ATTENTION—SURFACE TRANSPORTATION STAKEHOLDERS

(U) In light of recent world events and the upcoming holiday weekend, the Transportation Security Administration (TSA) is providing this Security Awareness Message to our industry partners in an effort to encourage continued vigilance and timely reporting of suspicious incidents observed by their employees and customers during the Thanksgiving holiday period, November 24–29, 2015. The Thanksgiving holiday weekend is associated with increased travel during which crowds often take public transportation to large celebrations and mass gatherings. The Department of Homeland Security (DHS) has not issued a National Terrorism Advisory System (http://www.dhs.gov/alerts) alert.

(U//FOUO) The recent attacks in Paris—although not targeting transportation—displayed similar tactics to those previously used against surface transportation. According to TSA’s Office of Intelligence and Analysis, terrorist tactics against transportation have remained fairly consistent, with the use of improvised explosive devices (IEDs), arson, firearms, and knives as the most prevalent attack methods.

(U//FOUO) In addition, insider threat continues to be a concern for surface transportation. The attached FBI document, The Insider Threat, provides helpful guidance to employers for identifying and addressing this issue. Extremist groups or radicalized individuals could increase their knowledge of transportation systems and capabilities by recruiting or collaborating with industry insiders or individuals with in-depth knowledge of transportation systems.

(U//FOUO) TSA recommends that transportation operators review their security and emergency response plans to ensure they are up-to-date. TSA encourages transportation stakeholders to continue their employee security training programs and public awareness campaigns such as “If You See Something, Say Something.” TSA encourages security personnel to ensure employees are complying with their company’s policy on responding to active shooter incidents. The attached DHS publication, Active Shooter, How to Respond, addresses this topic.

(U//FOUO) For mass transit and passenger rail operators, Operation RAILSAFE is scheduled for November 25, 2015. Law enforcement agencies in the areas where Amtrak operates are encouraged to increase security presence for railroad stations and the railroad rights-of-way. Additional information can be found at http://police.amtrak.com/operation-railsafe. If eligible under program guidance, transit and passenger rail systems that have received Transit Security Grants may reprogram funds to cover operation RAILSAFE activities, including overtime expenses.

Sonya T. Proctor
Director, Surface Division
Office of Security Policy and Industry Engagement
Transportation Security Administration
Department of Homeland Security
Recent Insider Theft Cases

Michael Mitchell became disgruntled and was fired from his job due to poor performance. He kept numerous computer files with his employer’s trade secrets; he entered into a consulting agreement with a rival Korean company and gave them the stolen trade secrets. In March 2010, he was sentenced to 18 months in prison and ordered to pay his former employer over $187,000.

Xue Huang was employed by two different US companies. He admitted that from 2007 to 2010 he delivered stolen trade secrets from both companies to individuals in Germany and China. The stolen materials were used to conduct unauthorized research to benefit Chinese universities. Huang also pursued steps to develop and produce the trade secrets in China. The aggregated loss from both companies was between $7 and $20 million. Huang pleaded guilty to charges of economic espionage and theft of trade secrets, and was sentenced in December 2011 to eight months in prison and three years supervised release.

Yuan Li, a former research chemist with a global pharmaceutical company, pleaded guilty in January 2012 to stealing her employer’s trade secrets and making them available for sale through Abby Pharmatech, Inc. Li was a 50% partner in Abby. Between October 2008 and June 2011 Li accessed her employer’s internal databases, downloaded information to her personal home computer, and made them available for sale through Abby. She was sentenced to 18 months in prison.

Elliot Doxer sent an e-mail to the Israeli Consulate stating that he was willing to provide information from his employer that might help Israel. An undercover FBI agent posing as an Israeli intelligence officer spoke to Doxer and established a ‘dead drop’ where the two could exchange information. For the next 11 months, Doxer visited the dead drop at least 62 times. Doxer provided customer and employee lists, contract information, and other trade secrets. He pleaded guilty to one count of foreign economic espionage and was sentenced in December 2011 to six months in prison, six months home confinement, and fined $25,000.

Greg Chung spied for China from 1979-2006. Chung stole trade secrets about the space shuttle, the Delta IV rocket and the C-17 military cargo jet for the benefit of the Chinese government. Chung’s motive was to “contribute to the Motherland.” He stole hundreds of thousands of documents from his employer. He traveled to China under the guise of giving lectures while secretly meeting with Chinese agents. He also used Mak (below) to transfer information back to China. In February 2010 he was sentenced to over 15 years in prison.

Chi Mak admitted that he was sent to the United States in 1978 in order to obtain employment in the defense industry with the goal of stealing US defense secrets, which he did for over 20 years. He passed information on quiet electric propulsion systems for US submarines, details on the Aegis radar system, and information on stealth ships being developed by the US Navy. The Chinese government tasked Mak to acquire information on other technologies. Mak recruited family members to encrypt and covertly courier information back to China. In May 2007, Mak was convicted of conspiracy, failing to register as an agent of a foreign government, and other violations. He was sentenced to over 24 years in prison.

This brochure serves as an introduction for managers and security personnel on how to detect an insider threat and provides tips on how to safeguard your company’s trade secrets.

The Insider Threat

Deterring an Insider Spy

Disgruntled
Working odd hours
Unexplained affluence
Unreported foreign travel

An introduction to detecting and deterring an insider spy

Report theft of trade secrets to your local FBI office or submit a tip online: tips.fbi.gov

U.S. Department of Justice
Federal Bureau of Investigation
PROTECT YOUR INTELLECTUAL PROPERTY

Theft of intellectual property is an increasing threat to organizations, and can go unnoticed for months or even years. There are increased incidents of employees taking proprietary information when they believe they will be, or are, searching for a new job. Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights to protect innovation and ensure that egregious or persistent intellectual property violations do not merely become a standard cost of doing business. A domestic or foreign business competitor or foreign government intent on illegally acquiring a company’s proprietary information and trade secrets may wish to place a spy into a company in order to gain access to non-public information. Alternatively, they may try to recruit an existing employee to do the same thing.

PERSONAL FACTORS

There are a variety of motives or personal situations that may increase the likelihood someone will spy against their employer:

- Greed or Financial Need: A belief that money can fix anything. Excessive debt or overwhelming expenses.
- Anger/Revenge: Disgruntlement to the point of wanting to retaliate against the organization.
- Problems at work: A lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, a pending layoff.
- Ideology/Identification: A desire to help the “underdog” or a particular cause.
- Divided Loyalty: Allegiance to another person or company, or to a country besides the United States.
- Adventure/Thrift: Want to add excitement to their life, intrigued by the clandestine activity, “James Bond Wannabe.”
- Vulnerability to blackmail: Extra-marital affairs, gambling, fraud.

Behavioral Indicators

- Some behaviors may be a clue that an employee is spying and/or methodically stealing from the organization:
  - Without need or authorization, takes proprietary or other material home via websites, thumb drives, computer disks, or e-mail.
  - Inappropriately seeks or obtains proprietary or classified information on subjects not related to their work duties.
  - Interest in matters outside the scope of their duties, particularly those of interest to foreign entities or business competitors.
  - Unnecessarily copies material, especially if it is proprietary or classified.
  - Remotely accesses the computer network while on vacation, sick leave, or at other odd times.
  - Disregards company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.
  - Works odd hours without authorization; notable enthusiasm for overtime work, weekend work, or unusual schedules when clandestine activities could be more easily conducted.
  - Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or unreported overseas travel.
  - Inappropriately seeks or obtains proprietary or classified information.
  - Shows unusual interest in the personal lives of co-workers; asks inappropriate questions regarding finances or relationships.
  - Concern that they are being investigated; leaves traps to detect searches of their work area or home; searches for listening devices or cameras.

YOU CAN MAKE A DIFFERENCE

Organizations need to do their part to deter intellectual property theft:

- Educate and regularly train employees on security or other protocols.
- Ensure that proprietary information is adequately, if not robustly, protected.
- Use appropriate screening processes to select new employees.
- Provide non-threatening, convenient ways for employees to report suspicions.
- Routinely monitor computer networks for suspicious activity.
- Ensure security (to include computer network security) personnel have the tools they need.

GET ASSISTANCE

Being aware of potential issues, exercising good judgment, and conducting discrete inquiries will help you ascertain if there is a spy in your midst. However, if you believe one of your employees is a spy or is stealing company trade secrets, do not alert the person to the fact that he/she is under suspicion, but seek assistance from trained counterintelligence experts—such as the FBI. The FBI has the tools and experience to identify and mitigate such threats. If asked to investigate, the FBI will minimize the disruption to your business, and safeguard your privacy and your data. Where necessary, the FBI will seek protective orders to preserve trade secrets and business confidentiality. The FBI is committed to maintaining the confidentiality and competitive position of US companies. The FBI will also provide security and counterintelligence training or awareness seminars for you and your employees upon request.
ACTIVE SHOOTER
HOW TO RESPOND

October 2008
Emergency Numbers

<table>
<thead>
<tr>
<th>Emergency Services:</th>
<th>9-1-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Emergency Information Line:</td>
<td></td>
</tr>
<tr>
<td>Local Police Department:</td>
<td></td>
</tr>
<tr>
<td>Local Fire Department:</td>
<td></td>
</tr>
<tr>
<td>Local Hospital:</td>
<td></td>
</tr>
<tr>
<td>Local FBI Field Office:</td>
<td></td>
</tr>
<tr>
<td>Facility Security:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Facility Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td>__________________</td>
</tr>
<tr>
<td>__________________</td>
</tr>
<tr>
<td>__________________</td>
</tr>
<tr>
<td>__________________</td>
</tr>
<tr>
<td>__________________</td>
</tr>
</tbody>
</table>

Floor: _______ Suite/Room: ______________
Office #: _______________ Ext. ____________
PROFILE OF AN ACTIVE SHOOTER

An Active Shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearms(s) and there is no pattern or method to their selection of victims.

Active shooter situations are unpredictable and evolve quickly. Typically, the immediate deployment of law enforcement is required to stop the shooting and mitigate harm to victims.

Because active shooter situations are often over within 10 to 15 minutes, before law enforcement arrives on the scene, individuals must be prepared both mentally and physically to deal with an active shooter situation.

Good practices for coping with an active shooter situation

• Be aware of your environment and any possible dangers

• Take note of the two nearest exits in any facility you visit

• If you are in an office, stay there and secure the door

• If you are in a hallway, get into a room and secure the door

• As a last resort, attempt to take the active shooter down. When the shooter is at close range and you cannot flee, your chance of survival is much greater if you try to incapacitate him/her.

CALL 911
WHEN IT IS SAFE TO DO SO!
HOW TO RESPOND WHEN AN ACTIVE SHOOTER IS IN YOUR VICINITY

Quickly determine the most reasonable way to protect your own life. Remember that customers and clients are likely to follow the lead of employees and managers during an active shooter situation.

1. Evacuate
   If there is an accessible escape path, attempt to evacuate the premises. Be sure to:
   • Have an escape route and plan in mind
   • Evacuate regardless of whether others agree to follow
   • Leave your belongings behind
   • Help others escape, if possible
   • Prevent individuals from entering an area where the active shooter may be
   • Keep your hands visible
   • Follow the instructions of any police officers
   • Do not attempt to move wounded people
   • Call 911 when you are safe

2. Hide out
   If evacuation is not possible, find a place to hide where the active shooter is less likely to find you.

   Your hiding place should:
   • Be out of the active shooter’s view
   • Provide protection if shots are fired in your direction (i.e., an office with a closed and locked door)
   • Not trap you or restrict your options for movement

   To prevent an active shooter from entering your hiding place:
   • Lock the door
   • Blockade the door with heavy furniture
If the active shooter is nearby:
• Lock the door
• Silence your cell phone and/or pager
• Turn off any source of noise (i.e., radios, televisions)
• Hide behind large items (i.e., cabinets, desks)
• Remain quiet

If evacuation and hiding out are not possible:
• Remain calm
• Dial 911, if possible, to alert police to the active shooter’s location
• If you cannot speak, leave the line open and allow the dispatcher to listen

3. Take action against the active shooter
   As a last resort, and only when your life is in imminent danger, attempt to disrupt and/or incapacitate the active shooter by:
   • Acting as aggressively as possible against him/her
   • Throwing items and improvising weapons
   • Yelling
   • Committing to your actions
HOW TO RESPOND WHEN LAW ENFORCEMENT ARRIVES

Law enforcement’s purpose is to stop the active shooter as soon as possible. Officers will proceed directly to the area in which the last shots were heard.

- Officers usually arrive in teams of four (4)
- Officers may wear regular patrol uniforms or external bulletproof vests, Kevlar helmets, and other tactical equipment
- Officers may be armed with rifles, shotguns, handguns
- Officers may use pepper spray or tear gas to control the situation
- Officers may shout commands, and may push individuals to the ground for their safety

How to react when law enforcement arrives:

- Remain calm, and follow officers’ instructions
- Put down any items in your hands (i.e., bags, jackets)
- Immediately raise hands and spread fingers
- Keep hands visible at all times
- Avoid making quick movements toward officers such as holding on to them for safety
- Avoid pointing, screaming and/or yelling
- Do not stop to ask officers for help or direction when evacuating, just proceed in the direction from which officers are entering the premises

Information to provide to law enforcement or 911 operator:

- Location of the active shooter
- Number of shooters, if more than one
- Physical description of shooter/s
- Number and type of weapons held by the shooter/s
- Number of potential victims at the location

The first officers to arrive to the scene will not stop to help injured persons. Expect rescue teams comprised of additional officers and emergency medical personnel to follow the initial officers. These rescue teams will treat and remove any injured persons. They may also call upon able-bodied individuals to assist in removing the wounded from the premises.

Once you have reached a safe location or an assembly point, you will likely be held in that area by law enforcement until the situation is under control, and all witnesses have been identified and questioned. Do not leave until law enforcement authorities have instructed you to do so.
TRAINING YOUR STAFF FOR AN ACTIVE SHOOTER SITUATION

To best prepare your staff for an active shooter situation, create an Emergency Action Plan (EAP), and conduct training exercises. Together, the EAP and training exercises will prepare your staff to effectively respond and help minimize loss of life.

Components of an Emergency Action Plan (EAP)

Create the EAP with input from several stakeholders including your human resources department, your training department (if one exists), facility owners / operators, your property manager, and local law enforcement and/or emergency responders. An effective EAP includes:

- A preferred method for reporting fires and other emergencies
- An evacuation policy and procedure
- Emergency escape procedures and route assignments (i.e., floor plans, safe areas)
- Contact information for, and responsibilities of individuals to be contacted under the EAP
- Information concerning local area hospitals (i.e., name, telephone number, and distance from your location)
- An emergency notification system to alert various parties of an emergency including:
  - Individuals at remote locations within premises
  - Local law enforcement
  - Local area hospitals

Components of Training Exercises

The most effective way to train your staff to respond to an active shooter situation is to conduct mock active shooter training exercises. Local law enforcement is an excellent resource in designing training exercises.

- Recognizing the sound of gunshots
- Reacting quickly when gunshots are heard and/or when a shooting is witnessed:
  - Evacuating the area
  - Hiding out
  - Acting against the shooter as a last resort
- Calling 911
- Reacting when law enforcement arrives
- Adopting the survival mind set during times of crisis
Additional Ways to Prepare For and Prevent an Active Shooter Situation

- **Preparedness**
  - Ensure that your facility has at least two evacuation routes
  - Post evacuation routes in conspicuous locations throughout your facility
  - Include local law enforcement and first responders during training exercises
  - Encourage law enforcement, emergency responders, SWAT teams, K-9 teams, and bomb squads to train for an active shooter scenario at your location

- **Prevention**
  - Foster a respectful workplace
  - Be aware of indications of workplace violence and take remedial actions accordingly

For more information on creating an EAP contact the U.S. Department of Labor, Occupational Health and Safety Administration, www.osha.gov.
PREPARING FOR AND MANAGING AN ACTIVE SHOOTER SITUATION

Your human resources department and facility managers should engage in planning for emergency situations, including an active shooter scenario. Planning for emergency situations will help to mitigate the likelihood of an incident by establishing the mechanisms described below.

Human Resources’ Responsibilities

- Conduct effective employee screening and background checks
- Create a system for reporting signs of potentially violent behavior
- Make counseling services available to employees
- Develop an EAP which includes policies and procedures for dealing with an active shooter situation, as well as after action planning

Facility Manager Responsibilities

- Institute access controls (i.e., keys, security system pass codes)
- Distribute critical items to appropriate managers / employees, including:
  - Floor plans
  - Keys
  - Facility personnel lists and telephone numbers
- Coordinate with the facility’s security department to ensure the physical security of the location
- Assemble crisis kits containing:
  - radios
  - floor plans
  - staff roster, and staff emergency contact numbers
  - first aid kits
  - flashlights
- Place removable floor plans near entrances and exits for emergency responders
- Activate the emergency notification system when an emergency situation occurs
Reactions of Managers During an Active Shooter Situation

Employees and customers are likely to follow the lead of managers during an emergency situation. During an emergency, managers should be familiar with their EAP, and be prepared to:

- Take immediate action
- Remain calm
- Lock and barricade doors
- Evacuate staff and customers via a preplanned evacuation route to a safe area

Assisting Individuals with Special Needs and/or Disabilities

- Ensure that EAPs, evacuation instructions and any other relevant information address to individuals with special needs and/or disabilities
- Your building should be handicap-accessible, in compliance with ADA requirements.
RECOGNIZING POTENTIAL WORKPLACE VIOLENCE

An active shooter in your workplace may be a current or former employee, or an acquaintance of a current or former employee. Intuitive managers and coworkers may notice characteristics of potentially violent behavior in an employee. Alert your Human Resources Department if you believe an employee or coworker exhibits potentially violent behavior.

Indicators of Potential Violence by an Employee

Employees typically do not just “snap,” but display indicators of potentially violent behavior over time. If these behaviors are recognized, they can often be managed and treated. Potentially violent behaviors by an employee may include one or more of the following (this list of behaviors is not comprehensive, nor is it intended as a mechanism for diagnosing violent tendencies):

- Increased use of alcohol and/or illegal drugs
- Unexplained increase in absenteeism; vague physical complaints
- Noticeable decrease in attention to appearance and hygiene
- Depression / withdrawal
- Resistance and overreaction to changes in policy and procedures
- Repeated violations of company policies
- Increased severe mood swings
- Noticeably unstable, emotional responses
- Explosive outbursts of anger or rage without provocation
- Suicidal; comments about “putting things in order”
- Behavior which is suspect of paranoia, (“everybody is against me”)
- Increasingly talks of problems at home
- Escalation of domestic problems into the workplace; talk of severe financial problems
- Talk of previous incidents of violence
- Empathy with individuals committing violence
- Increase in unsolicited comments about firearms, other dangerous weapons and violent crimes
MANAGING THE CONSEQUENCES OF AN ACTIVE SHOOTER SITUATION

After the active shooter has been incapacitated and is no longer a threat, human resources and/or management should engage in post-event assessments and activities, including:

• An accounting of all individuals at a designated assembly point to determine who, if anyone, is missing and potentially injured
• Determining a method for notifying families of individuals affected by the active shooter, including notification of any casualties
• Assessing the psychological state of individuals at the scene, and referring them to health care specialists accordingly
• Identifying and filling any critical personnel or operational gaps left in the organization as a result of the active shooter

LESSONS LEARNED

To facilitate effective planning for future emergencies, it is important to analyze the recent active shooter situation and create an after action report. The analysis and reporting contained in this report is useful for:

• Serving as documentation for response activities
• Identifying successes and failures that occurred during the event
• Providing an analysis of the effectiveness of the existing EAP
• Describing and defining a plan for making improvements to the EAP

References

Safety Guidelines for Armed Subjects, Active Shooter Situations, Indiana University Police Department, April 2007.

Safety Tips & Guidelines Regarding Potential “Active Shooter” Incidents Occurring on Campus, University of California Police.

Shots Fired, When Lightning Strikes (DVD), Center for Personal Protection and Safety, 2007.

