Spring 5-2019

Risky Business: A Comparative Analysis of Risk Instruments of Sports Security Arenas

Antonia Peterson
University of Southern Mississippi

The University of Southern Mississippi

Risky Business: A Comparative Analysis of Risk Instruments of Sports Security Arenas

by

Antonia Peterson

A Thesis
Submitted to the Honors College of
The University of Southern Mississippi
in Partial Fulfillment
of the Requirements for the Degree of
Bachelor of Science
in the Department of Criminal Justice,
Forensic Science, and Security

May 2019

Approved by:

_____

Joshua B. Hill, Ph.D., Thesis Adviser
Assistant Professor of Criminal Justice

_____

Lisa Nored, Ph.D., Director
School of Criminal Justice, Forensic Science, and Security

_____

Ellen Weinauer, Ph.D., Dean
Honors College

Abstract

Risk assessments in the sports security domain are generally accepted as objective reports with a small margin of subjective information included. The researcher interviewed 10 risk professionals in the sports security industry to evaluate and compare the handling of objective information such as statistical data and historical reports to expert judgment. Interviews were examined using a grounded theory methodology with the Atlas T.I. software program to create overarching themes and a theory of the roles of objective and subjective information within security discourse. Findings pointed to a heavy reliance on expert opinion in comparison to data reports. A moderate amount of subjectivity is beneficial for decision-making because the evaluator can draw conclusions that either support or reject previous notions based on their own judgements (Park, Peacey, Munafo, 2014). Using an acceptable amount of subjectivity allows the evaluator to consider the information provided by other evaluators and weigh the quality of that information to formulate their own conclusions based on both the knowledge provided and their own ideas (Park, Peacey, Munafo, 2014). The risk assessment process takes into account a larger degree of subjectivity than what is deemed ideal by Park, Peacey, and Munafo (2014). By doing so, sports evaluators are more likely to generate false hypotheses and misappropriate risks and mitigation tactics.

Keywords: risk assessment, grounded theory, subjectivity, objectivity, expert opinion, mitigation

Dedication

I would like to dedicate this thesis to my parents, Todd and LaDona Peterson, and my sister, Kaylei Peterson, who have provided me with constant encouragement and love throughout this entire process. Thank you for everything you do, not just today, but every day. I love you.

Acknowledgements

Completion of this thesis would not have been possible without the guidance and support from my thesis advisor, Dr. Joshua Hill. With his mentorship, I have learned valuable lessons regarding the research process and applicability of Criminal Justice. I would not have been able to complete this thesis without him.

I would also like to extend my gratitude to the participants who were involved in my research endeavors. I appreciate every one of you for setting aside time in your busy schedules to discuss your risk assessment practices with me and make this research possible.

Finally, I would like to thank my friends, family, and the Honors College for all the help and encouragement they have provided, not only throughout this process, but also during my four years at USM. A special thank you to Randall Dias, Olivia Shelton, Zack Hempfleng, and my parents for proofreading material for me and being part of the best support system I could ever ask for.

Table of Contents

List of Tables

List of Illustrations

List of Abbreviations

DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
GAR	Green Amber Red
ISO	International Organization for Standardization
NCS4	National Center for Spectator Sports Safety and Security
RSAT	Risk Self-Assessment Tool
SAFETY Act	Support Anti-Terrorism by Fostering Effective Technology Act
TTX	Tabletop Exercise

Chapter 1: Introduction

The attacks that occurred September 11, 2001 on the World Trade Center and Pentagon showed the nation just how vulnerable organizations and their respective venues are to damage and destruction. As a response to 9/11, the security industry began strengthening and expanding the measures taken to provide protection and safety to individuals, changing the security atmosphere in the United States forever (Hall et al., 2012). In 2005, the Department of Homeland Security released a report that identified sport stadiums as soft targets for terrorist activity (Miller, Veltri, & Gillentine, 2008). As a response to the 9/11 attacks and the DHS report, sporting and special event organizations acknowledged and took steps to develop improved risk identification and response measures. Although the United States' sporting and special event venues began striving to advance security protocols shortly after 9/11, threats to large structures such as sporting arenas were prevalent before then both nationally and internationally. In regard to crowd management alone, there have been several reports of serious injury made within the past fifty years. Incidents include the Hillsborough Stadium Disaster in which 96 spectators were killed after a surge of soccer fans rushed through an open emergency exit during the FA Cup semi-final game on April 15, 1989 and the Rhode Island Fire in West Warwick, Rhode Island where a fire broke out during a Great White concert resulting in the death of 100 people and injured over 250 in under five minutes (NCS4, 2018). Post 9/11, events such as the 2002 FBI alert where Al-Qaeda's *Manual of Afghan Jihad* pointed to U.S. college football stadiums as a prospective target for terrorism. The 2005 University of Oklahoma suicide bomber who prematurely detonated a bomb outside an 84,000-seat stadium, and 2006 NFL dirty bomb threat demonstrate that the dangers of

terrorism remain persistent concerns of sporting and special event locations (Hall et al., 2012). The higher the participation at such events, the higher the risk involved; therefore, it is imperative to develop sound policies and procedures to ensure the safety of participants. To do so, organizations utilize risk assessment and management strategies. These methods are meant to identify, analyze, and evaluate risks unique to the event and venue.

It is evident that society as a whole has become increasingly interested in risk and protection measures over the course of the past few decades. This awareness and hyper-vigilance supports Ulrich Beck's (1992) theory about living in a risk society. The risk society thesis holds that the development of new technologies and industrialization has manifested an increase in risk which effects the economy, security, environment, and politics (Mythen & Walklate, 2005). As a result, society has grown more and more conscious of danger and developed a relatively strong sense of fear. This mindfulness, in turn, sparks a need for risk management as a means to avoid experiencing loss (Ericson & Haggerty, 1997). Sporting and special event organization operators attempt to achieve this through a form of risk discourse by defining the vulnerabilities existing at their venues and developing methods to deal with those identified (Ericson & Haggerty, 1997). There are three main types of risks that sporting and special event operators investigate: mission, asset, and security risks. Mission risks include anything that hinder the organization from achieving its goals and objectives. Asset risks encompasses anything that poses a threat to physical property, and security risks relate to everything that can cause potential harm to individuals and informational data (Hall et al., 2012).

When discussing the process in which professionals in the field assess threats, the term "risk" and its meaning are extremely important. A risk is defined by the International Organization for Standardization (2009) as an effect of uncertainty on an organization's goals or objectives. Based on this definition, an expressed risk is dependent on the objectives set forth by a venue. As a result, characterizations of risk vary slightly between organizations. This disparity is partly due to the difference between contexts for individual organizations (ISO, 2009). One must first understand the context in which risk is defined for a particular venue before an assessment is conducted. By establishing the context, the intentions of the organization, environment, stakeholders, and diversity of risk criteria are identified by the evaluators (ISO, 2009). To classify these factors, both the external and internal context must be reviewed. In addition to considering other contextual factors, the perceptions, values, and relationships with stakeholders are examined on the internal and external levels (ISO, 2009). Internal and external stakeholders' perceptions of risk and specific values can shift the venue's objectives based on how much influence they may have at that particular location.

To identify potential threats and minimize the probability of negative occurrences, organizations take part in risk management processes. Risk management and managing risk are two relatively separate entities that complement one another to satisfy the objectives of the organization (ISO, 2009). The risk management framework only works if the organization enforces the framework in its entirety and all related principles. According to the International Organization for Standardization (2009) guidelines, the risk management process should hold a key role in all organizational processes and reflect the best available information in a systematic and structured fashion. Decision

makers become more informed about the nature of risk in relation to their organization or venue based on the results reported during the risk management process. These results allow decision-makers to make educated judgments as well as prioritize and determine actions, inactions, and possible alternatives (ISO, 2009).

One of the main aspects within the risk management process is the risk assessment. Risk assessments are aimed at determining the level of risk within a venue and providing a report that will aid decision-makers' conclusion to take an action in an effort to mitigate risks. These reports examine the venue's current security model and focus its attention on areas of vulnerability that may need to be strengthened in the near future (Hall et al., 2012). Organizations use risk assessment reports as a means for justifying the implementation of particular countermeasures and increasing security awareness (Hall et al., 2012). Assessments use a combination of both information and knowledge to reach a conclusion (Ericson & Haggerty, 1997). While information includes documents such as news articles, statistics, and legislation, knowledge encompasses interpretations of context, conceptualization, and relatedness (Ericson & Haggerty, 1997). Some risk assessments today are conducted with a mixed method approach, using both expert opinion and scientific or logical data such as statistics and past reporting while other risk assessments utilize one or the other.

In order for the risk process and security to be effective, society must be able to trust the organization and the manner in which the organization strives to assess and mitigate risk. Security in this sense refers to the method in which organizations choose to manage risk and enforce safety policies (Ericson & Haggerty, 1997). Successful securities are dependent on the balance of trust and acceptable risk developed by the

organization (Ericson & Haggerty, 1997). While risks are subject to change based on social, cultural, and political factors, trust is built on a foundation of faith and intangibility where society may not directly observe the assessment and mitigation of risks but trusts that risk professionals are tending to them as best as possible (Ericson & Haggerty, 1997). Organizations strive for a strong balance between trust and acceptable risk through risk management and assessment frameworks to lessen the probability of negative events that may occur. Security operators implement mitigation tactics such as barriers, camera systems, and metal detectors as a means to minimize the likelihood of threats occurring at their facilities. As the probability of negative events decreases, the probability of positive events should increase. As a result, society's trust in the organization to maintain a respectable level of security would inevitably increase. Risks and their interpretations are essentially subject to adaptation based on the political or cultural climate (Ericson & Haggerty, 1997). Perception of risk changes from person to person; therefore, decisions made during the risk process may be partially based on an individual's perception of risk or some level of bias. What one organization may define as a moderate risk, another organization may define as a high risk. One person's perception of risk can influence other evaluators to adopt similar viewpoints about the same topic which can lead to possible false hypotheses and misevaluations of risk based on an organization's subjective definition of risk. (Park, Peacey, Munafò, 2014).

Data collection for risk assessments include, but are not limited to, security audits, site visits, and interviews with personnel. Data obtained is expected to characterize the facility by describing the physical aspects of the venue, identify unfavorable events, and identify critical assets (Hall et al., 2012). While information encompasses documents

such as reports, statistical data, news, legislation, and facts, knowledge refers to the interpretation of information by observing the context, relevance, and conceptualization of collected data (Ericson & Haggerty, 1997). Information contains objective data that are based on the factual existence of incidences. Knowledge is largely subjective because it's central focus is on the understandings and experiences of the evaluator.

While risk assessments utilize either expert opinion, formulated data, or a mixture of both, there is one question that remains in regard to this process. How do individual perceptions of risk shape the assessment and management process? In this study, risk processes and data sources of large sports security arenas were examined to determine the degree of objectivity versus subjectivity inherent in their risk management processes. To do so, interviews with risk and security professionals were collected and analyzed to better understand the relationship between the two in the risk process. Additionally, findings were applied to the risk society thesis proposed by Ulrich Beck (1992) and examined for implications.

Chapter 2: Literature Review

Introduction

This thesis examines the relationship between subjective and objective information and their implications within the risk decision-making process for large sporting venues. This chapter will first explore society's awareness of unplanned events and risks of modern life within the risk society. The risk management and assessment processes acknowledge these effects and are designed to mitigate identified risks. This chapter will also discuss the importance of the risk process within sporting venues. Lastly, perceptions of risk will be considered to frame the research question. Perceptions of risk alter the definition of risk, which inevitably influences the overall success of the management and assessment process.

Risk Society

People encounter, assess, and mitigate risks at varying levels every day. Areas with moderately large mobile populations are subject to many potential risks. Practically anywhere individuals choose to congregate, such as schools, shopping malls, airports, or sporting arenas, are susceptible to at least a moderate level of risk (Hall et al., 2012). The ISO (2009) defines risk as an "effect of uncertainty on objectives" that expresses both the consequences and likelihood of occurrence for a particular event (p. 1). As society industrializes and strives to make life safer for everyone, the general public has become more concerned with risk. Society sees itself as more exposed to risk than people in the past and believes it is continually getting worse (Slovic, 1999). How society perceives risks and hazards is continuously changing (Slovic, 1999). These changes, in turn, make it difficult to gauge how individuals will react to different threats if and when they arise.

In the sporting and entertainment domains specifically, security personnel must utilize a risk assessment process to take into account potential risks and the effects risks will have on the general public and society as a whole. The proper assessment and management of such risks are meant to minimize the potential for detrimental consequences such as mass casualty or an economic downturn (Hall et al., 2012).

The collective fear experienced by a society, in addition to a premonition of danger, shapes society's values and its perception of risk (Ericson & Haggerty, 1997). Risk society is rooted in the notion that society not only cares deeply about future occurrences but also focuses on being cognizant of the risks linked to the different surroundings in which they may interact. Society embraces negative logic by fixating on fear and prevention of the worst outcomes possible rather than emphasizing progress (Beck, 1992 & Ericson & Haggerty, 1997). Through statistics, research, and media outlets, people have begun to understand that there is a certain amount of risk associated with each action taken. The shared fear among members of society increases the need for the latest information regarding risk, and the acquisition of risk information, in turn, becomes a manufacturer of risk perception within society at large (Ericson & Haggerty, 1997).

When a society accepts the knowledge of experts in risk professions, society loses its "cognitive sovereignty" (Ericson & Haggerty, 1997). Any occupation that claims to possess a level of abstract knowledge regarding addressing risk concerns and providing expert risk management services is defined as a risk professional (Ericson & Haggerty, 1997). The role of these occupations is to identify, rationalize through assessment and validation processes, and interpret risks to create and implement standards for safety and

security (Ericson & Haggerty, 1997). Risk professionals utilize both risk management and risk assessment to satisfy their role. While risk management focuses on the enforcement of risk decisions and management policies, risk assessment determines and evaluates risks as they relate to an organization's risk criteria.

Society's demand for risk knowledge, in addition to the subsequent creation of risk due to that knowledge, indicates a need for effective risk communication through the use of security. Security refers to circumstances where mollification of a particular risk or hazard occurs (Ericson & Haggerty, 1997). Because security is supported by institutions and organizations, society assumes that these securities can be trusted to protect individuals from loss or harm (Ericson & Haggerty, 1997). In regard to an organization or institution's risk distribution, individuals decide tolerability of risks within the system as a method of control (Beck, 1992). Tolerable values of risk are seen as harmless, but they are also "blank checks" that can potentially damage a system over some time while they remain under the accepted level (Beck, 1992). For example, the amount of pollution in the environment may be determined to be at an acceptable level, but pollution of the environment is still occurring despite the evaluators' decision to not mitigate it. Continuation of pollution over time can eventually become a primary concern to the evaluators because the accumulation of pollution now poses a threat to the integrity of the area in question (Beck, 1992). Handling risks induces a generalized perception between theory and practice, across margins of specialties and disciplines, political, public, science, and economic communities, and between value and fact (Beck, 1992).

Society's awareness of risk and its associated consequences reinforces the expectation from the risk society to be protected against these threats through assessment

and mitigation conducted by risk professionals and security. In order for risk professionals to assess risk and manage identified threats, they must apply risk management principles to their process.

Risk Management

The ISO provides a guide for organizations to manage and assess risk in general terms in their Internal Standards for Risk Management (ISO, 2009). Organizations use the principles and frameworks provided within the document to shape their own risk management and assessment methodologies. While different organizations will have varying and unique methods for identifying and mitigating risks depending on individual goals and objectives, every establishment is expected to follow the ISO guidelines and implement them in their approaches (ISO, 2009).

To manage risk, organizations must identify and analyze risk. Afterward, evaluators determine if the risk should be manipulated through risk treatments to satisfy the organization's risk criteria (ISO, 2009). Risk management differs distinctly from managing risk; while "risk management" refers to the principles, frameworks, and processes that are utilized, "managing risk" refers to the enforcement of those principles, frameworks, and processes to specific risks (ISO, 2009). For risk management to be effective, the organization must comply with all three sections of the process (ISO, 2009).

Figure 1 illustrates the risk management principles, framework, and process in its entirety as ISO recommends it to be conducted (ISO, 2009). The principles section begins the risk management process by setting a list of standards for the process to follow as shown in Figure 1. The analyzed information has to be the best available to the organization, and the overall procedure should be systematic, organized and timely in

nature. Risk management influences the responsibilities of management and strategic planning, rather than being separate from other organizational processes (ISO, 2009). The process creates better-informed decision-makers, so they can prioritize and evaluate appropriate courses of action (ISO, 2009). Ideally, the overall process should contribute to the objectives of the organization and improvement of performance by keeping both human and cultural factors in mind. Additionally, the context should be inclusive in that it acknowledges external and internal capabilities, perceptions, and intentions. The possibility that circumstances will change, new risks will emerge or disappear, or knowledge will evolve is always present; therefore, the risk management process should be adaptable and responsive to change. Organizations must continually improve their risk management process to better tailor it to their organization and stay up to date with new information (ISO, 2009).

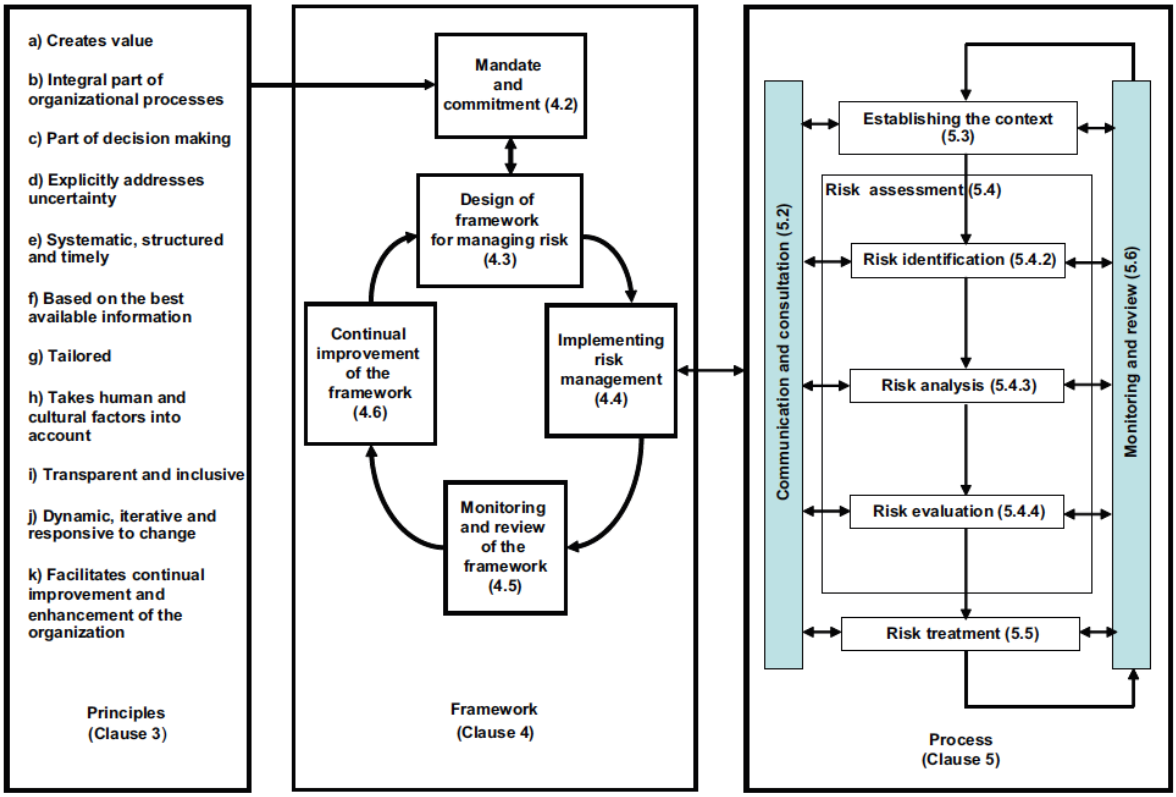

Figure 1. Risk management principles, framework, and process (ISO, 2009)

The risk management framework provides the foundations and arrangements in which risk management will be inserted into the organization (ISO, 2009). The five main parts of the framework begin with mandate and commitment. The remaining four pieces connect in a continuing cycle and include the design of the frame for managing risk, implementing risk management, monitoring and review of the framework, and continual improvement of the framework. At the mandate and commitment level, the organization's management ensures that the organization complies to the risk management policies established by communicating the benefits to stakeholders, aligning the objectives of the organization with the system, and keeping every level of the organization accountable (ISO, 2009). The mandate and commitment step connect to the design of the framework

for the managing risk step in the overall framework; these two steps resemble one another to some degree because they evaluate some of the same factors to command their particular roles within the frame such as commitment, accountability, and context.

When designing a framework for a specific organization, additional factors such as allocating the proper resources and instituting communication and reporting mechanisms must be considered (ISO, 2009). After the design, implementation occurs. At this point, the organization consults with stakeholders and holds training sessions for members of the organization to keep everyone informed. Additionally, the risk policy is applied to organizational processes at all relevant levels of the organization (ISO, 2009). Following the implementation of risk management, the framework is monitored and reviewed by measuring performance, effectiveness, and deviation from the risk management plan (ISO, 2009). Once the framework is evaluated, it should be continually improved to guarantee that the organization is equipped to manage risk as effectively as possible (ISO, 2009).

The risk management process has two steps that occur at all stages of the process: the communication and consultation stage and the monitoring and review stage. Communication with internal and external stakeholders occurs during every step of the process. This constant communication ensures that the professionals responsible for implementing the risk management process and the stakeholders all understand the reasoning behind decisions made (ISO, 2009). Continual monitoring and review throughout the risk management process allow for the gathering of supplementary information and identification of new potential risks (ISO, 2009).

The first step in the risk management process, separate from communication and monitoring, defines the internal and external contexts. The external context refers to influences from the external environment and can be social, political, cultural, economic, natural, financial, or legal in nature. Even external stakeholders can impact context through relationships with the organization or their values and perceptions (ISO, 2009.) Internal context refers to influences from the internal environment and focuses on understanding the goals and objectives of the organization. To do so, the culture of the organization, standards and guidelines, relationships with internal stakeholders, and contractual relationships are evaluated (ISO, 2009). Positive stakeholders are involved in the identification and treatment of risk, offering help throughout the entire process, while negative stakeholders resist the process (NCS4, 2018). Establishing the context as it relates to stakeholders helps those involved to better understand the situation before beginning the process. As the context is defined, evaluators can determine the proper risk criteria appropriate for the organization. The risk criteria reflect the organization's objectives, available resources, and values to assess the significance of risk (ISO, 2009). Following the establishment of context is the risk assessment. There are three steps within the risk assessment: risk identification, risk analysis, and risk evaluation. Once the risk assessment is complete, the organization chooses which risks will be treated and decides which treatment methods will be taken to mitigate select risks (ISO, 2009).

Within the risk management framework, there is a step set aside for implementation of risk management. This is where the risk assessment process takes place.

Risk Assessment:

Risk assessments combines science and judgment and is influenced by psychological, cultural, political, and social considerations (Slovic, 1999). The risk process calls for evaluators to identify, analyze, and evaluate risks using the ISO standards as a guide (NCS4, 2018). A list of risks is generated that could either create, improve, inhibit, degrade, accelerate, or postponement the accomplishment of the organization's objectives (ISO, 2009). Identification includes consequences and significant causes (ISO, 2009). Risk analysis considers the positive and negative implications of the risks identified and weighs the likelihood of each result occurring (ISO, 2009). The report can be qualitative, semi-qualitative, quantitative, or a combination depending on the situation (ISO, 2009). Differing expert opinions, uncertainty, and the availability, quality, or quantity of information can influence the analysis (ISO, 2009). During the risk evaluation process, information obtained during the examination is compared with the risk criteria to assist decision-makers with risk treatment measures. Sometimes, evaluation leads to certain risks to be analyzed further before decisions are made (ISO, 2009).

Organizations can utilize risk assessment tools and techniques to identify, analyze, and evaluate risk assuming the devices are suited to the goals and objectives of the organization (ISO, 2009). Tools such as the Risk Analysis and Management for Critical Asset Protection (RAMCAP) framework suggest using event tree analysis to determine the likelihood of attack success (Cox Jr., 2008). Event tree analysis is a systematic manner in which data can be arranged into branches representing cascading events to determine system dependability (Kabir, 2017). The study can illustrate how one

single event can affect the entire system by showing how different variables interact with one another within the system, and how the event can result in system failure (Ruijters & Stoelinga, 2015). However, studies show that a more complete risk assessment is generated when risk is viewed in both the linear and networked context, meaning evaluation of individualized risk and risk as it relates to other vulnerabilities and threats cascading through the system (Clark-Ginsberg, Abolhassani, & Rahmati, 2018).

Probability methods can be used to account for uncertainties encountered during the assessment process. Techniques such as fuzzy logic, Bayesian methods, the Dempster-Shafer belief approach, human failure estimates, and analytic hierarchy processes have been suggested as means to address uncertainties associated with risk (Pasman & Rogers, 2018). Suggested methods to validate and increase the credibility of risk assessment results include the SAPHEDRA model protocol, Quantitative Risk Assessment maturity model, peer-reviewed assessments and the separation of the analysis and decision-making processes. The SAPHEDRA model encourages an evaluation protocol to be developed while the Quantitative Risk Assessment Maturity Model assists with issues and possible failures that should be avoided in the risk assessment (Pasman & Rogers, 2018). Peer reviewing the results of the risk assessment can decrease confirmation bias through means of having outside figures evaluate the contents of the analysis (Pasman & Rogers, 2018). Additionally, by separating the analysis and decision-making process, influence by stakeholders is minimalized to a degree, and the evaluator can focus solely on the study of risk (Pasman & Rogers, 2018).

The formula *Risk = Likelihood x Vulnerability x Consequence* (*L x V x C*) is also utilized as a method to assess risk. Each factor of the formula is scored on a scale

between zero and five. If a value is scored as a five, the evaluator is without a doubt sure of its likelihood, vulnerability, or consequences. The probability of an event occurring can be determined qualitatively or quantitatively, subjectively or objectively (NCS4, 2018). The product of the scores cannot exceed one hundred twenty-five. Once each risk has a *L x V x C* value, the risks can be prioritized based on ratings and order of importance (NCS4, 2018). When prioritizing risks, Cox (2008) argues that allocating resources to only threats with the highest risk scores is not the best method of risk management because various constraints on budgeting and costs of countermeasures can minimize rather than optimize the management of risks an area faces.

The practices adopted to assess risk are essential to the management of risk and potential consequences. Sporting venues utilize the principles and frameworks set forth by ISO to mold their own methodologies for risk assessment and alleviation as a way to strengthen their chances of being prepared for any threat that may cause harm to their facilities, events, and spectators.

Sporting Events and Risk

Sporting events capture the attention of spectators and athletes alike from all over the world. In 2012, approximately 30.3 million people reportedly attended or participated in sporting events in the United States throughout the year (National Endowment for the Arts, 2018). As of 2015, the North American Industry Classification System reported 4,315 spectator sporting establishments were employing approximately 128,000 people within the United States (Bureau of Census, 2018). The statistics show high participation at both the employment and attendance level within the spectator sporting industry, which spans across over 4,000 venues in the United States. However,

with high involvement comes a high potential for risk. In the event a terrorist attack was successful at any major sporting event, the sizeable amount of participation expected could lead to relatively high casualty and fatality rates.

Risk assessments consider the risks for both “events” and “incidents” by taking an all-hazards approach to prepare and protect organizations against potential threats related to a particular venue or event (Hall et al., 2012). These hazards include but are not limited to terrorist activity via the use of a weapon of mass destruction or explosives, active shooter situation, weather threat or natural disaster, civil disturbance, cyber threat, and event cancellation (Hall et al., 2012). While "events" are planned and generally have information readily available for evaluators to examine, "incidents" are unexpected and do not always provide enough information (NCS4, 2018). For industries such as sports, it is important to use risk assessments for the planning and management of events as well as a preparatory measure for incidents (NCS4, 2018). Sporting events and the facilities in which they take place contribute to the nation's critical infrastructure; therefore, the impact from either a human-made or natural threat would present significant consequences for the industry and society as a whole (Hall et al., 2012). If a sporting facility fails to be adequately prepared for potential threats, mass casualties, economic or social damage, increases in insurance premiums, and liability issues can be expected (Hall et al., 2012). To evade risks as much as possible, planning and preparation using information reported from risk assessments before the event can effectively limit disturbance (NCS4, 2018).

Sporting events generally have an increased media presence covering the event that would publicize not only an incident at the facility but also influence the reactions of

the general public in the aftermath (Hall et al., 2012). The Olympics, as one of the most highly publicized and attended sporting events for the entire world, is susceptible to myriad threats including terrorism. Both the 2004 and 2008 Olympics had domestic terror incidents occur before the Games, with the Kalithea district bombing in Athens and the attack on the paramilitary border police headquarters in the Xinjiang province, respectively (Jennings, 2012). During the1972 Olympics in Munich, eleven athletes and coaches were kidnapped and murdered by Palestinian militants. This event is known as one of the most infamous terrorist attacks during an Olympics (Jennings, 2012). Large scale events such as the Olympics generate a host of uncertainties and hazards for governing and ensuring the game runs as smoothly as possible (Jennings, 2012). Professional or college sports should consider similar risk factors, but the scope in which the risks are evaluated and managed are on a smaller scale due to the difference in venues and events taking place.

How sports owners and operators assess and mitigate risk has evolved dramatically since the attacks that occurred on September 11, 2001 (Miller, Veltri, & Gillentine, 2008). While the terrorist attacks that occurred on 9/11 were not related to the sports industry directly, the attacks significantly reformed the methods in which safety and security were approached throughout the nation by altering the current mindset regarding risk at the time. In the aftermath of the attacks, security personnel at sporting and entertainment venues recognized the need to become more proactive in response rather than reactive to risks that their site was vulnerable to. Funding opportunities for safety and security at major sporting events were more prevalent post-9/11. Money from government funding supplied facilities with additional police personnel and provided

workforces with improved intelligence and technological means (Hall et al., 2012). While risks are different for every facility based on the events held and the location, there is a need for facility operators to determine a set of security standards to abide by (Hall et al., 2012). Sports owners and operators began conceptualizing risk in broader terms for their facilities. In the post-9/11 era, facilities are more cognizant of the potential for terrorist threats in addition to other risks that may occur.

Therefore, owners and operators of sporting facilities take an all-hazard approach to implementing countermeasures to manage threats and vulnerabilities at individual venues. Countermeasures considered by owners and operators include, but are not limited to, installing security cameras, conducting background checks for vendors, creating a credential and record keeping system, and developing emergency operations and evacuation plans (Hall et al., 2012). The Department of Homeland Security Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act was created as a response to the lawsuits that were filed shortly after the 9/11 attacks (Hall et al., 2012). The SAFETY Act is meant to help lessen the liability occurring as a result of terrorism and the standards expressed in the document can be applied to any facility on alert for an attack (Hall et al., 2012). In addition to the utilization of the SAFETY Act, owners and operators of sporting facilities have the opportunity to participate in benchmarking or communicating with other facilities to better compare policies and best practices to improve the overall security standards for the sports industry (Hall et al., 2012).

Sports venues possess a certain degree of trust and expectation from the general public to provide the best safety and security practices available to event participants. To do so, risk professionals must employ assessment and management strategies, but the

manner in which risk information is interpreted by these professionals greatly influences the overall process and mitigation tactics.

Risk Perception

For the risk process to work, society must be able to trust those who are charged with determining risk. The individuals who control the definition of risk also control the venue or organization's response to it (Slovic, 1999). This means the controller of risk is also in control of the objectives of the organization. Because risk is an effect of uncertainty on an organization's goals or objectives, an expressed risk depends on the targets set in place and contrasts slightly between individual organizations due to the difference of contexts (ISO, 2009). The organization must balance both trust and acceptable risk to maintain security (Ericson and Haggerty, 1997). To build confidence, a combination of effective communication and respect for the knowledge and attributes of others has to be maintained (Hall et al., 2012). Without trust, risk communication efforts are ineffective and limited (Slovic, 1999). Experts have to slowly gain the public's trust and be careful not to lose it once attained. The public tends to pay closer attention to the contrary, trust-destroying events rather than positive, trust-building events, making it easy for trust to be lost and never regained (Slovic, 1999.)

Risk discourse forces the public to agree with expert knowledge as the practical response to risk and reminds society that wisdom always holds some degree of ignorance (Ericson and Haggerty, 1997). Although it is not feasible to completely subtract risk from a given system, danger can be evaded, transferred, or minimized to some degree (NCS4, 2018). Society relies heavily on expert judgment regardless of whether or not personal experience aligns with the expert's assessment. A study involving skepticism of experts

and risk demonstrated 59.6% of the sample population believed the expert rather than experiences of friends and showed no feelings of doubt (Austen, 2009). Factors that influenced the sample population's decision include knowledge gained from the school, respectability, and superiority of the teacher, and bias of the sample population (Austen, 2009). It is only when experts begin to lack a consensus among themselves that inexperienced individuals start to search for their knowledge regarding risk. This is where a cross between expertise and experience occurs (Giddens, 1991; Austen, 2008). Inexperienced individuals tend to think of risk in broader terms than those deemed experts (Austen, 2009). While experts supply risk assessments characterized by objective, analytical, rational judgments of "real risk," the public relies on subjective perceptions of risk that are often hypothetical, emotional, and irrational (Slovic, 1999).

It is assumed that physical and natural processes produce the probability and consequences of events in a manner that can be quantified objectively through risk assessment. However, social science analysis rejects this claim by arguing that risk is fundamentally subjective (Slovic, 1999). The subjectivity of assessment cannot be stated clearly, and the objectivity of assessment is arbitrated through the frame of the subjective (Orr, 2010). Similarly, a study involving the decision-making process for peer review of scientific journals revealed the level of subjectivity applied could greatly change the outcome of the possibility of herding, misperception, and acceptance concerning submissions within the scientific community (Park, Peacey, Munafò, 2014). In this regard, a moderate degree of subjectivity is nearly ideal to combat the influence of the rest of the scientific community which may lead to an incorrect hypothesis (Park, Peacey, Munafò, 2014). The occurrence of information from peers within the scientific

community sway a reviewer to a decision despite their own convictions is known as herding. According to Park, Peacey, and Munafò, herding is to be expected to some degree regardless of the level of subjectivity utilized or rationality and motivation of the reviewer (2014). This is partially due to rational individuals taking into account all information available before making a definitive decision, including opinions from peers. People who take this approach understand that humans are imperfect beings that make mistakes, and additional opinions may reinforce or weaken their own perceptions (Park, Peacey, Munafò, 2014).

This thesis examines the risk process at large sporting venues to investigate the association between subjectivity and objectivity within that process. It is hypothesized that assessments and the instruments used to generate them contain a large amount of subjective data, but quantification makes the assessments appear more objective than they are. The risk processes and data sources of large sports security venues will be examined primarily through interviews to contextualize the analysis. Specifically, in-depth interviews with security professionals at major sports arenas were conducted to better understand practices utilized when assessing risk. These interviews were coded using a grounded theory methodology to ascertain how objective or subjective these experts believe their risk assessment methodologies to be. Additionally, the types of data (e.g., expert opinion versus counts of incidents) will be assessed through these interviews to understand the role of subjectivity in the risk assessments better.

Chapter 3: Methods

The overarching goal for this project is to evaluate the risk assessment process in large sporting venues to better understand the subjective and objective elements used by risk professionals. It is hypothesized that these assessments and the tools used to construct them are primarily subjective in nature, but quantification of information gives the impression that final reports are more objective than they actually are. The risk processes and data sources of large sporting and entertainment venues were reviewed through interviews with experienced security professionals to investigate this relationship. The interviews provide a better understanding of the practices used by risk professionals when assessing risk for these facilities as well as information regarding the perception of those carrying out the evaluations regarding how they see information within the process. A grounded theory approach was used to code and develop the theory within the interviews to determine the objective and subjective elements in the participants' risk assessment methods.

Grounded Theory and Procedure

Grounded theory methods provide guidelines for gathering and studying qualitative data (Charmaz, 2014). While there are different approaches to grounded theory, every strategy has six variables in common. These include: coding collected data, discovering social processing within the data, inductively developing abstract categories, refining categories through theoretical selection, memo writing in-between coding and writing, and assimilating categories into a conceptual frame (Charmaz, 2014; Glaser & Strauss, 1967). All six characteristics listed must be exhibited for a methodology to be accepted as a "grounded" method (Charmaz, 2014). The process first begins with a

research question. For this thesis, the use of objective and subjective information within the risk assessment process was the primary focus. Data was collected through interviews with professionals in the sports security industry to explore the interaction between the two.

Sampling

A convenience sampling technique was utilized to recruit participants for the study. Vice Presidents of Security for professional sporting teams as well as Police Chiefs for Universities were among the points of contact. A formal request for interview participation was sent via email to both the listed point of contact, typically the Chief Security Officer or Vice President of Security for the venue, and to potential participants. First, the point of contact was asked for permission to research with personnel who fit the sampling frame of experienced sports security professionals. The email provided the point of contact with information regarding the goals of the study as well as the introduction letter that was emailed to potential interviewees. Once permission was granted, the introduction letter was emailed to prospective participants inquiring interest in conducting an interview. In this email, the purpose, as well as the risks and benefits of the study, were noted. Interviews were conducted either in person or over the phone. Interview questions focused on seven primary categories of interest: qualifications and training, internal and external context of assessment, risk assessment tools and methodology, risk criteria, data analysis, mitigation tactics, and perceptions of risk.

Participants in this study are individuals who have experience working with risk instruments and data sources in large sports and entertainment venues. To participate in the study, individuals were required to possess a familiarity with the risk process for

organizations tasked with public protection at mass gatherings or have experience working with risk instruments and data sources. All participants had to sign a consent form allowing responses to be used for research purposes and acknowledge they were above the age of eighteen. The identities of the participants and venues at which they are employed will remain anonymous throughout the thesis to maintain confidentiality. The researcher has assigned pseudonyms to participants and their associated venues for the sake of privacy.

Ten interviews were completed. Out of the 10 interviews, two were from Police Chiefs of Universities, three were from VPs of Security for professional teams, and five were from security managers for large sporting arenas. The distribution of expertise among the sampling pool is listed the table below.

Interviews Conducted			
Background of Respondents	Number of Participants	Males	Females
University Police Chief	2	2	0
Vice President of Security for Professional Team	3	3	0
Security Managers of Large Sporting Arenas	5	4	1

All 10 participants have experience working with sporting and special events at their respective venues and were familiar with the risk assessment process. Every interview was audio recorded and fully transcribed. Interviews with participants ranged between 30 minutes and one hour and seven minutes.

The objective is to construct theory through an examination of processes and actions expressed within the data set; however, before a theory can be generated, the data must be collected and coded (Charmaz, 2014). Transcriptions of the interviews and

research memos were imported into the Atlas T.I. software program to perform qualitative analysis. This software helps with the organization and interpretation of data obtained from the interviews. Using Atlas T.I., transcriptions will be coded line by line to explore theoretical possibilities shared in the interviews and assist with the generation of conceptual categories used for developing theory later in the analysis.

Initial coding highlights language that reflects action (Charmaz, 2014). During the initial coding process, it is important to remain open-minded about concepts being examined (Charmaz, 2014). Focused coding occurs after initial coding is complete. At this point, the initial codes are analyzed in large groups based on which codes occur most frequently to test developing theories and direct the analysis (Charmaz, 2014). Throughout the coding process, any relevant thoughts that come to mind about the data or research question are documented in the form of a memo in Microsoft Word and imported in Atlas T.I. to be coded as well.

Codes and Categories

In total, there were 132 codes identified from open-coding the data obtained. From the open-coded information, eight code groups were generated. These groups were decision-making, experience and expertise, information sharing, information used, mitigation tactics, perceptions of risk, selection of process, and training. The primary codes of interest are listed below with their groundedness, density, and code groups. While every code created provided relevant information, twenty-five codes with a groundedness score of ten or higher were isolated and examined more closely.

Code Name	Groundedness	Density	Groups	Number of Groups
Utilization of partners	43	11	Decision-Making, Information Sharing, Information Used, Mitigation Tactics, Selection of Process	5
Decison-making	32	10	Decision-Making, Mitigation Tactics	2
Training	43	9	Experience and Expertise, Training	2
Best practices	22	5	Decision-Making, Information Sharing, Information Used, Mitigation Tactics	4
Qualifications	13	5	Experience and Expertise, Training	2
Group think	30	4	Decision-Making, Information Sharing, Information Used, Mitigation Tactics, Selection of Process	5
Experience	37	4	Experience and Expertise, Information Used, Perceptions of Risk	3
Factors being evaluated	35	4	Decision-Making, Information Used, Mitigation Tactics	3
How events shift area's atmosphere	11	4	Information Used, Perceptions of Risk	2
Awareness	13	3	Decision-Making, Information Sharing, Perceptions of Risk	3
Data analysis	21	3	Decision-Making, Information Used	2
Individual interpretations	14	3	Decision-Making, Perceptions of Risk	2
Certification	12	3	Experience and Expertise, Training	2
Probability	10	3	Decision-Making, Information Used	2
Sharing of information	17	2	Decision-Making, Experience and Expertise, Information Sharing, Information Used	4
External risk assessment	12	2	Decision-Making, Selection of Process	2
Different levels of training	10	2	Experience and Expertise, Training	2
Prioritation of risk	10	2	Decision-Making, Perceptions of Risk	2
Understanding of circumstances	10	1	Experience and Expertise, Perceptions of Risk, Selection of Process	3
Subjectivity	27	1	Information Sharing, Information Used	2
Determination of risk	23	1	Decision-Making, Perceptions of Risk	2
League recommendations	17	1	Information Sharing, Information Used	2
Editing of assessment	11	1	Decision-Making, Selection of Process	2
Discretion	10	1	Experience and Expertise, Mitigation Tactics	2

Chapter 4: Analysis

This thesis applied grounded theory methodology to a collection of interviews conducted with leaders in the sports security field (Charmaz, 2014). The researcher generated codes within the data that focused on the risk process as the evaluators' understand it. The identified codes facilitated the theoretical development explaining subjective and objective foundations used in the risk assessment process. This chapter first focuses on the selection of risk assessment methodology among different venues and then delves into how world events and personal perceptions affect this process.

Additionally, the qualifications and level of expertise needed in order to complete assessments are explored. The actual decision-making practices are discussed by focusing primarily on the identification of risk, evaluation among risk professionals, utilization of probability methods, prioritization of risk, and use of training exercises and how all these elements shape the final report. Finally, the mitigation tactics chosen by organizations are considered by taking a closer look at how stakeholders and availability of resources influence recommendations of risk management from evaluators.

Selection of Process:

Threats fluctuate event to event, location to location, facility to facility; therefore, venue operators have to set a designated standard for security based on their specific venue's capacity and location (Hall et al., 2012). Currently, there is minimal legislation existing that mandates stadium operators to follow international or national safety and security standards (Hall et al., 2012). The ISO (2009) provides a basic framework from which organizations are meant to develop a risk assessment process applicable to their individual facilities; however, the framework provided by ISO is so arbitrary that it is almost completely left up to the organization to determine the best methods to conduct their risk assessment. The International Standard encourages organizations to implement consistent practices to identify and manage risk, but in reality, the assessment process is relatively fluid and inconsistent in nature both on the individual level and within the sports security industry as a whole (ISO, 2009). When interviewees were asked about their organization's methodology, respondents stated that none of their organizations adhere to one specific process. Instead, they endorse various methods based on the

circumstances surrounding the venue and event being evaluated. One respondent with over thirty years of law enforcement experience stated:

> So, baseball uses-there's different models that they use. They don't really stick to any one model in response to your question. There's you know, there's risk, there's different risk analysis methodology that people subscribe to. So, I think most of them combine a little bit of everything. And then you know for us, obviously, a lot of it ultimately centers around some kind of assessment of business continuity of if an event takes place how do we continue to function as a team and to get beyond any particular event.[1]

The methods which organizations choose to utilize for their facility varies from venue to venue. Their goals remain the same, but the approach to accomplishing the goals set forth are different. Since organizations approach risk differently from one another, the risks identified, analyzed, and managed have the potential to be dramatically dissimilar simply due to the information utilized and margin in which that information is expended to draw conclusions. A respondent further supported this notion when discussing best practices by stating:

> …the communication within the industry and law enforcement kind of led us to look at what the best practices [are] for us. And every place you're going to go to, it's going to have a different set of circumstances.

Risk identification and mitigation are relatively dependent on the methods chosen by the organization. The objective is to collect as much information as possible from various sources such as data from agencies and outside recommendations to generate an

[1] Phrases such as "you know" were eliminated from quotations for continuity purposes.

assessment that is complete and best represents the contexts established by the venue. According to ISO (2009), in order for the overall process chosen to be effective, the methodology must submit to all three sections of the risk management framework. One respondent elaborated on the usage of multiple assessments by claiming:

> Well, it's good to get different ones. Some venues will only do one type of assessment. You have DHS come out and just do one looking at terrorism. That's great. What about theft? What about you know transportation? About bio? What about food protection? There's so many different things that you can do and think about, so it's better to have all these different ones come in and give you an assessment.

With large variety of risks to identify, evaluate, and analyze, comes various risk assessments tailored to focus on specific areas relevant to the facility. Whether the organization chooses to utilize multiple assessments or not is up to them. By not using more than one assessment, there is a greater possibility of overlooking threats or misappropriating identified risks.

Security and safety protocols adapt based on the event and its draw rather than the venue itself. The venue is the vulnerable structure, but the individuals visiting are the priority. The more people or attention brought to an event, the closer personnel will work to maintain safety and security. A respondent commented on the indefiniteness of the mitigation process by stating, “I mean there might be some things we get softer on and then there may be some events we get harder on.” By saying this, the respondent emphasizes the fact that some events are treated with more attentiveness than others.

Another respondent with 25 years of law enforcement experience reinforces the claims made by the previous respondent by saying:

> So we use the same ops plan for it and we just populate the fields differently based, on you know, what event, the crowd size expected, any kind of trends, any kind of threats that have been made to the event, and if there's something that really pings and looks a little funny, we get together and really dig into it deeply. Or if it's going to be a very largely populated event, we dig into it really deeply and just make sure we're extra careful.

The influence of participation at the event is a determining factor in how attentive to risks the evaluators choose to be when going through the assessment process. Another respondent maintained this conception by commenting on the influence of crowd size further:

> A volleyball game or match is played at the same venue as the basketball game, but the basketball game brings 8,000 people whereas the volleyball game would bring, I mean, frankly, a hundred fifty. A lot of them are parents too. It just doesn't have the draw. So yeah, we-manpower would be different. I wouldn't have the 20 people working that we would at basketball and I'm just talking 20 police. A lot of that has to do with traffic, getting pedestrians across an intersection where the parking decks are. We don't have those worries when the volleyball team is playing because 15 people at a time can just go on crosswalks and cross based on the lights.

Not only does the crowd size effect the evaluators' attitudes towards the assessment process, but it also impacts the number of staffing and mitigation techniques implemented during the event.

Influence of Events:

In risk society, there is a core focus on danger and constant skepticism that management of such dangers is being done (Ericson & Haggerty, 1997). This communal fear among members of society has shaped how not only the public perceives risk but also how evaluators know and understand it. Acts of terrorism such as 9/11, Munich Olympics hostage situation, and Athens Olympics bombing have made individuals more aware of possible risks associated with events and large structures (Hall et al. 2012). When discussing the evolution of risk assessment and impact world events have had on it, one respondent stated:

> So as these things have unfortunately happened more and more nationally and internationally, the whole, I mean, the whole risk assessment field or the threat assessment field has just boomed so it is a constant driver in situations with police departments trying to protect their citizenry. So it's evolved with the events. By events, I mean the bad acts.

Society became more cognizant of the vulnerabilities associated with large structures and events through the continual attention being given to extreme acts of terrorism. Science defines risk while the public perceives it (Beck, 1992). The public's lack of acceptance for the scientific definition of risk is not reflective of an illogicality within the population but rather points to incorrect assertions of cultural acceptability

made within scientific and technical declarations (Beck, 1992). One respondent stated how their cognizance of risk has evolved over time:

> I think that over my career, I've just become more aware, more vigilant, taking a look at risk that anything could possibly affect an event that we're at.

Another respondent mirrored the previous respondent's notion of awareness increasing over time by reflecting on past events that have shaped their own understanding of risks:

> I just don't ever remember there would be shootings, but not where somebody came in and just indiscriminately just wanted to kill people. So over the course of my career those trends, I mean, the terrorism both internationally that we're talking about or you're having foreign nationals come over here and fly planes into buildings and go into the Pulse Nightclub and shoot up people, and in California, they were shooting at that company-their Christmas party yelling "Allah Akbar." That's kind of stuff was all new over the course of my career, and then towards the end of my career the whole driving up and running over people thing became a thing and that just, I mean, you have to be ever vigilant.

The respondent discusses their observation of risks as they appear to be more present over the course of his or her career. Effects from events such as active shooter incidents and acts of terrorism have shaped the respondent's current perception of risk and what threat means in terms of structures and participants. The risks, however, have always been there. Throughout history, there have been countless tragedies, such as the 1989 Hillsborough Stadium Disaster and 1985 Bradford Fire, that have occurred at large venues, including sporting facilities (Hall et al., 2012). It is not the risks that have changed, but security professionals' and the public's consciousness of threats and

vulnerabilities that have altered. This has led to more involved and sensitive evaluation. Another respondent commented on this progression of assessment sparked by world events by stating:

> Oh, it's totally changed. It's increased it, matter of fact. I mean, there wasn't really event management, so say, security event management to the extreme it is now 20 years ago. I mean, you had security. You had police, but it wasn't to what it is now. I mean, you weren't looking for-mostly it was just to get the drunk out of the building or something of that nature, but now it's, I mean, you have to encompass so much more. Why is that bag sitting there to that drunk so, I mean you got to get up just to another level.

Respondents further expanded on this concept by explaining the mentality of risk professionals prior to society becoming aware of threats such as acts of terrorism:

> Well, I mean, it's-everybody really evolved at the same time, so I can tell you 25 years ago when we-when there were events like that, there was no real risk assessment. The only concern was like, "Hey, we've got to get these people across the street, so I need some guy to stand intersection to make sure they don't get run over by just a drunk driver or somebody who's running a red light."

According to the respondent, risk professionals lacked a sense of hyper-vigilance and attitudes towards risk were relatively mild in comparison to today. People in society believe they are more visible to risk than those before and that the exposure and risks present are persistently getting worse (Slovic, 1999). Shifts in the definition of risk by organizations and public perceptions within the past twenty to thirty years molded the general principles of risk assessment into what they are today.

Perception of Risk:

Trust is a state of mind that evolves from the actions people take rather than what they say. Organizations have to communicate honestly, respect knowledge, skills, and abilities of other individuals, sustain confidentiality, and maintain unguarded exchanges (Hall et al., 2012). While they must maintain and improve the public's trust, they must also be able to trust the individuals involved in the risk process. When asked about trusting those involved in the process, one respondent remarked:

> …you've got to rely on a lot of people, and you've got to know who you've got there. What their background is and that goes all the way down to who gets the credentials from athletic staff.

By trusting those conducting the evaluation and others involved in the implementation of decisions, the organization recognizes their background and ability to determine risks at the venue based on the evaluator's understanding of the goals and objectives of the organization.

In a large portion of the interviews, there was mention of at least one additional assessment being used in conjunction with an internal evaluation. Gathering more than one assessment is meant to help generate a more thorough, complete evaluation. If people perceive risks differently, a combination of several assessments by different agencies both internal and external are supposed to level out one specific group's perceptions by providing multiple interpretations of the same environment. There is expected to be overlap between these assessments, but each assessment is unique in itself because it could offer a new perspective on the topic and offer different solutions. It is up to the organization being evaluated to determine the best practices and countermeasures

to implement as a result of these assessments. The more input placed in the assessment, the more objective the assessment appears to be because multiple people are giving their input. A respondent stated decisions regarding effective mitigation "… comes from looking at the problem and then talking to other sources and try to figure out what's within our realm of possibility to mitigate it." If the internal assessment and supplementary assessments all report relatively the same vulnerabilities, people view the overall assessment as a comprehensive document that accurately reflects the risks associated with the venue.

A moderate degree of subjectivity in the review process is thought to be beneficial in reducing misconceptions because evaluators who do not follow the herding trend will ultimately offer new information and insight to the report (Park, Peacey, & Munafo, 2014). However, the approach mentioned above is more than moderately subjective because it focuses primarily on individual thoughts and recommendations of risk coming together to create a better understanding of the venue and its vulnerabilities. A respondent discussed the benefits of having both novice and experienced individuals take part in the assessment process:

> So, I think when you hear a new view, that that can be very refreshing and they can see something that you don't see. And when you give them some experience that you've been through, they're like, "Wow, I didn't even think of that." So, combining both can really make you a much better assessor as a team.

The respondent also mentions how experience can provide a form of enlightenment for novice evaluators. According to the statements made by the respondent, experience is not necessarily important to the assessment process because people with various

backgrounds can still contribute, but having some experience gives the evaluator a better understanding and mindfulness of the risks being investigated.

Risk discourse fosters uncertainty and forces the public to trust experts' knowledge of risk as the best method of appraising threats and hazards (Ericson & Haggerty, 1997). The public trusts the judgment of experts regardless if their own experiences support the expert's findings (Austen, 2009). One respondent commented on how their personal experience and opinions guide the evaluation process at team meetings:

> Well, since I run the risk assessment meeting, I-it does help kind of shape the meeting, but again, like I said, I'm very open and I listen to all of the different views. So, my personal experiences and my opinions of what's happened over the years, I throw them out there because I want people to hear them, but I also want to listen to others and make sure that we use all of these opinions in the room to make a thorough assessment.

The respondent's experience and opinions set the tone for the entire process at that particular venue and heavily influence the end result. While the respondent allows input from multiple persons, his or her perceptions are more prevalent in the discussion because they are running the meeting. Another respondent mentioned how experience can impact risk management decisions by stating:

> …so we allow law enforcement to come in, sworn officers, if they have their badge, their ID. We sign them in and get their seat location and tell them to come back to that same location if something happens so that we can deploy them. A lot of venues don't do that, and I understand why. [The football stadium] does not do

> it, our football stadium, because it's owned by a different owner. The security director over there has had bad experience with friendly fire. When he was a cop, there was some friendly fire, but it was bad. So he's always nervous about having guns and alcohol mix, but we tell our cops when they come in, "You can't drink. You know this already. You can't-you're a cop. You can't drink while you're here with your gun on. So, enjoy the game come back here if there's a problem." We've never had a problem. Other venues may have had problems. That's why they have different policies, but we've talked to the cops coming in. They all know.

While the respondent's organization allows off-duty sworn officers to enter their facility armed, another organization does not because someone did not have a positive experience with firearms. The disparity between the two mitigation tactics demonstrates how important experience and perception are in the assessment and management process.

Training and Expertise:

Individuals within the organization rely heavily on training and observations of risk to conduct the bulk of their assessments. Experience and judgement drive the assessment process. Without it, the evaluator may not feel competent enough to conduct the evaluation his or herself. They feel the need to utilize third parties to complete the assessment. Evaluators trust their training and experience to the point where they would rather conduct a whole assessment without the aid of a governmental third party such as DHS. One respondent who supports this notion said:

> Now, if I didn't have this experience, I might have to look at bringing in Homeland Security, State or Federal Homeland Security to help me do this. And we still, I mean, we have them. They have done assessments of our-all of our

> facilities just as a whole just to come look at it as a whole, but if I didn't have all this experience, then yeah, I may have to have them help me do the whole thing. But with experience and training, I'm lucky enough here to be able to say "hey we can manage it."

Trusting one's own experience and training rather than seeking additional aid gives room for an increased utilization of subjectivity from a small group of individuals rather than developing a collective agreement among various groups about the risks present. By only conducting an internal evaluation, there is a higher probability of overlooking a risk and inputting a larger margin of bias in the report.

A court decision made on April 29, 2008 established certain requirements for facilities on notice for the possibility of a terrorist attack by demanding organizations aware of the risk take "reasonable" steps to mitigate it (Hall et al., 2012). The decision changed the liability landscape for all environments that possess potential terrorist threat by focusing on whether operators are aware of the threat and if the venue possesses reasonable and necessary mitigation tactics. In light of the decision, sport operators were charged with the responsibility to be proactive rather than reactive to such threats by communicating with other agencies and facilities and applying principles within the Department of Homeland Security's SAFETY act (Hall et al., 2012). The interviewees were asked what qualifications are needed for a risk assessor to conduct an evaluation at their respective venues. All the responses mentioned one or both categories: proper certification or training and a certain degree of experience. This notion is similar to Ericson and Haggerty's (1997) definition of a risk professional. According to Ericson and Haggerty (1997), a person is deemed a risk professional if they claim to have a level

of abstract knowledge addressing risk concerns and providing expert risk management recommendations. One respondent stated an individual is qualified "…through background, through experiences, through education, through certification such as like the safety act-DHS safety act. Things like that." Another respondent said:

> So, to have a risk-if we have a third party do a risk assessment for us, then, we make sure they have all the qualifications, meaning that they're actually certified to do a risk assessment, that they have previous experience doing risk assessments, and that they've provided us documentation of previous risk assessments that they've done. Meaning not necessarily a confidential document, but "hey, we did a risk assessment on a Major League Baseball facility and these-this is some of the feedback we provided." Again, nothing specific, but showing us that they have conducted it, that they do have the experience, and a lot of these come with-we take a look at their backgrounds, meaning the individual who's actually conduct the risk assessment, so whether they were in law enforcement for twenty years, or they were-what kind of education they got, backgrounds like that.

It is evident that in order for an organization to trust the individuals evaluating the venue, the appropriate parties must have some recognizable certification and experience with assessments. Inexperienced persons tend to consider risk in broader terms in comparison to those who identify as experts (Austen, 2009). Another respondent reinforces the idea that a surveyor needs to possess suitable credentials in order to be acceptable for use by the organization by stating:

> That's a tricky thing. The government only sends out their people, so you, I mean, you've got companies-you can go into the Yellow Pages and find companies that

> will come out and do a risk assessment for you, but who trained them? Where are they from? Are they just some guy who took a class. I mean, you want someone from the Department of Homeland Security, someone who's been involved in planning attacks and defending attacks. That's what you want.

The respondent would rather have someone who is trained by Homeland Security specifically and deemed an expert by DHS because they do not want to select someone any person who claims they can conduct an assessment. Based on this response, it appears the training programs for risk assessors are not always trustworthy and are ambiguous at times depending on the program, so anyone interested in risk assessment can take a class and think they understand how to identify and analyze risks.

In regard to training, there were mixed responses on how people are trained to be risk evaluators. One respondent stated the training came primarily through the police academy and a few classes that occur every now and again:

> Now, when you talk about on the structural side of things and guarding structures, there would be some basic stuff that would go on in the police academy itself, just very basic stuff as part of their just a very basic of training, but the more in-depth stuff where they really learned how to target hard, there were really only a few people that would go to these training classes. We try to get as many people into it as we could, but that was not always the-the training does not come around all that often and it fills up really quick.

While the respondent discusses the training received in the police academy and occasional classroom training, it is important to note that not every risk assessor is a police officer or attended a police academy. The respondent continued their statement by

mentioning additional training that is accredited by the state and designated assessment groups:

> They [risk assessors] went through specialized training and got accredited in that subject field as well. So they had-they went to specialized school, specialized classes, where they learned how to do that kind of stuff and were qualified based on the state, based on getting those accreditations to go into a place and give opinions on where you had issues and where you didn't...I are already talked about ATAP, the Association of Threat Assessment Professionals. You could get different levels of training with them, but you could also take a course and then a test and I'm trying to think of what the name of it was but it was a specialized designation which basically meant that you're kind of like a master assessor and I'm probably using the wrong terminology.

Evaluators can attend various trainings from different entities and receive some form of certification recognized by the State or other organizations, but there is no designated training program mandated for all assessors to attend. For others, training is conducted internally through a variety of courses. Another respondent stated:

> So we have a training matrix, so it's different levels…All of our security staff take ICS 100, 200, 700, 800. Those are all FEMA classes. They have to go through a four hour-all colleagues go through a four-hour orientation. So that's a welcome to the [arena], welcome to our company, sexual harassment policy, if you get injured on the job, how do you punch in and punch out, what the dress code is, the attendance policy, all that. And then we talked a little bit about during that four hour orientation, I do a-me or one of my managers do a two hour part of it called

> "See Something, Say Something," but we talk about this is, what a bomb looks like, this is the four components of bomb, these are some of the things-a lone wolf, improvised explosive devices.

It appears there is no designated training mandated for everyone who claims to be an assessor to attend and get certified. Training courses are either accredited by the State, a Federal agency, or entity groups designed to advance the knowledge of assessors. This demonstrates that the type of training and quality of training received varies within the field, making the risk assessment process convoluted with individuals who may or may not be taught "proper" assessment methods.

Risk professionals claim to possess exclusive abstract knowledge of the best ways to tackle risks and provide risk management services as experts in their field (Ericson & Haggerty, 1997). Such individuals are expected to be reflexive enough to effectively identify an issue and firm enough to discontinue considerations of risk and take action (Ericson & Haggerty, 1997). Risk professionals ultimately control the definition of risk and the objectives established within their respective organizations (Slovic, 1999). Interviewees were asked what makes an expert an "expert" and the overarching response was:

> Through experiences. I mean, really through experiences. I think if you've-you didn't look at something one time and something took place, then obviously you're going to look at it the next time.

The response shows that security operators believe risk expert to be someone who is knowledgeable in their field and has had enough experiences in their career to be able to

identify a risk and make recommendations on how to handle them. When asked at what point is someone experienced enough to be deemed an expert, one respondent claimed:

> The tipping point is different. I mean, literally, you can't say "everyone after 10 years of experience and 10 years in law enforcement and 4 years of college." I think you have to be kind of open-minded and really kind of do some research on what the individual or the company. If it's a third party company, what they've done as a whole. I just don't think there's a tipping point that says "hey, after five years" or "we've been in business for eight years or twelve years and we've done 30 different risk assessments that makes us qualified to handle what I want them to do." I take a good look at them, get as much information as I possibly can, and I really love to rely on other sources, meaning people I know or companies that I know or organizations that I know that have used the same company I'm looking at because if they've gotten a thorough, a very thorough written documentation of a risk assessment, that also helps me in my decision.

The rate at which an individual accumulates quality experiences that hone their skills and broaden their perceptions of risk is inconsistent between individuals because not everyone lives the same life. With this in mind, the acceptability of expertise is relative. How one decides to convey they have enough life and career experience was not mentioned, but it would be up to the organization to determine if the experience disclosed is sufficient enough to conduct an assessment. Discussions between different organizations who have used the evaluator in question validate the organization's decision to either work with the evaluator or not.

Decision-Making Process:

Identification of Risk

Personal attitudes towards risk kickstart the assessment process and influence the evaluators' theories of what risks exist at a particular venue and the methods to best manage them. Evaluators, then, seek to obtain objective data such as trends and incident reports to provide some form of contextual support or rejection of notions previously determined by the evaluator. The data can possibly be manipulated or misinterpreted to support opinions that are solely those of the evaluator and not necessarily reflective of the organization, venue, or actual threats present. Information includes, but is not limited to, statistical reports, news, facts, judicial decisions, and formal reports while knowledge is referred to as the interpretation of context, relatedness, and conceptualization (Ericson & Haggerty, 1997). Information being analyzed should be the best available to the organization, and the general methods should be systematic and timely in nature. The overall process creates better-informed decision-makers that can more appropriately prioritize and weigh mitigation tactics (ISO, 2009). One respondent referred to their organization's use of third-party assessment as a way to essentially confirm theories of risk that the organization had already recognized:

> He [the third party assessor] came through and he risk assessed the building for us and we have his assessment on file and based on that, based on frankly our own assessment because a lot of what he does is a lot of common sense and we kind of figured it out on our own. We put up certain barriers.

By confirming what the organization had previously observed, the third-party evaluation gave the organization a foundation for which they could argue to implement certain

countermeasures. By using information from other sources to support preconceived notions of risk, these organizations can confirm their theories of risks affecting the facility.

In addition to third party assessments, organizations refer to information collected by other agencies on trends and best practices. According to one respondent, sharing information between agencies is crucial to understanding risks:

> He [my boss] believes we should all get around the table and talk about things. And he's the first one to-he'll go to some other venues to see what they're doing, and then he'll share openly with them what we're doing and get a better understanding.

Sharing of information within the sports security industry helps the industry develop a more uniform conceptualization of risk among security professionals. Beck (1992) states, as mentioned in Chapter 1, the management of risk creates an oversimplified perception between theory and practice, across disciplines, and between opinions and factual information. Information used during the assessment process can be from a myriad of sources. When asked what kind of information the interviewees' organizations analyze, the primary answer revolved around some form of intel gathering between different departments. One respondent commented:

> …we evaluate numerous things. Whether it's a give-away at a game because that produces more fans, whether it's an FBI report, a DHS report, a local police stating "hey, this is what's been going on in the area," worldwide events such as the mosque shootings, I mean, we use numerous resources and unlimited amount

> of incidents that have taken place. We use all kinds of things. It's not just a set boom, boom, boom.

Another respondent echoed the previous respondent's answer to utilization of information by stating:

> We have some people that you-we have a lot of years of expertise, some in baseball, some in law enforcement, so we put all that together. And we also use-we'll pull police data, FBI data, DHS data, so we use both.

When venues ask for reports and information from other entities such as the FBI and DHS, the type of material gathered can either be subjective or objective in nature. One respondent's remarks discussed how they go about asking different agencies for information:

> We'll work with the FBI, ATF, Homeland Security, joint terrorism task force, and we'll sit down with them before football season two to three months before and say, "Okay. What we do we have going on in the area that we need to be aware of? What is some risk assessment? What is some suspicious-what kind-some cases you're working on? Not so say who or what, but if you get-have you got a-are you working a possible terrorism case in this area? You work-is there an armed robbery spree going on in the area? Is there property crime? Is there some auto burglaries going on the west side of town?" We do all that assessment of what's going on, even what's going on here.

When groups of individuals are asked by the organization if there are any threats or trends they should be aware of, the agency can either supply the organization with information based on what the individuals being asked have observed over time or

provide data in the form of statistics and Suspicious Activity Reports (SARs). The uncertainty of which form of information available for collection by the evaluator makes the evaluation process even more subjective.

Some organizations try to collect data internally by documenting incidents and statistical evidence. One respondent elaborated on one of the methods their organization utilizes to file incidents that occur at their stadium:

> So we have an ISS 24/7, that is the leader in event management & event incident reporting. Most of the teams-probably 90% of the teams use it. It allows you to log everything coming in. Deliveries, incidents, medicals, you name it. We track all of our colleagues coming in by access control system that we have, and then for guests, it allows any time a guest has an incident, we can track it and keep it on the summary.

By referring back to the data collected over a period of time, evaluators can observe trends within the venue in question in addition to applying information from outside sources. Application and quantity of information obtained can vary depending on the organization. One respondent commented on this when referring to preferences for looking at risks from a "realistic" perspective rather than solely relying on numerical data by saying "…that's the constant battle back and forth is I'd rather look at in realistic terms and these guys tend to sometimes just look at it in black and white numbers." Even when there is numerical, objective data available, some evaluators still prefer to rely on their own conceptions and experiences with risk.

Evaluation

Rational people process all available information that can be provided prior to making a decision. A rational individual can and should be impacted by what other individuals think in order to support or reject personal opinions regarding similar topics (Park, Peacey, & Munafo, 2014). Early findings within the process can be rebutted by subsequent evidence, allowing the formation of groups that interpret the same evidence in significantly dissimilar ways. This occurrence may lead to convergence of false hypotheses (Park, Peacey, & Munafo, 2014). A respondent noted how the evaluation process takes into account everyone's positions on the vulnerability as the venue and how it affects mitigation:

> …it's a matter of we believe everything should be implemented and if it-best practices, if there's something that changes, then that's obviously with the chain of command within the organization. But if it's a strong feeling that people feel really strong about it, then, the decision is usually made; if it's not there at that meeting, it will go up through the chain of command all the way up to the highest possible all the way up to the owners and it comes back down to us. Hopefully with the right decision.

If someone strongly believes that a certain risk is present at the facility, it is usually incorporated into the assessment regardless of whether other individuals agree or disagree with the notion. However, the chain of command within the organization ultimately determines the legitimacy of those perceptions. One respondent shed some light as to how this process is conducted:

> We have an internal security risk assessment committee that's made up of executives and myself and representatives from our insurance company. So if there's a major problem, we meet, and we meet at least once before the season and once after the season, but for any major problems, we would meet-conduct an unscheduled meeting. So that would be the first way we would look at it and then typically a lot of that falls on me to-if something's identified is to immediately determine the best remedy so often times I'll look at outside sources.

When executives in the security branch determine risks present, the decisions made are influenced by the individuals at the meeting and the upper chain of command's ideas on how to treat identified risks.

Differing expert judgements, ambiguity, and quality, quantity, or obtainability of information can affect analysis of risks identified at any particular facility (ISO, 2009). Peer review should diminish the number of concerns addressed, but if the review process is often not conducted correctly. In order for peer review to be effective, evaluators have to safeguard the quality and legitimacy of scientific information (Park, Peacey, & Munafo, 2014). When asked if the assessors usually agree with one another's assertions of risk, one respondent stated:

> Yeah, and it's maybe not necessarily an agreement, but it's an awareness. That's what I kind of like to make it is that when you have a risk assessment, not everybody has to agree that such and such is a risk, but everyone becomes aware of it. So, the awareness and what we need to do to mitigate that risk, that's what's important. So, yeah, I think if there's ten, fifteen people or fifteen, twenty people,

> I think everyone becomes aware of what potentially someone in the group thinks is a risk and then no matter what, we are gonna try to mitigate that risk.

If someone on the assessment team identifies a risk that the other evaluators do not necessarily detect, the risk is placed in the overall assessment with little to no validation. Even if it is not seen as a primary risk designated by the entire group, reporting that at least one person observed it increases the organization's alertness to the possibility it exists.

Probability Methods

Events that draw a sizeable amount of participation create a multitude of uncertainties and threats for governing (Jennings, 2012). There is always a possibility that circumstances will change and bring rise of new risks relevant to the facility or decrease the presence of previously identified risks. As circumstances change, organizations must update and improve the risk management process to fit the objectives of the organization (ISO, 2009). When doing so, risk assessors look at the likelihood of certain risks impacting the venue. Ideally, probability calculations minimize uncertainty to a level that the evaluator feels relatively assured in taking action (Ericson & Haggerty, 1997). People assume probability and consequence of physical and natural processes can be quantified objectively in the risk assessment process; however, social science analysis challenges this notion by declaring risk as fundamentally subjective (Slovic, 1999). While probability of occurrence can be established quantitatively or qualitatively, subjectively or objectively, most security operators predominantly utilize a more subjective approach (NCS4, 2018). When asked about the usage of probability methods,

every respondent claimed their organization uses them, but not on a regular basis. A respondent's comments on probability usage support this notion by stating:

> I wouldn't say every time, but I think if there's something that rises to that need, then we will-we're not afraid to use a probability method… I'm trying to think of a good example. Like I can't think of one off the top of my head, but you know, we-different GARs. I mean, we've used different GAR methods and something ends up in the red, then obviously, it's a probability method.

For most, the probability methods are entirely subjective because they rely on expert judgement rather than statistical trends and reports to determine the likelihood of an event happening. One respondent explained how their particular organization approaches likelihood by saying:

> I wouldn't say mathematical. It's more of, "What do we know? What's the common trends? What do we know? What [does] this group like to do? What's that group like to do? What's popular with them? What's the hot things going on in this area?"

In these situations, deciding the likelihood of an event occurring is dependent on the experience of the individuals conducting the assessment and may eventually lead to a heavily subjective prioritization of risks in the mitigation stages. Additionally, probability can be influenced by criteria established from other sources. One respondent mentions this by stating:

> We don't necessarily use a numeric ranking system, but we do prioritize and through Major League Baseball, they-Major League Baseball has established that

> stadium operating practices criteria which is heavily set around the SAFETY Act, the Department of Homeland Security SAFETY Act.

While some organizations utilize guiding principles set forth by other entities, others rely on expert opinion to determine the probability of risks at the venue. The overall determination of probability then influences the prioritization of those risks from tolerable to unacceptable.

Prioritization of Risk

Risk cannot be completely eradicated from any particular venue, but it can be minimized, transferred, or evaded through prioritization driven by the established objectives of the organization (NCS4, 2018). Based on ISO's (2009) definition, the expression of risk is dependent on the identified objectives of the organization and varies from organization to organization. Evaluators determine the level of tolerability for risks identified from the assessment and distributed within the facility as a manner of control (Beck, 1992). When asked how prioritization is conducted at interviewees' respective facilities, there was a mix of responses that discussed their process, but the approaches mentioned still maintained various levels of subjectivity via knowledge and judgement of risks. One respondent stated:

> I mean, we don't necessarily rank things, but we sit around. We have a meeting, like I said, and uh first of all, we all have an opportunity to look at a lot of the information. So, we come in to the meeting with a pretty good knowledge of what we think might be some risk that we may need to mitigate, and then, we sit there and we talk about it, discuss it and, like you said, there's a lot of expertise around

> the table and on the conference call and there's a lot of data that goes around. So, it's a pretty thorough process.

For this particular approach, there is a substantial amount of reliability on expertise and individual interpretations of information gathered during the assessment. Another respondent's account of their prioritization process stems from criteria set forth by DHS and experience:

> It is expert knowledge. It is based off of the RSAT. That's the first one that we did that was government done. We bring them in. They do it, and we use that same rating system for our assessments because once again, the safety act because that question would come up as to the Department Homeland Security say, "How do you rate your-how was your assessment done? How was the rating done?" We go, "We use your system." Can't argue. "We use your system. So you can't say this a bad system lets you're saying your system is bad." We're using the Department of Homeland Security rating system. So that's what we use.

Both approaches utilize the thoughts and opinions of experts but in different ways. While one approach focuses on the group's analyzation of data through discussion at a meeting, the other applies criteria for ranking from a specific framework and uses expert knowledge to categorize risks using the respective benchmarks.

Use of Operational Exercises

The Department of Homeland Security's Exercise and Evaluation Program, commonly referred to as HSEEP, contains seven discussion-based exercises. Within the program, there are two routes operators can choose to utilize. One of which is functional in nature where stadium staff participate in drills and full-scale exercises, but this is a

relatively difficult course of action to conduct due to circumstances surrounding the venue such as quantity of resources available. Instead, most venues utilize seminars, workshops, game simulations, and tabletop exercises (TTX) to validate current practices, identify gaps in resource allocation, and clarify roles of staff and partners (Hall et al., 2012). When discussing these exercises, one respondent explained how the program can aid security professionals with observing the practicality of current mitigation tactics:

> Every time we have a table top, the next two weeks, I'm getting questions from all these Vice Presidents saying, "Oh yeah, that was really great. You know, I want to learn more." But it gives you a chance to poke holes where you know you're vulnerable, and then see if people will respond.

Every respondent mentioned using tabletop exercises as a means to account for current practices and validate their applications to the venue. In addition to TTXs, some venues utilize drills such as random screening checks to accomplish the same goal of inspecting effectiveness of countermeasures. One respondent discussed this further by stating:

> …they [auditors] come over and I'm sure they collect data on that with the numbers. But they're coming over. They're testing a door to see if they can get in with-the common thing, we do is we put cell phone in the front pocket with a knife. Walk through the metal detector and go, "Oh!" They say, "Right here, you went off right here on the side." You pull out your phone and go it was my phone and they go, "Okay, you're good." No, they're supposed to stop, rescan that area with the phone out, and then see that the knife is there. That's the most common mistake. Very common. So, we test on that-we'll have them come over and test a

> couple of our screeners and see if it'll work. See if we can get through. If we do get through, then we pull them aside and retrain them.

When inconsistencies are observed using these exercises, security operators are responsible for implementing corrective actions to fix recognized issues.

Mitigation

Stakeholder influence

Social, political, cultural, economic, natural, financial, or legal factors can influence the external context that evaluators account for. Relationships with both internal and external stakeholders can impact the context through stakeholders pushing their personal perceptions on the assessment team (ISO, 2009). Negative stakeholders reject the entire process and decisions made, and positive stakeholders immerse themselves in the identification and management process by offering consultation from beginning to end (NCS4, 2018). While stakeholders may not be able to "edit" the assessment document, they do hold some influence over the process itself in regards to approaches of risk and mitigation. When the assessment and management processes are conducted separately, influence from stakeholders can decrease slightly, allowing the evaluators to consider risks exclusively (Pasman & Rogers, 2018). One respondent hinted at this when discussing the clear bag policy:

> I'm not a big proponent of the clear bag policy… And it's not that I'm against the clear bag policy. I'm for it if it's league mandated. If the NBA and NHL say, "We're going to clear bag policy." I am 100%. I think it's the most effective way to the to check bags. It's quicker. It's more effective. You can't have hidden

compartments in a clear bag. Hundred percent agree. It's the safest way to go. But if you're not going to mandate it by the league, it's tough.

Despite the respondent agreeing that the clear bag policy is effective and a helpful mitigation tactic for collecting contraband during the screening process, they do not fully support it because the sports leagues associated with the venue do not mandate or recommend it to be a best practice. Had the leagues recommended the clear bag policy, the respondent would most likely be on board with the mandate. Lack of such a mandate influences how the respondent and other evaluators choose to manage the screening process. When stakeholders such as sports leagues dictate specific methods of mitigation as best practices, the organization typically abides by the standards established. If there are multiple stakeholders influencing mitigation decisions, the standards are compared to determine the best out of the group. A respondent expanded on the usage of recommended best practices by saying:

> So, NHL has a-they come out with what's called a NHL security standards and recommendations every year. We take from that, that says you must do screening, you must do this, you must provide security for parking for the bench, for locker rooms. NBA comes out with one as well a little bit more aggressive than the NHL. Then, we look at the baseball-even though this is an arena, we look at baseball and football and pull their best practices… We take all those best practices, and we put them all together on one big spreadsheet and say, "what's the best of each one?" And that's what we try to do. We don't just do the NHL version of what's best for screening. We'll do whatever is the highest of all the league's, we'll pick that one and do the highest.

The decision as to which practice is the best out of a group is determined by which provides the higher level of security, and it is decided on by a small group of individuals who keep up with the changing recommendations on a yearly basis.

Limitations of Resources

Allocating resources to only identified risks with high risk scores is not necessarily the most ideal management technique limitations placed on budgeting and costs for countermeasures (Cox, 2008). The mitigation process is impacted by the quantity of resources available to the venue. Evaluators have to make decisions that are both practical and best for ensuring security. When asked about utilization of resources and the mitigation process, one respondent stated:

> Everything we do is risk driven. That's what it's all about. We-because you can't stop everything. You have to make decisions, smart decisions, about what you're going to put your resources in.

While some mitigation tactics may be the most ideal for guaranteeing safety and security, they may not be the most practical actions based on available resources and application. One respondent elaborated on this notion by stating:

> So yeah, you got to make decisions that are going to protect the most people the but are also feasible. Somebody may say, "You know, we need to? We need to you know encompass the [stadium] in one big brick wall that's 50 feet high." Like yeah, that would keep threats out, but that's not feasible and it's expensive. Can't do it. So we'd have to look at the idea that the person had or the suggestion and see if it was feasible financially, but as well as like practically too.

When resources are not readily available or solutions are not necessarily practical to apply to the venue, evaluators have to get imaginative in ways to handle risks. A respondent recalled an occasion where they had to implement a creative solution to mitigate one of the organization's chief concerns:

> I found some creative ways like when I came here, they had repeatedly had a stadium that it was identified as a risk to a vehicle-borne attack, especially against pedestrians and they had budgeted some money to put barriers in, but it really wasn't a practical solution. So I ended up talking to some different people looking at some different venues and we ended up landscaping the area and put giant boulders in there and making it a rock garden, which the fans think looks really great, but the reality of the matter is that each of those boulders is big enough to stop a fairly decent size small truck.

Venues may not be able to uphold mitigation tactics the industry deems as most effective which allows security operators to generate their own versions of solutions to minimize risk.

From beginning to end, the risk assessment process is largely subjective. There are various approaches to risk assessment that security operators can choose to utilize based on what they believe is best for their facility. When selecting risk evaluators, security operators desire individuals with a relative amount of experience and training backed by local, state, or federal entities. An evaluator's perceptions of risk are subject to change based on witnessing or observing the impacts made by catastrophic world events like 9/11 or the Munich Olympics hostage situation. Professional experiences, and consequently perceptions, vary among individuals because not everyone experiences risk

in the same terms. Evaluators regularly call upon their own experiences and judgements to assess venues, and several organizations call upon multiple evaluators' recommendations to create a more holistic assessment of their venue. While objective information such as trends, statistics, and reports obtained from internal and external sources are examined, this information is generally used to support or reject evaluators' personal perceptions of risk. When determining the probability of occurrence for identified risks, assessors utilize their own perceptions of likelihood more often than objective calculations. These conclusions ultimately impact the prioritization of risks because threats with higher probability scores are more likely to be addressed when choosing mitigation tactics. Risk management measures are impacted by stakeholders' recommendations and best practices as well as availability of resources. Evaluators must be realistic when choosing the best mitigation tactics by deciding upon what would minimize risks effectively based on the recommendations established by stakeholders and resources accessible to them.

Chapter 5: Conclusion

This thesis focused on how the influence of risk perceptions among sports security operators effect the overall risk assessment and management process. Throughout the sports security profession, risk assessments are viewed as relatively objective; however the information gathered demonstrated that such practices is almost entirely designed with an overt subjective influence. While a moderate level of subjectivity is best for assessment, the risk process uses more than a moderate amount of subjectivity which can lead to misperceptions and false hypotheses of risk (Park, Peacey, & Munafo, 2014). From the beginning steps where an organization develops

methodology to fit their particular venue to the final decision-making and mitigation, subjectivity is present in high quantity by depending on the training and expertise of the individuals completing the review. Information employed in the process ranges from expert opinions both internally and externally, trends reported from outside agencies, and internal data collection through the use of camera systems and incident reports. While the decision-making process utilizes objective information provided by external partners and internal reports, expert opinion is more heavily relied on to commit to decisions.

The assessment methods chosen by the security operators include internal evaluation, external evaluation, or a mix of both. While organizations use different forms of risk assessment methodologies, they all follow ISO's (2009) standards for risk assessment. Although risk assessment models exist, most of the participants stated they do not utilize models such as the RSAT for their facilities. There are also different types of assessments that may review the overall risks or a specific category such as structural integrity, food and safety, or biological threats. They make determinations of risk based on observations from security staff at the venue and outside partners. Along with observations and identification of risk from these parties, the operators collect a wide range of information from in-house data collection to interviews of external entities and their respective reports. With internal evaluation, the security operators at the venue examine risks while being cognizant of the reputation of the facility, circumstances surrounding the area, and persons effected by risk decisions, and these assessments can hold a degree of bias. External evaluation allows security operators to collect what they hope to be an unbiased interpretation of dangers existing within the area. When the two evaluation types are combined, operators compare findings and seek overlap. If there is

overlap in results, the risks from the internal assessment are validated and mitigation tactics are implemented.

The risk assessment process has evolved over the course of the past two decades because unperceived risks of the past and their likelihood to occur have been exploited by individuals partaking in acts of terrorism such as bombings, active shooter incidents, and vehicle-rammings. As a result, individual perceptions of risk have advanced to consider a broader conceptualization of risk and consequences. Society has developed a sense of fear of danger and trusts security professionals to protect them from loss or injury when participating in events (Ericson & Haggerty, 1997). Everyone experiences risk differently, and these experiences are regularly called upon during risk assessments. Although likelihood of occurrence can be defined using qualitative, quantitative, subjective, or objective information, participants claimed to rarely use mathematical probability methods because they could draw conclusions themselves based on what they have experienced or observed in the past (NCS4, 2019). This, in turn, is reflected greatly when evaluators prioritize risks that they believe should be mitigated.

Throughout the process, evaluators communicate with one another to understand individual thoughts on threats at the venue and determine a collective report of these findings. Risk assessment teams meet with one another to make conclusions on the risks identified, and any risks mentioned by a single individual can be discussed and inserted in the report simply to ensure the organization awareness of its possibility, regardless if other evaluators agree or not. Conflicting expert judgements, uncertainty, and quality, quantity, and accessibility to information from different sources can impact the analysis and outcomes of the process (ISO, 2009). These individual perceptions of risk are

created by keeping in mind past events on a global, national, and local scale as well as personal experiences and information gathered from internal and external parties. A surveyor may already have an idea of what they believe to be existing threats by drawing on experiences and observations, but information accumulated from various sources can be used to further support their conceptions. External evaluations are sometimes guided by security operators working at the facility, and these individuals influence the final results from the outside entity to confirm what they, the internal party, already deemed a risk.

Expertise and training are the primary factors inspected for an organization to select evaluators. Training on risk assessment can come from the local, state, or federal level, and specialized courses outside the police academy are limited in frequency. Organizations prefer persons to have at least one form of certification such as the SAFETY act certification from the Department of Homeland Security and a relative amount of experience conducting risk assessments. Organizations will communicate with one another during the selection process to determine if the evaluator in question is qualified. Recommendations from other venues are based on that organization's opinions the evaluator's performance at their facility and quality of their assessment.

Limitations

The sample population was limited to the accessibility and availability of individuals established in the sports security domain. Only 10 participants were interviewed for this study, which limited the amount of information obtained about risk practices and information generally utilized in the field. Additionally, individuals interviewed were primarily men who held high ranking security titles and were in charge

of security operations for their respective facilities. To generate a more complete conclusion of the use of expert knowledge and interpretation compared to impartial data, sampling could take into account an increased number of risk professionals' accounts of the assessment process.

The research was conducted by a single researcher. Though grounded theory was applied to the data collected to create theories, the codes created by the researcher were determined based on their understanding of information discussed in interviews. If another individual did the same study, they may have different codes, but they should still identify similar patterns as the researcher from this study.

Future Research

Because this study was limited in quantity of participants, the same research could be conducted with an increase in sample size to get a better picture of how subjectivity and objectivity are distributed in the risk process. Testimonies from external agencies could also be obtained to establish the methods adopted by those entities and the relationship between internal and external evaluation. The research may be expanded to encompass accounts from other evaluators who are not Vice Presidents of Security, Chiefs of Police, or Security Managers in charge of all security operations at the venue but are still involved in the decision-making process. Additionally, examination of stakeholders and their influence could be further reviewed.

Another recommendation for further investigation would be to take a deeper look into how exactly risk perception and ultimately the risk process changed as a result of world events. From this study, we know there was a shift in how assessments were approached, but research could pinpoint when exactly this shift occurred both in the

United States and throughout the world. It would be important to note why this time period was the turning point in the assessment process and whether it was a slow or rapidly growing evolution that only a few or large majority of venues accepted to follow in the beginning. The researcher could also seek information about other influences that may have shaped the reformation of risk assessment and perceptions of individuals.

While this study demonstrated evaluators use a variety of resources to complete an assessment, the data collected differed from venue to venue due to availability of resources. Although every participant mentioned the usage of other agencies for recommendations and intel gathering, the quantity and quality of information at the facility were vaguely defined. It would be interesting to see if the information collected from various venues all make the same recommendations or lead to the same conclusions and how they affect the assessment and management process. A study could also be conducted to directly test the level of subjectivity by examining the differences between multiple assessments of single facilities to understand the impact of different assessors and information types.

In conclusion, the risk assessment process, though usually thought to be an objective process with a small margin of bias, it actually relies on a sizeable amount of subjective input from internal and external evaluators. Due to this, risk assessment and mitigation is dependent on the experiences of evaluators and how they identify and analyze risks. As Park, Peacey, and Munafo (2014) reported in their own study, implementation of peer review can alter the results of such assessments and lead to misperception and acceptance of conclusions within the industry. The details regarding quantity and quality of information gathered remains to be determined, but this study

established that opinions and experiences are consistently called upon to make decisions. Primarily trusting expert opinions and experiences to make decisions increases the possibility of misappropriating resources and generating false hypotheses.

References

Austen, L. (2009). The social construction of risk by young people. *Health, Risk & Society*, *11*(5), 451–470. https://doi.org/10.1080/13698570903183871

Beck, U. (1992). *Risk society: Towards a New Modernity*. London; Newbury Park, Calif.: Sage Publications.

Bureau of Census (2018). Arts, Entertainment, And Recreation-Establishments, Employees, And Payroll By Kind Of Business (NAICS Basis): 2015 And 2016 ProQuest Statistical Abstract of the U.S. 2018 Online Edition. Retrieved from https://statabs.proquest.com/sa/docview.html?table-no=1249&acc-no=C7095-1.26&year=2018&z=8A2D5F2A32851A9AA318B01B51B8F69F2032E5CA

Charmaz, K. (2014). *Constructing grounded theory* (2nd ed.). London, U.K.: SAGE Publications.

Clark-Ginsberg, A., Abolhassani, L., & Rahmati, E. A. (2018). Comparing networked and linear risk assessments: From theory to evidence. *International Journal of Disaster Risk Reduction*, *30*, 216–224. https://doi.org/10.1016/j.ijdrr.2018.04.031

Cox Jr., L. A. (Tony). (2008). Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks. *Risk Analysis: An International Journal*, *28*(6), 1749–1761. https://doi.org/10.1111/j.1539-6924.2008.01142.x

Ericson, Richard V., & Haggerty, Kevin D. (1997). *Policing the Risk Society*. Toronto and Buffalo, Ontario: University of Toronto Press.

Glaser, Barney & Strauss, Anselm. (1968). *The Discovery of Grounded Theory: Strategies for Qualitative Research.* New Brunswick, U.S.A. & London, U.K.: AldineTransaction.

Hall, Stacey A., Cooper, Walter E., Marciani, Lou, & McGee, James A. (2012) *Security Management for Sports and Special Events an Interagency Approach to Creating Safe Facilities.* Champaign, Illinois; Windsor, Ontario; Stanningley, United Kingdom; Lower Mitcham, South Australia; Torrens Park, South Australia: Human Kinetics.

International Organization for Standardization. (2009). Risk management—Principles and guidelines. *ISO 31000, 1*, 1-34.

Jennings, Will. (2012). *Olympic Risks*. Houndmills, Basingstoke, Hampshire RG21 6XS, England. Palgrave Macmillan.

Kabir, S. (2017). An overview of fault tree analysis and its application in model-based dependability analysis. *Expert Systems with Applications*, *77*, 114–135. https://doi.org/10.1016/j.eswa.2017.01.058

Mythen, Gabe, & Walklate, Sandra. (2005). Criminology and Terrorism. *Brit. J. Criminol*, 46, 379-398. https://doi:10.1093/bjc/azi074

National Endowment for the Arts (2018). Attendance At/Participation In Various Leisure Activities Including Reading By Selected Characteristics: 2012 [By Sex, Race, Age, Education, And Income] ProQuest Statistical Abstract of the U.S. 2018 Online Edition. Retrieved from https://statabs.proquest.com/sa/docview.html?table-no=1258&acc-no=C7095-1.26&year=2018&z=94C2471654D517C39179960998A12007E138FA7E

Orr, S. (2010). “We kind of try to merge our own experience with the objectivity of the criteria”: The role of connoisseurship and tacit practice in undergraduate fine art assessment. *Art, Design & Communication in Higher Education*, *9*(1), 5–19. https://doi.org/10.1386/adch.9.1.5_1

Park, I.-U., Peacey, M. W., & Munafò, M. R. (2014). Modelling the effects of subjective and objective decision-making in scientific peer review. Nature, 506(7486), 93-96. https://doi.org/10.1038/nature12786

Pasman, H., & Rogers, W. (2018). How trustworthy are risk assessment results, and what can be done about the uncertainties they are plagued with? *Journal of Loss Prevention in the Process Industries*, *55*, 162–177. https://doi.org/10.1016/j.jlp.2018.06.004

Ruijters, E., & Stoelinga, M. (2015). Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Computer Science Review*, *15–16*, 29–62. https://doi.org/10.1016/j.cosrev.2015.03.001

Slovic, P. (1999). Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield. *Risk Analysis*, *19*(4), 689–701. https://doi.org/10.1111/j.1539-6924.1999.tb00439.x

The National Center for Spectator Sports Safety and Security. (2018). Risk Management Challenges for International Sporting Events Training Course. *Project STADIA, 1*, 1-369.

Appendix A: Interview Guide

Subjectivity and Objectivity in Regards to Risk Assessments
Guided Interview:

This document is to serve as an interview guide for which the interviewer will utilize when posing questions during the interview process. As such, the document is strictly a guide and further questioning in some areas may occur in order to gain information. This will allow the participant to shape the conversation within the areas included in the interview based on responses received from questions presented in the guide.

Qualifications and Training:

1. What training and certifications must someone possess in order to conduct a risk assessment at this particular facility? How many hours are dedicated to training? How often is training offered? How consistently do individuals attend training? Is training paid for via the company putting on the event or self-sponsored? Is training mandatory or "encouraged"?
2. What is your background as it relates to this field?
3. What, [in your opinion?], qualifies someone to conduct a risk assessment?

Internal and External Context:

1. Describe the physical barrier/perimeter the risk assessment covers. How was the perimeter determined? Do the internal and external contexts of the assessment change with respect to evaluator or does context remain fairly constant throughout the process regardless of the evaluator?
2. How often is the venue inspected for repairs as a preventative measure against risk factors?
3. When creating emergency operations plans in the event something tragic does occur at the venue, what is taken into account (modes of transit, communication between security and civilians, etc.)? Who is involved in that process?

Risk Assessment Tool and Process:

1. How often is a threat assessment conducted at the facility? How many people are typically involved in conducting a risk/threat assessment for this particular venue? Are threat assessments conducted by individuals who work for the venue or are companies privately contracted out to conduct an assessment?
2. Does the facility utilize any particular risk assessment model? If so, which one and why that particular model? What steps are taken in order to complete the assessment using the specified assessment model?
3. Once the assessment is complete, can stakeholders edit or request changes to the document?

Risk Criteria:

1. What is this organization's risk criteria? At what level/point/threshold is a risk deemed acceptable or tolerable? How was this decided upon? Who/what was involved in determining the criteria? What methods are used to identify and prioritize risks in the evaluation/treatment steps of the assessment process? What conditions are taken into consideration during prioritization (level of risk, budget for countermeasure, etc.)?
2. According to the current risk assessment, what is considered the number one risk this venue faces? Why is it the number one risk as declared by the assessment? How was this determined? How has this risk been mitigated to a tolerable level to ensure the safety of those who may enter the venue?

Data Analysis:

1. Would you describe your risk assessment process as quantitative, semi-quantitative, qualitative, or semi-qualitative? How is the data used in the assessment obtained and analyzed? How do you account for uncertainties that arise during your assessment?
2. When evaluating the likelihood of individual risks occurring, what probability methods or data analyses, if any, are involved with that process?
3. Do you attempt to validate or further verify results prior to completing an assessment? If so, how?

Mitigation Tactics:

1. What types of controls/countermeasures are implemented at the venue to modify the level of potential risk internally and externally decided upon the assessment? How were those controls chosen as the best fit?
2. Does the same person(s) conducting a risk assessment also have a say in how the company/venue mitigates the risks identified? If so, how much weight does the assessor's input have in that decision making process in comparison to other stakeholders? Are ways of mitigation chosen based on best practices, most safe, most cost-effective, or a combination of any of the listed attributes?
3. Which agencies regularly work security at the venue? If an attack did occur, who would have jurisdiction and why? Is every security officer briefed on the risks identified from the assessment and operations plan prior to a major event at the venue/are they familiar with the venue and security precautions?

Perception of Risk by Professional Involved in Risk Process:

1. How have your attitudes towards individual risks (e.g. crowd violence, human trafficking, and terrorism) changed throughout the years? Has this translated to the risk assessment process? If so, how?

Appendix B: IRB Approval

Date: 1-29-2019

IRB #: IRB-18-39
Title: Risky Business: A Comparative Analysis of Risk Instruments of Sports Security Arenas
Creation Date: 10-1-2018
End Date: 11-13-2019
Status: Approved
Principal Investigator: Antonia Peterson
Review Board: Sacco (Exempt/Expedited Board)
Sponsor:

Study History

Submission Type Initial	Review Type Expedited	Decision Approved

Key Study Contacts

Member Antonia Peterson	Role Primary Contact	Contact antonia.peterson@usm.edu
Member Joshua B. Hill	Role Co-Principal Investigator	Contact Joshua.B.Hill@usm.edu
Member Antonia Peterson	Role Principal Investigator	Contact antonia.peterson@usm.edu