Organizational Threat Assessment and Management Teams: **Developments and Challenges after** 20 Years of Practical Application in **North America Presented by** James S. Cawood, CPP **Factor One** jcawood@factorone.com

2015 Copyright Factor One, Inc.

Elements of Threat Assessment Team Development

- ◆ Team mission and purpose- Choosing a scope and emphasis for your team
- ◆ Naming of the team to accurately reflect mission and purpose
- ◆ Team composition, size, and leadership
- ◆ Team functions- forming a team, developing policies and procedures, determining ongoing team functions
- ◆ Common pitfalls and obstacles

(adapted from (Higher Education Mental Health Alliance (HEMHA), 2012)

2015 Copyright Factor One, Inc.

Potential Benefits of a Threat Management Team

- ◆ Utilizing specialized knowledge to increase insight and available tools, while decreasing intellectual and emotional blind spots, situational bias, cognitive distortion (i.e. minimization, rationalization, and denial), and rigid application of rules to dynamic situations leading to improved accuracy of assessments, efficacy of interventions, and increased scope of ongoing monitoring and reassessment
- ◆ Providing more resources to address the complex problem of potential violence- assessment, intervention, monitoring and support of individuals

Common Potential Obstacles and Weaknesses in Threat Management Teams

- ◆ Different levels of personal commitment to the group process
- ◆ Differing status given to various disciplines and/or team members
- ◆ Subgroup dynamics within the team that reduces cooperation and communication
- ◆ Unequal benefits given to certain team members for participation (i.e. education, promotion metrics, training, etc.)
- ◆ Role confusion, including role of team leader
- ◆ Heavy time commitment for interdisciplinary approach
- ◆ Regular turnover in team members, impacting training, communication, and team bonding
- ◆ Inconsistent application of assessment, intervention, and monitoring processes, including variations in information gathering, use of assessment tools, and applications of intervention methodologies
- ◆ Ineffective and inconsistent communications between team members and between the team and organizational stakeholders

Elements that Contribute to Success of Interdisciplinary Teams

(partially adapted from Schofield & Amodeo, 1999)

- ◆ Common, Clear, Superordinate Goals
- ♦ Leadership Support
- **♦** Committed Expertise
- Breadth of Ideas
- ◆ Compatibility of Organizational Design
- ◆ Team Building (Bonding)
- **♦** Persistence
- ◆ Sufficient Resources (i.e. time, support, money)
- ◆ Overcoming disorganization, miscommunication, and problemsolving difficulties by teaching skills of problem mapping, group direction, effective communication, appropriate solicitation of group member insight, and structured problem-solving

Types of Incidents Proactively Addressed by A Violence Risk Assessment and Management Approach

- ◆ Threats Verbal or written
- ◆ Assaults with or without Battery (Physical contact)
- ◆ Displaying of Weapons on the Organization's property
- **♦** Sabotage or Vandalism
- ◆ All forms of Physical Violence

Later were added stalking, cyberstalking, intimidation, harassment,

Initial Types of Relationships which can Cause Concern and Require Assessment

- ◆ Employee and Employee
- ◆ Employee and Client/Visitor
- ◆ Employee and Manager or Supervisor

2015 Copyright Factor One, Inc.

Current Types of Relationships which can Cause Concern and Require Assessment

- ◆ Employee and Employee
- ◆ Employee and Student/Client/Visitor/Claimant
- ◆ Student/Client/Visitor/Claimant and Same on Organizational property
- ◆ Employee and Manager or Supervisor
- ◆ Employee and Supplier or Vendor
- ◆ Employee and Family Member or former Family Member
- ◆ Non-associated individuals who come on school property (e.g. stalkers, criminals, vandals, mentally or emotionally destabilized persons, community members, others, etc.)

Summary: All relationships with organizational personnel and between parties on property owned or controlled by the organization can be sources of concern and cannot be ignored.

Incident Management Team Members

- ◆ IMT = Core Members and Area Specific Members
- ◆ Core Team Members (includes DMR):
 - Senior Human Resources Representative
 - Organization Security Representative
 - Legal Counsel
- ◆ Area Specific Team Members:
 - Regional/Divisional/ Department Senior Management Representative
 - Manager of Victim or Instigator's Department, if appropriate

IMT Team Member Assignments

- ◆ Designated Management Representative (DMR)
 - Handle Initial Incident Report
 - Conduct Initial Incident Information Gathering
 - Make the First Assessment of whether an Immediate Law Enforcement Response is Necessary
 - Contact the IMT and Provide Incident Information in Detail

IMT Team Member Assignments (Cont.)

- **♦** Human Resources Representative
 - Personnel & Benefit File Access
 - Control of Employment Related Actions
 - Referral of Personnel to Necessary Care Providers-Post Assessment
- **♦** Legal Counsel
 - Advise on all Legal Issues
 - Review the text of all communications to the Instigator or Employees in connection with IMT incidents
 - Control all legal activities, including the obtaining of Restraining Orders

IMT Team Member Assignments (Cont.)

- ♦ Organization Security/Law Enforcement Representative
 - Security Site Surveys and Planning
 - Initiation of Background Investigations
 - Maintain Ongoing Liaison with Appropriate Law Enforcement Agencies
 - Coordination of any On-Site Response
 - Supervise Any Armed Security Personnel

IMT Team Member Assignments (Cont.)

- ◆ Threat Assessment & Response Specialists
 - Initial and Ongoing Assessment of Incident & Instigator concerning the potential for violence
 - Conduct Background Investigation of Instigator
 - Establish and Implement Protective Plan
 - Advise on potential placement of Armed Security Personnel
 - Facilitate On-going Incident Communication with All Team Members and Outside Resources, including Law Enforcement
- ◆ Risk Manager

Later dropped or excluded from most teams

• Advise IMT on Risk Issues, including Risk mitigation tools available in each incident

IMT Operational Support Team Membersas needed for specific case

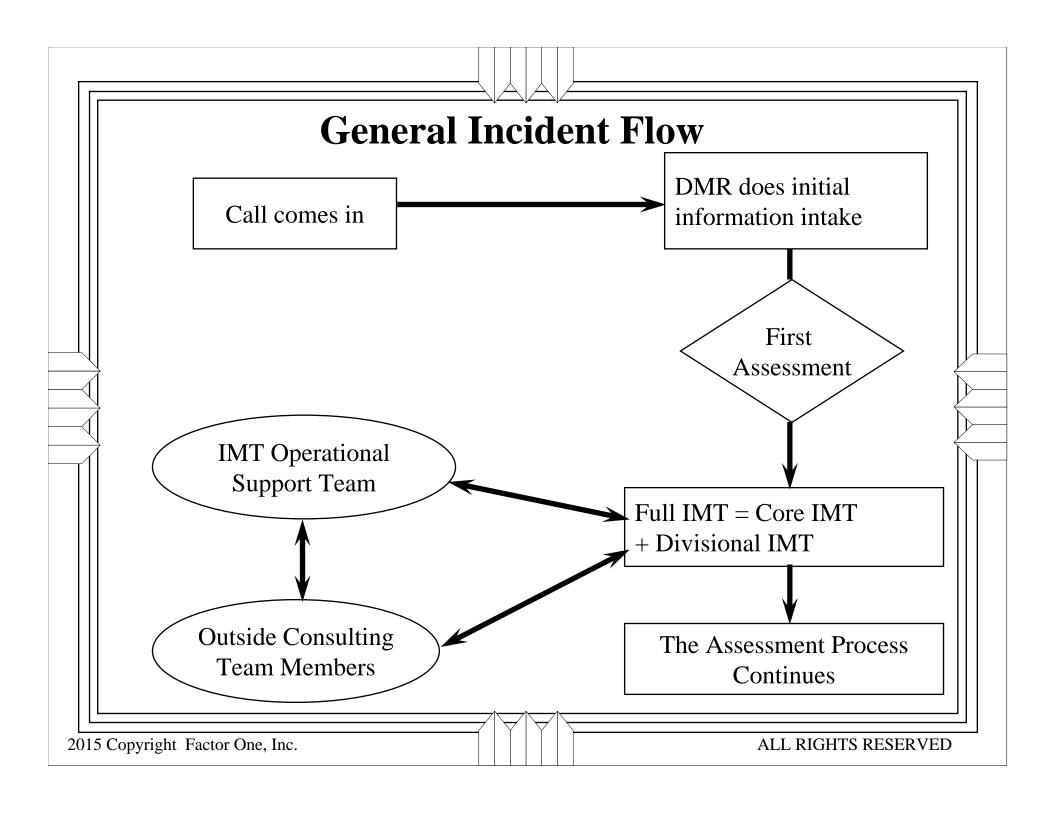
- ◆ Employee Assistance Program (EAP) Representative
 - Provide access to and aid in selection of necessary counseling or evaluation services
 - Provide monitoring of service use
 - Provide a conduit for Tarasoff type notices, as they arise
- ◆ Public Affairs/Corporate Communications Representative
 - Provide media management during incidents that involve public interest
- ◆ Records and Benefits Representative
 - Provide accelerated access to personnel files and benefits information
- ◆ Personnel Liaison(s)
 - Provide insight into current effected workgroup dynamics and personalities of employees involved in the incident

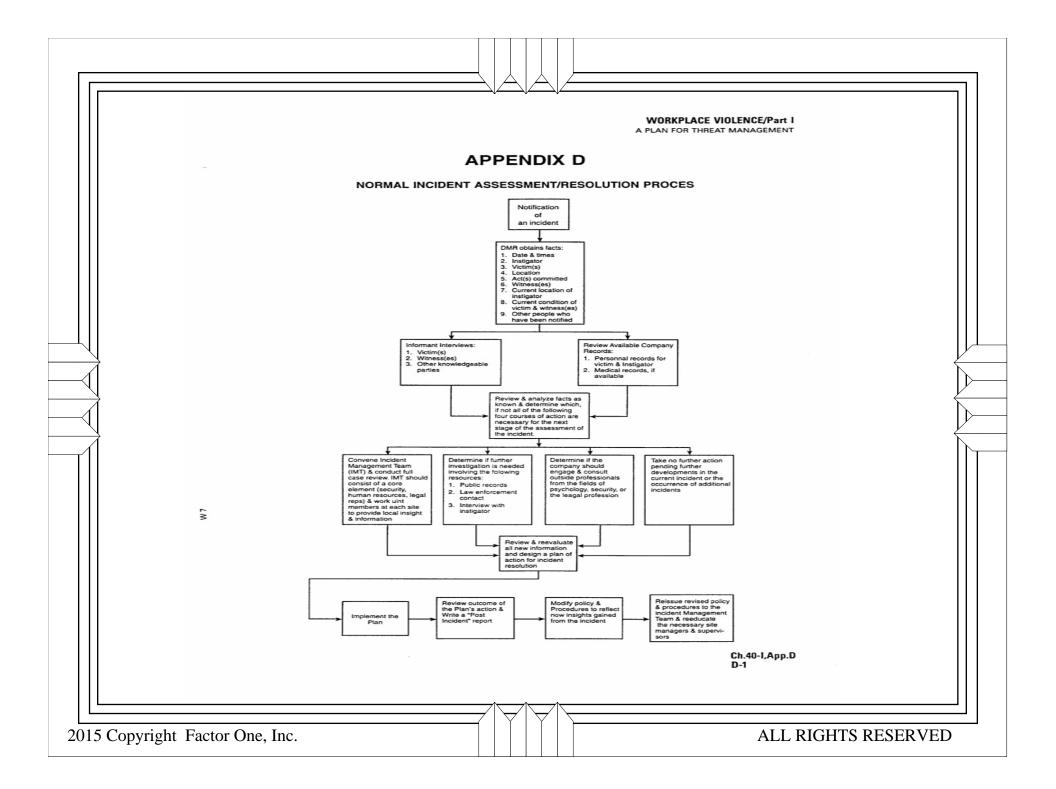
IMT Operational Support Team Memberscontinued

- ◆ Facility Services Representative
 - Provide current knowledge and access to physical properties of any organization site. This could include floor plans, electrical plans, HVAC plans, operation of the physical security system, elevators, water system, sewage system, etc.
- ◆ Information Technologies (IT) Representative
 - Provide knowledge of current email, voicemail, data network, IP phone systems
 - Provide computer system search services
 - Provide computer system monitoring of electronic traffic to and from particular locations, nodes, or devices on the network
 - Provide internet search services, if appropriate- including proxy server access
 - Provide data recovery services, as needed
- ◆ On-site Contract Security Representative (if applicable)
 - Provide enhanced surveillance on the access routes to the site
 - Provide enhanced access control at site access points
 - Provide warning of security breaches in progress
 - Provide notification of security incidents to law enforcement, if requested

Outside Consulting Team Members and Their Roles

- ◆ Security & Investigations Professionals
 - Conduct background investigations in other jurisdictions
 - Provide armed security personnel, as needed
 - Provide security at non-organization locations, if appropriate
- ◆ Psychiatrist or Psychologist Assessment Specialist (if Applicable to the Case)
 - Assessment of incident and instigator when certain factors are present
 - Evaluation of potential for future violence when certain factors are present
 - Initial intervention to calm organizational or individual personnel anxiety, as appropriate
- ◆ Additional Legal Support
 - Obtain restraining orders in various courts
 - Provide employment law advice for employment related cases
 - Provide legal analysis for looking at various legal risks





Incident Assessment/Resolution Process

Notification of an Incident

Λ

DMR obtains the facts:

- 1. Date & time
- 2. Instigator
- 3. Act(s) committed
- 4. Victim(s)
- 5. Location
- 6. Witness(es)
- 7. Current location of instigator
- 8. Current condition of victim & witness(es)
- 9. Other people who have been notified

Interview:

- 1. Victim(s)
- 2. Witness(es)
- 3. Other knowledgeable parties

Review Available Company

Records:

- 1. Personnel records for victim & instigator
- 2. Medical records, if available

2015 Copyright Factor One, Inc.

Incident Assessment/Resolution Process (Cont.)

Yes, further action

Review & analyze facts as known & determine* which, if not all, of the following four courses of action are necessary for the next stage of the incident assessment.

* See Profile Characteristics Grid.

No further action

Convene Core
IMT or convene
full IMT and
conduct full
case review.

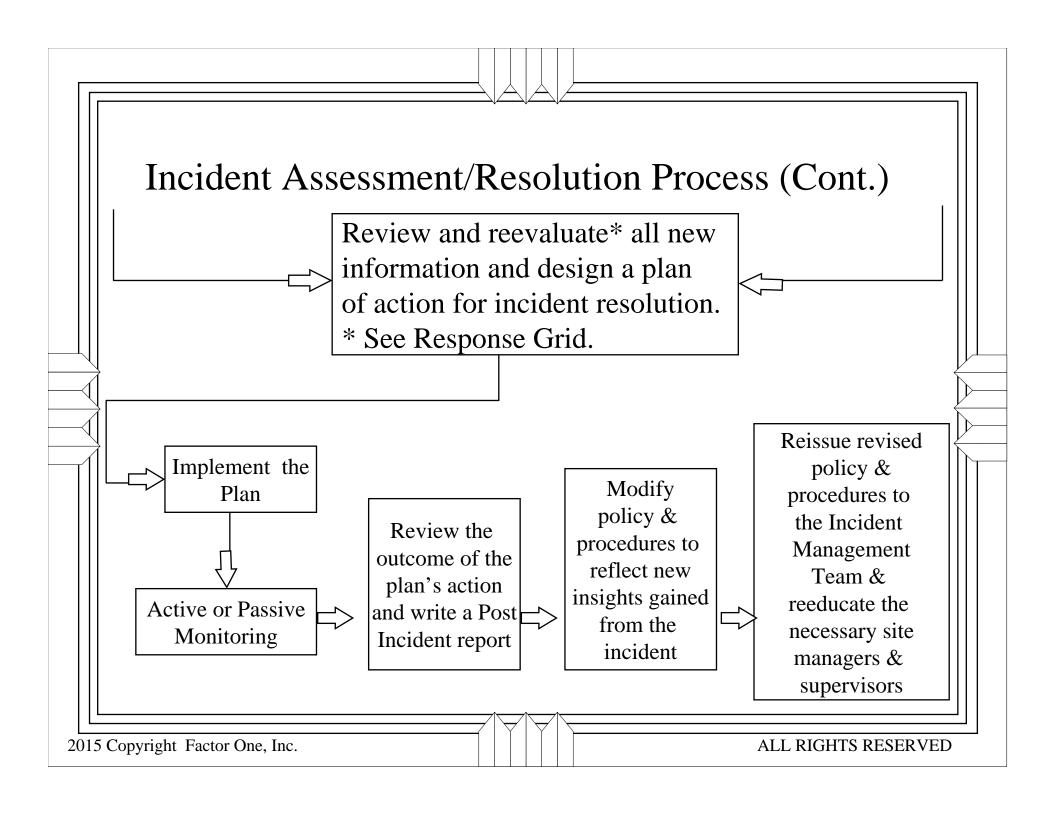
Determine if the company should engage & consult outside professionals from the fields of psychology, security or the legal profession.

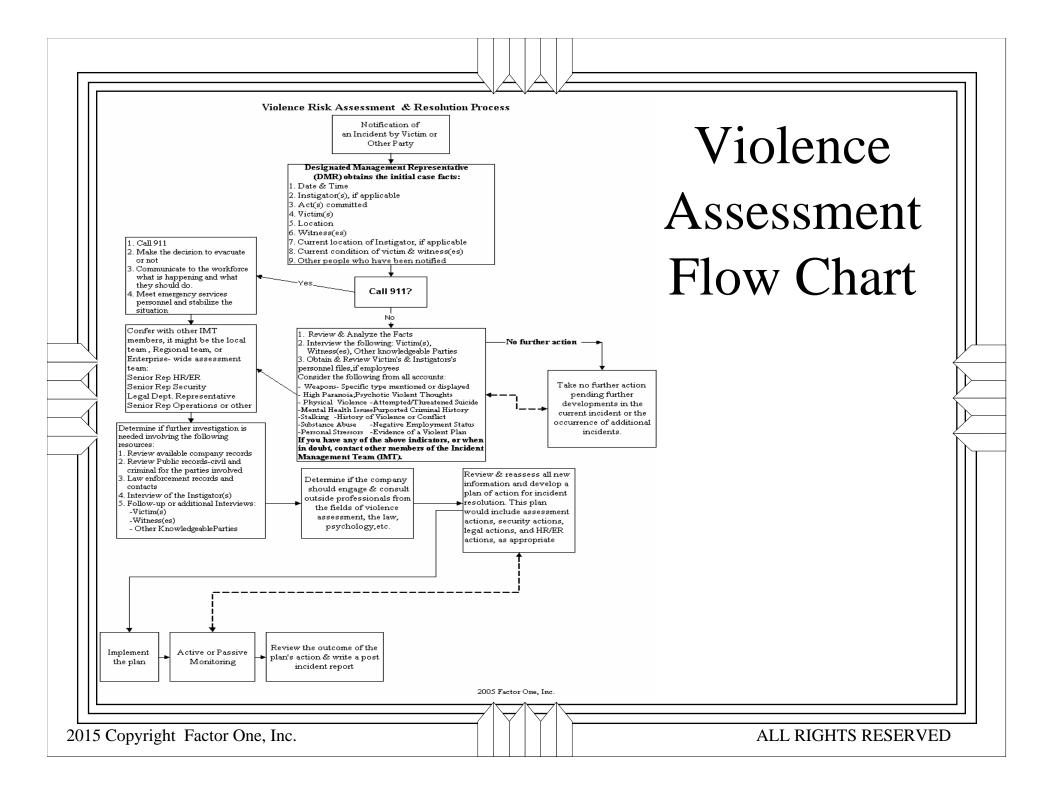
Determine if further investigation is needed involving the following resources:

- 1. Public records
- 2. Law Enforcement contact
- 3. Interview with instigator.

Take no further action pending further developments in the current incident or the occurrence of additional incidents.

2015 Copyright Factor One, Inc.





Policy

An essential element in this policy is that all employees are responsible for notifying the designated management representative (DMR) of any threats, or perceived threats, they receive or have perceived. Employees should also notify the management representative if they have been told that another employee has received or perceived threats. Additionally, they should alert the representative when they witness threatening behavior that could be job related, carried out on a company-controlled site, or connected to company employment. Employees are responsible for making this report regardless of the relationship between the person who initiated the threat or behavior and the person who was threatened. The emergency phone system should be used to report any threat or perceived threat that has immediate life threatening consequences.

Policy (Cont.)

◆ This policy also requires all individuals who apply for -- or obtain -- a restraining order listing company locations as protected areas, to provide a copy of the petition, temporary restraining order, or permanent restraining order to the designated management representative. (Company) has an obligation to provide a safe workplace and protect employees from threats to their safety, and that cannot be done unless (Company) receives information concerning individuals who have been ordered to maintain a distance from company locations.

2015 Copyright Factor One, Inc.

Implementation Considerations for the Use of Any Violence Risk Assessment Tool in a Team

(Wright & Webster, 2011)

- ◆ Initial consultation with colleagues is vital
- ◆ A thorough training program tailored to the teams' requirements is essential
- ◆ Responsibility for actual coordination and completion of the risk assessment on each team must be delegated to and accepted by an individual with experience and authority
- ◆ All disciplines should contribute to the discussion process
- ◆ During both initial training and refresher training it must be emphasized that assessors should not push for low or high scores
- ◆ Always remember that the main aim of risk assessment is risk management
- ♦ Follow-up training is essential to ensure adherence to the original assessment scheme
- ◆ The nature and limitations of the instrument must be a part of the educational program.

ASIS/SHRM WPVI.1-2011

- ◆ Released on September 2nd, 2011 after a four year, multi-disciplinary development effort.
- ◆ Purpose: Establish an American National Standard (ANSI) for workplace violence prevention and intervention.
- ◆ Provides new definitions (e.g. violence risk screening), as well as creating a standard for everything from how you plan a program to involving law enforcement.

Major Areas of Coverage

- ◆ Establishing Multidisciplinary Involvement
- ◆ Planning a Workplace Violence Prevention and Intervention Program
- ◆ Implementing the Program
- ◆ Threat Response and Incident Management
- **♦** The Role of Law Enforcement
- ◆ Post Incident Management
- ◆ Integrating the Issue of Intimate Partner Violence into Workplace Violence Prevention Strategies

2015 Copyright Factor One, Inc.

- ◆ 5.2.5: Union Leaders are encouraged to actively participate in prevention and intervention efforts
- ◆ 5.2.6: Employee Assistance Programs (EAP) are mentioned as possible violence risk *screeners*, but only with specialized training
- ♦ 6.2.1: Policy should be a "No Threats, No Violence" policy, not a "Zero-Tolerance" policy
- ♦ 6.2.2.1: Process should have access to outside experts in the area of violence risk assessment, law, and security
- ◆ 6.2.7: Process should include a system of centralized record keeping for both recording and tracking of cases.
- ♦ 8.7: "...when formal violence risk assessment is warranted, the organization should engage an external threat assessment professional to assist..."
- ♦ 8.10.2: "Studies show that once violence begins, actions with the greatest impact on outcome will be taken by persons already at the scene, before law enforcement arrives. For that reason, emergency responders should be considered as merely one element of a broader violence response plan."

8.3.1 The Incident Management Process in Non-Urgent or Non-Emergency Situations

If a reported situation does not appear to present an immediate threat to physical safety, the Incident Management process should include the following components:

- a) Conduct an initial gathering of information from readily-available sources;
- b) Perform a preliminary violence risk screening, based on information known at the time;
- c) Develop a plan for early actions based on the initial risk screening;
- d) Conduct a deeper, continued investigation and re-evaluate risk based on new information learned;
- e) Implement further needed Incident Management actions, such as a formal violence risk assessment and other needed interventions;
- f) Develop recommendations for appropriate responses to resolve an incident and assist relevant management with implementation;
- g) Perform continued monitoring and follow-up actions as appropriate; and
- h) Debrief to evaluate the effectiveness of Incident Management and identify required process improvement.

8.4.3 Evaluating Information for the Initial Risk Screening

Once it gathers initial information, the Threat Management Team should conduct a preliminary risk screening with a view towards ascertaining, in a gross or general manner, the urgency presented by the situation in question. The team should consider all information it has gathered consistent with Section 8.4.1 and 8.4.2 above that indicates or mitigates a risk of violence and then assess, from a lay person's perspective:

- a) Is a concern for violence unwarranted, so that the incident can be handled (when involving an employee) within normal human resources, disciplinary, or employee relations protocols, as opposed to by the Threat Management Team?
- b) Is some concern for violence warranted but not significant or urgent, so that the Team can continue with additional fact-gathering and its Incident Management process?
- c) Is a concern for violence urgent, so that emergency or urgent action should be taken, such as immediate consultation with a violence risk assessment professional or law enforcement?

8.7 The Importance of Setting Appropriate Limits to Internal Violence Risk Assessment

Many organizations' Threat Management Teams, through training and accumulated experience, will be adept at screening cases for potential risk and at developing risk mitigation strategies. However, when the Team lacks that training and experience, or when a formal violence risk assessment is warranted, the organization should engage an external threat assessment professional to assist with Incident Management. The Team should acknowledge the limits of its expertise and experience, and obtain external assistance when needed.

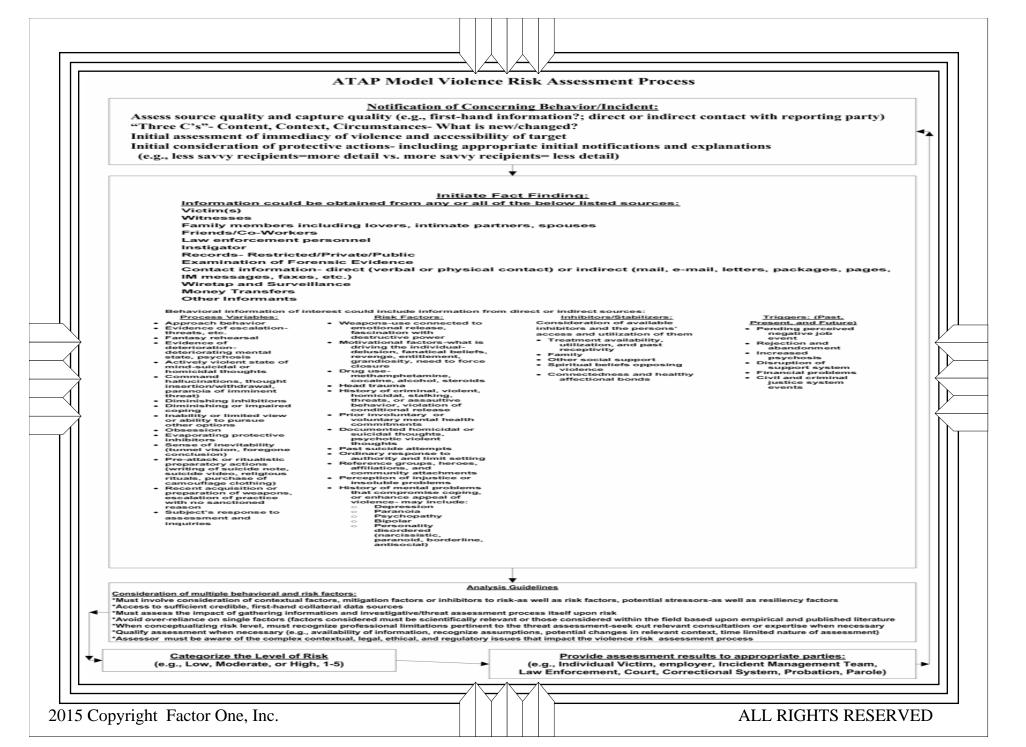
Outsourcing a violence risk assessment to a qualified threat assessment professional can enhance the quality of Incident Management; in addition, it can help to mitigate the organization's liability by ensuring that the organization has allowed a qualified person, not the organization's own employees, to assess violence risk.

In selecting an external threat assessment professional, the organization should consider such factors as the person's:

- Education, training, and experience in violence risk assessment, especially in the workplace context;
- · Licensing, credentialing, and insurance;
- Reputation;
- · Experience in the industry;
- Availability, flexibility;
- · Style, approach, and sophistication; and
- General familiarity with relevant criminal, civil, and employment law.

Association of Threat Assessment Professionals (ATAP): RAGE-V

- ◆ RAGE-V = Risk Assessment Guideline Elements for Violence
- ◆ Released on September 20th, 2006 after a four year, multi-disciplinary development effort
- ◆ Purpose: Establish a common framework for conducting violence risk assessments and assessing the validity of the process used to provide the results.
- ◆ Comprised of three practice advisories (Psychology, Law, and Information Gathering) and a model violence risk assessment process



Threat Management Program Hoped for 1st Evolution

Before

- ◆ No Policy
- Varying Knowledge
- ◆ Role Ambiguity
- ♦ Lack of Reporting
- ◆ No Valid Assessment Process
- ♦ Reactive to Incidents
- **♦** No Monitoring
- Individual Fragmented Approach
- ◆ Inappropriate Use of Resources
- ◆ Uncertainty & Fear

After

- ◆ Policy
- ◆ Training & Common Knowledge Base
- ◆ Clear Ownership & Roles
- Mandatory Reporting
- **♦** Threat Assessment Protocol
- ◆ Proactive Response
- ◆ Case Review & Monitoring
- ♦ Multi-disciplinary Approach
- ◆ Proper Use of Specialists
- ◆ Increased Control & Safety

2015 Copyright Factor One, Inc.

Threat Management Team Current Challenges

- Policy may not reflect current expansion of behaviors (i.e. stalking, cyber-bullying, cyber-stalking, connection with sexual harassment, etc.)
- ◆ Updating knowledge, given the explosion in the empirical literature involving violence risk assessment, intervention, and legal decisions
- ◆ Stability of team membership
- ◆ Role re-examination & cross-training for unifying team methodology
- Frequently meeting and interacting to maintain relationships, share new information, and decrease the tendency to defer responsibilities to others or develop sub-groups
- ◆ Maintaining team authority to act independently, using appropriate resources of the organization
- Continuous adherence to an agreed upon assessment process, requiring adequate information gathering (inside and outside the organization), full sharing of the information with all team members, individual assessment before team analysis, and use of a valid and appropriate assessment tool
- ◆ Maintenance of intervention tools including current knowledge of employee benefits programs; strong relationships with community resources (i.e. mental health, law enforcement, victim services, courts, etc.); current understanding of the relevant civil and criminal laws, restraining order procedures, regulations, standards, etc.; interviewing skills; and current security hardware and new methodology
- ♦ Maintenance of adequate case monitoring (i.e. frequency of checking for new behavior, documentation and communication of new behavior to the team, reassessment of new information, application of appropriate additional interventions)
- ◆ Centralized record keeping, possibly separate from all other organizational systems; with multi-point access, monitoring of assignments and results, notification of changes; encrypted and accessible on multiple platforms and devices

Threat Management Program Actual Evolution

Current

- Policies, but fragmented in many organizations
- Multi-disciplinary approach, but various teams and team compositions per organization; rarely are all members fully engaged and participating
- Common, expanded, knowledge base- but varying levels of knowledge improvement
- Clearer roles, but differing levels of engagement in the process
- Mandatory reporting expectations, but not consistent
- Various degrees of reactivity to incidents
- ◆ Valid assessment processes, but various degrees of use, primarily at the low use end
- ♦ More appropriate use of intervention resources, but with wide variations of engagement of outside expertise and community resources
- Monitoring, but of various durations and with varying effectiveness

Future Areas of Continual Improvement

- ◆ Policies that continue to evolve to address emerging violence risks
- Granting of team budget and organizational support and control for case assessment and management
- Expectation and delivery of proactive response
- ◆ Multi-disciplinary approaches with a strong, committed, leadership and member commitment to full participation, and collaboration, including full information review and individual analysis
- Cross-training for all members for a more comprehensive insight into all roles
- ◆ Connecting behavioral reporting to performance and promotion metrics
- ◆ Increasing adherence to empirically based violence risk assessment methodology, appropriately validated- if available
- ◆ Expanded intervention options, including enhanced community coordination
- More consistent case monitoring with better case documentation and case change communications to team members

Reference and Resource List

- ◆ Aarnio, M., Nieminen, J., Pyörälä, E., & Lindblom-Ylänne, S. (2010). Motivating medical students to learn teamworking skills. *Medical Teacher*, 32, e199-e204. doi:10.3109/01421591003657469
- ◆ ASIS International, & Society for Human Resources Management. (2011). *Workplace violence prevention and intervention: American national standard*. Arlington, VA.
- ◆ Association of Threat Assessment Professionals. (2006). *Risk assessment guideline elements for violence*. California: Author.
- ◆ Benedek, D. M., Ursano, R. J., Fullerton, C. S., Vineburgh, N. T., & Gifford, R. K. (2006). Responding to workplace terrorism. *Journal of Workplace Behavioral Health*, 21(3-4), 21-33. doi:10.1300/J490v21n03_02
- ◆ Cawood, J. S. (1993). Chapter 40: A plan for threat management. In C. Sennewald (Ed.), *Protection of assets manual* (pp. 1-23). Arlington, VA: Merritt Publishing.
- ◆ Cawood, J. S., & Corcoran, M. H. (2009). *Violence assessment and intervention: The practitioner's handbook-2nd edition* (2nd ed.). Boca Raton, FL: CRC Press.
- ◆ Deisinger, G., Randazzo, M., O'Neill, D., & Savage, J. (2008). *The handbook for campus threat assessment & management teams*. Stoneham, MA: Applied Risk Management.
- ◆ Fay, D., Borrill, C., Amir, Z., & Haward, R. (2006). Getting the most out of multidisciplinary teams: A multi-sample study of team innovation in health care. *Journal of Occupational and Organizational Psychology*, 79, 553-567. doi:10.1348/096317905X72128
- ◆ Fein, R. A., & Vossekuil, B. (1998). Protective intelligence & threat assessment investigations: A guide for state and local law enforcement officials. Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.
- ♦ Hall, W. A., Long, B., Bermbach, N., Jordan, S., & Patterson, K. (2005, March). Qualitative teamwork issues and strategies: Coordination through mutual adjustment. *Qualitative Health Research*, 15(3), 394-410. doi:10.1177/1049732304272015
- ♦ Higher Education Mental Health Alliance (HEMHA). (2012). *Balancing safety and support on campus:* A guide for campus teams. The Jed Foundation.

Reference and Resource List-continued

- ♦ Kane, B., & Luz, S. (2011). Information sharing at multidisciplinary medical team meetings. *Group Decisions & Negotiation*, 20, 437-464. doi:10.1007/s10723-009-9175-9
- Miller, T. (2013, February). How to build an effective threat assessment team. *Security Magazine*.
- ◆ O'Connor, G. C., Rice, M. P., Peters, L., & Veryzer, R. W. (2003, August 1). Managing interdisciplinary, longitudinal research teams: Extending grounded theorybuilding methodologies. *Organization Science*, *14*(4), 353-373. doi:1047-7039/1404/0353
- ◆ Schofield, R. F., & Amodeo, M. (1999, August). Interdisciplinary teams in health care and human services settings: Are they effective? *Health & Social Work*, 24(3), 210-219.
- ♦ Van Der Vegt, G., & Bunderson, J. S. (2005). Learning and performance in multidisciplinary teams: The importance of collective team identification. *Academy of Management Journal*, 48(3), 532-547.
- ♦ Watt, K. A. (2010). Domestic violence fatality review teams: Collaborative efforts to prevent intimate partner femicide, Graduate College-Psychology, University of Illinois at Urbana-Champaign.
- ◆ Wright, P., & Webster, C. D. (2011). Implementing structured professional judgment risk assessment schemes: An example of institutional change. *International Journal of Forensic Mental Health*, 10(1), 1-6. doi:10.1080/14999013.2011.552365