Risk Management in the Hospitality Industry:
Know When to Hold ‘Em and
Know When to Fold ‘Em

Presented by:
Helaine S. Weissman, CPA, CHAE, Partner, PBMares
Todd Swisher, CPA, CGMA, Partner, PBMares

Topics
• Risk and Risk Management
• Types of Risks
• Battling Risks – Strategic Planning
• Conclusion
Risk and Risk Management

• What is Risk?
  – Something happening that may have an impact on the achievement of objectives.

Risk and Risk Management

• What is Risk Management?
  – A corporate and systematic process for assessing the impact of risks in a cost-effective way
  – Dynamic
    • Current risks may disappear
    • New risks may surge
Risk and Risk Management

– Deals with controlling your exposure to loss –
Applying common sense in a consistent and deliberate fashion

Risk and Risk Management

– An important aspect of our lives
  • Exposed to risk daily - at work and at home
  • Often manage it subconsciously
Risk Management Process

1. Identify the risk/threat
2. Assessment of potential loss
3. Probability of occurrence
4. Controls already in place
5. Other alternatives available to eliminate or reduce identified risk/threat
Risk Management Process

6. Insurance coverage needed
7. Management philosophy
8. Cost/benefit analysis

What Threats?

- Threats to being successful in business
- Adverse effects on Objectives
  - Golf
  - Tennis
  - Banquets
  - Capital Projects
  - Swimming Pool
  - Guest/Member Security
  - Occupancy
What Threats?

Establishing Objectives =>
Identify possible events that would affect =>
Managing/Making Decisions

Types of Risk

• External Environment
• Internal Environment
• Every Entity is unique!
Considerations

• Geographic: Denver vs. Miami vs. Hawaii (Snow vs. Hurricane vs. Volcano)
• Entity Type
• Population: Young? Unisex? Seniors?
• Niche

Types of Risks

“We want someone who’s willing to take risks.”
Weather Risk

Financial Risk
Operational Risk

Cyber Risk
Workplace Environment
Types of Risks

• Approach
  – Objective-Oriented Risk Assessment
  – Entity-wide objectives and Entity’s divisions objectives

Examples of Types of Risks

• Decision-making Risk (Board’s decisions)
• Compliance Risk: Federal regulation, state regulation
• Reputation Risk: Society expectations/perceptions, environmental, etc.
• Foresight Risk: Horizon scanning – Future new issues and their impact
• Employee Turnover Risk: Key employee – over-reliance
### Assessing the Risks

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Low Risk</th>
<th>Medium Risk</th>
<th>High Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Likely</td>
<td></td>
<td>Medium Risk</td>
<td>High Risk</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Low Risk</td>
<td>Medium Risk</td>
<td>High Risk</td>
</tr>
<tr>
<td>Highly Unlikely</td>
<td>Insignificant Risk</td>
<td>Low Risk</td>
<td>Medium Risk</td>
</tr>
<tr>
<td></td>
<td>Slightly Harmful</td>
<td>Harmful</td>
<td>Extremely Harmful</td>
</tr>
</tbody>
</table>

### Managing the Risks

- **Avoid**
- **Reduce**
- **Accept**
- **Transfer**
Operations

• Control over usage of pesticides, fertilizers, water quality and quantity, mowing. Safety trained employees?
• Construction projects - a source of accidents
• Waste management and recycling

More Operations

• OSHA policies
  – Personal protective equipment provided?
  – Used when required?
• Repetitive-motion problems are common in turf maintenance
More Operations

• Precautions to avoid injuries in odd positions while doing the same task for long periods (standing mats)

Worker’s Compensation

• Review past claims
  – Consistent claims
  – Employee training
• Independent contractors
  – True contractors?
  – Own insurance policies
Sports
Might be more engaging to use photos instead of words

Susan Miller, 9/14/2018
Vehicles

• Hotel Shuttles
  – Employee(s) driving vehicles in public places with current licenses?
  – Any policy to track expiration dates or other changes in employee’s licenses?

• Golf carts = enormous liabilities
  – Increase use of golf carts instead of caddies
  – More golf carts = more accidents
  – Are problematic carts put out-of-service until repair?
  – Control on who operates
  – Intoxication
Weather Emergencies, Natural Disasters

- Does entity have a written emergency response guideline?
- Defibrillators for heart emergencies?
- Fire safety training program for employees and evacuation plans for guests?
- Lightening (or other weather) notification
More Weather

• Cautioning members about poisonous plants, snakes, alligators, etc.? (Evidence of awareness reduces liability awards.)
• Development of a disaster plans?

Financial

• Cash
• Internal controls
• Access to property
• Bonding of employees
• Volunteers with access to money
• Approval route for cash transport
Cybersecurity

- Cyberspace
- Cyber Attack
- Cybersecurity

The Rise of Personally Identifiable Information (PII)

- Hackers now focused on obtaining PII
- Attacks on entities with PII have increased
- Hospitality entities have lots of PII
Cyber Stats

Breach Incidents by Industry

Cyber Stats

Data Breaches by Type
Cyber Stats

Data Breaches by Source

<table>
<thead>
<tr>
<th>Source</th>
<th>2017</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious Outsider</td>
<td>1269</td>
<td>1336</td>
</tr>
<tr>
<td>Accidental Loss</td>
<td>326</td>
<td>393</td>
</tr>
<tr>
<td>Malicious Insider</td>
<td>164</td>
<td>179</td>
</tr>
<tr>
<td>Hacktivist</td>
<td>4</td>
<td>49</td>
</tr>
<tr>
<td>State Sponsored</td>
<td>1</td>
<td>20</td>
</tr>
<tr>
<td>Unknown</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

Cyber Stats

Top Threat Actions – Accommodation Industry

- RAM Scrapper
- Use of Stolen...
- C2
- Use of...
- Spyware/Keylo...
- Brute Force
- Backdoor
- Phishing
- Export Data
- Possession...

Series 1
2017 Trends

- Identity theft leads the way
- Poor security practices
- Spear-phishing
- Ransomware attacks continue to rise

2017 Trends - Continued

Top Threat Actions – Accommodation Industry
Cyber Breaches

• Two types of breaches
  – Infrastructure – not a matter of if, but when
  – Information
• Attacks are on the rise and more sophisticated

Be Prepared

• Remember what the Buddha said: “Pain is inevitable, suffering is optional.”
• An information breach can be prevented with the right control environment (monitoring, detection, training, application controls)
Be Prepared

• Information breaches can cause irreparable damage to an organization
• 60% of small businesses shut down within 6 months of a breach
  – Mainly because of inadequate Incident Response Plan (IRP)

Why Cybersecurity?

• There is no real way to measure (quantify) ROI for cybersecurity until a breach occurs.
• How do we measure what we’ve spent in terms of protecting the organization?
• Peach of mind
Direct Costs of a Data Breach

- Forensics and Recovery: $12,000 to $100,000+
- Breach Notification (per individual): $0.50 to $5
- Credit Monitoring (per individual): $10 to $30
- Crisis Communications: $10,000+
- Legal Fees: $5,000+
- Security Updates: $15,000

Data Breach Costs – The Unquantifiable

- Loss of business operations
- Loss of reputation
- Fines and penalties (government or private compliance agency)
- Future oversight and scrutiny
- Potential ransom payment or extortion
I’m Not Worried...I’ve Got Insurance!

• Is it the right coverage?
• Is it enough?
• As more claims are filed, insurance companies are looking for ways to avoid paying claims
• Weak IT controls = Claim could be denied/ limited

Types of Coverage

• Website Phishing
• Extortion
• Breach Notification
• Business Interruption
• Breach Liability
• Breach Expense
• Data Restoration
How to Head Off an Attack

• Cyber Risk Assessment
• Vulnerability Scans (Internal and External)
• Incident Response Planning
• Employee Awareness Training

How do we reduce risk?

• Establish Controls
• Evaluate cost of replacement
• Training
• Liquor control
• Transfer of risk
  – Contractors
  – Insurance
Define Procedures

• Members and guest filing claim
• Board involvement
• Risk Management committee
• Disaster plan
• Legal counsel
• Understand coverage and cost

Common Questions to Consider
Conclusion

“Common sense always speaks too late. Common sense is the guy who tells you you ought to have had your brakes relined last week before you smashed a front end this week. Common sense is the Monday morning quarterback who could have won the ball game if he had been on the team. But he never is. He’s high up in the stands with a flask on his hip. Common sense is the little man in a grey suit who never makes a mistake in addition. But it’s always somebody else’s money he’s adding up.”

Raymond Chandler (Philip Marlowe, Playback, 1958)

Contact

R. Todd Swisher, CPA, CGMA
Partner, Hospitality Industry Team Leader
(804) 323-0022
tswisher@pbmares.com

Helaine S. Weissman, CPA, CHAE
Partner
(703) 385-8577
hweissman@pbmares.com