



RISK AND LIABILITY

Presented by: Jessie Beaudoin

DEFINING THE THREAT

- The kinds of threats or risks affecting the assets to be protected
- The probability of those threats becoming actual loss events
- The effect on the assets or on the enterprise if the loss occurs

THREATS TO GAMING/HOTELS

- Cheating at Gambling
- Advantage Play
- Promotional Scams and Fraud
- Internal Theft and Fraud
- Liability
- Workplace Violence/Sexual Harassment
- Theft or Harm to Guests
- Gaming Violation

THREAT RECOGNITION

- Patrol and/or monitor assigned area.
- Observe for the indicators/tells of threats associated with the area being monitored.
- This means that you must know your tells.
- Upon recognition of threat immediately establish tri-shot coverage to identify those involved and obtain evidence.

THREAT EVALUATION

- Determine the nature of the threat: criminal, employee misconduct, advantage play, policy/procedure violation etc.
- Determine the probability of the threat occurring and/or the effect/loss that will result if the threat occurs or continues to occur.
- Decide if the threat warrants immediate response or should be delayed for future response, or no response at all. In other words: stay and handle, file for later, or move on.

THREAT EVALUATION EXAMPLES

- Possible Dealer/Agent: Stay and handle for as long as it takes to prove or disprove.
- Slot Floor-person and player seem to know each other: File for later
- \$10 flat wagers by player: Move on

THREAT RECOGNITION AND EVALUATION

- Threat recognition and evaluation is the most critical skill in Surveillance. The ability to recognize threats and non-threats allows you to move quickly through your patrol area by eliminating observation of time wasting non-threats or events thus, isolating the critical threats that may affect our property, guests or employees.

THREAT PRIORITIZATION

- There will be many occasions when you detect a potential threat and while you are attempting to evaluate, another event occurs. This is a normal situation in an active surveillance operation.
- If you can't hand off one of the events to another investigator you must handle both. This is because you don't know which one, at this point, will result in the most damage.

THREAT PRIORITIZATION

- You, as an investigator, must determine which event to address immediately and which one to address when the first one is completed.
- Your ability to handle more than one event at a time directly impacts the protection of our guests and the company.

THREAT PRIORITIZATION

- In most cases, selection of which event to monitor is easy. For example, observing a high action game as opposed to a theft in progress is a simple choice: protect the company from the sure loss of assets by responding to the theft. The high action game will be there when you're done or will end with or without you. Video review can be conducted to ensure the game was not cheated or taken advantage of, if necessary.

THREAT PRIORITIZATION

- Or: lets change the situation around: If the high action play consists of a refused name player, playing minimum to maximum bets for no apparent rhyme or reason, and is already ahead of us thousands of dollars, the amount of time you can spend on a small theft should be limited. However, as a rule of thumb, it is important that you attack the threat where the company stands to lose the most.

THREAT PRIORITIZATION

- Investigators will normally have to prioritize in the table games area.
- During a busy shift, you may be counting down one game, and two more calls reporting play and/or requesting an evaluation.
- In the event that you must handle each call you should perform the following:

THREAT PRIORITIZATION

- Immediately check and display each game reported. Establish coverage with at least one camera.
- Determine which game poses the most immediate and/or largest threat. Usually this means the game with the largest wagers. Establish Tri-Shot coverage.
- Once you've identified the primary threat, evaluate it, determine if it is a threat, resolve the threat or move to the next threat in line and perform the same procedure until you have cleared each game.

THREAT RESPONSE

- When a threat is detected that is where you should be and what you should be focused on regardless of the amount of money involved or whether the situation involves a guest or an employee.
- The only time you must prioritize is when multiple incidents occur at the same time.

THREAT RESPONSE

- Follow chain of command and report incident. Follow instructions.
- Or: Follow established standard operating procedures as detailed in your manual.
- Do not hesitate to ask or request assistance if necessary. Utilize every resource that is available to you to resolve the threat.

THREAT ANALYSIS

- You can and should identify what you should be looking for!
- The days of catching someone putting money in their pocket are over!
- If you are waiting for something to happen, its too late!

THREAT ANALYSIS

- Regularly gather intelligence to plan your operations and to direct your staff :
 - Win/Loss Reports (all games)
 - Stiff Report/Games Statistics
 - Exception Reports
 - Food and Beverage Cost of Sale
 - Crime Reports/Trends
 - Employees!

IDENTIFY THE RISKS

- Understand the Organization
 - People: (employees, guests, vendors, bad guys)
 - Property: (assets, cash, games, high-theft items, “goodwill” or reputation)
 - Information: (Trade secrets, customer lists, employee and guest information, marketing plans)

SPECIFIC LOSS/RISK EVENTS AND VULNERABILITIES

- What types of events or incidents could occur based on history of previous events?
- What types of events or incidents (crimes) are common to the industry?
- Recent developments or trends
- Don't forget non-criminal events
 - Natural disasters
 - Labor disputes

ESTABLISH THE PROBABILITY OF LOSS/RISKS AND FREQUENCY OF EVENTS

- Probability: Likelihood that an event will occur
- The degree of probability will affect the determination of the appropriate solution to be applied to potential risk exposure
 - Distract and grab
 - Advantage Player
 - Player Club Fraud
 - Shooting

FREQUENCY OF EVENTS

- How often does an exposure exist per event type?
 - Natural disaster
 - Shooting
 - Advantage Player
 - Cheating at Gaming
 - Employee Theft
 - Distract and Grab

DETERMINE THE IMPACT OF THE EVENT

- Direct Cost
 - Financial loss
 - Insurance premiums increase
 - Deductable Expense
 - Lost business
- Indirect Cost
 - Negative media coverage
 - Loss of reputation
 - Shareholder/employee dissatisfaction

DEVELOP OPTIONS TO MITIGATE

- What can you apply to mitigate the event should it occur?
 - Security measures (patrols, audits, tripwires, safes, controls, etc.)
 - Insurance
 - Accept risk as cost of doing business

STUDY THE FEASIBILITY OF OPTIONS

While financial cost is often a factor, also consider that a security strategy may affect the operation of the business.

Must find a balance between a security strategy and operations.

PERFORM A COST/BENEFIT ANALYSIS

- Consider cost of strategy against the impact of the loss
- \$100,000 security measure vs. \$5,000 loss?

THREAT/RISK PRIORITIES

- Internal Theft and Fraud
- Cheating at Gaming
- Advantage Play
- Slip/Falls
- Criminal Liability
- Theft by Computer
- Sports Book
- Purchasing Fraud
- Player Club and Promotions
- Collusion
- Marker fraud
- TITO Theft/Fraud
- Player Rating fraud



QUESTIONS

