Theme Park Emergencies—How Do These Businesses Prepare?

Steve K. Brown, Echelon Security
Matthew Frowert, Tyco Integrated Security
Cynthia L. Roth, Ergonomic Technologies Corp.
Seminar Objectives

➢ Learn about emergency situations facing major theme parks and places of assembly and their loss control measures

➢ Explore potential emergencies through a team-based activity and follow-up discussion

➢ Effectively reach similar types of clients by incorporating response plans and underwriting best practices into your work
Our Panelists

• Steve K. Brown, Echelon Security

• Matthew Frowert, Tyco Integrated Security

• Cynthia L. Roth, Ergonomic Technologies Corp.
Situations

- Active-shooter preparedness
- Insider threats/terrorist mitigation
- Other hazards (food defense, weather, chemical spills, pandemics)
Framework

- Prevention
- Response
- Recovery
- Loss control/underwriting
Active-Shooter Preparedness (10 min)
RUN. HIDE. FIGHT.®
Recognizing and Preventing Workplace Violence (10 min)

Overview

• Mindset of Awareness
  – Workplace Violence
    • Definition
    • Myths
  – Workplace Violence Spectrum
  – Behaviors of Concern
• Commitment to Action
  – Flash Point
  – Formula
  – Action Point
  – Common Inhibitors to Reporting
  – Available Reporting Options
Defining Workplace Violence

• Behaviors that can cause:
  – Personal injury
  – Damage property
  – Impede the normal course of work
  – Cause workers/managers/customers to fear for their safety
Defining Workplace Violence

• Include:
  – Threats
  – Harassment
  – Intimidation
  – Bullying
  – Assault
  – Stalking
  – Domestic Violence
  – Workplace Homicides

• Homicides merely represent the “tip of the iceberg”
Defining Workplace Violence

• Four broad categories:
  – **TYPE 1**: Violent acts by criminals who have no other connection with the workplace, but enter to commit robbery or another crime
  – **TYPE 2**: Violence directed at employees by customers, clients, patients, students, or others to whom service is provided
  – **TYPE 3**: Violence against coworkers, supervisors, or managers by a present or former employee
  – **TYPE 4**: Violence committed in the workplace by someone who doesn’t work there, but has a personal relationship with an employee—an abusive spouse or domestic partner
Myths

• “Out of the blue…”

• “Just snapped…”

• “If left alone, events will resolve themselves…”

• “Employees can’t do anything to stop it…”

• “It couldn’t happen here…”
Workplace Violence Spectrum

- Spectrum
  - May not be a linear progression
  - To the right are acts of overt violence causing physical injury and/or death
  - Moving to the left are psychological and emotional violence
  - To the far left are Behaviors of Concern
    - No profile of a workplace violence offender
From: 
Sent: Thu 12/24/2009 11:29 PM 
To: 
Subject: Wishes for Christmas and New Year

My wishes for you, bunch of crooks: a bullet into your head or many years in jail!

It's exactly what you deserve for being a crook and forming or being part of criminal conspiracy.

You'll be punished, don't worry. This will happen very soon!
Behaviors of Concern (FBI Bulletin)

**CHANGES IN BEHAVIOR**
- Poor personal hygiene
- An obsession with guns
- A Romantic or sexual obsession

**CHANGES IN ATTITUDE**
- Lower tolerance for work stress
- Dissatisfaction with how a conflict/grievance was resolved

**DEMONSTRATIONS OF VIOLENCE**
- Verbal threats
- Physical assaults
- Use of weapons in physical assaults
Petersburg man given 38 years in shotgun slaying at Chester workplace

By Mark Bowes

Published: December 9, 2009

Though no clear motive was presented at trial, evidence suggested that Clagon was having a relationship with Wiley's wife, Delilah, who also worked at Pre Con, and he killed Wiley to eliminate his romantic rival. Police said the two had been romantically involved.

Wiley, a former Pre Con employee who had recently quit to resume a truck-driving career, had arrived that morning to pick up his wife from work. The shooting occurred as scores of employees were leaving or arriving during the plant's 7 a.m. shift change.
Triggering Event

- A reprimand, termination, or layoff
- Financial troubles, a separation, a divorce, or a death
- A loss, whether real or perceived, in someone’s personal or professional life
- “Injustice collectors”
  - Will not forget or forgive those wrongs or the people he believes are responsible
Indicators of Violence

- Does the suspect have a grievance?
- Does the suspect suffer from a mental disorder?
- Does the suspect have an unwanted romantic interest in a coworker? What is the degree of intimacy?
- Is the suspect not accepting of criticism?
- Is the suspect delusional or displaying psychotic behavior?
- Has the suspect made inappropriate contact with the victim? (letters, phone, unannounced visits)
- Has the suspect identified with a notorious figure, stalker, or assassin?
- Does the suspect have the ability to circumvent security? (employee with pass ID, relationships)
- Does the suspect have a desire for revenge?
- Has the suspect conveyed threats of violence?
- Has the suspect researched the victim?
- Has the suspect created a journal or diary?
- Has the suspect made repeated approaches to the victim or victim’s coworkers?
- Has the suspect exhibited random travel/targeted travel?
- Has the suspect obtained or have a fascination with weapons?
Inhibitors of Violence

- Does the suspect convey a fear of consequences?
- Does the suspect own a home?
- Does the suspect have viable monetary investments?
- Does the suspect enjoy positive contact with relatives on a regular basis?
- Is the suspect happily married?
- Does the suspect practice a religion denouncing violence?
- Does the suspect enjoy career employment?
- Does the suspect enjoy a positive reputation with coworkers, relatives, or community?
- Is the suspect in good health?
- Does the suspect enjoy a sense of dignity?
- Does the suspect have a normal self-esteem?
- Does the suspect have minor children?
Flash Point

• The point on the Workplace Violence Spectrum where actual violence occurs
  – Exact location can vary from one situation and individual to another
• Different actions in the work environment can trigger or cause a Flash Point
  – May be the result of non-work related situations
    • Domestic Violence
    • Other Personal Issues
Action Point

• Recognition that violence may be an outcome; respond with an appropriate action

• Important to exercise caution when setting an early Action Point
  – Important not to delay reporting a threat
    • Better chance of containing a potentially violent event
    • Minimize harmful consequences and prevent a recurrence
  – Stress tolerance and coping skills are highly subjective
Common Inhibitors to Reporting

- Lack of awareness
  - Not trained to recognize Behaviors of Concern
- Psychological barriers
  - Busybody or snitch
- Fear of retaliation
- Believe it is someone else’s responsibility
  - If a flash point is triggered, it will affect you
Workplace Violence

• Very few organizations will ever experience disturbed employees engaging in shooting sprees that wound and kill multiple victims

• A far greater number will face other forms of workplace violence
  – Threatening behavior and violent events that are less spectacular and less deadly
  – Nonetheless, significantly damage the well-being of an organization and place employees in harm’s way
Summary

• Work from a mindset of awareness
  – Don’t ignore Behaviors of Concern
  • Will not go away and can escalate
  – Learn how to recognize and diffuse potentially violent situations
  – Alert supervisors to concerns
  – Report all incidents
Applications to Underwriting

- What types of businesses do you write coverage for that might benefit from having a formal program to prepare for workplace violence threats?

- How would you go about underwriting a risk with the potential for workplace violence threats in mind?
  - What questions would you ask?
  - How would you evaluate the effectiveness of the program?
Did you know?

- Average cost per incident is $412,000.
- Average loss per industry is $15 million over 10 years.
- In several instances, damages reached over $1 billion.

FBI Articles

// Naval Espionage: Stopping a Dangerous Insider Threat
// Insider Threat: Soldier Receives 16-Year Sentence for Attempted Espionage
Insider Threats Overview

• Research
• Definitions
• Motivations and behavioral indicators
• Developing your program and marshaling resources
The Insider Threat

• There is not one "type" of insider threat.
  ➢ Threat is to an organization’s critical assets:
    • People
    • Information
    • Technology
    • Facilities
  ➢ Based on the motive(s) of the insider.
    • Impact is on confidentiality, availability and integrity.

• There is not one solution for addressing the insider threat.
  ➢ Technology alone may not be the most effective way to prevent and/or detect an incident perpetrated by a trusted insider.
Motivation for a Program

- To ensure the responsible sharing and safeguarding of classified national security information on computer networks

- To ensure protection of and appropriate access to intellectual property and other critical assets, systems and data, including
  - People
  - Business processes
  - Technology
  - Facilities
  - Information

- To be prepared and ready to handle such events in a consistent, timely and quality manner including understanding
  - Who to involve
  - Who has authority
  - Whom to coordinate with
  - Whom to report to
  - What actions to take
  - What improvements to make

Source: Executive Order 13587, quoted in GCN (http://s.tt/1ai6l)
What Is a Malicious Insider Threat?

- Current or former employee, contractor or other business partner who:
  - Has or had authorized access to an organization’s network, system or data and
  - Intentionally exceeded or misused that access in a manner that
  - Negatively affected the confidentiality, integrity or availability of the organization’s information or information systems.
What Is an Unintentional Insider Threat?

- Current or former employee, contractor or other business partner who:
  
  - Has or had authorized access to an organization’s network, system or data and who, through
  
  - His or her action/inaction without malicious intent
  
  - Caused harm or substantially increased the probability of future serious harm to the confidentiality, integrity or availability of the organization’s information or information systems.
Violence, Sabotage, and Espionage: Predispositions, Motivations, Personal, Stress Red Flags

- M.I.C.E.: money, ideology, compromise, ego
- Disgruntlement: anger and revenge
- Divided loyalty—allegiance issues
- Alcohol and other substance abuse
- Gambling
- Financial complications
- Mental health issues
- Adverse personnel actions
- Security violations
- Criminal history
- Victimized or perceived so
- Personality issues (narcissistic, psychopathic)
Research Findings

Saboteurs and spies had common personal predispositions that contributed to their risk of committing malicious acts.

In most cases, stressful events, including organizational sanctions, contributed to the likelihood of physical violence, insider IT sabotage and espionage.

Concerning behaviors were often observable before violent acts and during IT sabotage and espionage.
• Technical actions by malicious insiders could have alerted the organization to planned or ongoing malicious acts.

• In many cases, organizations ignored or failed to detect concerning behaviors/rule violations.

• Lack of physical and electronic access controls facilitated violent acts, IT sabotage and espionage.
Do You Detect a RAT?

- Routine activity theory (RAT) is one of the main theories of “environmental criminology.”

- The theory states that a crime occurs when the following three elements come together in any given space and time:
  1. The presence of a motivated offender
  2. The absence of capable guardians that could intervene
  3. An accessible target

Developed by Marcus Felson and Lawrence E. Cohen
Corporate Espionage and Sabotage Prevention requires a *RAT* in action:

- Capable Guardianship
- Demotivated Offenders
- Protecting the Crown Jewels
It All Begins With…Access

- At the gates—screening
- Inside the perimeter
- Expectations of privacy
- Nondisclosure agreements
- Monitoring
- Social media and engineering
- The hostile foreign threat and recruitment
“Actionables”

• Develop risk-indicator instruments.

• Look at case-study information in relation to concerning behaviors, stressful events and personal predispositions across sabotage and espionage events.

• Look at technical data not related to insider threat—false positive detection.

• Evaluate available tools, policies and methods for auditing behaviors and technical actions indicative of IT sabotage and espionage.
“Actionables” (Continued)

• Assess the relationship between policy enforcement for policy and rule violations and the risk of insider IT sabotage and espionage.

• Analyze current access control policies and practices for the purpose of identifying and evaluating options to mitigate insider-threat risk.

• Develop a “risk indicator” instrument to acquire better information on the base rates and baseline level of risk factors in proportion to actual insider activity.
Separate the “Target” From the “Impact” From the “Actor”

**Target**
- Critical Assets
  - People
  - Technology
  - Information
  - Facilities

**Impact**
- Confidentiality
- Availability
- Integrity

**Actor(s)**
- Employees
  - Current
  - Former
- Contractors
- Subcontractors
- Suppliers
- Trusted Business Partners

**WHAT**
**HOW**
**WHO**
### Summary of Insider Incidents

<table>
<thead>
<tr>
<th>Current or former employee?</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Former</td>
<td>Former</td>
<td>Current</td>
<td>Current (within 30 days of resignation)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of position</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical (e.g., sys admins, programmers or DBAs)</td>
<td>Non-technical (e.g., data entry, customer service) or their managers</td>
<td>Technical (e.g., scientists, programmers, engineers) or sales</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Gender</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>Male</td>
<td>Fairly equally split between male and female</td>
<td>Male</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Target</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network, systems or data</td>
<td>PII or customer information</td>
<td>IP (trade secrets) or customer info</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access used</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized</td>
<td>Unauthorized</td>
<td>Authorized</td>
<td>Authorized</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>When</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outside normal working hours</td>
<td>During normal working hours</td>
<td>During normal working hours</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Where</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote access</td>
<td>At work</td>
<td>At work</td>
<td>At work</td>
</tr>
</tbody>
</table>
The Three Pillars of a Robust Strategy

- Accurately Trust
- Right-Size Permissions
- Effective Monitoring

No Insider Threat
Some Takeaways …

**Establish a See Something, Say Something, Do Something Culture**

<table>
<thead>
<tr>
<th>Behavioral science and empirical research are your friend:</th>
<th>The past informs the present; don’t buy the “secret sauce.” Base your protection standards on lessons learned from available cases studies and apply them to your organization’s culture.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The role of criminology:</td>
<td>Be the capable guardian. Demotivate the threatener. Protect the “crown jewels.” Strive for excellence in each category.</td>
</tr>
<tr>
<td>Develop a multidisciplinary threat-mitigation team:</td>
<td>IA, Security, CI, HR, OGC. Liaison with law enforcement. Develop threat response options.</td>
</tr>
<tr>
<td>Know the signs of emerging illicit conduct:</td>
<td>Evolving anomalies in employee personal predispositions, stressors and concerning behaviors.</td>
</tr>
<tr>
<td>Conceive of mitigation strategies:</td>
<td>Before a potential threat escalates into disastrous consequences. Plan to intervene!</td>
</tr>
<tr>
<td>Establish and set cyber and brick-and-mortar-world insider-threat detection methods, techniques, and standards at points of access and exfiltration.</td>
<td></td>
</tr>
</tbody>
</table>
Common Sense Guide to Mitigating Insider Threats

http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm
# Best Practices for Insider-Threat Mitigation

<table>
<thead>
<tr>
<th>Consider threats from insiders and business partners in enterprise-wide risk assessments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearly document and consistently enforce policies and controls.</td>
</tr>
<tr>
<td>Incorporate insider threat awareness into periodic security training for all employees.</td>
</tr>
<tr>
<td>Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.</td>
</tr>
<tr>
<td>Anticipate and manage negative issues in the work environment.</td>
</tr>
<tr>
<td>Know your assets.</td>
</tr>
<tr>
<td>Implement strict password and account-management policies and practices.</td>
</tr>
<tr>
<td>Enforce separation of duties and least privilege.</td>
</tr>
<tr>
<td>Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.</td>
</tr>
<tr>
<td>Institute stringent access controls and monitoring policies on privileged users.</td>
</tr>
<tr>
<td>Institutionalize system change controls.</td>
</tr>
<tr>
<td>Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.</td>
</tr>
<tr>
<td>Monitor and control remote access from all endpoints, including mobile devices.</td>
</tr>
<tr>
<td>Develop a comprehensive employee termination procedure.</td>
</tr>
<tr>
<td>Implement secure backup and recovery processes.</td>
</tr>
<tr>
<td>Develop a formalized insider-threat program.</td>
</tr>
<tr>
<td>Establish a baseline of normal network-device behavior.</td>
</tr>
<tr>
<td>Be especially vigilant regarding social media.</td>
</tr>
<tr>
<td>Close the doors to unauthorized data exfiltration.</td>
</tr>
</tbody>
</table>
Building an Insider-Threat Program
Insider-Threat Program Participants (Notional)

- **Insider Threat Team Program Manager**
  - VP / CIO
    - Assistant Director
  - CISO
    - Assistant Director
- **President & CEO**
  - Director
- **VP / CFO**
  - Assistant Director
- **VP / COO**
  - Assistant Director
- **VP / Chief Legal Counsel**
  - General Counsel
  - Legal Counsel

The diagram illustrates the roles and responsibilities within an Insider Threat Program, highlighting key participants such as the Insiders Threat Team Program Manager, VP / CIO, CISO, VP / CFO, VP / COO, VP / Chief Legal Counsel, Director of IT, Information Assurance, HR Director, Physical Security Director, and Legal Counsel.

**Insider Threat Core Team**

- **Data Owners**
- **Legal**
- **Human Resources**
- **Information Technology**
- **SOC/C SIRT**
- **Software Engineers**
- **Union Representative**
- **Physical Security**
- **Facilities Operations**
- **Non-management workers**
- **Internal Audit**
- **Quality Assurance**
- **Contracting Group or COTR**
- **Partners Suppliers and Contractors**

*Note: Text below the separator in each box notes the federal government’s equivalent position*
CERT Resources

- Insider Threat Center website (http://www.cert.org/insider_threat/)


- Insider-threat workshops

- Insider-threat assessments

- New controls from CERT Insider Threat Lab

- Insider-threat exercises

- *The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)* (SEI Series in Software Engineering) by Dawn M. Cappelli, Andrew P. Moore and Randall F. Trzeciak
Ask the Experts: Contact Information

Stephen R. Band, Ph.D.
behavioralintelligencespecialist@starpower.net
http://www.drstephenrband.com/

Randall F. Trzeciak
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-7040
rft@cert.org
http://www.cert.org/insider_threat/

Catch their webinar in its entirety:
http://e.tycois.com/Insider_Threats_07242014
Applications to Underwriting

- What types of businesses do you write coverage for that might benefit from having a formal program to prepare for insider threats?

- How would you go about underwriting a risk with the potential for insider threats in mind?
  - What questions would you ask?
  - How would evaluate the effectiveness of the program?
The Importance of Communication

- *Any* situation reaching a critical phase, a decisive moment or crucial time

- *Any* unplanned event, occurrence or sequence of events yielding specifically undesirable consequences
Crisis

- **Crisis public relations**: An intensive, concentrated form of public relations, usually based on an explicit plan.

  - It uses specific techniques for generating two-way communication.

  - Successful crisis public relations enable organizations to relay information to the public during and after any drastic event until they are back to normal operations.
• **Internal communication**: A *two-way relationship within an organization, enabling an exchange of information between employees.*

  ➢ Includes a rehearsed plan, immediate management, long-term management and image restoration.
  ➢ Remember those old-fashioned fire drills? They are not so old fashioned: get a plan; get specifics; make it unplanned; and practice, practice, practice. Don’t take anything for granted.
  ➢ Communication is major.
  ➢ A crisis can occur anywhere at anytime.
• **Defensive avoidance**: A term describing irrational managerial decision making during a crisis caused by panic and/or disbelief.

  - These snap decisions usually occur at the onset of a crisis.
  
  - According to Dieudonne ten Berge, author of *The First 24 Hours*, **defensive avoidance** is a major cause of poor short-term decisions during a crisis.
Communication

• Any company must develop policies and procedures.
• These must be clearly communicated to everyone in the company.
• HR must add them to new-employee packages and discuss upon hiring.
• These must be updated on a regular basis as things change, such as:
  ➢ Growth
  ➢ Physical changes
• Must have a plan in place that allows strangers (park attendees) to understand where, why and when to go, in multilanguage explanations from employees.

• Management may not be able to prevent the crisis, but they are responsible for solid safety actions to prevent more injuries.
Communication

• Additional Communications:
  – Emergency Responders
  – Public Health
  – Local Law Enforcement
  – Fire
  – Government Agencies as Appropriate
Communication

• Do we need housing assistance?
• Do we need clothing and food assistance?
• Infant and children needs
• Do we ask the Red Cross for assistance?
• FEMA
Modeling the Social Amplification of Risk Following a Terrorist Strike: Methodological Challenges

William J. Burns
Cal State San Marcos, bburns@csusm.edu

• Following a terrorist attack, emergency response systems, information and communication channels, and social support organizations are likely to interact in a nonlinear fashion to produce a wide range of physical, social and economic impacts.

• Developed hypothetical threat scenarios that principally compare accidents with terrorism across two damage mechanisms: explosions and infectious diseases.
• Number of casualties, type of victim and whether negligence or suicide was involved were manipulated as well.

• The setting is a local theme park.
Videos

• **Actionable Food Defense**
  - Interviews with Kellogg and MillerCoors leaders discussing use of video to aid security auditing to help with food defense.

• **Natural Disaster Simulator**
  - Prepare. Respond. Recover.
Thank You

Cindy Roth
CEO
Ergonomic Technologies Corp

www.ergoworld.com
croth@ergoworld.com
Applications to Underwriting

• What types of businesses do you write coverage for that might benefit from having a formal communication program in place?

• How would you go about underwriting a risk’s communication strategy in the event of a crisis situation?
  ✓ What questions would you ask?
  ✓ How would evaluate the effectiveness of the program?
Simulation #1—Active Shooter
Simulation #2—Loss Control Presentation
Group Discussion/Take Aways
Panelist Contact Information

Matthew Frowert, Tyco Integrated Security
mfrowert@tyco.com

Steve Brown, Echelon Security
sbrown@echelonsecurity.com

Cindy Roth, Ergonomic Technologies Corp.
croth@viscardicenter.org