

HEALTHCARE THREAT ASSESSMENT MANAGEMENT PROGRAMS

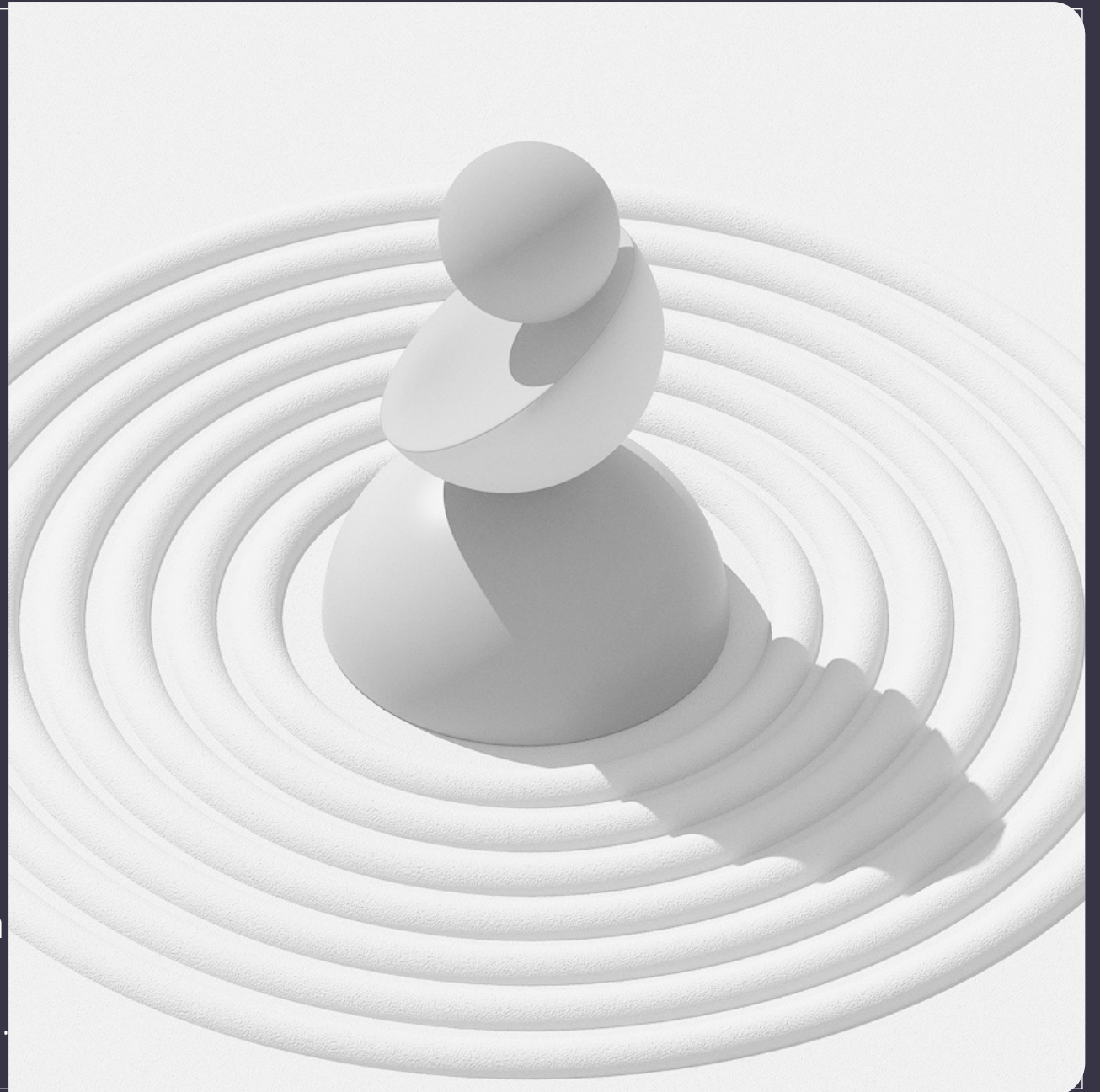
Melissa Jones, BC-HSP, CHPA, CADC, CEM
302-531-6763




Objectives

By the conclusion of this session, participants will be able to:

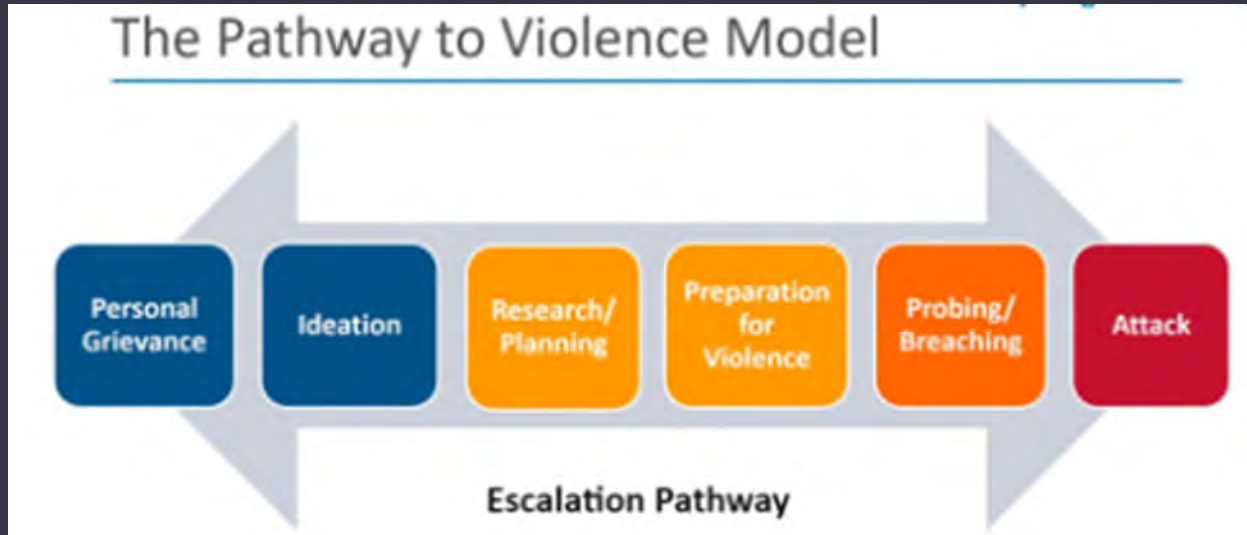
- Articulate the purpose, strategic value, and organizational imperative of implementing a Threat Assessment and Management Program.
- Identify behaviors, communications, and other indicators that may signal a developmental pathway toward violence or otherwise warrant concern.
- Describe the essential components, roles, and procedural steps that define an effective Behavioral Threat Assessment and Management framework.
- Evaluate and select appropriate intervention strategies to reduce risk, support individuals of concern, and promote a safer community.



A young man with brown hair, wearing a dark hoodie, is sitting at a wooden table in a library, focused on writing in a notebook with a blue pen. An open book lies on the table next to him. In the background, other students are visible: one wearing headphones, another looking towards the camera, and a man standing near bookshelves. Large windows in the background let in bright light. The text "PREVENT GUN VIOLENCE BEFORE IT STARTS" is overlaid in white, bold, sans-serif font across the middle of the image.

PREVENT GUN VIOLENCE BEFORE IT STARTS

Threat Assessment Management Defined



- A systematic, fact-based method of inquiry and examination that blends the collection and analysis of multiple sources of information with published research and practitioner experience
- Focuses on an individual's patterns of thinking and behavior to determine whether, and to what extent, an individual is moving toward an act of violence
- A course of action that responds to and mitigates a threat of potential violence, utilizing a multi-disciplinary team

88 Hospital shootings between 2012-2016

Perpetrators had a personal grudge with 235 of those victims

60% were bystanders of the violent event

A Threat Assessment Case Study

Bronx Lebanon Hospital Shooting June 30, 2017

Shooter: Henry Michael Bello

- Fired/Forced Resign: 2015
- Staff at Bronx-Lebanon stated that Bello “had a problem with almost everybody...that’s why they fired him”
- After termination, he sent a threatening email to the doctor who had been overseeing his residency and who Bello blamed for his termination.
- Bello made statements in 2015 warning his colleagues that he would return someday to kill them.
- Bello was terminated from his employment with the city one month prior to the shooting due to “consistent failure to report for work”.
- Before the shooting, Bello emailed the Daily News blaming his colleagues for forcing him to resign.
- Bello had a criminal history including burglary, sexual abuse, unlawful imprisonment, and unlawful surveillance.



Where do we go from here?



Understanding Threats...

AFFECTIVE VIOLENCE VERSUS TARGETED VIOLENCE

Affective Violence (Reactive or Impulsive Violence)

Affective violence is emotionally driven, impulsive, and reactive. It occurs in response to a perceived threat, provocation, or frustration. The primary goal is emotional expression—not premeditated harm. This type of violence is typically characterized by high arousal, rage, or panic, and is often spontaneous.

Example in healthcare:

A patient with a psychiatric condition strikes a nurse after a medication is denied or a visitor becomes aggressive after hearing distressing news about a loved one.

AFFECTIVE VIOLENCE VERSUS TARGETED VIOLENCE

Targeted or Predatory Violence

Targeted or predatory violence is planned, purposeful, and goal-directed. It is not driven by emotion in the moment but rather by deliberate intent to harm a specific individual or group. This type of violence is often preceded by observable behaviors, such as planning, surveillance, and leakage (i.e., threats or behavioral cues)

Example in healthcare:

A disgruntled former employee who blames hospital leadership for their termination begins surveilling a facility and ultimately attempts a violent attack against a specific executive.

What is a Threat Assessment Team?

- A threat assessment team is a multi-disciplinary group of leaders responsible to identify, evaluate, and address threats or potential threats to the safety and security of your healthcare system. The team should have a regular meeting cadence and can be convened when a potential targeted threat arises.
- This team receives and assesses all reports of threats and other alarming behaviors by any person that may impact the safety or well-being of the healthcare community. This can include people living within close proximity of the hospital/offsites who are exhibiting threatening or unusual behaviors that can have an effect on the staff or property.
- It is the Team's responsibility to evaluate the legitimacy of concerns reported to it, assess the likelihood that an individual may cause harm to himself/herself or others (or pose a significant disruption), develop strategies for reducing the risk, implement these strategies, and then monitor and re-evaluate the situation to ensure that they have been effective.

• Key Features of A Successful Threat Assessment and Management Team

Multi-Disciplinary: Combines input from Human Resources, Security, Clinical, Risk and Legal

Behavior Focused: Emphasizes observed behaviors over labels and assumptions

Preventative: Aims to stop violence before it occurs



THE THREAT
TEAM IS
ASSEMBLED...
NOW WHAT?



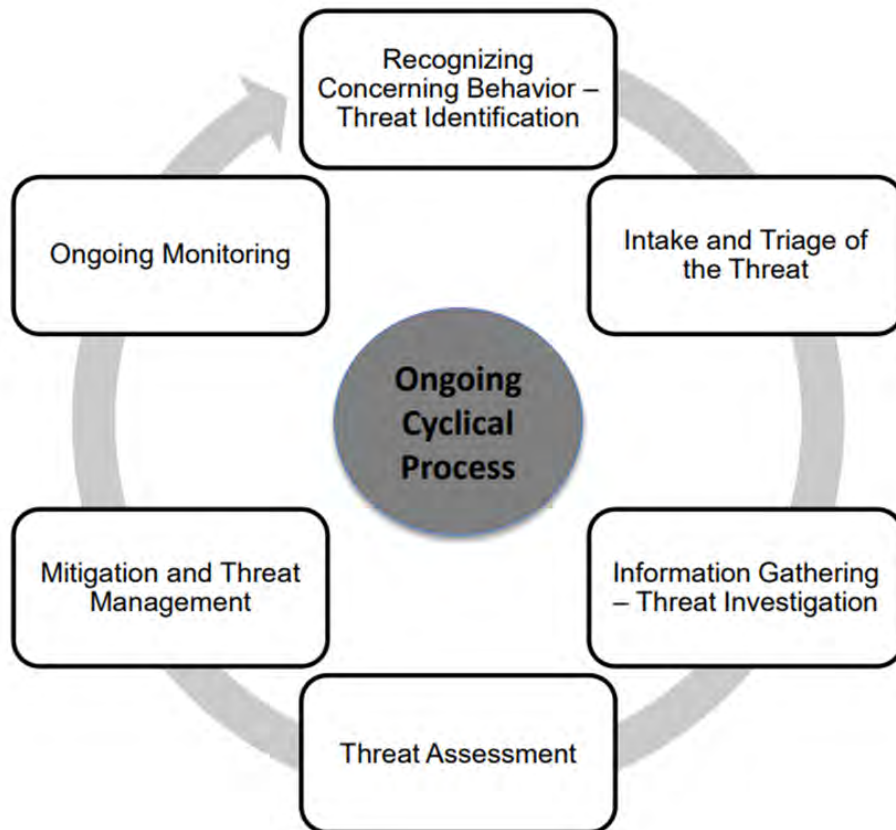
Overview of Threat Management

The major steps in the Threat Assessment and Management (TAM) process are:

1. **Recognize Concerning Behavior** – Threat Identification Identify early warning signs such as threats, stalking, or fixations that may indicate a risk of violence.
2. **Initial Intake and Triage of the Threat-** Quickly review the concern to determine the level of urgency and assign team resources appropriately.
3. **Information Gathering** – Threat Investigation Collect relevant information from diverse sources (HR, clinical, law enforcement, social media, etc.) to build a behavioral picture.
4. **Threat Assessment-** Evaluate the likelihood, intent, and capability of violence using structured tools and professional judgment.
5. **Mitigation and Threat Management-** Implement tailored strategies—such as counseling, legal action, or monitoring—to reduce or mitigate risk.
6. **Ongoing Monitoring-** Continuously track the situation, reassess risk as needed, and adjust management strategies.

Threat Management Process

How do we identify potential threats?



Leakage

This is where the individual reveals their intentions- whether intentionally or unintentionally- to commit a violent act through verbal, written, or behavioral clues.

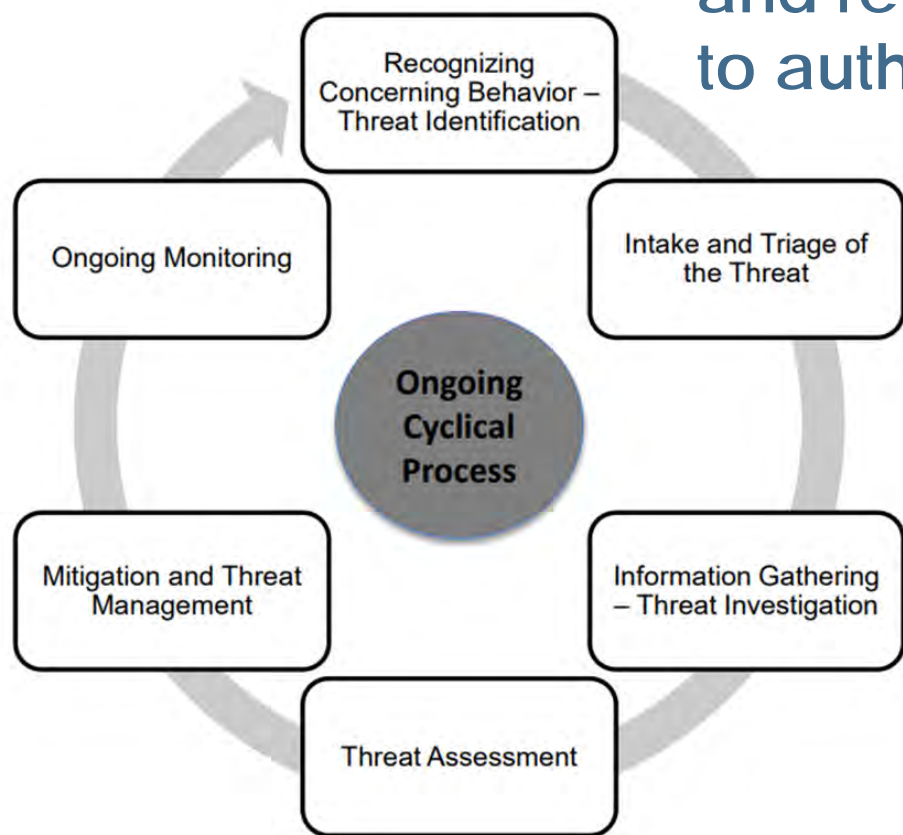
Verbal Leakage: A co-worker casually mentions “One of these days, I’ll make them pay for the way they treated me.”

Written Leakage: A disgruntled employee leaves a resignation letter describing fantasies of violent revenge or words of hate

Behavioral Leakage: A former employee returns to campus and walks around while taking notes of security measures

Threat Management Process

Bystander: A person who recognizes, intervenes, and reports concerning behaviors and indicators to authorities for violence prevention.



Categories of Bystanders



Family

- Parents
- Siblings
- Extended family



Peers

- Close friends
- Acquaintances
- Coworkers
- Classmates



Authority Figures

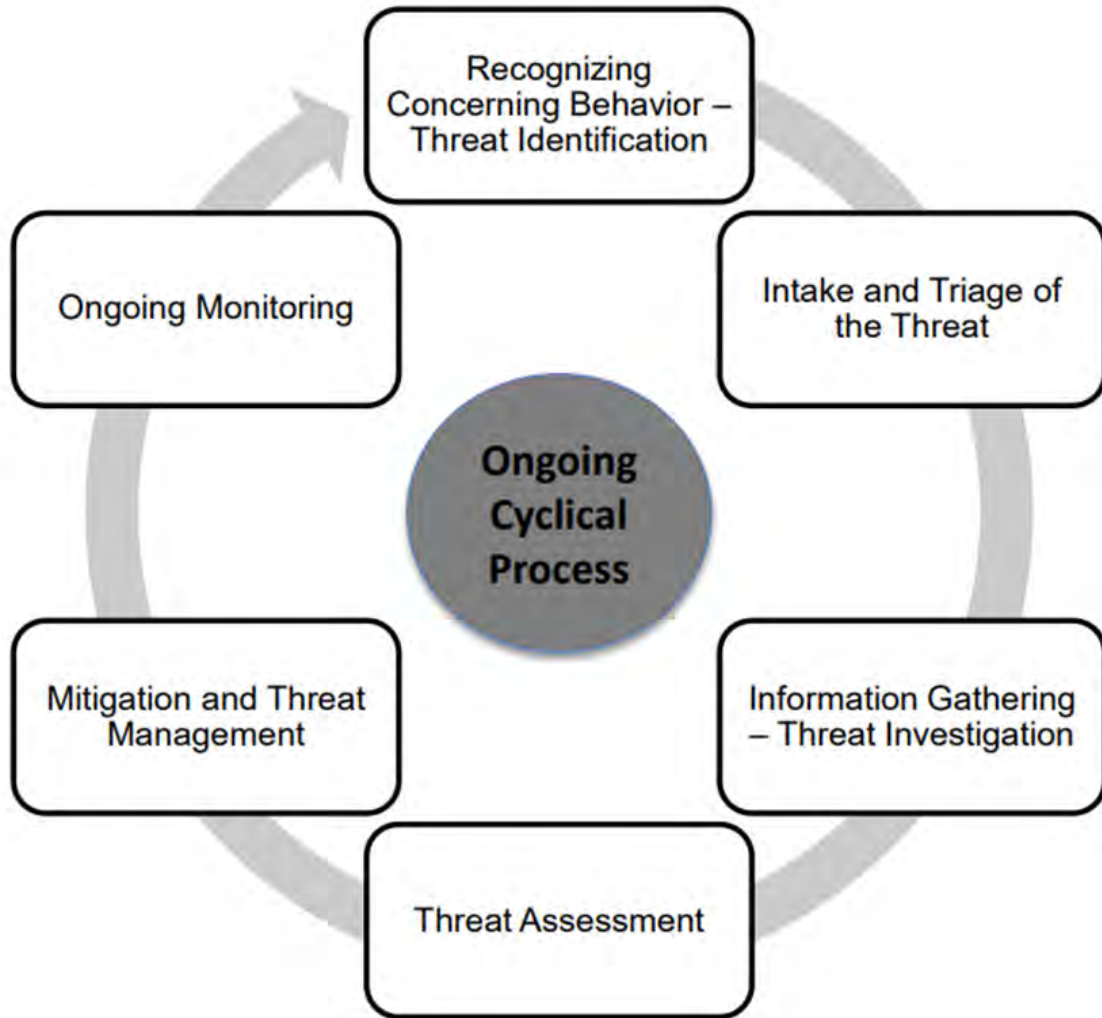
- Law enforcement officers
- Educators
- Workplace supervisors
- Health professionals
- Religious leaders



Strangers

- Commercial sector representatives
- Financial sector representatives
- Social media users

Threat Management Process



Initial Assessment/Triage of the Situation

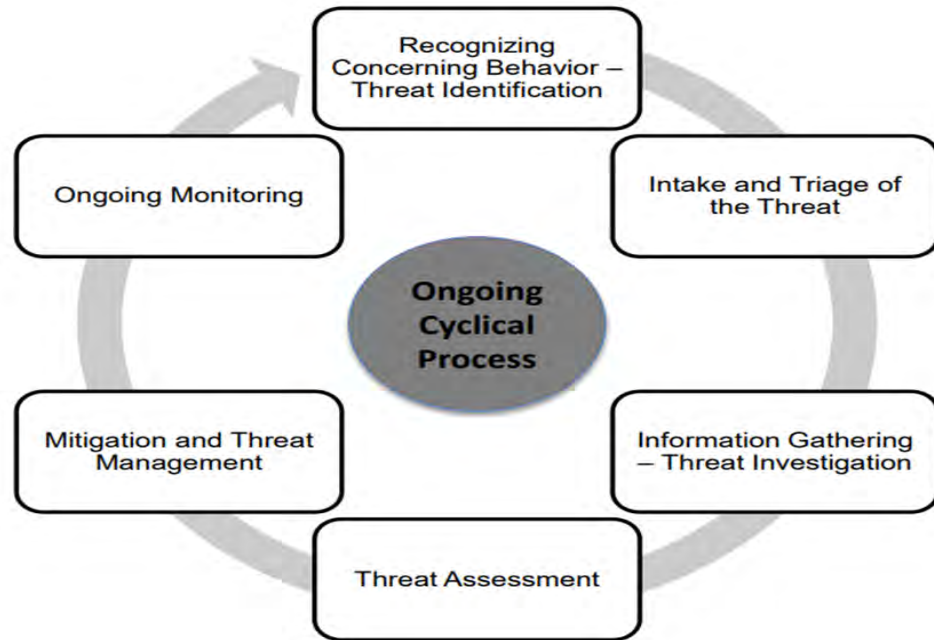
- A Threat Assessment Facilitator and Department Leader collaborate to gather initial facts about the event and review the reported information to make the determination of whether to convene the Threat Assessment Team (TAT).
- It's important to gather as much detailed information about the person of concern, the situation, the setting, and the identified target, if known.
- This can be seen more as a “big picture” assessment at this time in order to determine next steps.

Categories of Threats

- **Direct-** Clearly identifies a specific target in a straightforward and explicit manner
- **Indirect-** The plan, the intended victim and motive are vague, unclear, or ambiguous
- **Veiled-** Strongly implies, but does not specifically threaten violence
- **Conditional-** Warns that a violent act will happen unless certain demands or terms are met

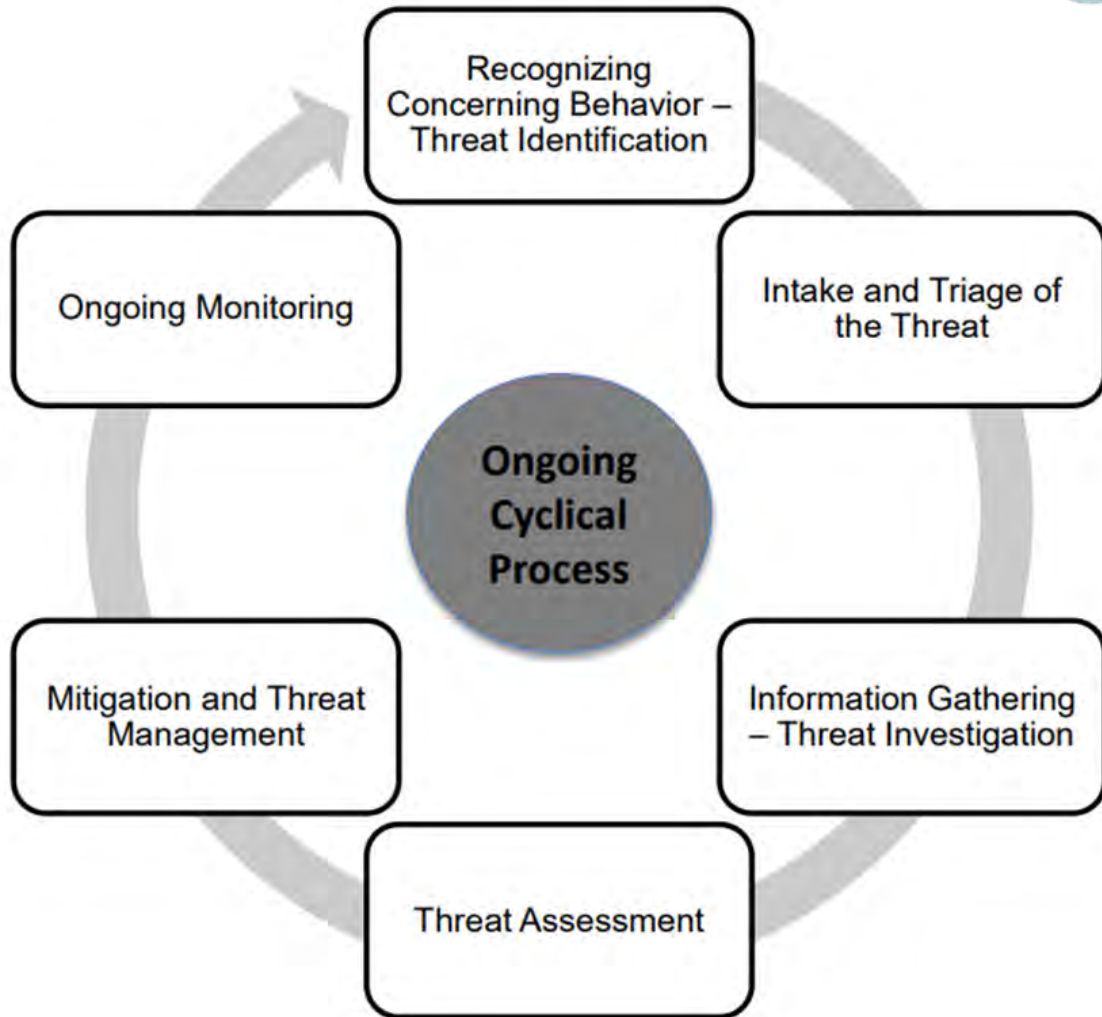


Threat Management Process



- Gather documentation and written statements from those involved and any potential witnesses.
- Unfortunately, there still may be gaps in the facts collected, but the Threat Assessment Team will need to continue the assessment without making assumptions that haven't been verified.
- **Potential Data Sources:**
 - Law Enforcement or Military Records
 - Education and Workplace Records
 - Medical and Mental Health Records
 - Expressions (correspondence with victims), Journals, online presence, and social media activity
 - Life and Relationships- living situation, habits, memberships, religious views, movies, video games
 - Other- Access to weapons, electronic devices

Threat Management Process



Threat Assessment:

- During the initial Threat Assessment meeting, the team will evaluate all information that has been collected.
- To make an accurate assessment of the event, it is important for the Threat Assessment Team to understand threat enhancers and threat mitigators.

THREAT ENHANCERS

These are observable behaviors or contextual factors that increase the likelihood that an individual may engage in violence. They help identify escalation and support a higher risk rating.

Examples:

- Expression of grievance and injustice fixation
- Leakage (communicating intent to harm to third parties)
- Planning and preparation (e.g., surveillance, acquiring weapons)
- Violent ideation or identification with others who have committed violence
- Narcissistic injury, humiliation, or perceived loss of status
- Substance abuse, especially when paired with agitation or paranoia
- History of violence or criminal behavior
- Resistance to help or refusal to engage in mental health treatment



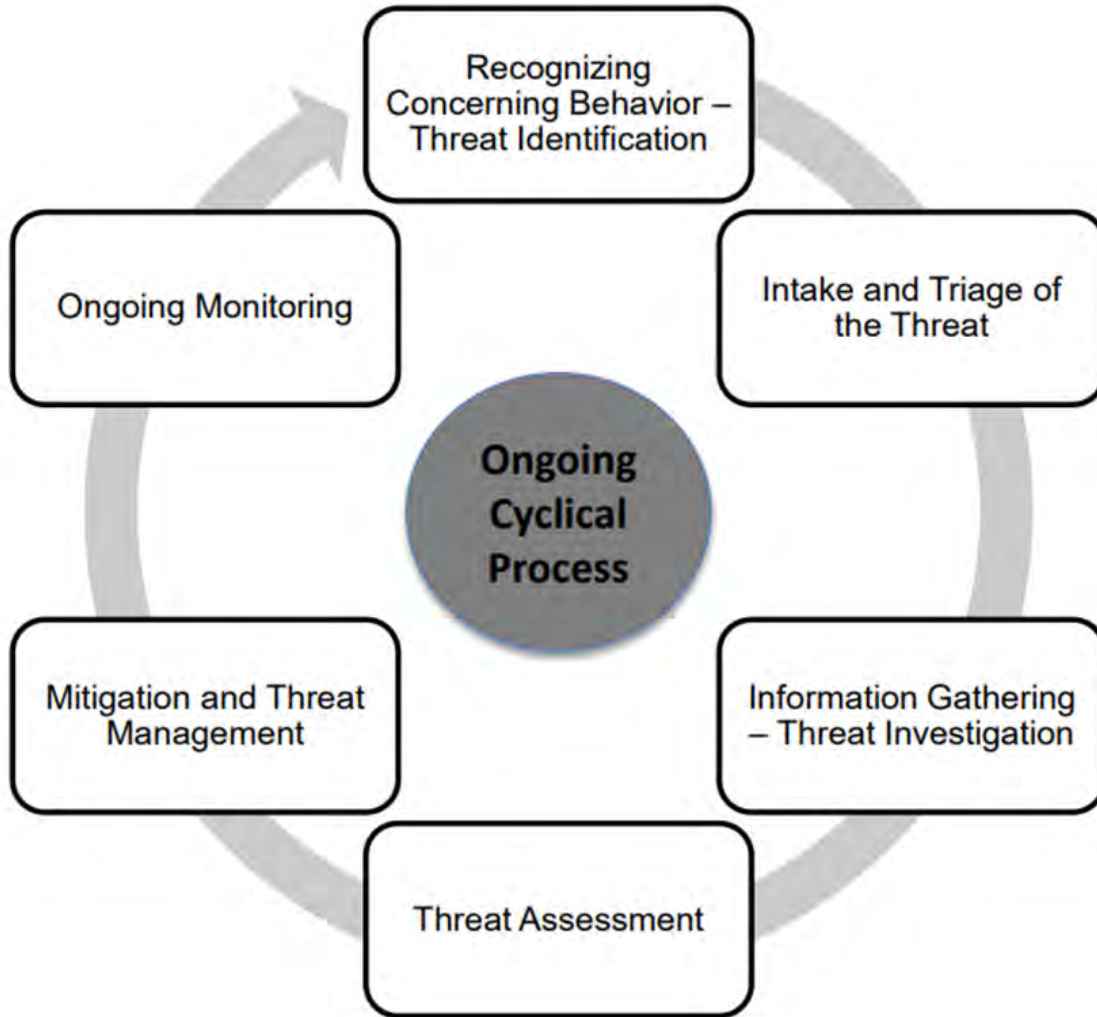
THREAT MITIGATORS

These are behaviors or conditions that decrease the likelihood of violence or indicate a subject is moving away from the pathway to violence. They help reduce the urgency or severity of the risk assessment.

Examples:

- Willingness to accept help or engage with support services
- Presence of strong protective factors (e.g., supportive family, employment)
- Demonstrated remorse or empathy
- Stable mental health care involvement
- Redirection of focus or abandonment of grievance
- Positive future orientation (e.g., plans for school, work, or family)
- Absence of planning or capability (no access to weapons or target)
- Compliance with organizational interventions or law enforcement orders

Threat Management Process



Mitigation/Safety Plan:

- The Threat Assessment Team will develop a mitigation plan to ensure the safety of the persons and property related to Children’s Health.
- The Threat Assessment Facilitator will ensure that the Threat Assessment Intake and Assessment is completed.
- A copy of the safety plan will be disseminated to the Threat Assessment Team and any other interested parties.

Target Based Interventions

- Focused on increasing the safety and resilience of the potential target(s) of violence.
- May include enhanced physical security, relocation of the target, safety planning, protective escorts, or changes in scheduling and environment.
- Often involves direct coordination with the intended victim to ensure awareness, cooperation, and appropriate safety protocols.

Examples of Target-Based Interventions:

- Providing the target with a safety plan including alternate routes and emergency contacts
- Assigning a visible security escort for high-risk movements
- Installing or enhancing panic alarms or surveillance in the target's workspace
- Temporarily reassigning work duties or relocating the target to a secure area
- Coaching the target on situational awareness and how to respond to direct contact

Subject-Based Interventions

- Focused on influencing the behavior, mindset, or circumstances of the person of concern.
- May include mental health evaluation and support, legal or disciplinary action, monitoring, engagement strategies, or restriction of access to persons or property.
- Goal is to disrupt the pathway to violence and reduce motivation, capability, or opportunity for harm.

Examples of Subject-Based Interventions:

- Conducting a behavioral risk interview with the subject
- Mandating or encouraging a mental health evaluation
- Implementing a no-contact or no-trespass order
- Limiting or revoking access to buildings, information systems, or certain individuals
- Maintaining regular contact through security, HR, or behavioral health follow-up
- Providing the subject with alternative dispute resolution or grievance pathways

Threat Management Process

- WPV/Security response to be developed by one of the Leaders in Security
- Tiered responses can and should be used in higher tier levels in addition to security measures listed in that response
- IR = Initial Response

Tier One Response

- Behavior/Safety Contract
- Parking Accommodations for Affected Staff
- Real-Time Training for Staff
- Notification and Involvement of WPV Staff
- Notification to the Security Manager
- Report out to Safety Calls
- Interdisciplinary Conference to Identify Needs and Action Plan

Director of WPV or Director of Security,
Department Leader in Affected Area, HR
Business Partner (if employee WPV)

Tier Two Response

- Additional Security Rounding
- Implementation of a High Risk Flag in the EMR (if patient event)
- CISM/Employee Wellness Resources Shared with Staff
- Notification to Security for Escort to Vehicle
- Risk Assessment of Area if Physical Hazards Exist
- Holtec Media Assessment

VP of Security, VP of HR (Employee Event), VP of Risk or Design, ACC, Facilities Personnel (for Physical Hazards), Leadership (AVP of Area)

Tier Three Response

- Deactivation of Matrix Capability
- Collection of Badge/Stragline
- BOLO to Security and Required Depts
- Contact with Local Law Enforcement if Necessary (Dependent on Event)
- Access Management at Entry Points
- Increased Security Presence at Entry Points
- Alternative Work Accommodation
- Contact with Marketing for Communication Effort
- Communication to Staff via the Emergency Management Platform

EVP, COO, CAO, CHRO, SVP Legal, IT
Leadership, CEO at Discretion of COO,
Communication to Senior Leadership,
Communication to Community if Necessary

Tier One Response

Patient/Visitor Events:

- Disruptive behaviors that impede the care of the patient
- Destructive behaviors that impede the care of the patient or potentially cause staff intimidation

Employee Events:

- Initial Domestic Violence Reported by Staff
- Verbal Altercation Between Staff Members or Bullying Event

Tier Two Response

Patient/Visitors Events:

- Multiple Events of Destructive Behaviors that Impede the Care of the Patient and Could Potentially Cause Damage to Inspira Property
- Dangerous Behaviors that Could Potentially Cause Harm to Staff or Other Patients

Employee Events:

- Secondary Event of Domestic Violence Reported by Staff with Protection from Abuse Court Order Provided
- Any Physical Altercation Between Staff or Threat of Physical Harm or Staff

Tier Three Response

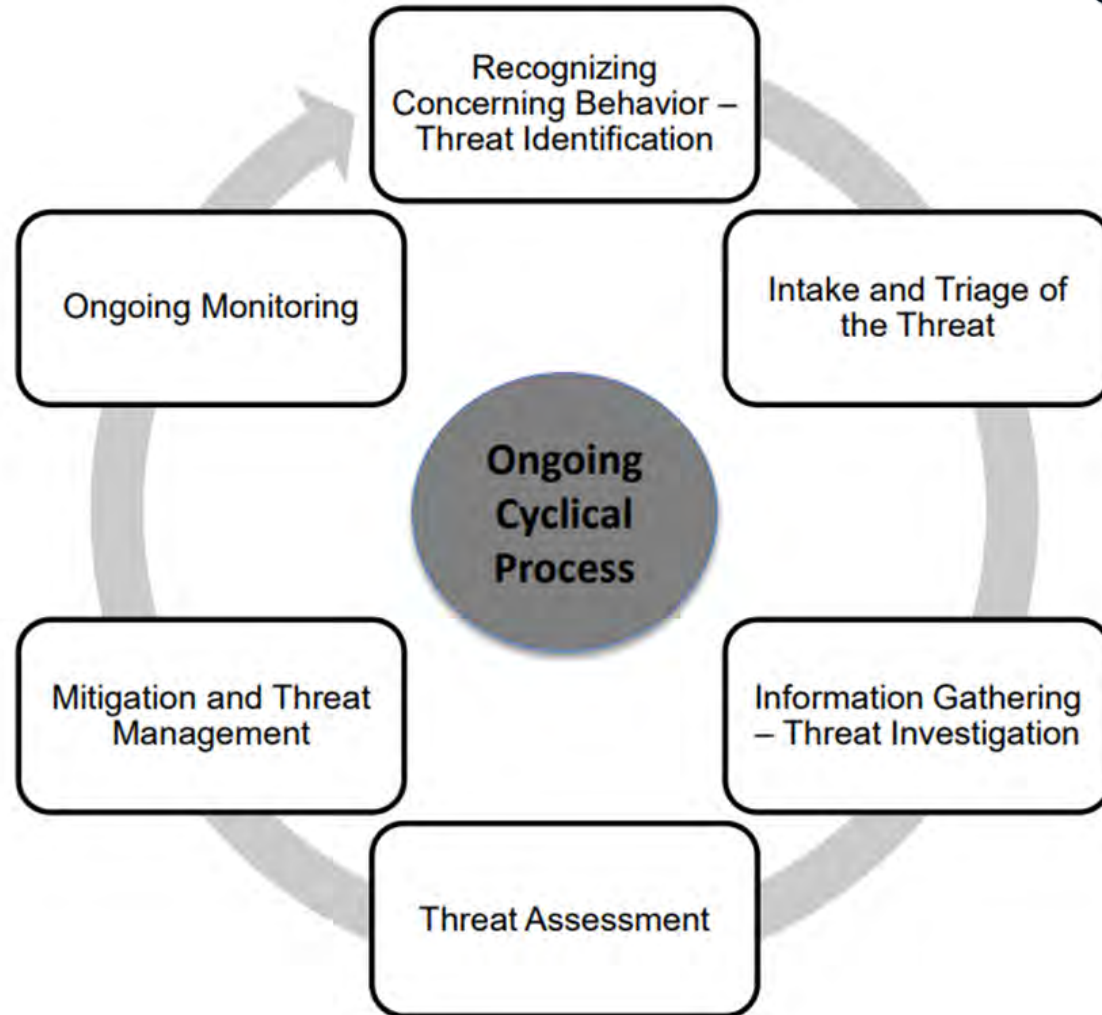
Patient/Visitor Events:

- Events Where Dangerous Behaviors of Patient/Visitor Have Caused Physical Harm to Staff or Other Patients/Visitors
- Threat of Physical Harm to Facility (Bomb Threat, Active Shooting, ect.)

Employee Events:

- Threat of Harm to Self or Others
- Weapon on Campus
- Threats on Social Media/Email
- Termination of Employment with Previous Threats of Harm

Threat Management Process



Ongoing Monitoring and Case Closure:

- The event-specific Threat Assessment Team will meet weekly to review the progress of the safety plan and make any necessary changes if required.
- At the weekly review meetings, the team will determine if there is still an active threat and ongoing need for a safety plan.
- If it is determined that the threat is no longer valid or credible, the threat assessment team should formally close out the active plan.

Threat Management Process

Threat Assessment Team - Event Closure			
Event Information		Threat Assessment Team (TAT)	
Date of Event		Department Leader	
Security Incident Report		Human Resources	
Type of Event		Risk Management	
Area(s) of Impact		Security	
Event Closure Date		Other(s)	
Considerations before closing event			
What has changed in the Individual of Concern's life that might make them more or less likely to attempt violent acts against the victim?			
What specific components of the Safety Plan seem to have directly impacted the Individual of Concern's thinking or capacity to initiate violence and to what extent?			
What life circumstances might occur that would again put the Individual of Concern at increased risk of contemplating or carrying out violent acts? Is there a time of day, month or year when the aggressor is at an increased risk of violent behavior? Examples: <u>payday</u> , tax time, end of month, court date, or holiday.			
<u>Are there supports</u> in place (or could be in place) that will be known and available to the Individual of Concern at a future time should they again move toward violent behavior?			
Is there an alert process or protocol in place to tell the victim / facility of changes in the Individual of Concern's life circumstance that may increase the possibility of violence?			
Have any of the following taken place (check):			
Dismissal – Global	Trespassed from NHC facilities (if not a <u>patient</u>)	Behavior Contract	Legal assistance requested
Ordered		Police Welfare Check	No Contact Order – Court
		Dismissal – Facility	

Case Closure:

- Threat Assessment Team will determine when a mitigation/safety plan can be closed based on the threat level changing.
- Status change should be communicated to all interested parties.
- Copies of all documentation from the threat event should be kept and filed in one central location.

Key Take-a-Ways

- **PREVENTION IS POSSIBLE!** Offenders don't snap, they decide. This progression from thought to action presents intervention opportunities
- Everyone has a role to play in keeping your organization safe
- Recognizing the early warning signs is critical for preventing targeted violence. Threat Assessment Management Programs are one of the best tools we have to prevent these incidents





Questions??

Melissa Jones, CHPA, BC-HSP, CADDC, CEM

302-531-6763