THE 2020 GUIDE TO THREAT ASSESSMENT APPROACHES FOR LAW ENFORCEMENT

Threat assessment means different things to different people. Security professionals, police, military personnel, psychologists, and school counselors all use the term and conduct tasks they describe as threat assessment. These tasks are all predictive in nature, but very different.

We have updated this guide for 2020. We originally published it in January 2019. I wrote it because I was having trouble differentiating between all the different “types” of threat assessment. It turns out lots of people use the term.

Since, publication this guide has proven to the most popular post on our blog, with 1,435 visitors last year from all over the world. For a small company like us, this is awesome. We are helping police everywhere identify techniques that can help them do their jobs and protect their communities.

I hope you too find this resources useful. Don’t hesitate to reach out if we can help you or your organization.

THREAT ASSESSMENT APPROACHES

Take a moment to think about what threat assessment in law enforcement means to you or even what problem you are hoping that threat assessment will help you solve.

Are you looking to:

1. plan for and protect facilities and critical infrastructure in your community against terrorist attacks, natural disasters, and other threats;
2. help your officers to identify and react to threatening individuals such as active shooters, terrorists, or other threats.
3. protect your computer networks, systems, and servers from attacks by malicious actors;
4. assess the likelihood of a specific individual for violent behavior; or
5. identify, assess, and intervene with a person who may commit targeted or instrumental violence.

Let's take a deeper dive into each threat assessment approach. Please understand these next sections do not represent a comprehensive review on each approach, instead they are meant to define and also help you

identify threat assessment training and resources that might help you, your officers, or your community.

---

1. The Security Threat and Risk Assessment

To people who work in the security or protection industry threat assessment is the first step in a risk and vulnerability analysis. This threat assessment task involves assessing the various threats and security risks associated with a particular location. It covers a broad range of threats: ranging from natural threats (tornadoes, hurricanes, floods, earthquakes), criminal threats (theft from location, violence against staff), to terrorists (active shooter, vehicle and person-borne improvised explosive devices) and potential accidents. (Renfroe and Smith, 2016)

SECURITY THREAT RISK ASSESSMENT AT A POWER PLANT

For a security threat risk assessment in law enforcement, let's take an example of a power plant in your jurisdiction. Potential threats to a power plant could include natural disasters (such as an earthquake or hurricane), a terrorist attack, or an accident such as a computer failure causing the plant to shut down. Each of these threats might require a different

response from you or your officers.

This security threat risk assessment includes not only an identification of potential threats but also an evaluation of the likelihood of occurrence for each; just because something can happen doesn't mean it will.

THE VULNERABILITY ASSESSMENT

The security risk threat assessment is the precursor to a vulnerability assessment. This vulnerability assessment has two parts. First, it involves a determination of the loss that would be incurred if the given location was successfully attacked; basically how much will it cost if the facility stops providing service. Second, it also includes an assessment of the level of attractiveness of the target (in the case of intentional attack) and the level of existing defenses against each different threat. (Renfroe and Smith, 2016)

In the case of this same power plant, it may be that there is a backup plant nearby that can cover the loss of energy if the facility goes offline; reducing

the overall damage or cost to the community if the facility is put out of service. For attractiveness, a power plant inside of an urban area may be a more attractive target than one in a rural area because of collateral damage.

These potential threats, impact associated with loss of the facility, and assessments of vulnerability are then reviewed in combination as part of a risk analysis. The risk analysis will also involve the study of existing and needed countermeasure to protect against threats and reduce risk. This analysis provides the opportunity to upgraded or improve existing countermeasures. (Renfroe and Smith, 2016)

LEARN MORE ABOUT THE SECURITY RISK THREAT ASSESSMENT

If you are interested in learning more about the security threat risk assessment associated with risk analysis here are some great resources.

1. The "Risk Management Process for Federal Facilities" Guide from the United States Department of Homeland Security (DHS); and
2. The DHS and State Department's "Guide to Critical Infrastructure and Security Resilience".

---

2. Active Threat Assessment

For a law enforcement officer, threat assessment is also used to describe a process through which an officer observes and identifies potential, immediate, or imminent threats (e.g., active shooters, terrorists, criminals). At Second Sight we use the term active threat assessment to describe the

identification of these immediate, imminent, or active threats by a law enforcement officer. These threats could be against your officers or the public.

THE ACTIVE THREAT ASSESSMENT METHODOLOGY

Active threat assessment involves a focused observation of behaviors & actions. It is a threat assessment methodology by which an officer systematically observes their environment, identifies potentially suspicious individuals (also known as a person of interest), and assesses the extent that person is a threat.

A person of interest (POI) as an individual whom by their suspicious activity, lack of an explainable objective or display of threatening behavior becomes a target for further investigation through observation or physical interdiction.

ACTIVE THREAT ASSESSMENT TRAINING

Second Sight offers active threat assessment training for law enforcement and security professionals. Our law enforcement classes is certified through the IADLEST NCP program. Our security program meets the same rigorous standards.

Further observation of the POI involves an assessment of threat indicators. Threat indicators are verbal or visual behaviors that imply an individual is being threatening, trying to hide in plain sight, or carrying contraband or weapons. These assessments, in combination, allow the identification of active threats.

To learn more about active threat assessment and active threat assessment training read our post about active threat assessment or take our free online *Intro to Active Threat Assessment* Course.

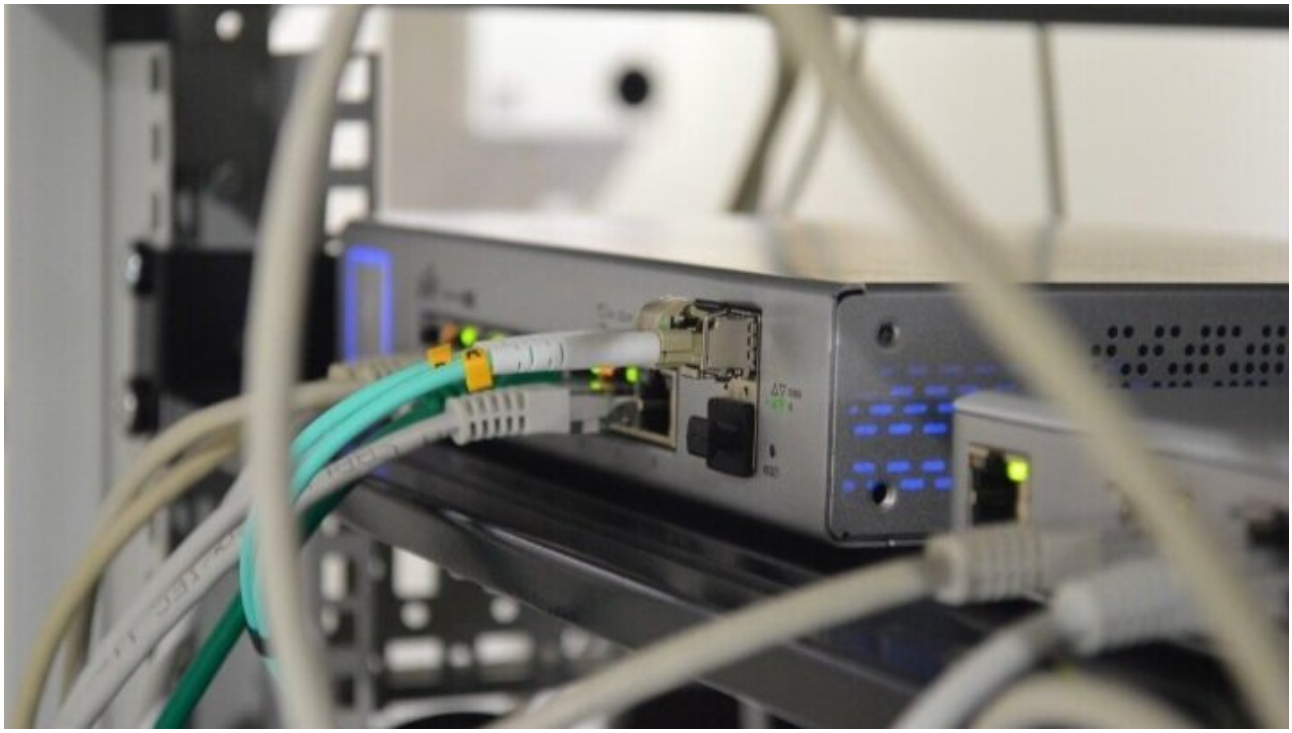
In this course, you can learn about the active threat assessment methodology and it can help you decide if our longer active threat assessment programs are right for you and your officers.

ENROLL NOW

3. The Cyber-security Threat Risk Assessment

The same threat risk assessment and analysis process can be applied to cyber-security. A cyber-security threat risk assessment in law enforcement can involve protecting information (e.g., your arrest data), networks (e.g., the internet at your station), software (e.g., your booking software), and

hardware (the laptops and desktops of your officers). The basic steps of a cyber-security risk assessment involve:



1. characterizing the type of system that is at risk;
2. identify threats to that system (unauthorized access, misuse of information, data leakage/exposure, loss of data, disruption of service);
3. determine inherent risks and impacts;
4. analyze and identify threat prevention, mitigation, detection, and compensation controls. Assess the extent existing controls mitigate the threats.
5. determine the likelihood of a threat occurring based on current controls; and
6. calculate risk rating based on a combination of impact and likelihood. (Metivier, 2017)

As with the security risk threat assessment, it is then possible to implement or improve controls based on the higher risk threats to cyber-related infrastructure.

If you are interested in learning more about the cyber-security-related threat risk assessment process, we recommend you review the National Institute of Standards and Technology (NIST) "Guide for Conducting Risk Assessments".

4. Threat Assessment for Instrumental Violence

The American Psychological Association describes another threat assessment approach that involves a broad spectrum of activities to identify and intervene with potentially violent individuals and prevent instrumental violence (such as a school shooting). It focuses on preventing a violent incident and to "help potential offenders overcome the underlying sources of their anger, hopelessness, or despair" (NASP, 2014). You or some of your officers might be part of a threat assessment team at one of your local schools and be involved in this threat assessment approach.

A noted authority on this threat assessment approach is the US Secret Service National Threat Assessment Center (NTAC). In a recent report titled Mass Attacks in Public Places, they noted many of the attackers in 2017 had similar backgrounds, including: a personal grievance; history of criminal behavior, substance abuse, or mental health symptoms; or, a stressor (such as financial instability). Many of these attackers also had communications of concern or elicited concern from others prior to the

attack. These situational and behavioral factors can serve as flags of individuals who may commit instrumental violence. (NTAC, 2018A)

THREAT ASSESSMENT IN SCHOOLS

This approach is focused on assessing the threat of a specific individual committing a specific attack. According to the NTAC, this broader threat assessment approach in a school setting has five steps:

1. Establish a multi-disciplinary threat assessment team;
2. Define behaviors that require intervention (e.g. threats, carrying weapons);
3. Establish and provide training on a central reporting system;
4. Determine a threshold for law enforcement intervention;
5. Establish an investigative driven threat assessment process or referred individuals focused on a range of factors, including, but not limited to, motive, communications, weapons access, stressors, emotional and developmental issues, and protective factor. (NTAC, 2018B)

Potentially threatening individuals are identified from information and referrals, these individuals are assessed for the extent they may commit an attack. As part of this threat assessment approach, those at-risk for violence are targeted with a variety of interventions. In the case of an imminent attack, law enforcement and the other professionals could take more immediate measures to control the individual. (Miller, 2014)

LEARN MORE ABOUT THIS APPROACH

If you would like to learn more about this type of threat assessment, more information is available from the sources below, and an internet search will reveal a variety of other resources on the topic:

1. The US Secret Service National Threat Assessment Center
2. The Association of Threat Assessment Professionals

---

5. The Violence Threat Risk Assessment

Violence threat risk assessments are generally legal and clinical in nature, estimating the likelihood of future violent behavior by an individual and the identification of risk factors and intervention strategies. This approach is somewhat different than the threat assessment for instrumental violence

somewhat different than the threat assessment for instrumental violence described above. This violence-risk approach focuses on assessing an individuals predilection for violence generally, not related to a specific attack against a specific target. Some of your officers may also perform these assessments in the course of their investigations or after an arrest.

These violence threat risk assessments can be used in release decisions for corrections and psychiatric facilities, civil commitment, criminal sentencing, or classification after admission into a correctional or treatment facility. (Violence Risk Assessments, ND)

As part of this task, a clinical professional may administer a battery of tests to evaluate for the likelihood of committing a violent act. These violent risk assessments can involve both actuarial-based assessments and the professional judgment of the clinician. Actuarial-based assessments involve predictive algorithms using a combination of risk factors which

determine the risk of violence. These actuarial-based models can also be interpreted based on the professional judgment of experienced evaluators. (Violence Risk Assessments, ND)

Please note, there are criticisms of the different techniques in the existing literature. If you are looking for research and support to conduct threat assessments related to individual risk and violence, we encourage you to access resources available from:

1. The Center for Disease Control (CDC)
2. The American Psychological Association

What's Next?

Depending on your needs, any of these approaches to threat assessment for law enforcement may be relevant to you or your officers. As next step, we recommend that you utilize the resources we have included here and continue your quest for to learn more about threat assessment. All these different approaches are important to protecting our community and keeping people safe.

Would you like to learn more about active threat assessment? Take a free 30 minute online course.

ENROLL NOW

Related Content

Before Defensive Tactics: 5 Training Approaches for LE-Citizen Encounters (Part I)

Sep 5, 2020

Active Threat Assessment In Action: Concealed Weapons at Protests

Jun 13, 2020

The 2020 Guide to Threat Assessment Approaches for Law Enforcement

Jan 18, 2020

References

Metvier, B. (2017). *6 Steps to a Cyber Security Risk Assessment*. Sage Data Security. Available at https://www.sagedatasecurity.com/blog/6-steps-to-a-cybersecurity-risk-assessment.

Miller, A. (2014). *Threat Assessment in Action*. The American Psychological Association. Available at https://www.apa.org/monitor/2014/02/cover-threat.aspx.

NASP School Safety and Crisis Response Committee. (2014). Threat Assessment for School Administrators and Crisis Teams. Bethesda, MD: National Association of School Psychologists.

National Threat Assessment Center (NTAC). (2018A). *Mass Attacks in Pubic Spaces - 2017*. United States Secret Service. Obtained January, 2019 from https://www.secretservice.gov/data/protection/ntac/USSS_NTAC-Mass_Attacks_in_Public_Spaces-2017.pdf

National Threat Assessment Center (NTAC). (2018A). *Enhancing School Safety Using a Threat Assessment Model: An Operational Guide for Preventing Targeted School Violence.* United States Secret Service. Obtained January, 2019 from https://www.secretservice.gov/data/protection/ntac/USSS_NTAC_Enhancing_School_Safety_Brief_7.11.18.pdf

Renfroe, N.A. and Smith, J.L. (2016). *Threat / Vulnerability Assessments and Risk Analysis*. Applied Research Associates. Obtained November 24, 2018 from https://www.wbdg.org/resources/threat-vulnerability-assessments-and-risk-analysis.

Violence Risk Assessments. (ND). Obtained from December 2018 from https://psychology.iresearchnet.com/forensic-psychology/violence-risk-assessment/

PREVIOUS

A Guide To The Provision Of Law Enforcement & Security Services During The Covid-19 Pandemic

NEXT

About Threat