying and analyzing digital leakage, integrating digital and behavioral data, assessing the impact of evolving digital platforms, and evaluating the effectiveness of intervention strategies. Recent studies identify four critical gaps: (a) a lack of comprehensive frameworks for detecting early signs of digital leakage (Hensley et al., 2024; Veijalainen et al., 2010), (b) insufficient methods for integrating digital and behavioral indicators for holistic threat assessment (Moore et al., 2024), (c) limited research on how advancements and changes in digital platforms influence behavior and threat potential (Raitanen & Oksanen, 2019), and (d) a need for a more thorough evaluation of current intervention strategies to assess their effectiveness in preventing violence and radicalization (Miller et al., 2017). Addressing these

gaps is vital for understanding how digital interactions impact real-world behaviors and how educational institutions can enhance their efforts to prevent and manage potential threats.

1. *Insufficient Understanding of Digital Behavior Indicators:* Although previous research by Veijalainen et al. (2010) had touched upon the digital activities of individuals who posed threats to school safety, there was a substantial gap in comprehensively understanding which behaviors precisely predicted violent actions (Hensley et al., 2024). The nuances of digital leakage—such as the type of content shared, frequency, and reaction of the online community—have not been fully mapped out in existing models.
2. *Integration of Digital and Behavioral Data:* Digital trace data and traditional behavioral threat assessments were not integrated. Existing methodologies often treated these streams separately, potentially missing a holistic view of a threat actor's profile. Understanding how online behavior correlates with offline actions has been inadequately explored (Moore et al., 2024).
3. *Technological Advances and Changing Digital Landscapes:* As technology has evolved, so have the platforms and means by which individuals communicate and express themselves. Raitanen and Oksanen (2019) found that research often struggled to keep up with these technological advances, creating a gap in assessing and interpreting new digital expressions and interactions.
4. *Prevention and Intervention Strategies:* The effectiveness of current prevention and intervention strategies that utilize digital traces needed assessment. Most studies have not followed long-term outcomes of interventions, nor have they explored unintended consequences, such as impacts on privacy or community trust (Miller et al., 2017).

To address these gaps in research, I explored the following research questions (RQ):

1. What patterns of concerning non-threat-related behavior and threat-related behaviors can be observed in K-12 settings from September 2022 to July 2024?
    a. What are the descriptive patterns of threat-related behaviors based on time, grade range, and gender, including the presence or absence of digital leakage, formal threat assessments, and immediate risk?
    b. What is the relationship between digital leakage, formal threat assessment, and threat types (FBI categories: *direct, indirect, veiled, and conditional*; SST: behavior only) in relation to threat-related behaviors?
    c. What are the descriptive patterns and relationships between the primary category of concerning behaviors unrelated to threats and the presence or absence of digital leakage in formal threat assessments?

Hypotheses and Anticipated Findings

To address existing gaps in research, this study aimed to explore patterns of concerning threat-related behaviors and non-threat-related behaviors in K-12 settings from September 2022 to July 2024. Given students' increasing dependence on digital platforms for communication and self-expression, I hypothesized that digital leakage—evident through social media posts, messages, or online forums—would be an important early indicator of potential threats and concerning behaviors in school environments.

Expected Patterns of Threat-Related Behaviors (RQ1a)

I anticipated that threat-related behaviors would show notable temporal patterns, with increased incidents occurring at the beginning of the school year, before extended breaks, and in the months leading up to summer. These fluctuations may align with academic stressors, social

conflicts, and changes in student support structures. Additionally, I expected differences across grade levels, with high school students displaying higher frequencies of digital leakage and more explicit violent threats compared to younger students, who may exhibit behavioral disruptions that warrant concern but lack direct violent intent. Gender-based patterns were also anticipated, with male students more frequently associated with externalized violent threats, whereas female students may display indirect or veiled threats, often related to relational aggression.

Digital Leakage, Threat Assessments, and Threat Type (RQ1b)

I hypothesized a strong correlation between digital leakage and formal threat assessments, particularly in cases involving direct and indirect threats as classified by the FBI framework. Given prior research indicating that students who engage in digital leakage often escalate to formal interventions (Fein et al., 2002; Meloy & O'Toole, 2011), I anticipated that threats categorized as immediate risks by school authorities would frequently involve digital leakage, such as social media posts, messages, or online forums.

The Salem-Keizer Cascade Model offers a structured framework for evaluating school threats, but it does not officially classify behavior-only threats. SST introduced this classification to address situations where students exhibit concerning behaviors—such as aggression, intimidation, or disruptive conduct—without making an explicit threat. Initially, I thought behavior-only threats might be less commonly linked to digital leakage since these behaviors usually appear as physical or verbal aggression rather than explicit online threats. However, research on youth violence and social media indicates that digital spaces often act as platforms for conflict escalation (Hinduja & Patchin, 2019; Patton et al., 2016). Students involved in physical altercations, bullying, or intimidation frequently engage in precursor behaviors online, including social media disputes, group chat escalations, or sharing violent content. Instead of

serving only as a predictor of explicit threats, digital leakage in behavior-only threats may function as an amplifier—escalating conflicts, reinforcing aggressive behaviors, or encouraging peer involvement. Therefore, I hypothesized that while behavior-only threats might not always contain explicit digital threats, they could still display identifiable online behaviors, contributing to risk assessment and intervention strategies. This aligns with research on the role of social media in peer aggression and school-based violence (Hinduja & Patchin, 2019; Patton et al., 2016) and emphasizes the importance of integrating digital analysis into behavioral threat assessments, even when no direct threat has been articulated.

Digital Leakage in Non-Threat-Related Concerning Behaviors (RQ1c)

For non-threat-related concerning behaviors, I hypothesized that digital leakage would be a common feature in cases involving harassment, bullying, and expressions of distress, such as self-harm ideation. However, since a substantial percentage of students witness or engage in online harassment without direct threats of violence (Vogels et. al., 2022), I expected that while digital leakage would be prevalent in formal threat assessments, it might not always lead to immediate risk classifications. Furthermore, I anticipated that incidents involving the glorification of violence—such as sharing violent imagery, discussing past attacks, or participating in extremist online communities—would have a stronger correlation with formal threat assessments due to their potential for escalation.

Potential Implications and Contributions

Ultimately, I hoped to highlight the importance of a multidisciplinary approach to school safety, emphasizing collaboration among educators, law enforcement, and mental health professionals to proactively identify and address early warning signs of violence in K-12 environments. Given the growing influence of digital platforms on student communication and

behavior, the study anticipated that digital leakage—evidenced through social media posts, messages, and various online activities—was a critical early warning sign of potential threats. By systematically studying patterns of digital leakage alongside formal threat assessments and observed behaviors, this research sought to provide empirical evidence supporting the integration of digital threat identification within school safety frameworks. This multidisciplinary strategy would ensure stakeholders had comprehensive, data-driven methods to detect, assess, and mitigate potential threats before they escalate into real-world violence.

CHAPTER III

METHODS

My study utilized a quantitative design, focusing exclusively on analyzing extant data provided by Safer Schools Together (SST) to address the research questions (Creswell & Plano Clark, 2018). This approach was selected for its effectiveness in providing a broad, generalizable overview of statistical trends and relationships across a large sample of school districts. The quantitative focus allowed for an analysis of measurable patterns related to the digital leakage of threats of violence. This approach was appropriate for investigating the prevalence and associations of specific variables linked to concerning behaviors in K-12 settings. The study generated actionable information about a significant societal concern: school violence by concentrating on statistical relationships and trends.

Research Design

This study used a descriptive and correlational research design to analyze secondary extant data provided by SST. This design was selected to summarize and examine associations between digital leakage and other key variables related to school safety while enabling the identification of statistical patterns and trends across a large sample. The study further investigated the relationship between digital leakage and incidents of school violence. It aimed to determine the patterns of concerning (threat and threat-related) behaviors in K-12 settings included in the sample.

Researcher Positionality Statement

As the researcher who conducted this study, I must acknowledge the background, beliefs, and experiences that may have influenced my approach and inferences. I serve as the Public Safety Manager for the Beaverton School District, overseeing Emergency and Threat

Management in Beaverton, Oregon. I hold a master's degree in educational leadership from the University of Notre Dame and have over sixteen years of experience in education, school safety, suicide prevention, and violence prevention. My professional role involves direct engagement with behavioral threat assessment protocols and emergency management planning, greatly enhancing my understanding of school violence prevention's complexities. My professional experiences have shaped my beliefs about the importance of proactive and preventive measures in ensuring school safety. I firmly believe in the effectiveness of threat assessment teams and the necessity of comprehensive safety protocols to decrease the risk and occurrence of violence in schools. These beliefs have influenced my topic, research questions, and methodological choices.

Given my professional background, I am familiar with the challenges and nuances of implementing violence prevention strategies in educational settings. My professional proximity to the research context might have introduced biases, particularly in interpreting data and findings. To mitigate this, I employed reflexive practices, including conducting regular peer debriefing sessions with colleagues and my doctoral adviser, who had diverse perspectives on school safety and data collection and analysis. Furthermore, my connection to the Beaverton School District gave me unique insights and necessitated a heightened awareness of ethical considerations. I ensured confidentiality and anonymity for all participants and adhered strictly to ethical research guidelines as reviewed by the Institutional Review Board (IRB). My position as a Public Safety Manager profoundly influenced my approach to this research. However, I aimed to conduct this study with integrity and objectivity through adherence to IRB-approved research strategies and ethical standards.

Institutional Review Board Approval

This study was approved by the IRB of the University of Oregon (UO). The IRB review process ensured that the study met all ethical standards and that the rights and welfare of participants were protected (American Psychological Association, 2017). A detailed research protocol was submitted to the IRB, outlining the study's goals, methods, participant redaction, and measures to ensure confidentiality and minimize risks (Office for Human Research Protections, 2018). An exempt application was submitted, and compliance with IRB requirements for ongoing monitoring was ensured (National Institutes of Health, 2016). As the primary researcher, I obtained training in human subjects research from the Collaborative Institutional Training Initiative (CITI) program to ensure familiarity with ethical principles and practices (CITI Program, 2019).

The study was granted exempt status on October 8, 2024, by the UO IRB due to its exempt classification and the complete removal of any subject identification. Research Compliance Services (RCS) at the UO carefully evaluated the proposed project (Study ID: STUDY00001544) and concluded that it qualifies as "Not Human Research" based on the description and materials submitted. This conclusion is recorded in the document titled *2024-10-08 Determination for STUDY00001544.pdf*.

The "Not Human Research" status indicated that the study did not involve activities meeting the regulatory definition of human subjects research under federal guidelines. This designation allowed the study to proceed without requiring further oversight by the UO IRB. However, RCS noted that any modifications in interactions with individuals or a shift in the study's aims would require the organization to determine if oversight by RCS and/or the UO IRB was needed before initiating such activities. This provision ensured that any future developments

within the study framework would maintain compliance with ethical standards and regulatory requirements. No modifications in interactions with individuals or shifts in study aim occurred; thus, additional university oversight was not required.

Data Collection, Preparation, and Management

The research utilized extant data provided by SST, which was collected from partner school districts in Canada and the United States as part of ongoing efforts to identify and manage potential threats in educational environments. Data included reports of students' behavior from K-12 school districts affiliated with SST. This dataset encompassed reported "incidents of concerning behaviors" related to digital leakage from September 2022 to July 2024. The inclusion criteria for the dataset focused on reported incidents that occurred within the specified timeframe and involved cases where digital leakage was present or absent, whether formal threat assessment was initiated or not, and whether the immediate risk was present. Data were examined descriptively and through correlations to identify patterns and statistical relationships between the key aspects of digital leakage and school violence listed below.

SST prepared the data utilized in this study and underwent de-identification at the school and individual student levels to ensure privacy and confidentiality before transferring to UO for this study. All identifying information was removed by a lead SST threat analyst before its use in the study, ensuring compliance with the ethical research standards of the UO IRB and RCS. This de-identification process guaranteed no personally identifiable information was included, maintaining the anonymity of all districts, schools, and individuals, including students, involved. SST organized data into two primary datasets for analysis: (1) incidents involving threat-related behavior (TRB dataset) and (2) incidents categorized as other non-threat-related behaviors (non-TRB dataset). The separation into two data sets was based on a chi-square test of independence

conducted by SST, which indicated that threat-related behaviors were significantly different from those deemed non-threat-related behaviors. This categorization allowed for a focused examination of threat-related behaviors while facilitating comparative analysis with other concerning behaviors, which were manually categorized and inputted into the data set by SST based on a standard intake form completed by partners reporting potential threats to SST (e.g., K-12 district faculty). The SST data intake form is shown in Appendix A.

After SST collected and prepared data, the TRB and non-TRB datasets were securely transferred and stored per institutional data protection protocols. Specifically, the dataset was encrypted and stored on my password-protected laptop and a secure server managed by Behavioral Research and Teaching (BRT) at the UO. Access to the data was strictly limited to the researcher, my advisor, and BRT research associate professor, Dr. P. Shawn Irvin, and committee members, Drs. Lina Shanley and Jen Doty, as necessary for the study. This controlled access protocol helped guarantee the security and confidentiality of the data throughout the study. The UO IRB approved the data management plan and procedures. The IRB confirmed that all ethical standards were satisfied, including secure handling, storage, and analysis.

Population and Sample

The target population for the study included students K-12 school districts across the U.S. and Canada that partner with SST. These districts reported incidents of concerning behaviors, which included digital leakage, as part of their threat assessment process. A purposive sampling strategy was used, leveraging an existing dataset collected and prepared by SST (Nyimbili & Nyimbili, 2024). This dataset consisted of reported incidents that met the study's inclusion criteria and documented cases of concerning behaviors submitted to SST by partner schools, ensuring relevance to the research questions. The total sample size across the two datasets was

2,647, which was determined by the scope of the dataset provided by SST, which included case files from September 2022 to July 2024. This large sample size helped ensure sufficient power to detect meaningful patterns and relationships within the data. For the two datasets, incidents involving threat-related behavior (TRB dataset) included 798 cases (RQ1a-b), and incidents categorized as other non-threat-related behaviors (non-TRB dataset) included 1,849 cases (RQ1c). All complete cases used in analyses met the inclusion criteria as having detailed records of concerning behaviors, digital leakage presence/absence, and threat assessment outcomes. Cases missing critical data on digital leakage or threat assessment outcomes were excluded.

Variables of Interest Analyzed

A comprehensive list of the variables is available in the data dictionary for both datasets in Appendix B and C. The variables of interest analyzed for both datasets are described below in alignment with the study objectives.

- *Presence of digital leakage* (content related to the incident or concern; yes or no)
- *Implementation of formal threat assessments* (yes or no)
- *Presence of immediate risk* (yes or no)
- *Threat type* (categorization of concerning non-threat-related behaviors; five categories: four FBI threat types—direct, indirect, veiled, and conditional—and one SST type, behavior only)
- *Grade level* (individual reported; elementary, middle, or high)
- *Gender* (individual reported, male, female, or unconfirmed)
- *Season of reported incident occurred* (academic quarter; fall [July-October], winter [November-February], or spring [March-June])
- *Concerning behaviors* (multiple levels—see Appendix B and C)

Data Analysis

Data were prepared and analyzed for descriptive and correlational statistics using a combination of Microsoft® Excel for Mac Version 16.93.1 (Microsoft Corporation, 2024) and Jamovi Version 2.3 (The Jamovi Project, 2022), both of which were well-suited for analyzing the TRB and non-TRB datasets provided by SST. Data from TRB and non-TRB datasets were analyzed using Excel to examine descriptive patterns of threat and non-threat-related concerning behaviors in K-12 settings, including with respect to the presence or absence of *digital leakage*, whether or not *formal threat assessment* was initiated, and the presence or absence of *immediate risk* (RQ1a and RQ1c). Descriptive statistics, including frequency counts, proportions for individual variables, and pivot tables for multiple variables, were used to summarize data, providing a descriptive overview of the occurrence and patterns of digital leakage incidents and the demographic profiles of the respondents (*gender* and *grade level*) and timing of reported threat-related behaviors (*season*).

The chi-square test of independence was conducted to examine the relation between *threat type* (direct, indirect, veiled, conditional, and behavior only) and the presence or absence of *digital leakage*, whether or not *formal threat assessment* was initiated, and the presence or absence of *immediate risk* (RQ1b). The chi-square test of independence was also conducted to examine the relationship between types of concerning (non-threat-related behaviors (e.g., bullying, substance use, potential violence) and the presence or absence of digital leakage in the non-TRB dataset (RQ1c). Statistical significance was set at $\alpha = .05$, with exact *p*-values reported in the results (American Psychological Association, 2020). Chi-square testing met assumptions: (a) variables were categorial, (b) all observations were independent, (c) contingency cells were mutually exclusive, and (d) there were no structural zeroes (i.e., expected values exceeded 1).

CHAPTER IV

RESULTS

This chapter presents the results of the quantitative analyses conducted to examine patterns of concerning and threat-related behaviors in K–12 educational settings from September 2022 through July 2024. The primary aim of this study was to explore how digital leakage, threat type, formal threat assessments, and immediate risk determinations interact within the broader framework of school safety and violence prevention. Specifically, the analyses addressed the overarching research question and its subcomponents, focusing on descriptive patterns by grade level, gender, time of year, relationships between digital leakage and formal threat management processes, and the nature of concerning behaviors not classified as threats. Descriptive statistics and chi-square tests of independence were employed to detail and identify associations among key categorical variables. Findings are organized by research sub-question (1a-1c) to provide an ordered results narrative. Additionally, the chapter identifies findings outside the scope of the research questions that contribute to a better understanding of digital leakage and threat behavior. These findings are presented at the end of the chapter and include descriptive and inferential patterns related to law enforcement involvement, threats (e.g., behavior-only versus communicated), and demographic considerations. This integrated approach lays the groundwork for the Discussion chapter, further contextualizing these findings and outlining implications for school safety practices and policies.

As noted in Chapter II, analysis is guided by three interrelated theories: Routine Activity Theory (RAT; Cohen & Felson, 1979), the General Aggression Model (GAM; Anderson & Bushman, 2002), and Social Cognitive Theory (SCT; Bandura, 1986). RAT offers a criminological perspective to comprehend the convergence of a motivated offender, a suitable

target, and the absence of capable guardianship. In this study's context, digital leakage is viewed as a visible indicator of offender motivation, which, if overlooked, demonstrates a failure in guardianship, especially in digital environments. The GAM underscores how situational and personal factors, including exposure to threatening digital content, can trigger cognitive, affective, and arousal mechanisms that escalate into aggressive behaviors. Lastly, SCT emphasizes how students may mimic behaviors seen in online contexts, reinforced by mechanisms of observational learning, reciprocal determinism, and perceived self-efficacy. Following each hypothesis, the results are presented alongside supporting statistical outputs and descriptive patterns. Each set of findings is analyzed through one or more guiding theoretical frameworks, which is detailed in the Discussion section. This process assesses whether the data support the proposed hypotheses and how the results align with, expand upon, or complicate the theoretical expectations embedded within RAT, GAM, and SCT.

Patterns of Threat-Related Behaviors (RQ1a)

A total of 798 incident reports from K–12 educational settings (September 2022 through July 2024) were analyzed. Most of these incidents (approximately 85%) were classified as threat-related behaviors involving an explicit or implicit threat. They could be categorized into five threat-type categories: direct, indirect, veiled, conditional, or behavior-only. The remaining 15% of cases concerned behaviors unrelated to threats, such as safety or disciplinary concerns, without a direct threat. Table 5 provides a frequency breakdown of incidents by type (threat versus non-threat), and Table 6 shows incidents by type (threat versus non-threat) by demographic variables.

Table 5

Incident Type and Demographics

Type	Frequency	Percentage
Threat Related	678	85.0
Non-Threat Related	120	15.0

Table 6

Frequency of Incidents by Type and Demographic Variables

Demographic Variable	Category	Threats (*n*)	Non-Threats (*n*)	Total (*n*)
Grade Level	Elementary (0–5)	5	14	19
Grade Level	Middle (6–8)	105	127	232
Grade Level	High School (9–12)	159	187	346
Gender	Female	34	21	55
Gender	Male	119	83	202
Season	Fall	64	101	165
Season	Winter	98	175	273
Season	Spring	121	157	278

Note. Note. Frequencies reflect the distribution of reported incidents categorized as threat-related or non-threat-related across different grade levels, gender categories, and academic seasons from September 2022 to July 2024.

Temporal Patterns

Figure 6 illustrates the temporal distribution of threat and non-threat incidents across the study period. Incidents occurred over the two years without a clear seasonal or temporal pattern. As shown in Figure 6, the number of reported incidents was lower in the fall compared to winter and spring. For example, as shown in Table 7, when combining data from the 2022–2023 and 2023–2024 academic years, the fall months experienced 165 total incidents (with 64 classified as threats), compared to 273 incidents in winter (98 threats) and 278 in spring (121 threats). The proportion of threat-related cases was highest in spring (43.5% of spring incidents) and lowest in winter (35.9%), with fall in between (38.8%). However, differences in actual versus expected counts of incident types were not statistically significant within season, χ^2 (2, N = 716) = 3.401, p = .183. The likelihood that a reported incident was a threat did not depend on the season

Figure 6

Temporal Distribution of Incidents

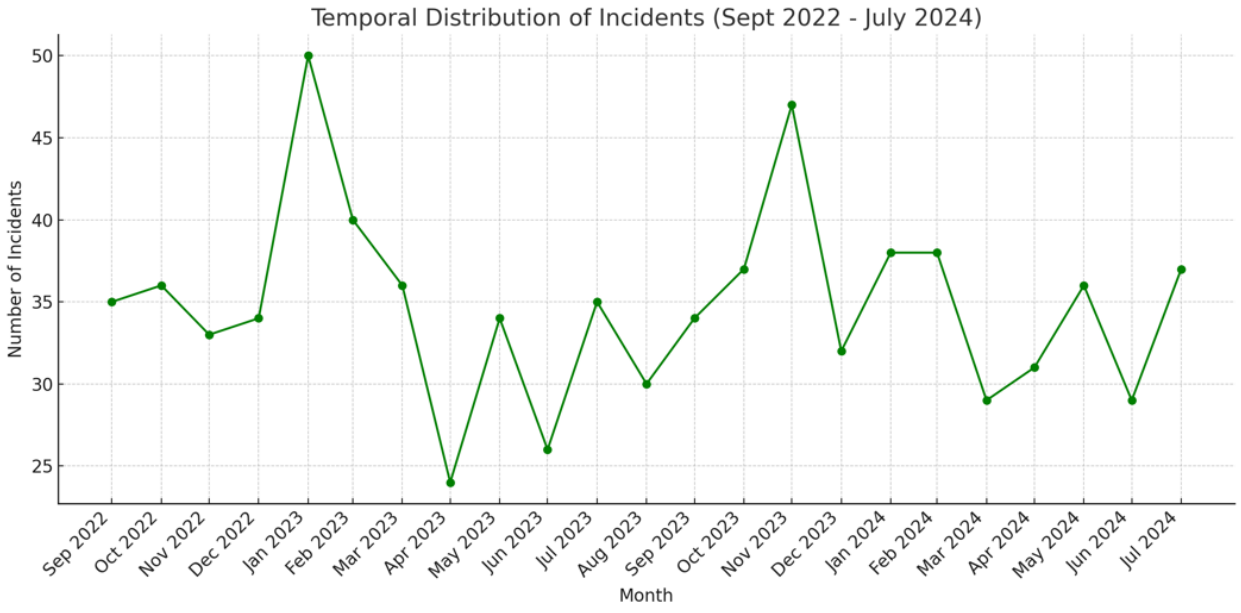


Table 7

Observed and Expected Frequencies of School Threats by Season

Season	Threat	Observed (*n*)	Expected (*n*)	Total (*n*)
Fall	No	121	122.557	165
Fall	Yes	41	39.443	
Winter	No	204	194.426	273
Winter	Yes	53	62.574	
Spring	No	197	205.017	278
Spring	Yes	74	65.983	
Total	No	522	N/A	690
Total	Yes	168	N/A	

Note. Percentages represent the proportion of threat-related versus non-threat incidents reported during each season. Chi-square analysis indicated no statistically significant differences in threat likelihood across seasons, χ^2 (2, N = 716) = 3.401, p = .183. Data were collected from K–12 educational settings between September 2022 and July 2024.

Grade-Level Trends

The grade range of students involved showed that most incidents occurred at the secondary level (Table 8). Of the K–12 incidents with grade information (n = 599), over half (58.1%) involved high school students (grades 9–12), about one-third (38.7%) involved middle school students (grades 6–8), and only 3.2% involved elementary students (grades K–5). A few cases fell outside K–12 (e.g., former students or no grade data) and were excluded from grade-specific analyses. Threat-related cases were likewise predominantly from high schools (348 of 599, 58.1%) and middle schools (232, 38.7%), with very few at the elementary level (19, 3.2%). There was no significant difference within grade level for the actual and expected counts of threat versus non-threat incidents, χ^2 (2, N = 599) = 0.837, p = .658). Within threat cases, grade

level was not significantly related to differences in actual versus expected counts of incidents. For instance, actual and expected counts of threat types (direct, indirect, etc.) also did not differ for high school, middle school, or elementary students, χ^2 (8, N = 597) = 8.512, p = .385.

Table 8

Observed and Expected Frequencies of School Threats by Grade-level

Grade Level	Threat	Observed (*n*)	Expected (*n*)	Total (*n*)
Elementary (K–5)	No	14	14.591	19
Elementary (K–5)	Yes	5	4.409	
Middle (6–8)	No	150	158.164	232
Middle (6–8)	Yes	82	83.836	
High School (9–12)	No	221	227.245	348
High School (9–12)	Yes	127	120.755	
Total	No	385	N/A	599
Total	Yes	214	N/A	

Note. Frequencies represent incidents reported by grade level. Chi-square analyses indicated no significant association within grade level for threat versus non-threat ($p > .20$), nor with the type of threat or immediacy of risk (p = .385 and p = .065, respectively). Data were collected from K–12 educational settings between September 2022 and July 2024.

High school-related threats exhibited a higher proportion of veiled threats (34 observed versus 27.8 expected) and a lower proportion of direct threats (115 versus 121.7 expected) than middle school. However, these differences were minimal and not statistically significant. Similarly, the rate at which cases were classified as immediate risks did not differ significantly within grade, χ^2 (2, N = 598) = 5.460, p = .065. There was a trend that threats in high schools were more often considered an immediate risk (61.1% of high school threat cases) than those in middle schools (51.3%), but this pattern did not reach significance. Formal threat assessment

practices were consistent across grade ranges: roughly two-thirds of incidents at each level resulted in a formal threat assessment, with no significant grade-level association ($p = .223$).

Gender Patterns

Gender information was available in only 38% of cases; among those 257 incidents with known subject gender, 78.6% involved male students ($n = 202$), and 21.4% involved female students ($n = 55$), reflecting a large proportion of reports where gender was unconfirmed (62.0%, $n = 420$; see Table 9). Therefore, all gender-based analyses were conducted on the subset with known gender. Overall, male and female cases showed broadly similar patterns regarding whether incidents were classified as threats and in most outcomes, with a few notable differences. The proportion of threat-related incidents (as opposed to non-threat concerns) did not significantly differ by gender, χ^2 (1, $N = 257$) = 0.152, $p = .697$.

Table 9

Observed and Expected Frequencies of School Threats by Gender

Gender	Threat	Observed (*n*)	Expected (*n*)	Total (*n*)
Female	No	34	32.743	55
Female	Yes	21	22.257	
Male	No	119	120.257	202
Male	Yes	83	81.743	
Total	No	153	N/A	257
Total	Yes	104	N/A	

Note. Observed and expected frequencies for school threat occurrences categorized by gender. Chi-square tests indicated no significant difference between observed and expected frequencies. Data were collected from K–12 educational settings between September 2022 and July 2024.

Both male and female involved cases were predominantly threat-related (roughly 40% for each). Once a threat was identified, the *severity* outcomes (immediate risk determination and formal threat assessment) were comparable across genders: Incidents involving male and female students were deemed immediate risks nearly as often (57.7% versus 52.7%, respectively), with no significant difference, χ^2 (1, N = 256) = 0.437, p = .509. Likewise, formal threat assessments were conducted in roughly four out of five male-student threat cases (78.7%) and in 74.5% of female-student instances, a difference that was not significant, χ^2 (1, N = 257) = 0.435, p = .510.

Although the overall frequency of threats and outcomes did not differ by gender, there was a significant gender difference within threat behavior. Female students were relatively more likely to make communicated threats (direct, indirect, veiled, or conditional) rather than engage in behavior-only threats. When threat types were dichotomized into *behavior-only* versus *communicated* (see RQ1b for definitions), gender was significantly associated with this distinction, χ^2 (1, N = 256) = 4.448, p = .035, φ = .132 (a small-to-moderate effect).

Among threats with known gender, only 31.5% of female-perpetrated threats were behavior-only (17 observed versus 23.8 expected), compared to 47.5% of male-perpetrated threats (96 observed versus 89.2 expected). Correspondingly, female students were responsible for more communicated threats (68.5% of female cases, 37 observed versus 30.2 expected) than males (52.5% of male cases, 106 observed versus 112.8 expected). In practical terms, this suggests that the girls in our sample more often made verbal or written threats. In contrast, the boys more often exhibited concerning behaviors indicative of a threat without a direct verbal threat. Apart from this difference in modality, other digital behavior patterns by gender were not statistically significant. For example, a higher percentage of female-involved incidents had some form of digital leakage (30.9%) compared to male incidents (19.8%), but this difference did not

reach significance (χ^2 (1, N = 257) = 3.090, p = .079). Similarly, digital leakage, threat assessments, and immediate risk rates showed no significant gender differences (all $p > .05$).

Leakage, Threat Assessments, and Immediate Risk in Threat Cases

Across all threat-related incidents, just under one-quarter involved digital leakage, or evidence of the threat or intent shared via digital means (e.g., social media posts, text messages, etc.). Specifically, 156 out of 676 threats (23.1%) had digital content associated with them (see Table 5), while the remaining 520 threats (76.9%) had no known digital leakage. In contrast, digital leakage was identified in only a small minority of non-threat cases (see RQ1c), underscoring that most digital warning signs in this dataset were linked to actual threats. Approximately half of all threat-related incidents were classified as posing an immediate risk ("Yes" in 54.6% of threats)—in 397 of 796 cases, this designation was made (missing data in <1% of cases). Likewise, a formal threat assessment was conducted in most threat incidents: 436 of the 676 threats on record (64.5%) underwent a documented threat assessment process. In total (including some precautionary assessments of non-threat concerns), 55.5% of all incidents received a formal threat assessment. These figures indicated that over the study period, schools were proactive in evaluating more than half of all incidents with a formal protocol, and they identified roughly half of all incidents as urgent situations requiring immediate intervention.

Digital Leakage, Threat Assessments, and Threat Type (RQ1b)

RQ1b asked about interrelationships between digital leakage, formal threat assessment, and types of threats (using the FBI threat categories—direct, indirect, veiled, conditional—and the SST category of behavior-only threats). Chi-square tests of independence were conducted to examine (1) whether digital leakage was associated with types of threats and (2) whether formal threat assessment implementation was associated with either digital leakage or threat type.

Digital Leakage and Threat Type

When examining the five threat categories, the presence of digital leakage did not differ significantly across types, χ^2 (4, N = 676) = 7.769, p = .100, Cramer's V = 0.10. Communicated threats (direct, indirect, veiled, conditional) were about as likely to involve digital content as one another and as behavior-only threats. For instance, as shown in Table 10, only 18.2% of direct threats (42 out of 231) had an associated digital trail, the lowest among the categories. In contrast, veiled threats (often vague or implied threats) had digital leakage in 27.8% of cases (15 of 54)—one of the higher proportions—and behavior-only threats had leakage in 27.1% of cases (83 of 306). These observed differences (e.g., 42 incidents of direct threats with leakage versus 53.3 expected; 83 behavior-only with leakage versus 70.6 expected) suggest a trend where direct threats were less likely and behavior-only/veiled threats were more likely to have digital evidence than expected. However, the overall variation did not reach statistical significance. In other words, knowing the category of a threat (for example, whether it was a direct spoken threat or a behavior-only warning sign) was unrelated to whether digital leakage would be present.

Table 10

Digital Leakage by Threat Type

Threat Type	With Digital Leakage	Total Cases	% Digital Leakage
Direct	42	231	.182
Indirect	8	48	.167
Veiled	15	54	.278
Conditional	8	37	.216
Behavior-Only	83	306	.271

Because behavior-only threats might involve different channels (e.g., posting ominous photos or videos without an outright verbal threat), the researcher conducted a focused analysis dichotomizing threat type into "Behavior-Only" versus "Communicated" threats, which combined direct, indirect, veiled, and conditional types; see Table 10). This analysis revealed a significant association with digital leakage. Behavior-only threats were significantly more likely to involve digital leakage compared to communicated threats, χ^2 (1, N = 676) = 5.159, p = .023, φ = .087. The effect size was small (φ = .087) but notable given the large sample. Among the 306 total behavior-only threat incidents, 27.1% had digital leakage (83 observed versus 70.6 expected with leakage), whereas, among communicated threats, only 19.7% had digital leakage (73 observed versus 85.4 expected). Thus, threats manifested purely as behavior (for example, a student bringing a weapon or writing a violent journal entry without directly communicating a threat) had statistically more digital leakage associated with them than directly communicating threats. Table 11 illustrates this difference, showing the higher observed count of behavior-only threats (n = 307) with digital content than the expected count under no-association conditions.

Table 11

Frequencies of Threat Type for Behavior Only and Communicated Threats

Threat Type	Total Cases	% Total Cases	Cases With Digital Leakage	% With Digital Leakage
Behavior Only	307	45.3%	83	27.1%
Communicated	370	54.7%	73	19.7%
Total	676	100%	156	23.1%

No other specific threat category stood out significantly regarding digital leakage; even the categories with the highest leakage rates (veiled and behavior-only) were not statistically different from others. It is worth noting that direct threats—often delivered in person or

verbally—unsurprisingly showed the lowest co-occurrence with digital evidence (observed 42 versus expected 53.3 with leakage), hinting that students making direct face-to-face threats may be less likely to post about them online in advance.

Formal Threat Assessment and Digital Leakage

Next, the researcher examined whether the decision to conduct a formal threat assessment was related to digital leakage. Overall, cases with digital leakage were about as likely to receive a formal threat assessment as those without. In the threat-related subsample, 58.3% of incidents with digital leakage evidence underwent a formal threat assessment, compared to 65.5% of incidents with no digital leakage resulting in formal threat assessment. This difference was not statistically significant, χ^2 (1, N = 689) = 2.784, p = .095. The observed counts were 98 assessments conducted *with* leakage present (versus 107.0 expected) and 341 assessments conducted *without* leakage (versus 332.0 expected). Thus, online or electronic warning signs did not substantially influence whether school teams initiated a formal threat evaluation process. In practical terms, schools conducted formal threat assessments for threat-related behaviors deemed concerning in most cases, regardless of whether the initial warning came via digital media or in-person channels.

Formal Threat Assessment and Threat Type

The relationship between specific threat types and the presence of formal threat assessment was also tested. There was no significant association between the threat type category and formal threat assessment, χ^2 (4, N = 676) = 2.999, p = .223. Formal threat assessments were conducted at high rates across all threat categories. For example, approximately two-thirds of communicated threats had a formal evaluation (in both direct and indirect threat cases, roughly 65–70% were assessed, based on descriptive counts), and a similarly high proportion (61.8%) of

behavior-only threats were evaluated (189 of 307). The observed versus expected counts for assessments were very close for each category. In the dichotomized view (behavior-only versus communicated threats), there was still no significant difference in formal assessment rates (61.8% for behavior-only versus 66.7% for communicated; χ^2 (1, N = 676) = 2.114, p = .146). These results indicate that once an incident was identified as a potential threat, schools were relatively uniform in applying the formal threat assessment protocol across different threat types. The likelihood of initiating a threat assessment was uniformly high, whether a student made a direct threat, a veiled threat, or exhibited threatening behavior. This is consistent with district policy, which requires caution and assessment of all credible threats, regardless of form.

Results from RQ1b indicate that digital leakage is modestly linked to threat type (with behavior-only threats yield statistically more digital leakage than communicated threats). Still, digital leakage did not markedly influence whether a case was formally threat assessed, nor did the likelihood of formal assessment differ by specific threat type. Threat assessment teams appeared to treat all categories of threats with similar seriousness, and digital evidence is present in about one in four threat cases, slightly more so for non-communicated threat behaviors.

Non-Threat Concerning Behaviors and Digital Leakage (RQ1c)

The focus of RQ1c centered on the subset of incidents concerning behaviors unrelated to explicit threats, examining their primary categories and whether any digital leakage was present in those cases (particularly those that prompted formal threat assessment). There were 121 non-threat incidents (15.2% of the total sample). These cases included a range of student safety concerns that did not involve threatening harm to others. For example, extreme emotional distress or suicidal ideation, intense verbal conflicts or bullying that stopped short of threats, possession of prohibited items without an expressed threat, or other behavioral red flags that did

not target others. Each non-threat case was coded with a primary category of concern. The most common categories in this group tended to be personal psychological crises (such as statements or behaviors indicating self-harm risk) and general safety rule violations (such as bringing a weapon or contraband without threatening anyone), followed by peer conflict/bullying incidents that were serious but not explicitly threatening. Owing to the relatively small *n*-count, the counts per category were modest (no single non-threat category exceeded a few dozen cases).

Digital leakage was relatively uncommon in these non-threat-related incidents. In contrast to the threat-related cases, where 23% had digital evidence, only about one-tenth of the non-threat cases involved digital leakage. Specifically, 12 out of 121 non-threat incidents (9.9%) had digital content associated with them (such as social media posts, text messages, or emails related to the behavior). Most non-threat concerns were identified through in-person observations or reports rather than digital scanning. Given the non-threat-related subset's low base rate of digital leakage, statistical analysis of its relationship with the concern type was limited. A chi-square test did not find a significant relationship between the primary category of non-threat behavior and the presence of digital leakage (*Frequency Count* tests for association were non-significant, $p > .05$). In most categories, the observed count of cases with digital leakage was at or near the expected count under the statistical assumption of no association. For example, in the category of self-harm/suicidal ideation, five of 40 cases involved students posting suicidal statements online (expected $n \approx$ similar), whereas, in categories like on-campus rule violations, virtually no cases had an online component (one of 35 cases). For RQ1c, the descriptive takeaway is that non-threat-related behaviors were usually identified through non-digital means. In such cases, digital leakage was infrequent and not systematically tied to any particular type of behavior.

Additional Findings Related to Digital Behavior and Potential Threats

In addition to the results tied directly to the proposed research questions, other findings emerged that provide context about digital behaviors and real-world responses to threats. These involve the role of law enforcement, the handling of immediate risks, and other practical outcomes of the threat cases.

Police Involvement

Nearly half of all threat-related incidents resulted in police involvement or notification (approximately 49.9% overall, $n = 397$ of 796 with data). Police involvement was strongly associated with the immediate risk level. Law enforcement was usually involved when an incident was deemed an immediate risk: 303 of 397 immediate-risk cases (76.3%) had police intervention, compared to only 94 of 399 non-immediate-risk cases (23.6%). This association was statistically significant, χ^2 (1, $N = 796$) = 93.817, $p < .001$, $\varphi \approx .34$, indicating a moderate relationship. In practical terms, almost all the immediately high-risk situations triggered a police response.

There was a similarly strong association between police involvement and the presence of a formal threat assessment, χ^2 (1, $N = 797$) = 145.630, $p < .001$. Incidents that underwent a formal threat assessment were significantly more likely to involve the police (346 observed with police versus 262.9 expected) than incidents that did not undergo an assessment (only 128 of 355 included police versus 211.1 expected), which suggests that the more serious the school's response (formal assessment, designation of high risk), the more likely it was to include involvement with law enforcement.

Digital and Traditional Threats and Police Involvement

There was a small but significant inverse relationship between digital leakage and police involvement. Cases that involved police were statistically less likely to have had digital leakage (only 22.0% of police-involved cases had digital content) compared to cases without police involvement (26.6% had digital content). This difference was statistically significant, χ^2 (1, N = 689) = 4.671, p = .031, φ = .082, although the effect size was small. The observed counts were 103 police-involved cases with digital leakage (versus 114.4 expected) and 366 non-police cases with leakage (versus 354.6 expected). Not all digital leaks escalated to police involvement, and not all police-involved cases had digital footprints. Schools and law enforcement seemed to respond vigorously to *any credible threat*, whether or not it appeared online beforehand.

Threat Type and Police Involvement

There was a marginally significant tendency for communicated threats to involve police more often than behavior-only threats. Among communicated threats, 71.8% ultimately had police involvement, compared to 65.2% of behavior-only threat cases, χ^2 (1, N = 676) = 3.471, p = .062). Although this difference was not technically significant at $p < .05$, it aligns with the notion that when a student overtly verbalizes or writes a threat (especially a direct threat), authorities are more likely to be called in, perhaps due to the explicit nature of the offense. Behavior-only cases (e.g., a student caught with a "hit list" or weapon but who made no direct threat) still frequently involved police (over 65% of the time) but not quite at the raw count rate of communicated threats.

Gender and Police Involvement

No significant differences were found in police involvement for threat-related behaviors by student gender (χ^2 (1, N = 257) = 0.640, p = .424). Male- and female-related threat-related

incidents involved police at similar rates (in the subset with known gender, 63.6% of female versus 69.3% of male incidents had police involvement, which was not a statistically meaningful difference. This indicates that the subject's gender did not influence the likelihood of law enforcement involvement.

Results Summary

In conclusion, the results show concerning behaviors in K–12 settings over the two years. Digital leakage was a factor in about one-quarter of threats, especially those manifested through behavior rather than direct statements, but it was relatively rare in non-threat concerns. Threat-related incidents were reasonably consistent across times of year and grade levels, with high schools contributing the most cases but no strong age-grade effects on outcomes. Gender differences in threat behavior emerged in how threats were conveyed (males more often through actions, females through communication) but not in the frequency of threats or the handling of those threats. Importantly, school safety responses (threat assessments and police involvement) closely tracked the perceived immediacy of risk rather than demographic factors or the presence of digital evidence alone. All high-risk situations underwent a formal assessment and involved a police partnership, underscoring a robust safety protocol. Additional analyses highlight that not all threats announce themselves online, and not all online warning signs lead to real-world violence, but they prompt serious preventive action. These findings contribute to our understanding of how digital behaviors intersect with real-world threat dynamics in schools, providing an empirical basis for improving threat assessment strategies by integrating digital threat assessment with traditional safety practices.

CHAPTER V

DISCUSSION

This chapter interprets the study's results on digital leakage, threat-related behaviors, and school threat assessment practices in K–12 settings (September 2022–July 2024) through the lens of the research questions and guiding theories. The discussion is organized around the main research questions (RQ1a–c), examining how the findings align with or challenge theoretical expectations from Routine Activity Theory (RAT; Cohen & Felson, 1979), the General Aggression Model (GAM; Anderson & Bushman, 2002), and Social Cognitive Theory (SCT; Bandura 1986) and empirical findings. Connections are made to existing literature, and practical implications are highlighted, particularly for enhancing school safety policy and practice in contexts like the Beaverton School District. The chapter concludes with recommendations for future research to address identified gaps and limitations. Each section below integrates the quantitative results with theoretical frameworks to illustrate how the study's findings support, extend, or complicate current understandings of school-based threats and prevention.

Patterns of Threat-Related and Concerning Behaviors (RQ1a)

Data revealed that most reported incidents were threat-related: Approximately 85% involved an explicit or implicit threat. In comparison, only around 15% were categorized as non-threat concerns (e.g., safety or disciplinary issues without a direct threat).

Patterns Associated with Season

Incidents occurred over a two-year period (September 2022 to July 2024) without any pronounced seasonal spikes. Fall months saw slightly fewer total incidents than winter or spring; however, differences in threat occurrence by season were not statistically significant. In practical terms, the likelihood of a given incident being a threat did not depend on the time of year.

Patterns Associated with Grade-level

Most incidents occurred in secondary schools as 58% involved high school students, approximately 39% involved middle school students, and only about 3% came from elementary students. Although these proportions suggest a higher frequency of threats at elevated grade levels, there was no significant correlation between grade level and whether an incident was classified as a threat or a non-threat concern, nor did grade level significantly relate to the type of threat or case outcomes ($p > .20$ in each analysis). In other words, younger students were less frequently involved in threats, but when they made threats, they were addressed similarly to those made by older students.

Patterns Associated with Gender

Gender patterns also emerged from the data. Notably, gender information was available for only 38% of cases ($n = 257$), of which 78.6% involved male students and 21.4% involved female students. This gender discrepancy indicates that males were approximately four times more likely than females to be reported as the subject of a threat-related concern, aligning with broader trends suggesting that males perpetrate the majority of violent or aggressive incidents in school contexts. The overall rates of threat involvement, however, were statistically similar for male and female cases in this subsample—the probability of classifying an incident as a threat (as opposed to a non-threat concern) did not significantly differ by gender. Likewise, once an incident occurred, the resulting outcomes (such as being deemed an immediate risk or leading to a formal assessment) were comparable between genders, with no statistically significant differences in how often male versus female cases were considered to pose an immediate risk (~58% vs ~53%, respectively) or were handled through a formal threat assessment. This suggests that school teams responded equally to threats, regardless of the student gender.

One notable gender-based difference was observed in threats: female students were significantly more likely to communicate threats (direct, indirect, veiled, or conditional threats conveyed via words or text) rather than engage in behavior-only threats (concerning aggressive behavior without an explicit verbal threat), compared to male students. Among threats where gender was known, only 31.5% of female-perpetrated threats were behavior-only, compared to 47.5% of male-perpetrated threats that were behavior-only. Similarly, females committed a higher proportion of threats that were verbal or written (about 68.5% of female cases) than males (52.5% of male cases). This difference was statistically significant, although with a minor-to-moderate effect size (φ =. 132). In practical terms, girls in this sample more often issued threats through communication (e.g., making a direct threat to someone or writing a threatening message), whereas boys more frequently engaged in threatening or violent behavior without explicitly announcing a threat. Aside from this modality difference, other digital behavior patterns by gender were not significant—for example, female-involved incidents showed a higher incidence of digital leakage (30. 9%) than male incidents (19.8%). Still, this gap did not reach statistical significance (p =. 079).

Implications for Theoretical Frameworks and Practice

These patterns provide several insights regarding the guiding theories. First, the lack of strong seasonal threat trends can be examined through the Routine Activity Theory (RAT) lens. RAT posits that crime (or, in this case, aggressive incidents) is more likely to occur when a motivated offender encounters a suitable target in the absence of capable guardianship (Cohen & Felson, 1979). One might expect that periods of decreased guardianship or increased stress—such as the beginning of the school year, exam times, or pre-holiday seasons—would lead to more threats. Indeed, the initial expectation was that incidents might spike at specific times (e.g.,

the start of the year or before breaks) when routine disruptions or stressors occur (Ahmed et al., 2023; APA, 2023). However, the data did not reveal a clear temporal pattern; threats were relatively evenly distributed across fall, winter, and spring. This finding suggests that the presence of the "motivated offender" and opportunities to threaten exist throughout the year. Regarding RAT, there was no season when guardianship diminished enough to result in a noticeable increase in incidents. Conversely, any seasonal stressors appear not significant enough to surpass guardianship in a detectable manner (Cohen & Felson, 1979; Vakhitova, 2025). It may be the case that schools maintain fairly consistent supervision and vigilance year-round or that students' motivations to make threats stem from personal conflicts and issues that are not strictly tied to the calendar. The absence of seasonal effects highlights that threat behavior is a constant concern, necessitating continuous guardianship (both physical and digital). This underscores the importance of sustaining robust threat assessment and prevention practices rather than focusing solely on anticipated high-risk months. RAT, along with the findings, would urge schools to remain vigilant during "routine" periods when complacency might set in because a capable guardian is needed to identify warning signs whenever they arise.

Although not significantly different from one another, the frequency and distribution of incidents by grade level—where high school students contribute the most threat-related behaviors and elementary students the least—aligns with developmental expectations and partially reflects insights from the General Aggression Model (GAM). GAM suggests that aggression arises from the interaction of personal and situational factors influencing a person's cognition, arousal, and affect, potentially leading to aggressive behavior. Older students (adolescents) are more likely to encounter various risk factors for making threats: They face more complex social pressures, have greater access to lethal means or knowledge about violent

events, and possess a higher cognitive ability to formulate explicit threats. Older students may also consume more violent media or engage extensively online, which the GAM identifies as situational inputs (e.g., exposure to threatening or aggressive content can prime aggressive scripts; Bushman & Anderson, 2020, Dou & Zhang, 2025, Kjærvik et al, 2025). The finding that high school and middle school students account for most threats aligns with research indicating that violence and school misconduct peak during adolescence. Elementary students rarely made threats in this dataset, which may reflect both a genuinely lower incidence (as young children are less likely to threaten serious harm) and potential underreporting (schools might address K–5 behavioral issues through internal discipline rather than formally recording them as "threats"). When young children did exhibit concerning behavior, it often lacked explicit violent intent and was qualitatively like older students' cases in terms of outcomes. This suggests that even when very young students raise concerns, schools approach the situation with similar caution, which is appropriate given that even a young child's threatening behavior (though rare) could still pose a danger or indicate serious underlying needs. From a GAM perspective, the absence of significant differences in threat outcomes by grade suggests that once a student of any age crosses the threshold of making a credible threat, the subsequent risk is taken seriously across the board. However, the overall lower frequency of threats among elementary students supports the notion that the precursors for aggressive threats (whether the cognitive ability to conceptualize a threat or exposure to violent models) are less prevalent in early childhood—a point consistent with developmental aggression literature and GAM's emphasis on both personal traits (such as impulse control developing with age) and situational influences (younger children's social world is smaller and more supervised, potentially reducing opportunities to develop violent intentions; Anderson & Bushman, 2002; Bandura, 1986; Olson et al., 2011).

Gender differences in expressing threats can be interpreted through Social Cognitive Theory (SCT) and the General Aggression Model (GAM). SCT posits that behavior is learned and modeled from others in the social environment, with the reinforcement of certain behaviors leading to greater enactment of those behaviors (Bandura, 2001). The finding that male students more often engaged in action-based threats (like bringing a weapon or acting aggressively without an explicit threat), whereas female students more often communicated threats verbally or in writing, is consistent with well-documented gender socialization patterns. Prior research has noted that males are generally encouraged (or at least modeled) to externalize aggression physically (Bjärehed et al., 2020; Coyne et al., 2018; Farrell et al., 2018). At the same time, females are often socialized to express aggression through relational or verbal means, such as social exclusion or rumor-spreading, rather than physical force, although recent research suggests these patterns are not universal and may vary by age, cultural context, and assessment method (Crick & Grotpeter, 1995; Navarro, 2016). Females in the sample tended not to brandish weapons or physically intimidate without words; instead, when involved in threats, they were likely to vocalize or write a threat. Conversely, males were more inclined to exhibit menace through actions (e.g., aggressive gestures, possessing a "hit list" or weapon) without explicitly stating a threat. SCT would explain this through observational learning and expected gender norms (Bandura, 2001)—students may mimic the behavior they see as typical for their gender. If male students have observed that high-profile school shooters or violent peers tend to act out physically (and if they have higher self-efficacy for physical dominance), they might (un)consciously follow that script. Female students might replicate more indirect forms of aggression they have observed, for instance, threatening messages or rumors, which are reinforced in media depictions of female aggression.

These differences extend existing theories by highlighting that "threatening behavior" is not monolithic and can manifest in gender-normative ways, even in a school violence context. At the same time, it is essential to emphasize that my findings showed no difference in the actual rate of threat involvement by gender when data were available. Similarly, the education system appears to treat threats from females just as seriously as those by males, as there was no statistical disparity in immediate risk or law enforcement response. This evenness in reaction to threat behaviors aligns with threat assessment best practices focusing on the behavior and context rather than demographic profiles (Cornell, 2020; Van Dreal, 2011). It also challenges stereotypes that female threats are less dangerous; in fact, females in our sample who did make threats were more likely to explicitly articulate violence, which is objectively alarming (e.g., a written hit list from a female student should not be taken any less seriously than one from a male student).

Additionally, the male predominance (around four out of five incidents with known gender-involved males) is noteworthy but not surprising. It aligns with broader criminological patterns and previous studies on school violence, which indicate that males are more frequently the perpetrators of severe aggressive acts (Madfis, 2020; Vossekuil et al., 2002), including the grim statistic that virtually all school shooters have been male (Peterson & Densley, 2021). This could be linked to GAM's personal factor component (higher trait aggression or propensities for risk-taking in males; Anderson & Busman, 2002) and to SCT's concept of modeling (boys might identify with aggressive role models to a greater degree; Bandura, 2001). Still, the fact that over one-fifth of cases involved females underscores that prevention and assessment efforts must also include female students. Female students can and do participate in threatening behavior, and sometimes in ways that may be less expected. For instance, a veiled threat by a female student

may be misconstrued as less dangerous when it is not. As noted, however, findings indicate that school authorities did not overlook female threats: The handling post-threat (immediate risk determinations, assessments, police involvement) was equivalent, which is a positive finding from a fairness and effectiveness standpoint.

In summary, the findings of RQ1a largely support several expected patterns (more threats at higher grades, primarily by males) while challenging others (no clear seasonal pattern emerged). They extend theoretical insights by illustrating how opportunities and motivations for school-based threats are pervasive rather than episodic. This aligns with RAT's emphasis on everyday routines, which creates risk if guardianship lapses. The results also refine GAM and SCT by demonstrating that while the demographics of those who make threats may follow general aggression trends, how those threats are expressed can vary by gender in line with social-cognitive norms. The absence of differences in outcomes based on demographic factors emphasizes that once a threat is posed, situational factors (such as the content or severity of the threat) take precedence over demographics in determining the response, which is consistent with the notion that situational risk (a core element in GAM's situational input) drives reactions, not the identity of the actor. These findings enhance the understanding of school threat incident profiles, reinforcing the need for *all* schools (K–12, at any time of year) to be prepared for threat incidents and that threat assessment frameworks should consider the varied forms of threat behavior. It is recommended that schools consistently ensure capable guardianship in hallways, classrooms, and online environments, as threats do not confine themselves to predictable moments. The profile of a "typical" threatener (older, male, acting out or explicitly threatening) that emerges from the data is valuable for awareness, but the data also warn against overly

narrow profiles, as a nontrivial minority were younger students or female students; therefore, schools must keep an open mind and assess threat behavior on a case-by-case basis.

Digital Leakage, Threat Assessments, and Threat Type Interactions (RQ1b)

The second sub-question (RQ1b) explored the interrelationships between digital leakage, the implementation of formal threat assessments, and the types of threats. This study defined digital leakage as evidence of a student's threat or violent intent communicated via digital means, for example, through social media posts, text messages, emails, or other online content. One key finding was that digital leakage occurred in just under one-quarter of all threat-related incidents. Specifically, 156 out of 676 threats (23%) contained digital content that served as a warning sign or part of the case evidence. Conversely, most (77%) threat cases documented no known digital leakage. This underscores that while digital leakage of intent was not uncommon, it was far from universal in school threat cases—roughly three out of four threats appeared to have been made or discovered through non-digital means (e.g., spoken directly, written on paper, observed behavior). In contrast to the threat cases, digital leakage was relatively rare among non-threat-related concerning behavior cases as only about 10% of non-threat incidents had any associated digital evidence. This difference highlights that digital warning signs were much more characteristic of actual violence threats than other types of student safety concerns, a point underscored with respect to RQ1c.

Patterns Associated with Immediate Risk and Formal Assessment

About half of all threat-related incidents in the study were deemed to pose an "immediate risk" to safety by school staff, meaning they required prompt intervention (just under 55% of threats were coded as immediate risk). A formal threat assessment—a structured evaluation process by the school's threat assessment team—was conducted for most threat cases. Of the 676

threats, 436 (about 65%) underwent a documented formal threat assessment process. When considering all incidents (threat and non-threat combined), just under 56% received a formal threat assessment, indicating that schools initiated their formal protocol in over half of the situations that came to their attention. This high rate reflects a proactive stance: More than half of all cases were scrutinized through a formalized procedure, and nearly two-thirds of all threats were evaluated by a multidisciplinary team following established guidelines.

RQ1b analyses indicated that digital leakage was unrelated to whether a formal threat assessment was conducted. Cases with evidence of digital leakage were about as likely to undergo a formal threat assessment as those without it. In numeric terms, about 58% of threats with digital leakage received a formal evaluation, compared to nearly 66% of threats without digital leakage—a slight difference in proportion but not statistically significant. The observed assessments were very close to expected counts under independence (98 assessments conducted among 168 leakage cases compared to 107 expected and 341 assessments among 521 non-leakage cases compared to 332 expected). In practical terms, school teams did not reserve formal assessments only for cases with an apparent digital trail; instead, they carried out formal assessments in most threat cases regardless of how the threat was communicated or discovered.

The analysis of threat type and assessment reinforces this finding. Again, no significant association was found between the specific threat category (direct, indirect, veiled, conditional, or behavior-only) and the likelihood of a formal threat assessment being conducted. Formal assessments were utilized at high rates across all threat categories. Roughly two-thirds of communicated threats (direct or indirect) were formally assessed, and a similarly high proportion (about 62%) of behavior-only threats were also evaluated. Even when simplifying the comparison to “communicated versus behavior-only” threats, there was no significant difference

in assessment rates, with close to 67% of communicated threats compared to about 62% of behavior-only threats received assessments. These statistics indicate that once an incident was identified as a potential threat, schools uniformly applied their threat assessment protocols independent of the threat type. Such consistency is in line with district policies that require all credible threats to be evaluated cautiously, regardless of how they are conveyed (Van Dreal et al., 2022).

Patterns Associated with Threat Type

While digital leakage did not statistically relate to whether an assessment occurred, one notable relationship was uncovered: The relationship between digital leakage and threat type. When examining the five specific threat categories individually, the differences in leakage prevalence did not reach conventional significance. Communicated threats of various kinds (direct, indirect, veiled, conditional) were equally likely to have digital content associated, and none of those categories stood out dramatically from the others in terms of frequencies. However, a statistical pattern emerged when threat types were dichotomized into "behavior-only" versus "communicated" threats.

In contrast, a communicated threat involves an explicit statement or message of intent to harm. Behavior-only threats were significantly more likely to affect digital leakage than communicated threats. Specifically, over 27% of behavior-only threat cases had digital evidence, compared to less than 20% of communicated threat cases. Although the effect size is modest ($\varphi \approx 0.09$), the finding is notable given the large sample size. In raw frequency counts, 83 out of 306 behavior-only threats had digital leakage (versus ~70.6 expected if no association), whereas 73 out of 370 communicated threats had leakage (versus ~85.4 expected). Thus, threats that were not directly spoken or written by the student were more likely to leave a digital footprint than

those that were directly articulated. Another way to interpret this finding: Students who *only* acted in threatening ways without saying anything were disproportionately often found to have posted, messaged, or otherwise signaled something online related to their threatening behavior, whereas those who outright verbalized a threat face-to-face or in writing were a bit less likely to have a parallel digital footprint. Interestingly, the majority (almost 73%) still had no digital leakage, even for behavior-only threats. Therefore, stakeholders should not assume a behavior-only case will automatically have online signals. However, behavior-only cases showed a higher co-occurrence with digital warning signs relative to communicated threats.

Meanwhile, no other specific threat category deviated enough to be significant. Even the threat categories with the highest observed leakage rates (veiled and behavior-only) were not drastically higher than others. Direct threats, which often occur in person impulsively, unsurprisingly had the lowest co-occurrence with digital evidence (only ~18% had any digital trace). It appears that students who threatened someone in person (e.g., "I'm going to hurt you") typically did not also post it online beforehand, which is intuitive if the threat was made in the heat of the moment or within a contained context (NASP, 2021).

Implications Related to Theoretical Frameworks

These findings regarding digital leakage and threat response hold significant implications for our theoretical understanding. Starting with RAT, digital leakage in approximately one-quarter of threats can be viewed as an opportunity for guardianship in the digital environment. RAT emphasizes that the absence of capable guardians facilitates offenses (Cohen & Felson, 1979). In this study's context, a social media feed, chat group, or email inbox could serve as an additional "place" needing guardianship. When a student broadcasts violent intent online, that digital platform becomes the scene where a motivated offender is revealed. If no one is

monitoring or paying attention (i.e., a lack of capable guardianship digitally), the opportunity for prevention is missed. The finding that many serious threats did *not* have digital leakage (77% did not) suggests that not all offenders leave an obvious trail. Some motivated offenders operate entirely offline or keep plans to themselves, which RAT would frame as fewer opportunities for guardians to detect them.

On the other hand, the fact that a sizable, and thus practically meaningful, minority leaked their intentions online confirms the concept of leakage as a critical opportunity for intervention. Prior studies on school shooters and violent actors have noted that leakage (of any form) is standard. For example, Meloy and O'Toole (2011) described leakage as a prevalent behavior in which a person intentionally or unintentionally reveals clues about an impending violent act.

My findings quantify digital leakage and show it is present in roughly 1 in 4 threatened incidents, providing empirical support to the idea that online behavior can serve as an early warning system. This extends prior qualitative observations (e.g., case studies of attacks often finding a Facebook post or manifesto in hindsight) by putting a percentage to digital warning signs in a broader range of cases, not just consummated attacks. Importantly, RAT also underscores the need for capable guardians—in this case, school officials, parents, students, or even algorithms—to be watching those digital spaces. Regardless of digital leakage, the uniform application of threat assessments might indicate that schools treat digital tips similarly to traditional ones. Still, it might also suggest that schools do not yet have differentiated protocols for detecting a digital warning versus when a threat comes via other channels (ICDTA, 2023). The lack of influence of digital evidence on whether an assessment was done suggests that teams responded to *any* credible report, which would be framed as a strength of current practices (NIJ,

2022). However, it also might reflect that many digital leaks were not discovered *until* someone reported them, or an incident occurred. For example, proactive digital assessment might not have been systematically in place, which would be framed as a weakness of current practices.

In RAT terms, digital guardianship is still developing. Schools primarily reacted to digital leakage when it was brought to their attention rather than actively patrolling cyberspace to catch threats early. With robust digital scanning, one might expect cases with digital leakage to be *more* likely to get formal assessment (since a digital warning could prompt an early assessment before a situation escalates). Instead, the study found no statistical difference, implying that many digital leakages were folded into the process only after some channels identified the threat. A practical takeaway is that strengthening digital guardianship (for instance, having systems or personnel that actively look for warning posts) could potentially lead to even earlier threat assessments and interventions in those ~23% of cases that offer such clues. At the same time, the findings caution that many threats will not present digital evidence, so traditional guardianship (e.g., students reporting suspicious behavior, staff vigilance in person) remains vital. The inverse relationship between digital leakage and police involvement found in the additional analysis (with police being statistically slightly less likely to be involved in cases that had digital leakage) supports this notion: It appears the most immediately dangerous cases, which overwhelmingly got the police involved, tended to be those with no prior digital signals—perhaps indicative of surprising, in-person threats. This suggests that when offenders broadcast their intent online, it might paradoxically give schools more lead time to handle it internally before it becomes an emergency, whereas threats that "come out of nowhere" face-to-face trigger urgent law enforcement action. In short, RAT's components are reflected here as motivated offenders sometimes signal themselves via digital targets, and if guardians catch those signals, they can

intervene before law enforcement is needed; otherwise, the situation may manifest as an immediate crisis offline.

These findings also engage with the General Aggression Model (GAM) by highlighting the role of digital stimuli in the aggression process (Anderson & Busman, 2002). The observation that behavior-only threats had a higher incidence of digital leakage than communicated threats is revealing. Initially, one might assume that a student who physically threatens others without speaking is purely an offline issue. However, data indicate that many such students were also active online in ways that foreshadowed their violent behavior, such as posting a photo of a weapon or writing something ominous that stops short of a direct threat (Peterson & Densley, 2021). This aligns with Peterson and Densely's research, suggesting that online environments can precipitate or amplify real-world aggression. Hinduja and Patchin (2019) and Patton et al. (2016) have documented how conflicts and aggression among youth can escalate via social media exchanges and digital communications, often spilling over into physical violence.

From a GAM perspective, exposure to aggressive content or antagonistic interactions online can serve as a situational input that increases a youth's aggression-related cognition and arousal. For instance, a student might get into an argument on a group chat or be influenced by violent extremist content; these inputs could prime them for aggressive behavior at school, even if they never explicitly announce a threat. My finding that those who engaged in behavior-only threats often had an online component is consistent with the idea that digital experiences fed into their aggressive behavioral output (Oshodi, 2024). It extends GAM by providing concrete evidence in a school setting that the modern "situational factors" for youth aggression often include digital interactions. The digital leakage in these cases may not have been an outright

threat, but possibly aggressive posturing or consuming violent material that contributes to the student's aggression (Huesmann, 2007). This supports the argument that threat assessment teams should consider a student's online activities as part of evaluating risk, not only looking for direct threats but also patterns of online aggression or fixation that could escalate aggression, a process well-described by GAM's routes to aggression (Anderson & Busman, 2002).

Conversely, why would communication threats have relatively fewer digital traces? One possibility is that some communicated threats are impulsive or context-specific; for example, a student blurts out a threat during a confrontation without premeditation or online planning. In those scenarios, the aggressive act (the threat itself) might occur without a long build-up that could be tracked. GAM would view this as more of an immediate appraisal and outburst, less influenced by prolonged exposure to online stimuli (Anderson & Busman, 2002). The data noted that direct threats (often spontaneous verbal threats) had the lowest rate of digital leakage (approximately 18%). This suggests two "paths" of threats: one path where a student stews and possibly signals online, with aggression built up through digital reinforcement, leading to a behavior-only or veiled threat, and another path where a student erupts in a threat without prior online activity, perhaps indicating more reactive aggression (Segura, 2020; Uddin & Rahman, 2022). Both paths are important, but the former is where digital assessment can make a difference in prevention. In contrast, the latter requires other assessment and intervention strategies, like in-the-moment de-escalation. Further exploration of the theory fell outside the scope of this study; consequently, some of the following ideas will require deeper examination in future research.

SCT provides another valuable perspective on these dynamics. SCT emphasizes observational learning, the imitation of models, and reciprocal interactions between personal

factors, behavior, and the environment (Anderson & Bushman, 2012; Bandura, 2001). The concept of digital leakage itself can be connected to SCT: Students who leak threats online may be modeling behaviors they have observed from others. For example, many school shooting perpetrators in the past left behind manifestos, social media posts, or warning videos; these cases are often publicized. A student absorbing those stories might subconsciously learn that "posting about my violent intentions" is something people do before an attack. In this way, leakage can be a socially learned behavior reinforced by the attention it garners if peers respond online or if it successfully scares others. The finding that a measurable proportion of students did post or message their intent (23% of threats) supports the idea that today's youth may have internalized the notion that one communicates plans or feelings of anger via social media. SCT's concept of reciprocal determinism is relevant; a student's online behavior (posting a threat) can alter their environment by prompting a response; for instance, friends might react with alarm or encouragement, or authorities might intervene, influencing the student's subsequent behavior. Some students might even test the waters by leaking online to gauge reactions, which SCT would frame as seeking social feedback to inform their next steps, increasing self-efficacy if not caught or deterring if confronted (Bandura, 2001). These patterns align with broader observations that youths' online and offline behaviors are interconnected (Anderson & Bushman, 2012).

Although I did not have specific data to analyze these patterns directly, SCT highlights the role of self-efficacy and expectations: a student who sees another get caught from a social media post might decide not to post their threat, having low self-efficacy for getting away with it, whereas a student who sees others brag about violent plans without immediate consequence might feel emboldened to do the same. The uniform handling of threats in the sample, with schools consistently assessing and involving police for high-risk cases, sends a clear message

that any threat will be taken seriously. If that message circulates among students, it could discourage some from making threats or encourage those who see something to report it. On the other hand, the data show that not all threats led to arrests or severe outcomes, especially if they were not immediate. How peers interpret that is unknown.

The gender difference in digital leakage (females showed a non-significant trend toward more leakage) might also be considered with SCT: girls may be more likely to express themselves in writing (online) rather than physical action, consistent with observed behavior patterns. Although not statistically confirmed here, this could be explored in future research. The fact that it was close to significant suggests that with a larger sample, we might find that female students who make threats tend to post about them more than male students do. If true, that would indicate that digital scanning could be instrumental in catching threats involving female students, whereas male students might require more in-person observation. This nuanced understanding could help tailor threat detection strategies (though every case is unique).

Implications Related to Practice

The findings imply that schools should integrate digital information into their threat assessment processes but not rely on it exclusively. The results show that digital leakage is a valuable warning signal when it occurs, but its absence does not indicate a lack of threat. For example, schools in the Beaverton School District (BSD) could consider implementing more systematic digital threat assessment (either through dedicated staff or safe reporting tools) to identify instances where students broadcast danger signs online. At the same time, the high rate of formal assessments, even without digital evidence, suggests that BSD's current protocol (modeled after Salem-Keizer Cascade) is robust—staff do not wait for a social media post before acting; they respond to any concerning behavior or report. This is a strength that should be

maintained. The fact that behavior-only threats often have digital correlates is significant for practitioners: If a student exhibits warning behaviors, such as fascination with weapons or intense anger, but has not made a direct threat, teams should proactively investigate that student's online activity. The findings provide empirical support for this practice, validate the additional "behavior-only" category introduced by the data provider (SST), and demonstrate that such cases frequently intersect with digital behavior. The findings support the argument that schools should pay close attention to those behavior-only cases and treat them within the threat management framework, including checking for digital leakage that might have been a catalyst or an after-the-fact warning.

Another practical takeaway was the confirmation that schools apply formal assessments across threat types – a commendable consistency that aligns with best practices. This indicated a level of maturity in the threat assessment system: Teams appeared to not be biased by whether a threat was direct or veiled and investigated thoroughly regardless. In BSD, which follows established threat assessment protocols, this finding reinforces the importance of maintaining fidelity to the protocol for *all* threat-related cases. Even if a threat seems low-level or a "joke," a formal screening should occur, which appears to have happened in the study data. Additionally, the strong association between immediate risk classification and police involvement (76% of immediate risks had police intervention) showed that schools correctly escalated the most dangerous cases to law enforcement. Interestingly, some 24% of immediate risks did *not* involve the police, which may merit review; however, it is possible that those were cases where the threat was mitigated quickly by other means, or the police were notified but did not formally intervene on-site. The moderate association between risk level and police action indicated a clear, though not absolute, correspondence. The finding of a slight inverse relationship between digital threats

and police involvement, with digitally leaked threats less likely to involve police than non-digital threats, suggests that when a threat is caught early through digital detection, schools might handle it at a lower level (e.g., discipline or mental health intervention) if it has not escalated to an imminent crisis. This pattern, while small in statistical effect, implies that not all online threats result in SWAT teams at the door—many can be resolved without heavy law enforcement if identified in time and assessed as not immediate.

On the other hand, when a student makes a direct threat face-to-face or when a weapon is discovered (without any digital trace beforehand), schools often have no choice but to involve the police immediately for safety. This nuance is crucial for policy: Districts should establish clear guidelines for involving law enforcement in cases of online threats. Current data suggest that schools may already be making such distinctions implicitly. Communicated threats tend to show a trend toward increased police involvement compared to behavior-only incidents (72% versus 65%, $p = .062$), indicating that explicit threats may be slightly more likely to activate law enforcement, possibly because an outright threat (particularly a direct one) constitutes a clear legal violation and raises greater alarm. This aligns with the notion that explicit threats leave less ambiguity, and thus, authorities are called in more readily. At the same time, in a behavior-only case, for instance, a student caught with a knife but who said nothing, the response might sometimes be managed administratively. In many cases, as observed, police are still involved approximately 65% of the time. None of the above diminishes the seriousness of any threat, but the findings offer insights that could help refine threat triage practices.

In theoretical terms, results associated with RQ1b broadly support integrating digital behavioral analysis into threat assessment, an approach advocated in emerging research. By empirically demonstrating that behavior-only threats are linked with digital signals, the study

extends the SCT and GAM frameworks into the digital realm: It shows that online and offline aggression are interwoven, reflecting reciprocal determinism (students' environment now includes online communities that affect their behavior) and multi-path aggression activation (situational factors like digital content contributing to aggressive action). It also supports RAT's notion that new "places" (cyberspace) need guardians. The data challenges any simplistic view that scanning digital media alone will solve threat detection—many threats give no digital warning—hence, any prevention strategy must be multipronged. Furthermore, the lack of effect of digital presence on formal assessment use might challenge an expectation (hypothesized in our study and others like Fein et al., 2002) that cases with digital leakage would be treated as more serious or more likely to escalate to formal intervention. The results did not indicate a presumed correlation; this may suggest that digital leakage does not correlate with a higher actual risk or that schools already identify most threats through other channels, resulting in a diminished correlation. It might also indicate that when a digital threat is detected, it is addressed like any other threat. Overall, these findings emphasize a crucial point: Digital leakage is a significant piece of the puzzle, but it represents just one aspect among many in threat assessment. Effective school safety practices must incorporate digital evidence into the traditional threat assessment frameworks without bias, treating digital threats as seriously as verbal threats and, conversely, not assuming a case is low risk solely because no digital evidence is found. The findings reinforce recommendations from threat assessment experts that teams should gather thorough background information for each case, which includes checking a student's social media or digital communications. In practice, districts like BSD can use this evidence to justify investing in training staff on digital threat assessment—ensuring that someone is tasked with reviewing the student's online activity within legal and ethical bounds for every threat case.

Furthermore, the results support strong collaboration with law enforcement for grave threats, as nearly all high-risk threats involve police. They also suggest that not all threats will be detected by flashy online warnings; some will only be known when a student or teacher comes forward or an incident happens, which underscores the need for maintaining a positive school climate where students trust adults with information as peers might be aware of a threatener's intent even if it is not posted publicly. Encouraging students to report concerning statements or posts, through initiatives like anonymous tip lines, such as SafeOregon, or the new federal bystander reporting toolkit, is a practical step that aligns with these findings.

Non-Threat-Related Concerning Behaviors and Digital Leakage (RQ1c)

The third research question (RQ1c) examined the nature of incidents that were *not* explicit threats—other concerning behaviors—and whether those incidents involved digital leakage. This subset comprised about 15% of the incidents (121 out of 798). These non-threat cases included a range of student safety concerns that did not entail a direct threat to others. Common examples included students experiencing extreme emotional distress or suicidal ideation, severe bullying or interpersonal conflicts that stopped short of threats, possession of prohibited items (like weapons or drugs) without an expressed intent to use them against others, and other "red flag" behaviors, such as disturbing writings or ideations that were not directed at a specific target. SST coded each of these cases with a primary category of concern (e.g., self-harm risk, bullying incident, weapon possession), and the frequencies of these categories were distributed—no single category dominated, given the relatively small frequency count per category (at most a few dozen in each). The key finding for RQ1c was that digital leakage was relatively uncommon in non-threat incidents. Only 1 in 10 cases (12 out of 121 non-threat incidents) noted a digital component. This contrasts sharply with about 23% in threat-related

cases, highlighting that digital traces were much less frequent when no threat was present. Statistical analysis confirmed no significant association between the type of non-threat concern and the presence of digital leakage. In most categories, the observed number of cases with digital leakage was at or very close to the expected number of digital occurrences, which were random, indicating no strong pattern. For example, a few self-harm cases involved students posting suicidal statements or cries for help online, which would be instances of digital leakage in that category, but this was roughly in line with expectations and not enough to constitute a statistically significant relation.

One interesting note from the results is that some non-threat cases triggered formal threat assessments, perhaps out of caution when the report appeared ambiguous or alarming. For instance, if a student posted something online that seemed like a potential threat, the school might have initiated a threat assessment, only to determine upon investigation that it was a self-harm reference or venting not aimed at others. Such cases illustrate how digital leakage can sometimes lead schools to investigate a situation as a potential threat, even if it ultimately is not one. For example, a student might post a message like, “Something big is going to happen tomorrow, you’ll see,” which could be interpreted as a threat and prompt a full assessment. However, later, the team finds the student meant self-harm or was referencing something else entirely. These instances were rare in our dataset, but they underscore the complexity of interpreting digital leakage. They also show that the school teams were erring on the side of caution: If in doubt, teams proceeded with assessment as if the behavior could be a threat, which is generally best practice. It is worth noting that some of these non-threat cases did activate formal threat assessments, usually out of an abundance of caution when initial reports were ambiguous. In the data, a few incidents initially investigated as possible threats (hence

undergoing a threat assessment) ultimately turned out to be non-threat concerns (e.g., a student's online post appeared threatening but was referencing self-harm). In such instances, by definition, digital leakage was the precipitating factor that brought the case to the threat assessment team's attention. However, analyzing patterns within that specific scenario was difficult because only a few non-threat cases underwent the formal threat assessment process (and most of those had digital clues). For RQ1c, the descriptive takeaway is that non-threat-related behaviors were usually identified through non-digital means. In such cases, digital leakage was infrequent and not systematically tied to any particular type of behavior. The broader descriptive takeaway, however, is that most non-threat-related concerns were identified and handled through traditional, non-digital channels. In most cases, these issues came to light via in-person observations, reports from students/staff, or other non-digital reporting avenues. Digital leakage was the exception rather than the rule for these problems.

Implications for Theoretical Frameworks and Practice

The RQ1c findings highlight an important boundary condition for the role of digital leakage; it seems considerably more pertinent to targeted violence or threat situations than to other forms of problematic behavior. Logically, "leakage" in threat assessment literature (Fein et al., 2002; Meloy & O'Toole, 2011) primarily pertains to attackers or potential attackers revealing their intent to commit violence. When a student does not intend harm to others, they are less incentivized to indicate violent intent online. Findings reinforce this distinction. For instance, a student who is severely depressed may share their feelings online, but that is not "leakage" of a plan to hurt someone else, but rather, a cry for help. A student engaged in bullying might post hurtful comments about a peer. Still, unless they threaten violence, those posts may not be flagged as needing a threat assessment (although they might be managed as a disciplinary issue).

RAT and GAM are less directly applicable to many of these non-threat cases because they focus on predatory or hostile intent. However, certain elements can still be considered. For example, from a RAT perspective, the low incidence of digital leakage in non-threat cases indicates fewer "motivated offenders" who broadcast their motivations online. Many non-threat cases involve the student as a potential *victim* (e.g., suicidal ideation) or revolve around rule-breaking without an interpersonal target. The RAT framework (offender-target-guardian) does not perfectly fit, for instance, a suicide risk case. There is no external target, and the "guardian" needed relates more to mental health intervention than crime prevention. We observe that capable guardians (teachers, counselors, peers) frequently identify these non-threat concerns through direct observation or conversations rather than scanning digital spaces. This suggests that, for issues like self-harm or general misbehavior, schools may still depend on traditional guardianship (relationships and observations) rather than digital assessment. However, there were a few instances of digital disclosure of self-harm intentions, indicating an area of overlap—where digital guardianship could also save lives by identifying personal crises. One could conceptually apply RAT by asserting that the "crime" to be prevented is self-harm or victimization, with the "motivated actor" being a student in crisis; digital posts about self-harm could be regarded as leakage of that intent. If no one intervenes (the absence of a guardian in the digital realm), the student might engage in self-harm. Scholars have noted that social media can provide indicators of suicidality (e.g., subtle cues in posts) and that proactive digital scanning could allow for earlier intervention (an ethical debate in itself; Marchant et al., 2017).

While this study's focus was on threats to others, this finding encourages schools also to consider digital scanning for signs of self-harm or victimization. The theoretical frameworks in this study did not explicitly address suicidality or non-aggressive behaviors. Thus, the findings

extend the discussion beyond traditional crime/aggression theories, underscoring the need for a multifaceted approach to student safety. A theory like SCT can partially apply; students sometimes model behaviors like self-harm challenges or venting online because they observe peers doing so (e.g., "suicide games" or contagion effects online). Therefore, an SCT perspective would suggest scanning for trends where students might imitate harmful behaviors they see on social media, for example, the 2022 viral challenges that encouraged school vandalism or threats on TikTok. Such instances exemplify where social learning resulted in bursts of non-targeted but dangerous behaviors. The data revealed some intense bullying cases—SCT would remind us that aggression can be learned and normalized in certain peer groups, which often now communicate digitally. However, suppose those bullying cases did not involve explicit threats. In that case, they may not produce digital leakage detectable by a threat assessment mechanism, even though they might involve significant digital communication (e.g., cyberbullying). It is conceivable that because cyberbullying is prevalent (estimates suggest a majority of teens have witnessed it; Vogels, 2022), schools prioritize only those instances that escalate. There might be an underrepresentation of pure bullying cases in this study's data because unless there was a safety concern, they may be addressed by deans or counselors rather than the threat assessment team.

An unexpected insight from RQ1c is how the formal threat assessment process sometimes intersects with non-threat cases due to digital leakage. This highlights a nuance in practice: Teams must differentiate between *threats to others* and *other concerns* quickly and accurately, especially when the initial report is a digital message. Misinterpretation can occur in both directions—a non-threat can look like a threat (false positive), or a real threat could be mistaken as a joke or non-credible (false negative). The findings show that in a few cases, the former happened (false alarm leading to an assessment). Fortunately, those were resolved as non-

threats. One might infer that there could also be cases (not apparent in this study's data) where a real threat was initially thought to be just "venting" and not taken seriously; those would be more problematic. This highlights the importance of context in accurately interpreting digital content. Having diverse expertise on the team (counselors, administrators, maybe law enforcement) is beneficial, as they can collectively assess linguistic and behavioral nuances. It also underscores why SCT's emphasis on understanding the individual in context (reciprocal determinism; Bandura, 1986) is crucial: The meaning of a digital statement can depend on the student's environment and personal state. Suppose a student has been bullied (environment) and has a history of depression (personal factor). In that case, a post saying "you'll all be sorry" might indicate suicidal ideation (wanting others to feel remorse after they are gone) rather than a threat to hurt classmates—two very different situations that require distinctly different interventions. The study hints at this scenario (i.e., students referencing self-harm being initially treated as potential threats). Therefore, the findings challenge us to refine our theoretical and practical frameworks to incorporate more concerning behaviors. Pure threat assessment models guided by RAT/GAM may need augmentation from models of suicide prevention or trauma-informed approaches when dealing with cases that masquerade as threats.

In summary, the results of RQ1c indicate that digital leakage is predominantly linked to targeted threat cases rather than general safety concerns. The absence of digital leakage in most non-threat instances emphasizes that schools cannot rely solely on social media scanning to identify every serious issue; many significant problems (such as a student quietly planning self-harm or a brewing fight) may never be revealed online ahead of time. Traditional communication methods—such as students confiding in teachers and teachers observing changes in behavior – remain essential. For cases that did involve digital elements (like suicidal posts), it suggests that

threat assessment teams and suicide risk assessment teams (often separate functions in schools) should collaborate. A practical implication is that schools ought to have protocols to swiftly involve the appropriate response team when a digital warning is detected: If a behavior is violent or threatening, engage the threat assessment process; if the behavior appears to indicate self-harm or victimization, initiate mental health crisis protocols. For instance, the BSD might ensure that its Public Safety Department (which handles threats) closely coordinates with its Student Services or counseling team for situations where the distinction between a threat and a cry for help is unclear. This also highlights the need for policy adjustments—definitions of "threat" in school policy may need to be clarified so that, for example, a self-harm post is not treated punitively as a threat but rather is met with support.

Theoretically, these findings remind us that not all school safety issues are based on aggression. Consequently, theories of aggression, such as the GAM, or victimization, like the RAT, likely have limitations. A comprehensive approach to school safety should incorporate theories related to youth development, mental health (to understand self-harm), and social behavior (to address issues like bullying). The study's collective theoretical framework did not explicitly include theories such as the Interpersonal Theory of Suicide or General Strain Theory, which could be relevant for cases not involving threats. The results underscore the need for a multi-theory approach—while RAT, GAM, and SCT adequately address the targeted aggression domain (the primary focus of this study), other frameworks are likely necessary to explain and address the remaining cases more fully. This insight might guide future research by expanding theoretical integration to encompass broader concerning behaviors that schools may encounter.

In conclusion, addressing RQ1c, non-threat-related behaviors typically manifest without digital leakage, which is usually detected and managed through non-digital means. Digital

guardians, such as social media scanners, play a much smaller role here than in threat cases. For school practitioners, this reinforces the importance of maintaining strong in-person relationships and communication channels so that students in distress or involved in misconduct are noticed and helped, even if they never post about it online. Additionally, it encourages a balanced investment. While resources should undoubtedly be devoted to scanning for violent threats online, resources are also needed for counselor staffing, student support programs, and anti-bullying initiatives that operate in the interpersonal realm.

Overall Implications for School Safety Policy and Practice

Across all three research questions, findings have significant practical implications for how schools develop policies and procedures to prevent violence and manage threats.

Multifaceted Technical Scanning

Broadly, the results call for a more integrated approach to threat assessment that incorporates digital threat scanning into existing school safety practices and a reaffirmation of the importance of consistent protocols (like formal assessments) and strong collaboration with law enforcement and mental health services. One of the most straightforward implications is the need for schools to systematically identify and address digital leakage. Because roughly 23% of threats in our study involved digital leakage, ignoring the digital sphere would mean missing nearly a quarter of severe cases. BSD and similar districts might consider investing in tools and training for digital threat assessment. This could include using software that scans public social media posts for local school-related threats, subscribing to services that alert schools to specific keywords, or designating staff to review social media when a concern is raised. It is essential to do this in an ethical and legally compliant way (respecting privacy and free expression rights). Still, there are established methods to focus on public or volunteered information (for instance,

accepting anonymous tips that include screenshots of concerning posts). The goal is to act as a *capable guardian in digital environments*. Many districts have begun this process by creating multidisciplinary threat assessment teams that now include a digital security specialist or training school resource officers and safety personnel in basic OSINT (open-source intelligence) techniques to track online threats. The findings support such practices.

For example, the district could partner with a company or a university research team to implement a system that flags potential threats on social media in real-time for one school year and then evaluate its effectiveness. This pilot could help refine which signals indeed predict incidents and how to reduce false positives. Many behavior-only threats had digital precursors; thus, scanning should not be limited to explicitly threatening words. Still, it should also look at content like students posting images of weapons, suicidal or violent ideation, or extremist propaganda. These might be subtle leakage indicators that a student is on a pathway to violence. The GAM supports this, as such content can fuel aggressive outcomes, and the data confirmed those links. By catching these signals, schools can intervene earlier, for instance, by convening a threat assessment before any direct threat is made. This shifts some approaches from reactive (after a threat is made) to proactive (based on leakage as an early warning). Embracing digital leakage as an early indicator could help revolutionize how schools approach threat detection and assessment, shifting from reactive to more proactive measures.

Professional Development and Training

Staff training is critical alongside technical scanning. Educators, administrators, and youth services officers (also known as school resource officers) need to recognize digital leakage and know how to respond effectively. A practical implication is to update threat assessment protocols and training materials to explicitly address digital evidence. For example, BSD might update its threat assessment handbook (based on the Salem-Keizer Cascade model) to include a checklist item: "Check for digital leakage (social media, texts, etc.) related to the threat." It could also include example case studies of how digital clues were handled. Training sessions can simulate scenarios where a threat is discovered via a screenshot from Instagram versus a handwritten note, discussing any differences in approach. The findings that teams were equally likely to do formal assessments with or without digital input is reassuring—it means staff already treat any substantive information seriously. However, staff could benefit from guidance on interpreting various forms of digital leakage. For instance, a student posting lyrics from a violent song versus posting a hit list—both are "leakage" but of very different severity (Özgür, 2020; Siddiqui & Schultze-Krumbholz, 2023). Guidelines could be developed (in consultation with mental health professionals) to help assess the content of digital leakage: Does it express intent? Does it name a target? Is it just venting or also planning? The study showed that misinterpretation is possible (some self-harm posts looked threatening), so training should also cover the importance of context. Schools could formalize digital behavior analysis as part of their threat assessment decision-making. The data supports this integration, demonstrating that digital behavior provides additional insights but must be weighed along with other factors (because it did not dictate outcomes like assessment use or police calls).

The results reaffirm that involving law enforcement is a common and often necessary practice when a case is deemed high risk or when a formal threat assessment is conducted. Nearly half of all incidents in the dataset had police involvement, and especially those labeled immediate risks (about 76% of high-risk cases) did. BSD should maintain strong partnerships with local police, ensuring clear communication channels for threat cases. The moderate effect size association is consistent, reflecting standard safety protocols. However, not every case with digital threats has police involvement, and vice versa, meaning schools are making nuanced decisions. One implication is to develop clear criteria or decision trees for when to involve law enforcement in a threat case, including those discovered online. These nuanced decisions should be documented so that they can be applied consistently. Given the slight inverse relation observed (digital cases are less likely to have police, possibly because they were assessed as having lower immediate risk), schools should examine whether there is any unintended hesitation to involve police for online threats. Training and protocols should reinforce that any explicit threat of serious violence, regardless of medium, merits law enforcement notification—even if, ultimately, it is not an immediate 911 emergency, police can assist with an investigation (e.g., tracing the source of a social media threat, which they are better equipped to do). This close collaboration is a best practice that needs to continue. In BSD's context, having a Youth Services Officer (YSO) or a direct liaison to the Beaverton Police on the threat assessment team can facilitate this, ensuring that information flows both ways.

Integrating Mental Health Supports

Collaboration with mental health professionals is essential. Many threats overlap with mental health issues, as a student making a threat may be in crisis or experiencing psychological difficulties. Additionally, non-threat cases such as suicidal ideation are strictly mental health

concerns. BSD should ensure its threat assessment team includes or has access to school psychologists or counselors. The study's findings about non-threat cases highlight that what seems threatening may indicate a different kind of crisis requiring counseling instead of security measures. A practical policy implication is to implement a dual-path system. When a case involves a threat *and/or* extreme personal crisis, convene the threat assessment and mental health crisis teams as needed. The Oregon School Safety and Prevention System guidance (ODE, 2021) already calls for multidisciplinary approaches, including behavioral safety and student wellness resources. The findings reinforce that guidance by showing the diversity of cases schools face.

Standardizing Threat Assessment Protocol

The evidence that formal threat assessments were used uniformly across threat types and demographics suggests that the threat assessment model is being applied with fidelity. This is an encouraging sign that policy is being followed. This implies that school districts should continue standardizing their threat assessment procedures and ensure all staff members know and follow them. The BSD, part of Oregon's statewide threat assessment system development, should continue emphasizing training in the model to maintain this consistency. One recommendation is to conduct regular case reviews or audits. For instance, review a sample of threat cases, including some with digital leakage and some without, to ensure that each step—from initial report to final resolution—was completed according to protocol. Given the finding that some immediate risk cases did not have a formal assessment, BSD might check that *every* high-risk designation indeed came with a formal threat evaluation. If any gaps are found, those are training and standardization opportunities. The findings showed consistent assessment (e.g., no bias by gender or type in who gets assessed), which is a testament to good practice. Continuing education and possibly certification of team members can help maintain standards.

Consistent and Transparent Communication and Reporting

Additionally, disseminating these findings to school staff can reinforce why the protocols exist: For example, explaining that BSD assesses all threats, even those that seem minor, because recent data show it is impossible to predict which threat will have serious intent. This kind of data-driven justification may reasonably bolster staff buy-in. Another practical implication involves recognizing the gender-related patterns in threat manifestations. While policies should not differ by student gender, responses did not vary in the study; awareness of these patterns can decrease potential bias and enhance threat triage. Staff can be mindful that a male student's highly concerning behavior (even without a spoken threat) should trigger as much alarm as a verbal threat from a female student. It appears teams generally already recognized this, as formal assessment rates were similar, and behavior-only cases were taken seriously. Essentially, it is vital to reinforce to staff that threat assessment is behavior-based, not profile-based, and to share data demonstrating why students of any gender or grade can pose a threat and must be evaluated based on the case's specifics, not assumptions. If supported by further research, the pattern of females more frequently leaking information digitally might suggest tailoring some prevention outreach to female students regarding the seriousness of making threats online. For male students, interventions might focus on addressing aggressive behaviors and encouraging them to discuss problems before acting. These nuances can be incorporated into violence prevention programs by schools, such as targeted social-emotional learning curricula that address different expressions of anger for males and females.

The findings highlight that not all threats will be directly observed by staff, particularly digital leakage, as peers are often the first to notice a concerning post or message. Therefore, it is important to encourage and facilitate bystander reporting. BSD can enhance programs like

SafeOregon, the state's anonymous tip line, or internal reporting apps by promoting them and educating students on their significance. The Secret Service and CISA's 2023 K-12 Bystander Reporting Toolkit (Mussington & Alathari, 2023) serves as a valuable resource to guide these efforts. It emphasizes that success stories, such as threats that were averted thanks to a student's report of an online post, can help build a culture where safety reporting is normalized. This approach aligns with SCT by fostering a positive norm of looking out for one another and viewing reporting not as "snitching" but as potentially lifesaving.

Cogent Consideration of Privacy Issues

As schools ramp up digital scanning, they must also navigate privacy concerns. A key implication for policy is to establish clear boundaries and transparency in digital assessment. Schools should communicate to families what they scan (e.g., public social media versus private communications), under what circumstances, and how data will be used. They should also ensure compliance with laws like FERPA and the First Amendment. For instance, identification should focus on threats of violence or self-harm, not on punishing students for opinions or minor misconduct outside school. The research highlights the benefit of catching threats early, but future research and legal will need to guide the limits of these practices. A short-term recommendation is that BSD convenes a policy review with legal counsel to update its student handbook and policies regarding off-campus online behavior and clarify when it can discipline or intervene. Several court cases, *Tinker v Des Moines 1969/ Mahanoy v B.L. 2021*, have set precedents in this area (e.g., schools can act on off-campus speech if it causes a substantial disruption or threat at school).

Since the data shows online threats correlate with actual risk, schools are on solid ground intervening for those. The key is to do so even-handedly and with documentation of why an

online statement was interpreted as a genuine threat (as opposed to artistic expression or joke). The practical implications extend to what happens *after* a threat is assessed. About half of the threats were deemed not immediate risks; presumably, many resulted in lower-level interventions (like counseling, discipline, or mediation). BSD could ensure that students who make any form of threat (whether transient or severe) receive appropriate follow-up support. This could mean referrals to counseling, behavior contracts, or other services to address underlying issues. The goal is to reduce recidivism–a student who has made a threat once should be guided away from doing so again, because the researcher found no outcome differences by demographics, and the situation (behavior) likely determined consequences. Ensuring those consequences include punitive measures and restorative or help-oriented measures is essential, such as conflict resolution training if the threat stemmed from peer conflict or anger management therapy from personal issues. Findings suggest many threats come from genuine grievances or emotional turmoil (given some overlap with self-harm and bullying contexts). Thus, treating threat assessment as a security measure and an entry point to provide help is an enlightened practice. This resonates with SCT's emphasis on the environment. By improving the student's support environment and teaching pro-social skills, we reduce the likelihood of future threats (altering the reciprocal cycle of behavior).

The above implications can be directly applied in the BSD context. As the Public Safety Manager in BSD (the researcher's role), the researcher is well-positioned to spearhead these suggested changes. An immediate step mentioned in the dissertation draft is implementing a pilot digital threat assessment program in BSD. This would allow the district to test the integration of digital assessment tools and refine protocols based on "real-world applications." Partnering with tech firms or universities could bring expertise and advanced tools.

Additionally, BSD could contribute to the broader Oregon effort by sharing data and strategies since Oregon has a statewide behavioral threat assessment initiative. The practical improvements made in one district can inform state guidelines and vice versa. All these steps tie back to the fundamental finding: digital and behavioral data must be unified in school safety efforts to identify and mitigate threats before they escalate effectively.

Study Limitations

While this study provides valuable insights, several as must be acknowledged to interpret the findings and guide future research accurately. First, there are limitations regarding the data source and its completeness. The data were obtained from Safer Schools Together (SST) incident reports. Although these reports are extensive, they may not fully capture the nuances of each situation. An initial limitation centered on the lack of certain demographic data such as the number of elementary, middle, and high schools involved; the average size; and if the school was in an urban, suburban, or rural area. A significant limitation is that digital leakage might be underreported in the dataset. If a threat had digital warning signs that school officials never recognized or recorded, the coding would indicate “no digital leakage” when the student did express intent (even if it went unnoticed at the time). In other words, the absence of evidence is not evidence of absence. This is a common issue in extant data analysis: we rely on documented information. Some threats may have involved a private message sent to authorities who were unaware. Thus, 23% might be a conservative estimate of how often students communicate their threats digitally. To address this limitation, SST could include more specific prompts in their intake forms, explicitly asking whether digital communications were reviewed and whether there were suspicions or unconfirmed reports of digital leakage. By clearly guiding data collection,

SST could enhance data specificity without significantly increasing the complexity of the intake form or reducing its accessibility.

Additionally, the dataset did not always contain complete information on every variable. For example, as noted, gender was unknown in 62% of cases, which limited the gender-based analysis to a subset and may skew those results—it is possible that gender was more often recorded in some instances. However, we have no evidence of systematic bias. Similarly, a few cases lacked data on immediate risk or outcome, although this was minimal. Another aspect is that the researcher categorized incidents and leakage based on available descriptions, which introduces subjectivity. Efforts were made to use clear criteria (e.g., any mention of social media, texts, etc., counted as digital leakage), but the original reports might not have been uniformly detailed. One school might thoroughly document, "Student posted X on Instagram," while another might say, "Student made a threat," without clarifying the medium, leaving the researcher to infer details. Such variability would affect the accuracy of our counts.

The scope and representativeness of the dataset are also limitations. The total sample of 798 incidents (threats and non-threats combined) was determined by what SST provided from September 2022 to July 2024. It could be that the data over-represent larger or more proactive districts that rigorously use SST's reporting tools. Districts or schools that do not use a structured reporting system or have less developed threat assessment teams might have very different outcomes. In other words, the sample may not fully represent the "average" U.S. school—it might tilt towards districts already engaged in higher levels of digital identification (since they contributed detailed reports). This potential bias means our findings (like 64.5% of threats getting a formal evaluation) might be an optimistic picture of what is happening in well-prepared districts. Schools without established threat assessment protocols might have much lower rates of

formal evaluation or might miss more digital leakage. Therefore, cautiously generalizing these findings to all K–12 settings should be done. The results most apply to contexts like those in the dataset (likely medium- to large-size districts with active safety reporting procedures, possibly in the Pacific Northwest region, given BSD's involvement).

Another limitation is the lack of qualitative context in understanding incidents. While we can quantify patterns (e.g., "veiled threats had 27.8% digital leakage" or "police were involved in 49.9% of cases"), we often lack the "why" behind those numbers. We do not know the content of the digital leakage beyond its presence. Nor do we know how threat assessment teams interpreted that content or how students reacted to interventions. This makes it difficult to accurately differentiate, for example, a case where digital leakage was a vague meme versus a case where it was a direct hit list posted online. Both would have been coded as "leakage = yes" in this example but have different school implications. The outcomes regarding whether violence was averted are unknown. The data did not explicitly track whether a given threat was carried out or mitigated. However, we cannot say how effective interventions were from a research perspective because there is no follow-up data on cases beyond immediate response.

Time frame is another consideration. The study data spanned roughly two school years, approximately two years from September 2022 to July 2024 (with summer 2023 possibly lightly included). This is a relatively short period and could coincide with unusual patterns. For instance, the tail end of the COVID-19 pandemic disruptions might have influenced student behavior in 2022-23 (some hypothesized increases in misbehavior or mental health issues when schools reopened). Any national events during this period (such as a high-profile school shooting or viral online challenges like the TikTok "devious licks" or threats in late 2021) might have impacted data, especially in fall 2022. Seasonal analysis did not show spikes, and specific dates

were not examined. Notably, December 2021 had a national TikTok shooting threat rumor that closed many schools; data in this study starts after that, but such phenomena can repeat. If one occurred in our window, it could cause a cluster of threats that is not "seasonal", but event driven. This analysis did not account for specific events because data lacked that detail, a limitation in understanding causal factors.

Measuring "immediate risk" and threat categorization is only as good as a particular team's judgment. There might be inconsistencies in how different schools apply the "immediate risk" label. One district might label a case high risk, while another with the same facts might label it moderate due to differences in training or risk tolerance. Those labels were treated as data but are somewhat subjective. Similarly, distinguishing between an "indirect" and "veiled" threat can be nuanced. The research relied on the data as given; any misclassification at the source could affect the results. Including the "behavior-only" category (not in classical threat typologies) was an adaptation. At the same time, its value is seen; other studies might not isolate that category, making direct comparison difficult.

Finally, the study was limited by its focus on quantitative correlations. The researcher could identify what was associated with what (e.g., digital leakage in relation to behavior-only threats), but could not definitively establish causation or the direction of influence. Online behavior may lead to real-life behavior. Still, it could also be that students prone to certain behaviors are more active online (third-variable factors). Without experimental or longitudinal data, we must be cautious not to over-interpret causality.

Recommendations for Future Research

Building on these findings and limitations, several avenues for future research are recommended to deepen our understanding of digital leakage and school threat assessment and to

address questions that remain unanswered: Future studies should include a more extensive and diverse sample of schools and districts, ideally from regions of varying sizes and with varying levels of resources. This would help determine how generalizable the patterns observed here are. A national or multi-state database of school threat incidents (if one can be compiled through federal grants or collaborations with school safety centers) would be invaluable. Ensuring consistent data recording is key; developing a standardized reporting template for digital leakage and threat outcomes could improve data quality. Partnering with organizations like the National Association of School Psychologists or state education agencies could facilitate broader data gathering. Expanding the scope also means including more years of data to observe trends over time (was 2022–2024 typical, or an outlier in some respects?).

A crucial next step would be to conduct longitudinal studies that track what happens after threats are identified and addressed. For instance, researchers could follow up on students subject to a threat assessment to see their outcomes: Did they receive effective interventions and cease making threats? Did any go on to attempt violence later (hopefully not, but this is critical to evaluate the effectiveness of interventions)? Such studies would help assess the long-term impact of early detection via digital leakage. If students whose threats were discovered through digital means receive earlier interventions, do they have better outcomes (e.g., lower likelihood of actual aggression) than students whose threats came as surprises? Similarly, tracking students' well-being in non-threat cases (like those with self-harm ideation) could inform how well schools connect them to support after a threat assessment referral. Ideally, this longitudinal research can validate that our current threat assessment and intervention strategies are preventing violence and helping students—or reveal areas to improve if some students continue to struggle.

To complement the quantitative patterns, in-depth qualitative research is needed to understand context and decision-making. Case studies of specific incidents (with interviews of the threat assessment team, the students involved, etc.) could illuminate how digital leakage was discovered, interpreted, and acted upon. For example, interviewing school principals or safety officers about a case where a student posted a threat online could shed light on how they decided to involve police or not, how they weighed that information, and what challenges they faced (did they have trouble identifying the student's account? Did they worry about the authenticity of the post?). Likewise, interviewing students (both those who made threats and their peers who might have reported them) could provide insight into the social dynamics of leakage— e.g., did the student intend for someone to see their post and intervene? Did peers feel scared or unsure what to do when they saw it? Such qualitative data would add depth to our understanding and perhaps explain some of the whys behind our statistical associations. A mixed-methods approach—for instance, starting with our quantitative overview and then selecting a subset of cases for qualitative follow-up—would be a robust design. This could extend to focus groups or surveys with threat assessment team members across districts to gather their perspectives on digital threats (what percentage of their cases involve social media, do they feel equipped to handle those, etc.). We noted that we do not know how teams interpreted digital evidence; interviews or surveys with team members could ask them: *"When you see a social media post as part of a case, how does it influence your risk rating?"* Comparing responses might reveal interesting variations in practice.

Research should also test and evaluate the efficacy of specific interventions to improve the detection or management of digital leakage. For example, a study could pilot an AI-based social media scanning tool in a set of schools and compare outcomes (number of threats detected,

time to intervention, any reduction in incidents) with a control group of schools not using the tool. This quasi-experimental design would provide evidence on whether investing in specific technologies yields significant safety benefits or just false alarms. Similarly, evaluating training programs—say one group of schools gets enhanced training on digital threat assessment and another does not—could show if training leads to more consistent handling of digital threats (e.g., maybe after training, schools involve police more appropriately for online threats, narrowing the gap we saw). Essentially, implementation research that examines how new practices (digital scanning, bystander training programs, etc.) impact the school threat landscape would be highly valuable. This echoes the idea of applying insights in practice and studying those applications, as mentioned for BSD's pilot program.

Future research should examine the accuracy and challenges of interpreting digital leakage. This might involve looking at cases of "leakage" that turned out not to signal an actual intent (false positives) versus cases where someone carried out or attempted violence without any leakage (false negatives). By compiling and comparing such cases, we can refine profiles of meaningful leakage. For example, is posting song lyrics a common false positive? Are there linguistic markers in posts reliably indicating a higher likelihood of real intent (perhaps something a computational linguistics study could analyze across many posts)? On the flip side, examining incidents of violence or close calls that were not caught beforehand could highlight what warning signs were missed and why (where they were but not reported, or indeed no signs?). This could be done through retrospective analysis of severe cases (for instance, using the U.S. Secret Service's reports on averted and completed school attacks to see how many had social media leakage). The study suggests many threats are caught, but we want to ensure we also learn from any that were not.

Another research direction would be to investigate into the motivations and psychological profiles of students who exhibit digital leakage versus those who do not. Are there differences in intent or personality? It could be hypothesized, for example, that students who leak their intentions (especially publicly) may be, at least in part, seeking attention or help—a phenomenon noted in some threat assessment literature where a cry for help and a threat can be intertwined. Others who plan in absolute secrecy might be more committed to the act and not want to be stopped. Studying these aspects (perhaps via psychological assessments or interviews with students who made threats) could inform how to interpret leakage: Is it often an implicit request for intervention (thus, those cases might benefit from a different approach, like more counseling, alongside discipline)? Additionally, gender differences in leakage could be explored psychologically: what drives the trend that female students might post about it more? Understanding that could help tailor prevention; for example, if it is related to how each gender socializes or communicates distress, interventions can be sensitive to those differences.

As schools increase assessment of student digital activity, moral and legal research is necessary to navigate privacy concerns. Scholars in education law and ethics could analyze questions such as: What are the limits of schools' authority to assess off-campus speech after the *Mahanoy School District v. B.L.* (2021) Supreme Court decision? How do districts balance student First Amendment rights with legitimate safety concerns? Empirical research could be done on stakeholder views—surveying parents, students, and educators about their comfort levels and expectations regarding digital scanning. Are students aware that school officials might watch their public posts? Do they find it acceptable if it is for safety? Understanding perceptions can guide how to implement policies in a way that maintains trust. It may also be fruitful to research outcomes regarding school climate: does intensive scanning create a chilling effect,

reduce incidents, or both? This intersects with our findings by ensuring that any recommendations to increase digital guardianship come with careful consideration of unintended effects.

Future studies could also examine how digital threat detection integrates with other violence prevention initiatives. For example, how does it complement behavioral intervention teams, bullying prevention programs, or social-emotional learning curricula? A holistic program that includes digital assessment, student education, and robust mental health support is most effective. Comparative research on different models of school safety (e.g., tech-heavy versus relationship-heavy approaches) could inform best practices.

Conclusion

My research identified several key patterns and implications regarding digital leakage, threat-related behavior, and school-based threat assessment practices in K–12 educational settings. First, digital leakage—defined as students communicating violent intent through digital platforms—was present in approximately 23% of threat-related incidents, significantly more than in non-threat-related cases, but still absent in most threats. Behavior-only threats, where no verbal or written threat was made, were *more* likely to involve digital leakage than communicated threats, suggesting that students who do not articulate threats aloud may nevertheless signal intent online. Importantly, school teams applied formal threat assessment procedures consistently across threat types and demographic variables, including gender and grade level, indicating fidelity to behavioral, not profile-based, evaluation practices. Findings also showed that male students were likelier to engage in behavior-only threats.

In contrast, female students were more likely to use verbal or written communication, a pattern aligned with Social Cognitive Theory's gendered modeling of aggression. However,

outcomes were handled similarly across genders, reflecting equitable threat management practices. Notably, most non-threat concerns, such as self-harm, bullying, or possession of prohibited items, rarely involved digital leakage and were typically identified through in-person observations or student disclosures.

Collectively, these findings support integrating digital assessment into comprehensive threat assessment systems while cautioning against overreliance on digital evidence alone. They reinforce that threats may emerge anytime and across all grade levels and demographics, emphasizing the importance of sustained vigilance, interdisciplinary response teams, and proactive intervention efforts. The results suggest that digital behavior can enhance early detection when it exists, but cannot substitute for robust interpersonal assessment, clear protocols, and trust-based reporting systems. The study contributes to theoretical frameworks—particularly Routine Activity Theory, the General Aggression Model, and Social Cognitive Theory—by extending them into the digital context and underscores the value of consistent, evidence-based threat assessment policies, especially in districts like the Beaverton School District, which demonstrate mature and responsive school safety practices.

Several questions arose that are worthy of exploration. By addressing these in future research, scholars and practitioners can build on these findings to create safer, more responsive school environments. The goal is a comprehensive system where digital and traditional methods work together to detect and address threats early while supporting students' well-being and rights. Continued research will be crucial, especially in collaboration with school districts (like BSD) that are at the forefront of implementing these strategies. Through an iterative cycle of study and practice—using data to inform action and action to generate new data—districts can

move closer to the ideal of preventing school violence before it occurs, effectively *"unveiling digital traces"* and acting on them in the service of safety.

APPENDIX A

SST INTAKE FORM

Safer Schools Together

Office: 1.604.560.2285

Toll-Free: 1.855.677.3720

Due to the increase of Digital Baseline Report requests, we are prioritizing reports based on the level of concern. Requests with a higher level of threat will be sent out within a timely manner. All requests will be acknowledged once they have been submitted. All districts will receive a summary of our findings within 24 hours of their request.

Submission Date

Is this an urgent request?

-- Please select -- No Yes

-- Please select --

Name of Caller / Position Title

School District

Please provide us with your contact information to receive a timely response.

Email Address

Phone Number

Provide details of the incident / situation that has occurred.

If a threat or threat-related behavior has occurred, please provide the exact language of the threat below. If screenshots are available, please include.

Date of incident?

Have you initiated a Threat Assessment (TA)?

If yes to the above, which immediate risk reducing interventions have you implemented? (See below for details)

Immediate risk-reducing interventions can include searching the SOC's backpack and locker to identify and secure any potential means, engaging law enforcement or school resource officers (SROs), removing access to the means, and implementing supervision, monitoring, and involvement of parents or guardians.

These actions are necessary when the subject of concern (SOC) has demonstrated imminent concerns, such as immediate access to the means, engagement in rehearsal or planning behaviors, or a significant shift in baseline behavior.

If the location of the SOC is unknown, consider the usage of geolocation apps like Snapmaps and FindMy on Apple devices.

Have you contacted law enforcement?

How did this come to your attention? (If screenshots are included, who originally provided them?)

Please provide the name(s) of the Subjects of Concern (SOCs) involved (first and last names, nicknames, or aliases).

Current school and previous school(s), if known.

Grade(s) of the Subjects of Concern (SOCs)

Age(s) of the Subjects of Concern (SOCs)

Shifts in the Subject of Concern's (SOC's) digital behavioral baseline include Frequency, Intensity, and Recency (FIR): change in the number of posts per day; intensity of posts and/or an escalation in worrisome behavior(s); how recent are the posts of concern?

Are you aware of any changes in the Subjects of Concern (SOCs) frequency and/or intensity of their social media posts (changes in digital behavioral baseline)?

Names of friends and/or peers.

Names of family members (parents, siblings, primary guardians, and/or other known family members).

Please provide known social media usernames and online aliases for the Subjects of Concern (SOCs) and peers below.

File attachment

Choose file

Additional information

If you have any additional files to attach, please send them to intake@saferschoolstogether.com

If this is time-sensitive, please put URGENT in the subject line of the email to Intake@saferschoolstogether.com.

APPENDIX B

DATA DICTIONARY PRIMARY DATASET

Variable	Definition	Level	Column Location
Case Type	Case resulted from an internal request, is associated with general community concern following an event or related to a protest/demonstration, or is based on a previous entry, not associated with a unique district	Internal, General Scan, Follow Up	A
Case Communication	Resulted from an anonymous student report. Not from a district request/intake form	ERASE/PSST	B
Gang associated behavior	Info provided by district request/intake form submission OR from content located by Threat Analysts	Yes/No	D
School Threat	Info provided by district request/intake form submission OR from content located by Threat Analysts	Yes/No	E
Primary Category of Concern	Determined by Threat Analysts based on criteria in "Categories of Concern – Glossary"	Threat-Related Behavior	F
Peer Names Provided	Names of those associated with the student of concern	Yes/No	G
Content Related to Incident/Concern	Online content found by Threat Analysts	Yes/No	H

Variable	Definition	Level	Column Location
Threat Type	FBIs four categories of threat behavior: A direct threat identifies a specific act against a specific target and is delivered in a clear, explicit manner: “I am going to place a bomb in the school’s gym.” An indirect threat tends to be a vague threat of violence. The plan, victim, motivation, and other aspects of the threat are masked or ambiguous. A veiled threat is one that strongly implies but does not explicitly threaten violence. A conditional threat is the type often seen in extortion cases. It warns that a violent act will happen unless certain demands or terms are met.	Direct, Indirect, veiled, conditional, and behavior ONLY	I
Grade Range		0-5 Elementary, 6-8 Middle, 9-12 OR High/Secondary, University, ADULT not enrolled, No Grade or School Data provided	J
Gender	Based on incident details, documented posts, or documented accounts to determine male/female. If unable to determine “unconfirmed” was selected.	Male, Female, Unconfirmed	K
Threat Quote	If applicable, only for written threats, images with no text were not included	“Quote” or No	L
Shift in Baseline	Change in behavior as noticed by reporting district/intake form	Yes, No, Unconfirmed	M

Variable	Definition	Level	Column Location
Date incident occurred vs date submitted		-Submitted on day of incident -Submitted < 7 days from incident -Submitted < 30 days from incident -Submitted < 90 days from incident - Incident date unconfirmed	N
Image of threat provided	Based on attachments by district request/intake from submission	Provided, Not Provided	O
Subcategory: If yes, what did the image contain		Written threat – virtual, Written threat – physical, Unique image of weapon or firearm, N/A	P
Target Specified	Person/victim	Yes/No	Q
Site Specified	location	Yes/No	R
Method/Means Specified	What was the injury causing method that was specified	Yes/No	S
Date Specified	Date violence was set to occur	Yes/No	T
Evidence/Description of Fluidity	Suicidal and homicidal ideations (harm of self & harm of other)	Yes/No	U
School Year	September – June Calendar Year	2022/2023, 2023/2024	V
Described as Immediate Risk		Yes/No	W
Police Involvement		Yes/No	X
Ongoing Threat Assessment		Yes/No	Y
Number of Student(s) of Concern		0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15	Z
Social Media Username		Yes/No	AA
Date Received		Month/Date/Year	AB
Numeric Identifier			AC

APPENDIX C

DATA DICTIONARY EXPANDED DATASET

Variable	Definition	Level	Column Location
Case Communication	Resulted from an anonymous student report. Not from a district request/intake form	ERASE/PSST	A
Month		Month/Year	B
Gang associated behavior	Info provided by district request/intake form submission OR from content located by Threat Analysts	Yes/No	C
Primary Category of Concern		Firearms, Bullying/Cyberbullying, Negative Digital Climate/Culture, Physical Violence, Weapons, Sexual Assault, Illegal Activity Misc., School Community Concerns, Suicidal Ideation, Risk of Sextortion	D
Peer Names Provided		Yes/No	E
Content Related to Incident Concern	Online content found by Threat Analysts	Yes/No	F
School Year		September 2022 – June 2023, September 2023 – June 2024	G
Immediate Risk		Yes/No	H
Police Involvement		Yes/No	I
Ongoing Threat Assessment		Yes/No	J
Number of Students of Concern		0-29	K
Social Media Username		Yes/No	L
Date Received		Month/Date/Year	M
Numeric Identifier			N

REFERENCES CITED

Ahmed, F., Dubey, D. K., Garg, R., & Srivastava, R. (2023). Effects of examination-induced stress on memory and blood pressure. *Journal of Family Medicine and Primary Care*, *12*(11), 2757–2762. https://doi.org/10.4103/jfmpc.jfmpc_925_23

American Psychological Association. (2020). *Publication manual of the American Psychological Association 2020: The official guide to APA style* (7th ed.). American Psychological Association.

American Psychological Association. (2017). Ethical principles of psychologists and code of conduct. *American Psychologist*, *57*(12), 1060–1073.

American Psychological Association. (2023, November 30). *Even a joyous holiday season can cause stress for most Americans* [Press release]. https://www.apa.org/news/press/releases/2023/11/holiday-season-stress

Anderson, C. A., & Bushman, B. J. (2002). Human aggression. *Annual Review of Psychology, 53*(1), 27–51. https://doi.org/10.1146/annurev.psych.53.100901.135231

Bandura, A. (1977). Soc*ial learning theory*. Prentice Hall.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory.* Prentice Hall.

Bartlett, T. L. (2023). *Participatory processes to address wicked problems in K12 schools: A case of reimagining school safety* [Doctoral dissertation, Arizona State University]. ProQuest Dissertations & Theses Global.

Bjärehed, M., Thornberg, R., Wänström, L., & Gini, G. (2020). Mechanisms of moral disengagement and their associations with indirect bullying, direct bullying, and pro-aggressive bystander behavior. *The Journal of Early Adolescence, 40*(1), 28–55. https://doi.org/10.1177/0272431618824745

Bureau of Justice Assistance. (2022). *Oregon Statewide Behavioral Safety (threat) assessment system development*. Bureau of Justice Assistance. https://bja.ojp.gov/funding/awards/15pbja-22-gg-04663-stop

Bushman, B. J. and Anderson, C. A. (2020). General Aggression Model. In J. Bulck (Ed.) *The International Encyclopedia of Media Psychology* (pp. 1-9). https://doi.org/10.1002/9781119011071.iemp0154

CITI Program. (2019). *Collaborative Institutional Training Initiative*. University of Miami.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

Cook, P. J., & Ludwig, J. (2000). *Gun violence: The real costs*. Oxford University Press.

Cornell, D. (2020). *Overview of the comprehensive school threat assessment guidelines*. University of Virginia. https://education.virginia.edu/research-initiatives/research-centers-labs/research-labs/youth-violence-project/school-threat-assessment/comprehensive-school-threat-assessment-guidelines

Cornell, D. (2003). Guidelines for responding to student threats of violence. *Journal of Educational Administration*, *41*, 705–719.

Cornell, D., Sheras, P., Gregory, A., & Fan, X. (2009). A retrospective study of school safety conditions in high schools using the Virginia Threat Assessment Guidelines versus alternative approaches. *School Psychology Quarterly, 24*(2), 119–129. https://doi.org/10.1037/a0016182

Cowan, R. G., Tedeschi, P. J., Corbin, M., & Cole, R. F. (2022). A mixed-methods analysis of averted mass violence in schools: Implications for professional school counselors. *Psychology in the Schools*, *59*, 817–831. https://doi.org/10.1002/pits.22647

Cox, J. W., Rich, S., Chong, L., Trevor, L., Muyskens, J., & Ulmanu, M. (2023, April 3). *More than 352,000 students have experienced gun violence at school since Columbine*. The Washington Post.

Coyne, S. M., Warburton, W. A., Essig, L. W., & Stockdale, L. A. (2018). Violent video games, externalizing behavior, and prosocial behavior: A five-year longitudinal study during adolescence. *Developmental Psychology, 54*(10), 1868–1880. https://doi.org/10.1037/dev0000574

Crick, N. R., & Grotpeter, J. K. (1995). Relational aggression, gender, and social-psychological adjustment. *Child Development, 66*(3), 710–722. https://10.1111/j.1467-8624.1995.tb00900.x

Daniels, J. A., Buck, I., Croxall, S., Gruber, J., Kime, P., & Govert, H. (2007). Content analysis of news reports of averted school rampages. *Journal of School Violence, 6*(1), 83–100. https://doi.org/10.1300/J202v06n01_06

Dorn, E., Hancock, B., Sarakatsannis, J., & Viruleg, E. (2020). *COVID-19 and learning loss—disparities grow and students need help*. McKinsey & Company. https://www.mckinsey.com/industries/public-sector/our-insights/covid-19-and-learning-loss-disparities-grow-and-students-need-help

Dou, Y., & Zhang, M. (2025). Longitudinal reciprocal relationship between media violence exposure and aggression among junior high school students in China: A cross-lagged analysis. *Frontiers in Psychology*, *15*, 1441738.

Farrell, A. D., Bettencourt, A., Mays, S., Kramer, A., Sullivan, T., & Kliewer, W. (2012). Patterns of adolescents' beliefs about fighting and their relation to behavior and risk factors for aggression. *Journal of Abnormal Child Psychology*, *40*(5), 787–802.

Hensley, M. S., Burrows, N. L., Galerneau, A. J., Bekkala, A. P., Hungwe, K. N. (2024). *Journal of Chemical Education*, *101*(3), 798–806. https://doi.org/10.1021/acs.jchemed.3c00620

Horgan, J. (2008). From profiles to pathways and roots to routes: Perspectives from psychology on radicalization into terrorism. *The ANNALS of the American Academy of Political and Social Science*, *618*(1), 80–94. https://doi.org/10.1177/0002716208317539

Huesmann L. R. (2007). The impact of electronic media violence: scientific theory and research. *The Journal of Adolescent Health*, *41*(6 Suppl 1), S6–S13. https://doi.org/10.1016/j.jadohealth.2007.09.005

International Center for Digital Threat Assessment. (2023). *Threat assessments and leakage: What your teams don't know can hurt you*. International Center for Digital Threat Assessment https://icdta.org/threat-assessments-and-leakage-what-your-teams-dont-know-can-hurt-you/

Jackson, J. R., & Viljoen, J. L. (2024). Preventing school violence: A review of school threat assessment models. *Journal of Threat Assessment and Management, 11*(1), 48–65. https://doi.org/10.1037/tam0000204

James, B. (2024, July 30). Legal Issues [Resource officer and school district obligations]. Oregon School Resource Officer Association Conference. Seaside, Oregon.

Kaati, L., Shrestha, A., & Akrami, N. (2022, November 10-13). *Predicting targeted violence from social media communication* [Conference paper]. 2022 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Istanbul, Turkey. https://doi.org/10.1109/asonam55673.2022.10068581

Kjærvik, S. L., Thomson, N. D. & Fanti, K. A. The impact of media violence, narcissism and sex on reactive and proactive aggression in adolescents: A one-year follow-up study. *Journal of Youth Adolescence*, *54*, 917–927 (2025). https://doi.org/10.1007/s10964-024-02106-3

L'Abate, L., & Baggett, M. S. (1997). *The self in the family: A classification of personality, criminality, and psychopathology*. John Wiley & Sons.

Langman, P. (2015). *School shooters: Understanding high school, college, and adult perpetrators.* Rowman & Littlefield.

Lee, L. K., Douglas, K., & Hemenway, D. (2022). Crossing lines—A change in the leading cause of death among U.S. children. *New England Journal of Medicine*, *386*(16), 1485–1487. https://doi.org/10.1056/nejmp2200169

Madfis, E. (2020). *How to stop school rampage killing: Lessons from averted mass shootings and bombings*. London: Palgrave Macmillan.

Marchant, A., Hawton, K., Stewart, A., Montgomery, P., Singaravelu, V., Lloyd, K., Purdy, N., & John, A. (2017). A systematic review of the relationship between internet use, self-harm and suicidal behaviour in young people: The good, the bad and the unknown. *PLOS One*, *12*(8), e0181722. https://doi.org/10.1371/journal.pone.0181722

Meloy, J. R., & O'Toole, M. E. (2011). The concept of leakage in threat assessment. *Behavioral Sciences and the Law*, *29*(4), 513–527. https://doi.org/10.1002/bsl.986

Meloy, J. R., & Hoffmann, J. (Eds.). (2021). *International handbook of threat assessment.* Oxford University Press.

Microsoft Corporation. (2024). *Excel (Microsoft 365 Subscription)*. [Computer Software]. Microsoft Corporation.

Miller, Stephanie A. (2017). *School shootings perpetrators' self-reported motives: A qualitative analysis of manifestos and other writings*. Georgia Southern University. https://digitalcommons.georgiasouthern.edu/cgi/viewcontent.cgi?article=1327&context=honors-theses

Moore, P., Jackson, B. A., Leschitz, J. T., Wolters, N., Goode, T., Diliberti, M. K., & Pham, P. F. (2024). *Developing practical responses to social media threats against K-12 schools: An overview of trends, challenges, and current approaches* (Research Report RR-A1077-5). RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1077-5.html

Mussington, D., & Alathari, L. (2023, May). *Secret Service and CISA release toolkit for K-12 schools to strengthen school safety reporting programs*. United States Secret Service. https://www.cisa.gov/news-events/news/cisa-and-secret-service-release-toolkit-k-12-schools-strengthen-school-safety-reporting-programs

National Association of School Psychologists. (2021). *Behavioral threat assessment and management (BTAM): Best practice considerations for K-12 schools*. National Association of School Psychologists. https://www.nasponline.org/resources-and-publications/resources-and-podcasts/school-safety-and-crisis/systems-level-prevention/threat-assessment-at-school/behavior-threat-assessment-and-management-(btam)-best-practice-considerations-for-k–12-schools

National Center for Education Statistics. (2023). *Violent deaths at school and away from school, school shootings, and active shooter incidents*. Institute of Education Sciences, U.S. Department of Education. https://nces.ed.gov/programs/coe/indicator/a01

National Institutes of Health. (2016). *NIH policy and guidelines on the inclusion of women and minorities as subjects in clinical research*. U.S. National Institutes of Health. https://grants.nih.gov/policy-and-compliance/policy-topics/inclusion/women-and-minorities

National Institute of Justice. (2022). *School safety research: Gathering tips and addressing threats*. https://nij.ojp.gov/topics/articles/school-safety-research-gathering-tips-and-addressing-threats

National Threat Assessment Center. (2021) *Averting targeted school violence: A U.S. Secret Service analysis of plots against schools*. U.S. Secret Service, Department of Homeland Security.

Navarro, R. (2016). Gender issues and cyberbullying in children and adolescents: From gender differences to gender identity measures. In R. Navarro, S. Yubero, & E. Larrañaga (Eds.), *Cyberbullying across the globe: Gender, family, and mental health* (pp. 35–61). Springer Science + Business Media. https://doi.org/10.1007/978-3-319-25552-1_2

Nyimbili, F., & Nyimbili, L. (2024). Types of purposive sampling techniques with their examples and application in qualitative research studies. *British Journal of Multidisciplinary and Advanced Studies*, *5*(1), 90–99. https://doi.org/10.37745/bjmas.2022.0419

Office for Human Research Protections. (2018). *The Belmont Report*. U.S. Department of Health and Human Services. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html

Olson, S. L., Lopez-Duran, N., Lunkenheimer, E. S., Chang, H., & Sameroff, A. J. (2011). Individual differences in the development of early peer aggression: Integrating contributions of self-regulation, theory of mind, and parenting. *Development and Psychopathology, 23*(1), 253–266. https://doi.org/10.1017/S0954579410000775

Oregon Department of Education. (2021). *School safety & prevention systems guidance.* Oregon Department of Education. https://www.oregon.gov/ode/students-and-family/equity/SSP/Pages/default.aspx

Oshodi, A. N. (2024). Enhancing online safety: The impact of social media violent content and violence among teens in Illinois. *World Journal of Advanced Research and Reviews*, *23*(3), 826-833.

O'Toole, M. E. (2000). *The school shooter: A threat assessment perspective*. FBI Academy. https://www.fbi.gov/file-repository/stats-services-publications-school-shooter-school-shooter/view

Özgür, H. (2020). A systematic review on cyberbullying interventions and preventions. *International Journal of Education*, *9*(1), 11-26. https://doi.org/10.34293/education.v9i1.3373

Page, J. (2016). *A qualitative investigation of completed and averted school shootings: Deciphering the characteristics that prevent school shootings*. West Virginia University Research Repository, West Virginia University. https://doi.org/10.33915/etd.6369

Patton, D. U., Eschmann, R. D., Elsaesser, C., & Bocanegra, E. (2016). Sticks, stones, and Facebook accounts: What violence outreach workers know about social media and urban-

based gang violence in Chicago. *Computers in Human Behavior*, *65*, 591–600. https://doi.org/10.1016/j.chb.2016.09.055

Peterson, J., Densley, J., Spaulding, J., & Higgins, S. (2023). How mass public shooters use social media: Exploring themes and future directions. *Social Media + Society*, *9*(1). https://doi.org/10.1177/20563051231155101

Peterson, J., & Densley, J. (2021). *The violence project: How to stop a mass shooting epidemic*. Abrams.

Poell, T., Nieborg, D., & van Dijck, J. (2019). Platformisation. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1425

Raitanen, J., & Oksanen, A. (2019). Deep interest in school shootings and online radicalization. *Journal of Threat Assessment and Management, 6*(3-4), 159–172. https://doi.org/10.1037/tam0000127

Randazzo, M. R., & Plummer, E. W. (2009). *Implementing behavioral threat assessment on campus: A Virginia tech demonstration project*. Virginia Polytechnic Institute and State University. https://rems.ed.gov/docs/vt_threatassessment09.pdf

Reeves, M. A. L., Brock, S. E., & Cowan, K. C. (2008). Managing school crises: More than just response. *Principal Leadership, 8*(9), 10–14.

Sandeeshwara Kasturiratna, K. T. A., & Hartanto, A. (2024). The moderating role of trait online disinhibition in exacerbating the online victim-bully cycle. *Journal of Technology in Behavioral Science*. Advance online publication. https://doi.org/10.1007/s41347-024-00450-6

Segura, L., Estévez, J. F., & Estévez, E. (2020). Empathy and emotional intelligence in adolescent cyberaggressors and cybervictims. *International Journal of Environmental Research and Public Health*, *17*(13), 4681. https://doi.org/10.3390/ijerph17134681

Siddiqui, S., & Schultze-Krumbholz, A. (2023). Successful and emerging cyberbullying prevention programs: A narrative review of seventeen interventions applied worldwide. *Societies*, *13*(9), 212. https://doi.org/10.3390/soc13090212

Skeen, S., Laurenzi, C. A., Gordon, S. L., Du Toit, S., Tomlinson, M., Dua, T., Fleischmann, A., Kohl, K., Ross, D., Servili, C., Brand, A. S., Dowdall, N., Lund, C., van der Westhuizen, C., Carvajal-Aguirre, L., Eriksson de Carvalho, C., & Melendez-Torres, G. J. (2019). Adolescent mental health program components and behavior risk reduction: A meta-analysis. *Pediatrics*, *144*(2), e20183488. https://doi.org/10.1542/peds.2018-3488

Slemaker, A. (2023). Studying mass shooters' words: Warning behavior prior to attacks. *Journal of Threat Assessment and Management*, *10*(1), 1–17. https://doi.org/10.1037/tam0000198

Speedy, J. (2023). *Warning behaviors and pathway to targeted violence of contemporary mass school shooters*. [Doctoral dissertation, Alliant International University]. ProQuest Dissertations & Theses Global.

The Jamovi Project (2022). Jamovi. (Version 2.3) [Computer Software].

Uddin, M. K., & Rahman, J. (2022). Cyber victimization and cyber aggression among high school students: Emotion regulation as a moderator. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 16(2).

U.S. Department of Justice. (2018). *A comprehensive report on school safety and security: Addressing school violence and school shootings*. U.S. Department of Justice. https://www.ed.gov/sites/ed/files/admins/lead/safety/preventingattacksreport.pdf

U.S. Secret Service & U.S. Department of Education. (2022). *Threat assessment in schools: A guide to managing threatening situations and creating safe school climates.* U.S. Secret Service & U.S. Department of Education.

Van Dreal, J. (2011). *Assessing student threats: A handbook for implementing the Salem-Keizer system*. Rowan & Littlefield. https://doi.org/10.1108/09578231211232059

Van Dreal, J., McCarthy, C., & Van Dreal, C. (2022). *Youth violence prevention: The pathway back through inclusion and connection*. Rowman & Littlefield.

Vakhitova, Z. I. (2025). Cyber-routine activity theory. *Oxford Research Encyclopedia of Criminology and Criminal Justice*. Oxford University. https://doi.org/10.1093/acrefore/9780190264079.013.784

Veijalainen, J., Semenov, A., Kyppö, J. (2010). Tracing potential school shooters in the digital sphere. *Communications in Computer and Information Science*, *76*, 163-178 https://doi.org/10.1007/978-3-642-13365-7_16

Vogels, E. A. (2022). *Teens and cyberbullying 2022*. Pew Research Center. https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/

Vossekuil, B., Fein, R., Reddy, M., Borum, R., & Modzeleski, W. (2002). *The final report and findings of the Safe School Initiative: Implications for the prevention of school attacks in the United States.* U.S. Secret Service and U.S. Department of Education. https://www2.ed.gov/admins/lead/safety/preventingattacksreport.pdf