- THE ISRAELI MODEL -
ADVERSARY BASED SECURITY
FOR YOUR SCHOOL
THREAT MITIGATION TRAINING

PETER CRABBE

SENIOR CONSULTANT / DIRECTOR OF SCHOOL OPERATIONS
“Security is the foundation of higher learning.”

Southern California Head of School

“Children who feel safe - learn better.”

Headmaster /Teacher
The Reactive System

Traditional Security in America
The Reactive System

THE OLD WAY

POLICE – CRIME/ NO CRIME

SECURITY – OBSERVE AND REPORT
The Reactive System

THIS IS NOT SECURITY!!!
THIS IS OBSERVE AND REPORT
TRADITIONAL SECURITY OFFICER

Observing and Reporting …

Does nothing to mitigate threat or protect people

Relies exclusively on hopeful deterrence

Has no “Plan B” if deterrence fails

Is reactive at best

Security cannot merely observe and report!
A lot of time, expense and resources are spent on traditional reaction-based security, on how to react well to an emergency or criminal/terrorist act after the act happened....however....
TRADITIONAL SECURITY OFFICER

Observe and Report

...wouldn’t it be better to stop crime BEFORE it happened? Before EMTs and police need to be called? Prevent it minutes, hours, days, weeks before the act happens?

It CAN be done!!!
Indiana School Security

THE ISRAELI SECURITY MODEL

PROACTIVE THREAT ASSESSMENT

THE NEW WAY

PREDICTIVE PROFILING (Detection)

SECURITY QUESTIONING (Determination)

DECISION OF ACTION (Deployment)
THE ISRAELI SECURITY MODEL

PROACTIVE THREAT ASSESSMENT

Proactive

Not waiting for something bad to happen – acting before it happens.

Threat Assessment?

An ongoing process of constantly evaluating the environment for possible threats to the security of people and property.
THREAT ORIENTED SECURITY

THREAT VS RISK

INDIANA SCHOOL SECURITY STANCE

Security cannot be measured against what did or did not happen.....

... but rather what could or could not take place.
We have a natural human tendency to be Risk Oriented - rationalizing conclusions based on previous experience.

"It's never happened before, so there's probably a good explanation."

DON'T BE RISK ORIENTED!
WHO IS YOUR ENEMY?

“To know your Enemy, you must become your Enemy.”
Sun Tzu
School Threats

- Organized Political Terrorists
- The Lone Wolf Assailants
- The Lone Criminal
- Mentally Impaired individual

Outside Threats

- Workplace Violence
- Student Assailant
- Domestic Violence

Inside Threats

- Outside Threats
- Insider Threats
The Lone Wolf

- Working with limited or no network of supporters or collaborators.
- Has the ability to operate off the radar.
- Usually operates close to where he lives.
- Usually does not receive any training from an organization or state. Tactics are self taught.
The Lone Wolf

Newtown CT, Sandy Hook
December 2012

Carlsbad, CA, Kelly Elementary School
October 2010
Internal Threat – Assailant Characteristics

- Suspicious comments
- Confrontational behavior
- Avoiding certain duties
- Keeping to oneself
- Fascination with guns, explosives etc.
- Conflicting allegiances (politics, religion, association)
HOW TO DETECT:
Predictive Profiling

An adversary is anyone that represents a threat to safety and security of Indiana School students, staff or guests.

But how will you know your adversary BEFORE he commits a crime?
Detection

Predictive Profiling
Detection

**Predictive Profiling:**

Assessing actions and/or objects (not people) versus what you know to be normal activities or objects in your environment.

So first, establish what’s normal in terms of what activities happen and what objects you see at your schools.
A good way to start thinking is
If I were a bad guy what would I be trying to achieve if I were doing what this guy is doing?
An Adversary's Method of Operation is the way by which a criminal or an assailant achieves his/her objectives.

The How
KNOW YOUR ADVERSARY

METHODS OF OPERATION

MARKING to Getaway

1. Marking
2. Intelligence Gathering
3. Surveillance
4. Planning
5. Tooling Up
6. Rehearsing / Training
7. Execution
8. Getaway

The Common Denominators
THREAT
MITIGATION
CHALLENGE!!!

Deviation from A Typical Profile

1. Marking
2. Intelligence Gathering
3. Surveillance
4. Planning
5. Tooling Up
6. Rehearsing / Training
7. Execution
8. Getaway

At which stage is the adversary most vulnerable and why?
Deviation from A Typical Profile

- Facing the crowd (not the tracks)
- Fixated on people
- Shirt not tucked in
- Dressed differently
KNOW YOUR ADVERSARY

RECOGNIZING SUSPICION

Behavior which isn’t normal for your environment + Association with a criminal method of operation = SUSPICION
To recognize this inconsistency, you have to be familiar with the norms of your environment!
KNOW YOUR ADVERSARY

RECOGNIZING SUSPICION

Suspicion Indicators = The noticeable elements of the Method of Operation.

Suspicion Indicators (SIS) are the activities or objects that you observe to be out of the ordinary … and

Are also consistent with known Methods of Operation.
Methods of Operation are what they do. Suspicion Indicators are what you see.
Types of Suspicion Indicators

- Story
- Belongings
- Situation
- Appearance
- Behavior
- Documentation
The Adversary will try to stick to his cover.

Cover stories will be full of facts some of which will be true.

A true story will include more personal experiences and personal accounts that describe events that truly occurred.
WHAT THEY DO . . .

METHOD OF OPERATION (MO)

WILL ENGAGE IN SURVEILLANCE AND INTELLIGENCE GATHERING PRIOR TO EXECUTING CRIMINAL ACT

MAY DISGUISE IDENTITY AND POSE AS A GUEST, PARTNER, TENANT, OR CITY OFFICIAL TO GAIN ACCESS TO RESTRICTED AREA OR GET INFORMATION

MIGHT BEFRIEND A SECURITY OFFICER TO LEARN VALUABLE INFORMATION
Please spend time at home (and ask all security personnel to spend time) looking at a school YOU KNOW NOTHING ABOUT – and see how much inside information you can gain from simply sitting at home. Try To build a legitimate cover story with this information.

The do it for your own school are realize how much people can find out about you.
Next realize all these individuals have the same information.
EXAMPLE OF TERRORIST MENTALITY

SYRIA BOMBER: Sebastian River High student a ‘normal kid’

A terrorist doesn’t always look radicalized
AMOS @ INDIANA SCHOOLS

WHAT THEY DO . . .

Each Criminal Act has its own MOs

Bomb Threat
Kidnapping
Mentally Impaired
Terrorism

Active Shooter

Theft of school property

Aggravated Assault

Drug Dealing

Sexual Misconduct

Protesters

Bullying

Stalking

Arson
Predictive Profiling is detection PRIOR to the Act. Now we must DETERMINE if the suspicious individual is a threat or not…. How?

- Overwhelmingly, most suspicious activity would be refuted if individuals were approached and questioned.
- Engagement with a suspicious individual is the best deterrent to future crime.

Detect – **Determine** - Deploy
SECURITY QUESTIONING

Determine

"Purpose of visit?"
Security Questioning puts the adversary on the defense.

The Best Defense is a Good Offense!

It allows you to move from being defensive – the normal role of security – to being offensive.

THE THREE DS
Detect
Determine
Deploy
Security Questioning: Definition

A proactive exchange of questions and answers between a security officer and an individual geared towards detecting, validating or refuting suspicion indicators.

Security questioning allows the officer to assess the person/situation and establish a threat/no threat decision.
One targeted and unexpected question that relates to a critical part of the cover story or the MO is more valuable than a long and unfocused questioning process.
WHY SECURITY QUESTIONING IS SO EFFECTIVE?

A Proactive Measure.

Puts the terrorist/criminal on the defensive.

Incorporates intelligence into security.

Does not cost money.

Mitigates terrorist and criminal activity at the planning stages.

Necessary in order to complete the security process (detect, determine, deploy).
Security Questioning – A Different Approach

<table>
<thead>
<tr>
<th>Security Questioning</th>
<th>Police Questioning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conversation</td>
<td>Interrogation</td>
</tr>
<tr>
<td>Detect intentions</td>
<td>Detect means</td>
</tr>
<tr>
<td>Refutation/Verification</td>
<td>Building a case</td>
</tr>
<tr>
<td>Mitigating the threat</td>
<td>Incrimination</td>
</tr>
<tr>
<td>Cooperative tone</td>
<td>Authoritative tone</td>
</tr>
<tr>
<td>(usually)</td>
<td></td>
</tr>
</tbody>
</table>
Only two options for making a decision in security

Threat

No Threat
Threat is suspicion that was not refuted
SECURITY QUESTIONING DONE RIGHT
Engineering Security Around Predictive Profiling

Deployment
Develop Real and Virtual Security Rings and Push Outward
Avoid Internal Security by Officers unless protected environment is commonly violent.
Security Rings

Protected Environment

Physical Guards

Electronic
Mall entrances extend outward. Security screening is done outside the building.
Harvest Your Data Points!

Bus Drivers
Nurses
Cafeteria Workers

Maintenance and Landscaping
Assistant Coaches
Volunteers
The Red Team

“Practice isn’t the thing you do once you’re good. It’s the thing you do that makes you good.” - Malcolm Gladwell
You accomplish your security objectives by:

being **proactive**, not reactive

remembering **people** always come before property

understanding it’s not observe and report, but observe and . . .

**detect**

**determine**

**deploy**
YOU ACCOMPLISH YOUR SECURITY OBJECTIVES BY:

UNDERSTANDING HOW CRIMINALS THINK AND COMMIT CRIMES:

LEARN THE MO FOR CRIMES THAT ARE POSSIBLE IN YOUR ENVIRONMENT

DETECT THE SUSPICION INDICATORS (SI) FOR THOSE MOs.

DETERMINE HOW SUSPICIOUS ACTIVITY MIGHT FIT INTO THE MARKING TO GETAWAY PROCESS
YOU ACCOMPLISH YOUR SECURITY OBJECTIVES BY:

BEING ALERT, ACTIVE, MOBILE, AND THREAT ORIENTED

PUSHING SECURITY RINGS OUTWARD AND INTRODUCING CONTINGENCIES

ENGAGING SUSPICIOUS INDIVIDUALS WITH A GOOD SECURITY QUESTIONING TECHNIQUE
The Key Question:

What is the most important quality for a guard to have?
Answer:
People tend to be threat oriented and not risk oriented when it comes to things they own or love.
REVIEW

You protect what you care about
1) ESTABLISH WHAT IS NORMAL IN YOUR OPERATING ENVIRONMENT
2) DETECT ANYTHING THAT DEVIATES FROM THAT NORM (SUSPICION INDICATOR)
3) DETERMINE WHAT AMO THE SUSPICION INDICATOR MIGHT BE USED FOR (ADVERSARY METHOD OF OPERATION)
4) ATTEMPT TO REFUTE THE SUSPICION INDICATOR USING SECURITY QUESTIONING WHEN POSSIBLE
5) MAKE A DETERMINATION OF THREAT/NO THREAT
6) DEPLOY AGAINST THE THREAT
The **Proactive** Security Process

**D**etect suspicion
**D**etermine method of operation
**D**eploy against the MO
BREAK – NEXT HOUR……..
THE ADVERSARY WORKSHOP
**PART 1 – BUILDING THE MO**

YOU are the enemy planning an attack against an Indiana School property.

<table>
<thead>
<tr>
<th>Method</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suicide Bombing</td>
<td>Planting a bomb/car bomb</td>
</tr>
<tr>
<td>Stalking/kidnapping</td>
<td>Ramming vehicle at event or school dismissal</td>
</tr>
<tr>
<td>Active Shooter/mass killing</td>
<td></td>
</tr>
<tr>
<td>Arson</td>
<td></td>
</tr>
<tr>
<td>Theft</td>
<td>Planting a bomb/car bomb</td>
</tr>
</tbody>
</table>
PART 1 – BUILDING THE MO

Think like the enemy.

1) Mark the target – what school?
2) Intel gathering – spend several minutes on your phone gaining intel, building a cover
3) Surveillance – when would you do it? How? What is your cover if approached?
4) Planning – what is your course of action – how many people? Lone wolf?
5) Tooling up? What items will you need to do it?
6) Rehearsal? What type of practice will you do to make sure you are successful?
7) Execution – the day of attack what do you do?
8) Get away – how will you cover your crime?
PART TWO – REVERSE HATS

Look at your plan and bullet point what you think would make you suspicious during the marking through get-a-way process.
PART THREE – WHAT ARE YOU GOING TO DO ABOUT IT WITHOUT SPENDING MONEY?

1) You know this is a potential crime against your school
2) You know how the enemy thinks
3) You know what actions you are likely to see and will make you suspicious
4) You know your requests for money to stop this crime with physical deterrents, more man power etc will be slow at best.
5) So what can you do?
PART THREE — WHAT ARE YOU GOING TO DO ABOUT IT WITHOUT SPENDING MONEY?

Some helpful ideas:

1) Share this information with your team/including faculty/staff/parents
2) Teach all community members to think proactively (a slow process but it does work)
3) Encourage security staff to engage EVERYONE (good practice) — a sharp officer constantly greeting and speaking to everyone costs no more money and mitigates threat. Customer Service for the good guy — deterrence for the bad guy.
4) Invite Police and SWAT teams to use your property for training often — you want them familiar with it and build good will.
5) Create Police Rooms — adversary wont know when they will be there — policing without cost and without routine.
THANK YOU!

Peter Crabbe
Chameleon Associates
pcrabbe@chameleonassociates.com
818 713-8848 o 805 402-2584 cell