Presented by the

Supply Chain and Transportation Council

MASS TRANSIT SECURITY

Project Lead, Horace Frederick Hayden

NOTE: *Much of the information in this white paper is drawn from the National Transit Institute's Terrorism Activity Recognition and Response Trainer Manual and its System Security Awareness for Commuter Rail Employees Trainer Manual, and other reports that reflect best practices in mass transit security awareness programs.*

Security awareness programs are effective training tools that help protect organizations from threats. Incorporating the terror threat cycle into staff awareness programs for mass transit and transportation can reduce risk of attacks on the systems and contribute to improved security.

Security Awareness Programs

Security awareness programs are defined as comprehensive training for employees to recognize, react, report, and respond to security and terrorism activities. By improving transit employee's knowledge, skills, and abilities in these areas a transit agency will be better prepared to deal with security issues. Training only select transit employees in security awareness results in gaps and vulnerabilities, leaving agencies susceptible to criminal and terrorist activities.[1]

Terrorism

The United Nations has no defined definition for terrorism worldwide. Identifying the local jurisdictions' definition is important for each transit system. Generally, the use of force to effect change to government or society, including the intimidation of civilian populations or specific portions of the population can be an accepted definition of terrorism.

While the definition of terrorism may change from country to country, the United States Federal Bureau of Investigation (FBI) defines terrorism as the unlawful use of force or violence against persons or property to intimidate or coerce a government or civilian population, or any segment thereof, in furtherance of political or social objectives.

There are three elements that make an event a terrorist act versus a criminal act. The first is that a criminal act must have occurred. (Speech does not make a terrorist act as it is protected by the First Amendment.) The second element is that some change must be the goal of the criminal act. The attack may be symbolic and the target not the actual goal. An attack on a bank for financial gain does not qualify, but

[1] American Public Transportation Association, *Security Awareness Training for Transit Employees*, APTA-SS-SRM-RP-005-12

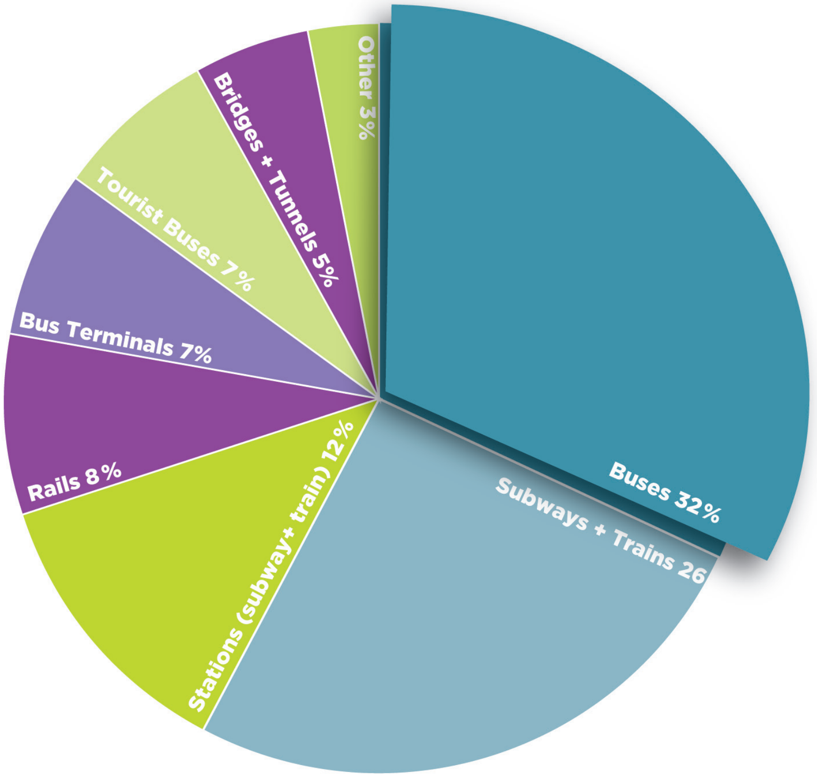
an attack on the bank to change geopolitical policies such as support for a government meets the criteria. The final element is the value of the act. The attack cannot be for financial gain or personal benefit.

What is the attack supposed to change or influence? The value of the attack is the change it creates. The March 2004, Madrid bombings helped influence an election and change a government, pulling Spanish troops from the Iraq war, thus fulfilling the third requirement of the FBI's terrorism definition.

Terror Threat Cycle

The terror threat cycle is a process of target selection, planning, and intelligence gathering, and/or practicing the attack and then the carrying out of the attack. Like most serious crimes, there is a process that can be disrupted and possibly prevent the attack. The threat cycle is like any criminal activity, so the incorporation of the cycle can easily be fit into the security awareness programs of all agencies.

The graph below illustrates the importance of incorporating the terror threat cycle on transportation systems.



International Transit Targets 1920-2000

**Note: Internationally, bus service is the most predominant form of public transportation.*

Source: ***Protecting Public Surface Transportation Against Terrorism and Serious Crime:*** *An Executive Overview, Mineta Transportation Institute, San Jose State University, San Jose, CA; October 2001*

Why Are Transit Systems Attractive Targets?

Transit systems are appealing to terrorist groups for several reasons. The most appealing reasons are:

- **Open and accessible**
- **Move large numbers of people**
- **Symbols of free movement**
- **Vital components of regional and local economies**
- **Often leave vulnerabilities unchecked**

The Effects of Terrorism on Transit

Service disruptions, delays, cancellations, and safety concerns related to terrorist threats and incidents quickly begin to erode the public's confidence in a transit system. An efficient and effective response to these situations is critical to maintaining the economic stability of the transit system and its employees.

The terror threat cycle should be incorporated into security awareness programs for transit employees to understand their security awareness responsibilities. A definition of terrorism and why the threat cycle is important should be included for staff to understand why the transit systems are attractive targets for those wishing to carry out a terror attack—regardless of political or ideological reasons.

Why Attack Transit Systems?

There are five main reasons for attacking transit systems:

1. **Large Number of People.** The greater number of victims the greater the fear generated and more media exposure.
2. **The Open and Accessible Nature of Transit Systems.** For transit systems to be feasible there needs to be easy access. Airports offer too many security layers and often are not options. Transit systems are generally convenient and openly accessible.

3. **The Economic Components of the Transit Systems.** Mass transit systems affect the economy in moving both workers and consumers in the local economy.
4. **Ability to Deliver to Targets.** Most transit systems connect with government financial, and symbolic targets. An attacker can take a bus, ferry, or train to a target rather than drive a vehicle and go through security at the intended target. A train may pass under a historic or symbolic target that is protected at the surface levels. An underground subway system allows for delivery of the device to the target area.
5. **Media Attention.** Any attack using mass transit will draw large media attention and coverage. The group responsible for the attack can get attention for its cause through the media response. The media response allows for the group to demand intimidation and shake confidence in transit systems safety.

Role of Transit Employees in the Security Awareness Program

It is critical for newly-hired employees to complete training on the policies and emergency practices important to their role within the agency. This can help enhance and contribute to the overall safety and security within the agency. However, skills need to be reinforced over time, so annual refreshers along with advanced knowledge in situational exercises should also be included in the awareness programs. Refresher training should include new information based on trends and world events to reflect new threat knowledge.

To stop or disrupt the threat cycle, security awareness of the agency is VITAL. Each phase can be broken down, and ways in which the security awareness program can disrupt the threat cycle should be explored.

In the Intelligence gathering phase, attackers gather as much information as possible prior to an attack. A comprehensive security awareness program can equip staff to recognize, react, report, and respond and ultimately disrupt terrorist or criminal activity by the increased security awareness of the agency. Training staff in security awareness and the importance of keeping information that can be exploited safe can deter intelligence gathering.

While mass transit is an open system with published schedules and ease of access, information that can be exploited such as access points to restricted areas, requirements, and policies should not be shared.

Gathering Intelligence

Gathering intelligence is the process of collecting relevant information for planning and carrying out a terrorist attack. It includes:

- **Seeking security sensitive information**
- **Conducting surveillance**

Intelligence gathering is the process through which terrorists collect information about:

- **Equipment**
- **Ridership**
- **Facilities**
- **Security measures and procedures**
- **Security personnel**
- **Employee routines in and around facilities**

By deterring access to the information needed to plan and carry out an attack this phase of the cycle can be disrupted. Security awareness training for employees can also disrupt this phase by making staff aware of how their routines and practices may be used to plan an attack. Staff should be made aware of information gathering techniques and report any suspicious activity or requests for information about policy and security procedures.

Surveillance

Another form of intelligence gathering is surveillance. Surveillance is recording or monitoring activities. During surveillance, terrorists may try to hide their activities by posing as a customer, contractor, delivery person, or employee. They may also conduct surveillance from a hidden location.

Indicators of surveillance are activities may include a person paying more attention to transit operations or facilities than a normal passenger would. Some specific indicators that someone may be conducting surveillance of your operations, assets, or facilities include individuals who are:

- **Seen multiple times at the same location or at various locations around the system–either on foot or in the same vehicle**
- **Sitting in a parked vehicle, outside a terminal, or along a bus route or rail right-of-way**
- **Waiting or loitering at bus stops or rail stations for extended periods and not boarding**
- **Carrying on long conversations on cell phones and**

not moving

- **Showing an interest in security measures**
- **Drawing or taking pictures in areas not normally of interest**
- **Taking notes or annotating maps**
- **Pacing off or measuring distances**
- **Recording arrival and departure times of buses and trains, as well as employees and passengers**

Things that are of interest to terrorists targeting your agency or adjacent assets are:

- **Employee activity**
- **Customer activity**
- **Operational patterns**
- **Facility access points, procedures, and exits**
- **Storage and maintenance facilities**
- **Communication centers**
- **Critical infrastructure and assets**

Some of the tools terrorists might use during surveillance include:

- **Cameras – video, still, or panoramic**
- **Notebooks or sketch pads**
- **Laptop computers or PDAs diagrams or maps**
- **Binoculars or other vision-enhancing devices GPS devices**

By teaching security awareness to all staff, which includes suspicious activity awareness based on behaviors and circumstance, employees can begin to detect when surveillance activity is taking place. Training should include the indicators of suspicious activity, and whom to report such activity to, and ensuring the proper authorities receive the information. The agency should also be involved in the regional fusion centers of the FBI and other information sharing organizations so knowledge of trends and threat detection is available.

Equipment Gathering

By developing a system to control access, the equipment gathering stage can be deterred. Access control by outside vendors and visitors, and reporting lost access cards, keys, and uniforms need to be in place. Ensure all employees know what to do if agency access cards, keys and/or uniforms are lost or stolen. Replacing locks and shutting down the access cards helps prevent any gathered equipment from being used.

Policies about the access of vendors with or without employee supervision, and the vetting of employees of the vendors through bonding process will help to deny aggressors from gaining access to equipment.

Dry Run

A dry run of a potential attack against a transit system may include:

- **Following routes to double check traffic flow and the timing of traffic lights**
- **Riding buses or trains to verify schedules, employee procedures, and passenger volumes and flow**
- **Carrying or planting “dummy” packages to see if they are noticed**

Security Tests

Terrorists will not want to carry out an attack if they think they will be noticed. Terrorists will test the system to determine:

- **Which security measures are in place and what they entail**
- **How employees react to security threats and minor incidents**
- **How well the agency and its employees enforce policies**
- **How well the agency controls access to its facilities, assets, and secured areas**

Tests of a system’s security can include:

- **Entering a restricted area and appearing lost when approached**
- **Attempting to gain access while claiming a lost or forgotten ID**

- **Asking for security sensitive information**
- **Leaving an unattended empty package or bag in a critical area**
- **Carrying a suspicious package or a concealed weapon**
- **Attempting to leave a package in the mailroom, with a receptionist, or in the maintenance shop**
- **Repetitive false alarms or bomb threats**

Through the development and implementation of policy and procedures about recognizing suspicious items, this phase can be disrupted. Staff should be trained in the indicators of suspicious activity, mail, items, and behavior. Staff should be trained and have the training reinforced that behavior is important and not based on race, religion, or nation of origin.

A Suspicious Package is...

One that matches something described in a threat or has a threatening message attached.

- **An out-of-place bag, box, or abandoned container**
- **An unattended package that is put in an out-of-the-way place such as next to a fueling station, under or behind a vending machine, in or behind trash con tainers, behind restroom fixtures or behind phone booths**

A Lost and Found Package is...

An unattended package that is often left:

- **On or next to a seat in a vehicle or waiting area**
- **Next to a phone booth or vending machine**
- **On or next to a vending machine**
- **In a restroom or on a station platform**

Employee Actions

Repetitive alarms or suspicious items may indicate an attempt to learn staff response and procedures, as well as learning rally points where people will evacuate.

Some indicators of suspicious activity or items include:

- **In an unauthorized area or appears lost**
- **On agency property without a proper ID, uniform, or safety gear**
- **Expressing an unusual level of interest in operations, facilities, personnel or equipment**
- **Pacing, nervous, or jumpy**
- **Acting in a disorderly manner, alarming or disturbing others**
- **Loitering, staring or watching employees, and abandoning a package and quickly leaving an area**
- **Studying or observing operations and activity over time**
- **Taking notes on a clipboard, computer or other electronic device**
- **Taking photos of secured spaces and equipment or areas**
- **Timing and recording operations, deliveries and other activities**
- **Measuring or "pacing-off" distances**
- **Carrying or using surveillance tools such as still and video cameras, binoculars, clipboards, and stop watches**
- **"Testing" employees' reactions to his/her behavior**
- **Observing employee locations, evacuation proce dures, and response activity during false alarms or training exercises**

Infiltration

Terrorists may also attempt to infiltrate the transit agency. They will try to blend in and appear as if they belong, or just secretly access secure areas. Infiltration is:

- **An attempt to gain access to a secure area for the pur pose of sabotage or deploying a device**
- **An attempt to acquire items such as uniforms, ID cards, access control swipe cards, keys, or security sensitive information**

There are a variety of ways in which terrorists can infiltrate a secure area. Some of the infiltration methods are:

- **Changing or tampering with locks**
- **Disabling surveillance equipment such as closed- cir cuit cameras, motion sensors, or other devices**
- **Compromising fences or rarely used gates**

- **Using stolen or forged identification cards, uniforms, keys, or access swipe cards**
- **Impersonating a delivery person or contractor, again using a stolen or makeshift uniform**
- **Using a decoy or distraction, such as a car accident, disturbance, or injury**
- **Vehicles that are following or "shadowing" agency ` vehicles and/or attempting to drive through security gates behind agency or contractor vehicles**

Security awareness training should also include the indicators of suspicious activity and packages along with suspicious persons. Once again, staff should be trained in the indicators as well as the process of reporting the suspicious situation, as well as whom to report it to.

Security staff should also randomly check for any access through maintenance areas, fencing, or transit right of ways to prevent infiltration or staging areas for attacks. A rail overpass or tunnel may be infiltrated allowing an attack on the rail system rather than infiltration to a train, as security may be tighter on rail equipment but not as tight on the access points along the rail corridor.

Operational Phase

Deploying Assets

Immediately before an attack, terrorists must put the final pieces in place. Deploying assets involves placing explosives or other devices that are ready to detonate and staging materials, people, and/or vehicles. This is the last chance anyone will have to alert authorities of the danger, avert the attack, and avoid loss of life. Look for signs of execution.[2]

Table 3

Signs of Terrorist or Criminal Activity Execution

Inappropriate clothing for the season	Repeatedly patting upper body
Exposed wires	Rigid posture with minimal body movement, arms close to sides
Excessive fidgeting, clock watching and area scanning	Appearing to be in disguise
Appearing in a trance	Drastic and sudden change of appearance (shaved body hair, shaved head, increased mass from explosive vest)
Unresponsive, distant, and/or inattentive	

An example of inappropriate clothing can be seen in this photo from *The Daily Telegraph* showing the July 7, 2005, London bombers entering the train system wearing jackets not appropriate for the hot weather. Their backpacks were concealing the detonators for their suicide devices.

The priority during the operational phase of the threat cycle is the protection of life and then properties. Having a trained staff can lead to an agency being able to respond to save as many lives as possible, initializing a continuity plan during the recovery phase, then recovering from the threat and establishing the trust of the transit agency patrons and the public.

A relationship with first responders and their familiarity with the transit system is vital. The more familiar first responders are with the system, the better prepared they will be for responding

[2] American Public Transportation Association, *Identifying Suspicious Behavior in Mass Transit*, APTA SS-SRM-RP-009-09

to attacks or emergencies on the transit system and transit facilities. Having first responders train on equipment and at facilities will increase effective response to incidents.

The incorporation of the threat cycle into agency security awareness training and public awareness messages can be vital to the prevention of an attack. In an article entitled, *Troubling Trends Emerge in Terrorism and Attacks on Surface Transportation*, Brian Michael Jenkins, director of Mineta Transportation Institute's National Transportation Safety and Security Center and a counter-terrorism expert, concluded:

> *We also see that vigilance works. From 2005-2015, 14 percent of all bomb attacks were stopped primarily because intelligence and law enforcement, security officials and citizens, passengers, and transit crew and staff were alert. Of these stopped attacks, passengers, citizens and employees can be credited with detecting at least 25 percent. Another 24 percent can be credited to those managing or carrying out security functions—be they military, police, or security or intelligence officials.*
>
> *Note that in the remaining 43 percent of the cases, it is not clear who found the device, but it is most likely vigilant intelligence and security officials, and then citizens, employees or passengers. This underscores not only the importance of "see something, say something" programs, but also of the investments in good, sensible security.*

By incorporating the terror threat cycle into the security awareness program for agency staff, it may be possible to deter the threat. But training must be robust and proactively reinforced on a consistent basis; it cannot be a one-off event that allows security awareness to erode and only become heightened in response to a crisis.

Bibliography

NTI Terrorism Activity Recognition and Response Trainer Manual

NTI Security Awareness Training for Front Line Commuter Rail Staff Trainer Manual

APTA SS-RP-SRM-007-12 | Recognizing and Responding to Unattended Packages, Objects and Baggage, American Public Transportation Association, Washington, DC: Approved December 2012 APTA Security Risk Management Work Group

APTA SS-SRM-RP-009-09 | Identifying Suspicious Behavior in Mass Transit American Public Transportation Association, Washington, DC: Approved October 15, 2009 APTA Security Risk Management Working Group

Security Awareness Training for Transit Employees, APTA-SS-SRM-RP-005-12, American Public Transportation Association, Washington, DC

Random Counterterrorism Measures on Transit Systems APTA SS-SRM-RP-006-11, American Public Transportation Association, Washington, DC: Published March 31, 2011, APTA Security Risk Management Working Group

Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview, Mineta Transportation Institute, San Jose State University, San Jose, CA, and October 2001

Troubling Trends Emerge in Terrorism and Attacks on Surface Transportation, Mineta Transportation Institute, San Jose State University, San Jose, CA

The information presented in this document is the work of the author(s). The views and opinions expressed therein, or the positions advocated, may not necessarily reflect the views, opinions, or positions of ASIS or any ASIS member other than the author(s).

ASIS disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance on this document. In issuing and making this document available, ASIS is not undertaking to render professional or other services for or on behalf of any person or entity. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstance.

ASIS INTERNATIONAL
Advancing Security Worldwide®

1625 Prince Street
Alexandria, VA 22314
+1.703.519.6200
asisonline.org