# Integrative Risk Identification Approach for Mass-Gathering Security

**Edward J. Glantz**
The Pennsylvania State University
eglantz@psu.edu

**Frank E. Ritter**
The Pennsylvania State University
frank.ritter@psu.edu

## ABSTRACT

Effective risk management begins with successful risk identification. Unfortunately, traditional approaches may lead to haphazard and incomplete results. To overcome this, we present a new integrative approach to improve risk identification that sequentially investigates protector-views and narrow scopes using literature review, ethnography, and subject matter expertise. This paper illustrates this approach by identifying man-made and natural threats to mass-gathering events in general, and stadium security as an example. Improving risk identification enhances resilience to known risks by enabling planning and development of targeted response strategies. Working from a more complete portfolio of risk resilience strategies may also improve flexibility and agility to respond to new and emerging risks.

### Keywords

risk identification, risk management, resilience, agility, crisis, stadium security, mass-gathering security.

## INTRODUCTION

Risk identification is the first step in risk management, and the primary focus of this paper's integrative approach to identifying risk. The motivation is to improve risk management by providing more structured methods to identify risks, so that treatment strategies may be applied to decrease risk. The straightforward ISO/IEC (2009) or NIST (2012) processes to manage risk presumes risks are not being overlooked. Despite good intentions, overlooked risks confuse preparation and defense with luck and probability. A stadium security case will illustrate this integrative approach.

Managers of stadiums, and other mass-gathering events with more than one thousand participants, are challenged to plan and manage security, including development of crisis response plans. This can be perplexing as even similar events held at the same facility may have drastically different risks and outcomes. In addition, security management is compounded with knowledge that terrorist-enabled actors are now targeting these venues, hoping to maximize psychological and economic impact.

Improving mass-gathering security and crises response is important, as millions attend these events. Each year in the United States, for example, over 5.5 million participants attend North American Stock Car (NASCAR) events, and another 165 million attend professional and collegiate sporting events. Identifying risks permits planners to more effectively prepare treatments to either lower risk likelihood, or reduce risk impact. For example, Mass-Gathering Medical Care (MGMC) currently provides standard preventative measures, primary care, and hospital referral, but is challenged to respond, assess, and treat emergency medical services needs (Milsten, Maguire, Bissell, & Seaman, 2002).

All organizations, including mass-gathering events, face uncertainty in the achievement of objectives caused by internal and external influences. The effects from these uncertainties are managed through the application of treatments, that are developed following the influence's identification, analysis, and evaluation (ISO/IEC, 2009). In general, the analyst begins with recognition of risks, and concludes with specific treatment, safeguard, or control recommendations reducing risk likelihood and/or impact. These recommendations are used by senior decision-makers, risk-owners, or protectors to select final implementation choices, given organizational priorities and resource constraints (ISO/IEC, 2009; NIST, 2012).

This paper begins with an overview of the steps in the integrative approach, relating risk management and security concepts, connecting identified risks and treatment strategies, and then applying the integrative risk

identification practice and creative methods to identify risks. Mass-gathering events illustrate the method, including the 2013 Boston Marathon bombing and 2015 Stade de France attacks. The paper concludes with steps to guide practitioners to apply the process using protector views, N+1 risks, and reference databases to improve future risk identification.

## OVERVIEW: AN INTEGRATIVE APPROACH TO RISK IDENTIFICATION

**Table 1** provides steps to conduct an integrative risk identification. Techniques enable asset identification, as well as associated threat and vulnerability analysis. The process begins with a protector-view that values the assets, and may optionally limit scope. Risks are identified and securely recorded, and the process repeats upon completion, expanding the knowledgebase going forward.

**Table 1 Integrative risk identification steps**

1. Use an existing risk management guideline or standard, such as ISO or NIST (ISO/IEC, 2009; NIST, 2012).

2. Analyze using a specific location for site-specific risks.

3. Use event-type data to identify elements influencing risk, such as communicable disease, weather, demographics, time of year, time of day, alcohol, crowd attributes, known aspects of first responder teams, and political stability.

4. Limit the scope of the investigation using process, function, or some other method (e.g., financial, operational, or regulatory), to make the task more manageable. The analysis can be repeated as needed across other scope domains.

5. Use an asset-oriented method to first list assets, then assign risks to assets:

- Select a protector-view, including owner, employee, customer, passerby, first responder, etc., to list assets in need of protection, and then rank those assets in importance to the organization.
    - Unrecognized assets may remain exposed if the protector-view is not used, or used too broadly. Some assets are shared, but others are unique to a specific protector and become more visible using the protector-view. A complete analysis repeats this approach for other views.
- Use the assets to identify a list of risks by noting threats and vulnerabilities for each asset. Use the practice and creative methods of literature review, ethnography, and structured analytics described in this paper.
- Append the final risk item "N+1" to the list. This is an important signal to the risk owner that risks are never completely identified, and the risk identification process never done. Ideally the completion of one risk identification process would launch the next.

6. Switch to a threat-oriented method, and test asset-sensitivity to new and emerging threats.

7. Switch to a vulnerability-oriented method, and test asset-sensitivity to new and emerging vulnerabilities.

8. Repeat the above steps for other locations, events, domains, and protectors as needed.

9. Use the list of risks to create a high level "dance-card" for each event or business activity. Use this card prior to, during, and after each event, and update the card upon major changes in leadership, technology, facility, or event type. Larger facilities and more complex events might consider implementing an automatic decision aid to reduce cognitive errors.

10. Archive the results in a secure database for monitoring and tracking.

11. Repeat the risk identification before risk treatments are implemented, as new risks may emerge from the treatment.

Assets and associated risks in the form of threat/vulnerability pairs are listed upon completion of the steps in **Table 1**, the focus of this paper.

Subsequent steps for future work assign relative risk values to each risk scenario by using methods to value assets, rank risk likelihood and impact, assign confidence values based on previous experience, and estimate of previously treated risks. The highest relative risks are assigned treatments to reduce likelihood in the best case, or reduce impact otherwise. Lower relative risks are accepted, and added to a watch list to monitor changes in likelihood or impact. Crisis management and communication plans should also be developed for known risks that exceed controls, and new risks. Crisis managers should be trained in mitigation plans to reduce risk impacts, such as evacuation processes, command, control, and communication operations.

## RISK MANAGEMENT

The goal of risk management planning is to improve security for an organization's most critical assets. Security describes a goal state of freedom from harm or difficulty for an asset that is valued by a protector, or risk owner. The protector's universe is divided into two states: that which is secure, and that which is unsecure. The goal of the protector is to enhance stability for the asset in the variable "insecure" boundary area separating secure and unsecure states (Manunta, 1997).

Enhancing stability in the border zone of insecurity is accomplished through risk and crisis management. **Figure 1** illustrates that risk management is a proactive planning and preparation process to analyze and control threats around an asset that might take advantage of a weakness or vulnerability in the asset. Risk is described as the likelihood and impact from the alignment of a threat/vulnerability pair acting on an asset. As such, risk management describes the attempt to reduce the likelihood of risk events where possible, or to reduce the impact of events otherwise (ISO/IEC, 2009; NIST, 2012). The bottom of **Figure 1** illustrates that crisis management may be required to provide reactive capabilities for either unforeseen risk events or anticipated events that exceeded preparation.


**Figure 1 Risk management should include the planning for crisis management**

**Figure 2** shows that crisis management extends risk management planning, and should be part of risk management, including assignment of crisis roles and responsibilities, and communication strategies.

The horizontal access represents time, and the vertical access represents operational capacity. At time of the incident, operational capacity is reduced, triggering an incident response. Crisis management uses mitigation plans to provide early detection to react and respond, and incident response plans to return operations to a minimal level, called the "recovery point objective" (**RPO)**, in a specific time, called the "recovery time objective" (**RTO**) (Snedaker & Rima, 2014).

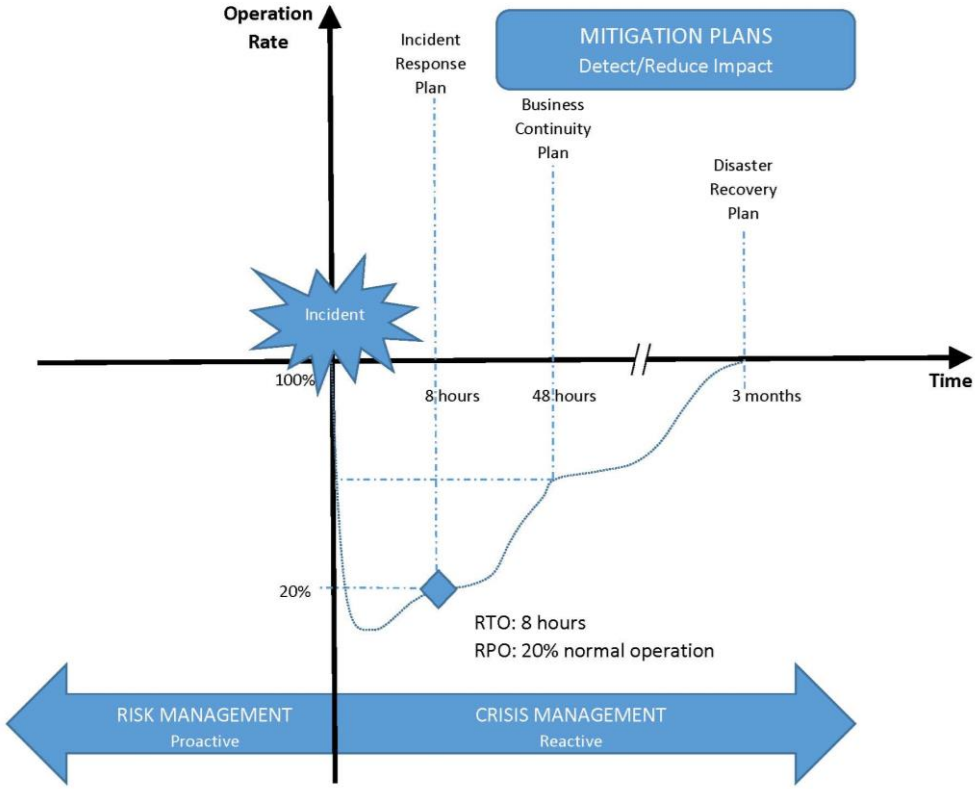


**Figure 2 Crisis management describes the reactive processes to mitigate disruptive incidents**

### Risk Treatments

Although the scope of this paper is to improve risk identification, it is useful to review the connection between identified risks, and the eventual recommendation of treatments for risks. Not all risks can be treated, as organizations are resource constrained, so the greatest *relative risks* from the pool of identified risks are determined based on likelihood, impact, and asset value. Analysts then envision and propose treatments for these risks for decision makers. As such, an incomplete risk pool may subvert the process to identify the greatest relative risks.

Treatment choices lower likelihood through prevention activities, reduce impact through mitigation plans, or lower asset value through substitution. The residual risk that remains after treatment should be equal to or less than the organization's risk appetite. Common risk treatment strategies can be described as avoid, transfer/share, mitigate, accept, and terminate (Boehm & Hansen, 2001; Pew & Mavor, 2007). Strategies may lower one or more risks, or may be combined to further lower a specific risk. Terminating a process does not eliminate all risk, but instead shifts the risk exposure curve from the planned activity to an alternate situation (ISO/IEC, 2009; NIST, 2012).

Treatments that lower likelihood are preferred, such as the avoid strategy. Avoid changes operational processes to replace higher risk exposures with lower ones. Transfer/share strategies may also lower likelihood through contractual arrangements with skilled specialists that possess better systems and expertise (ISO/IEC, 2009; NIST, 2012).

If treatments to reduce likelihood do not exist, such as an outage of grid power, then impact is treated.

Treatments to reduce impact include mitigation plans such as incident response, disaster recovery, and business continuity. Impact may also be lowered by transferring risk to specialists, or reducing financial impact by purchasing an insurance contract. Avoid strategies may also lower impact by changing the operational process (ISO/IEC, 2009; NIST, 2012).

Most identified risks fall below a threshold requiring action, and are thus simply accepted (ISO/IEC, 2009; NIST, 2012), although this should not be used as an excuse to ignore risks. The integrative risk identification approach appreciates the importance of all risks, including accepted risks that have potential to evolve and grow in likelihood or impact. Accepted risks may also be used to seed creative analysis techniques to disclose more substantial risks, or the possibility of risks combining.

### Hazards

A hazard is a situation that could threaten a valued asset. **Figure 3** illustrates the range of hazard probability from greater than zero percent to one hundred percent likelihood. Dormant hazards have less than fifty percent likelihood of harming the asset. Armed hazards are imminent, with likelihood greater than fifty percent. Active hazards are currently occurring. Incident describes an active hazard that has completed.

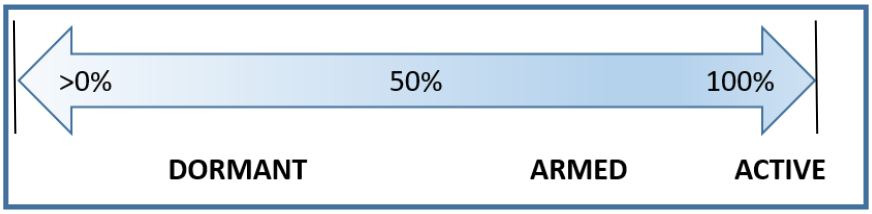


**Figure 3 Hazards can escalate and should be identified and tracked**

The motivation to apply treatments in risk management is to prevent a hazard from escalating beyond controls to create a crisis situation. **Figure 4** illustrates a resilience approach to risk management using incident response mitigation plans that sense and constrain the hazard's growth to the shaded area under the curve. Extreme events may exceed these resilience plans requiring an agile crisis response.

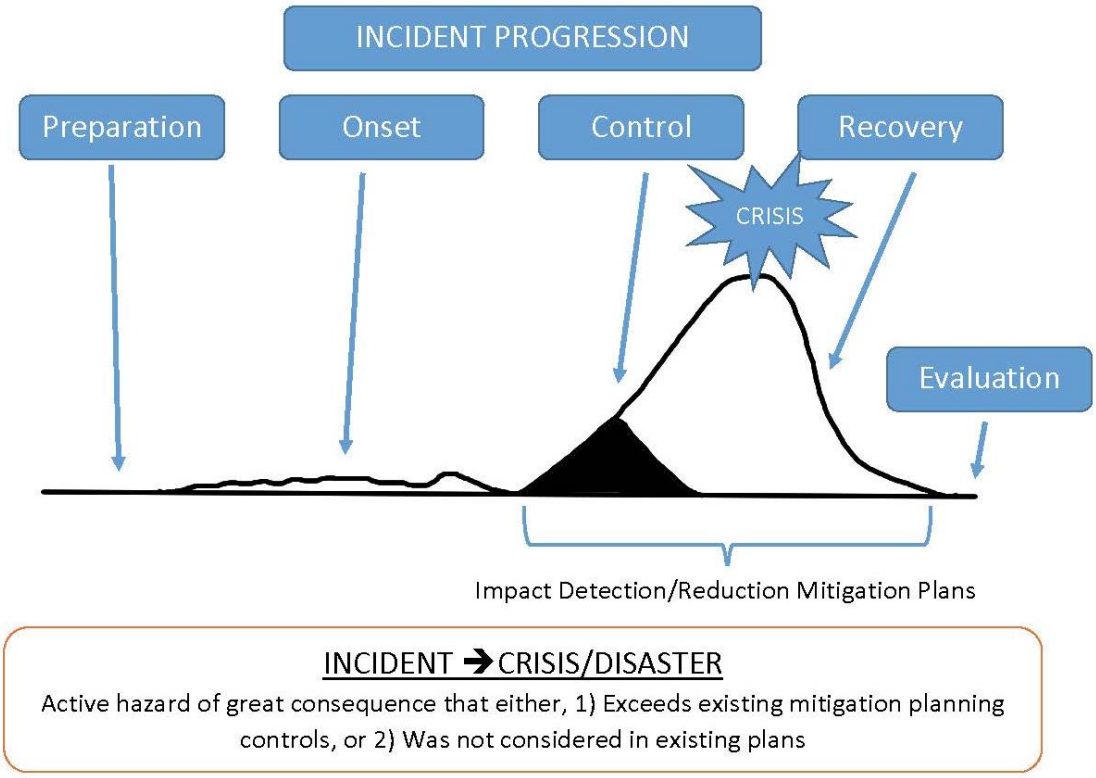


**Figure 4 Active hazards may escalate beyond existing controls to create a crisis situation**

## RISK RESILIENCE AND AGILITY

Resilience is the proactive capacity of a social system (e.g., organization, city, society) to adapt and recover from events exceeding normal and expected disturbances (Comfort, Boin, & Demchak, 2010). Incident response plans designed during risk management provide resilience through early detection and response to known risks.

As discussed, hazards may exceed incident response plans, and require crisis mitigation plans such as disaster recovery and business continuity. These plans should be proactively designed during risk management planning. Disaster recovery plans focus on short-term recovery, including emergency shut-down procedures if necessary, and reestablishment of services. Business continuity plans provide continued operations when the crisis exceeds the disaster recovery plan, including alternate facilities and systems from which to provide operations. These two crisis mitigation plans, disaster recovery and business continuity, may provide resilience to known risks, but their existence may also enhance agility to new risks.

Agility is reactive, building on anticipation of potential changes that might occur in the future, to return to a stable condition (Barthe-Delanoë, Carbonnel, Bénaben, & Pingaud, 2012; Barthe-Delanoë, Ramète, & Bénaben, 2014; Barthe-Delanoë, Truptil, & Bénaben, 2014; Wagner & Disparte, 2016). Adaptive capabilities can leverage risk resilience treatments for known risks to enhance flexibility for agile response to new risks.

## INTEGRATED RISK IDENTIFICATION APPROACH

The overall effectiveness of risk management depends on thorough and continuous identification of risks, as opposed to incomplete, non-recurring efforts. Risk analysis performed on an incomplete risk set is particularly dangerous, contributing to a false sense of security. Similarly, non-recurring risk identification prevents disclosure of new risks arising from organizational and environmental changes. Decision-makers deserve to be informed of new risks, and afforded the opportunity to evaluate them in accordance with organizational objectives and resources. Identifying risks, present and future, is necessary to adequately secure an organization's interests (Tchankova, 2002).

The integrated approach to risk identification is recurring, and combines discovery techniques grounded in practice and creativity. Practice-based scenarios recall risks known to have occurred through a review of the literature, including regulatory requirements, ethnography including domain insights gathered by analyst observation, and subject matter expert interviews. Creative-based scenarios identify risks that have not yet occurred, and can be creatively envisioned using Delphi (Markmann, Darkow, & von der Gracht, 2012), brainstorming (C.I.A., 2009), and other structured analytic techniques.

For example, practice-based methods would enable hospitals located in the path of Hurricane Sandy to better prepare from a review of hospitals located in Hurricane Katrina's path. Creative methods would enable airlines to identify new risks arising from risk treatments, such as the mental or physical health risks of a single pilot alone behind a fortified cockpit door.

## AUTOMATED METHODS

The identification and management of large numbers of risks from this integrative approach will benefit from automated methods for monitoring and tracking. Automated methods of machine learning and data mining have already enhanced risk identification and assessment of mass-gathering patient presentation rates (Serwylo, Arbon, & Rumantir, 2011), as well as risk areas in financial markets (Ozgulbas & Koyuncugil, 2011), pipelines (Wang, Zhou, & Zhang, 2013), food safety (Xin & Liu, 2015), and cloud security (Ahmed & Abraham, 2015).

Researchers have also applied web services and agents to develop novel architectures for anti-terrorism planning and resource allocation systems (Haynes, Kannampallil, Cohen, Soares, & Ritter, 2008).

Another advantage of automated methods is predictive modeling of risk variables to better manage mass-gathering event security. For example, the patient presentation rate application modeled variables such as number attending, event type, weather (e.g., heat index, humidity, temperature, wind chill), time, and availability of alcohol (Serwylo et al., 2011).

## CASE: MASS-GATHERING SECURITY

Mass-gathering security planning is a suitable case to apply the practice and creative-based scenarios using the steps in **Table 1** of the integrative risk identification approach. The practice-methods identify risks published in the literature from known historical events, including published regulatory compliance requirements and other

organizational records. This method continues with ethnography, including site investigations and interviews with subject matter experts. The creative-methods, on the other hand, attempt to envision conceivable risk scenarios that have not yet occurred, using Delphi and other structure analytic techniques.

Planning security for mass-gathering events is particularly difficult. Normal circumstances of crowd-related risks, including health, weather, and facility issues, provide a difficult threat-vulnerability surface area to analyze. This is further compounded by terroristic acts targeting these events, from the Black September attacks on the 1972 Munich Olympic games to the more recent German Christmas market attack.

### Protector-View and Scope

A complete asset list is required to formulate threats and vulnerabilities to each asset. A protector-view is used to reveal assets from the protector's perspective, and a complete risk analysis may use several protector views selected from associated stakeholders. For example, protector-views for a store might include owner, employee, customer, first responder, public, etc. The scope of the protector's activities can be further constrained to provide more scrutiny in asset identification. Methods to subdivide scope include process (e.g., input, process, output), or function (e.g., hardware, software, database, network, people, and process/facility).

### Practice-Methods: Literature Review

Starting with the literature review informs researchers of risks to consider in the divergent/convergent analysis, as well as when conducting the virtual site visit or subject matter expert interviews. Finding risk related literature is recursive, requires a time investment, and may involve various search engines, as well as organizational and regulatory databases. Finding a risk report for a specific location is not likely, so be flexible and search for related literature. Be persistent to find appropriate search terms. This example required a few iterations using Google Scholar to reveal "mass-gathering security" search terms were more effective than "stadium security." One should document search engines and search terms used. Literature includes scholarly reviews as well as industry whitepapers and even news articles.

Stadium and mass-gathering events represent a broad spectrum of known risk scenarios, both natural and man-made, varying in both emergency planning complexity and demand, as well as medical service requirements. The initial review of the literature identified several natural and man-made sources of risk that are summarized in **Table 2**.

**Table 2 Mass-gathering hazards from initial literature review**

| | NATURAL | MAN-MADE | MAN-MADE |
|---|---|---|---|
| **TYPE** | WEATHER, GEOLOGY, DISEASE | CROWD-RELATED | TERRORISM-RELATED |
| **HAZARDS** | • Weather hazards include drought, extreme temperature (hot or cold), and cyclonic Storms<br>• Geologic hazards include avalanche, earthquake, eruption, and tsunami<br>• Disease hazards includes water, air, vector, and food-born | • Hazards include crowd control, event access, fire safety, medical preparedness, and emergency response<br>• Includes errors by attendees and staff, e.g., Hillsborough disaster | • Hazards include intentional man-made crises designed to maximize psychological and emotional stress among victims and witnesses.<br>• Includes denial and deception |
| **SOURCE** | Soomaroo & Murray, 2012 | Milsten, Maguire, Bissell, & Seaman, 2002 | CCICADA, 2013 |

#### *Natural Risks in Literature: Weather, Geology, Disease*

The natural risks in **Table 2** are from a survey of events between 1988 and 2011 reviewing participant death, injury or illness during mass-gatherings. Twenty incidents were triggered by heat (5), cold (4), lightning and storms (5), and disease outbreaks (6) during sports, air shows, rock concerts, outdoor celebrations, and dignitary visits. Weather hazards included drought, extreme temperature (heat or cold), and cyclonic storms; geologic hazards include avalanche, earthquake, eruption, and tsunami; disease hazards include water, air, vector, and food-born (Soomaroo & Murray, 2012).

#### *Man-Made Risks in Literature: Crowd-Related and Terrorism*

Man-made hazards in **Table 2** are crowd-related variables, as well as terroristic acts, from a literature review investigating mass gatherings between 1977 and 2002. Crowd variables include crowd control activities, event access, fire safety, medical preparedness, and emergency response. This review identified variables associated with injury-illness patterns, using a medical-usage-rate based on patients-per-ten-thousand-persons in attendance. Crowd variables that increased medical care demand included event type and duration, crowd mood, attendance and crowd density, age, and alcohol and drug use (Milsten, Maguire, Bissell, & Seaman, 2002).

Terroristic acts are intentional man-made crises that use soft targets to maximize economic disruption and psychological stress among victims, witnesses, and the general public. Terrorists use an "attack utility" to measure target effectiveness. Stadiums, and other mass-gathering events, represent a high attack utility for terrorists seeking to maximize disruption and stress, as these venues are difficult to secure, and possess multiple vulnerabilities (CCICADA, 2013).

### *Practice-Based: Subject Matter Expert Guidelines*

Another way to elicit existing risk knowledge is through ethnographic techniques, such as site-observation and subject matter expert (SME) guidelines or interviews. For illustration, research from two university centers will illustrate guides from experts to identify hazards in stadium security.

The first SME guideline is the Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA) at Rutgers University, in New Jersey, USA. CCICADA has demonstrated expertise by leading several government and non-government organizations to compile a Best Practices in Anti-Terrorism Security (BPATS) guide. The guide's scope uses fifteen all-hazard National Planning Scenarios[1] to plan responses to a range of terrorist attacks (e.g., nuclear, biological, chemical, explosive, and cyber), as well as natural disasters (e.g., earthquake, hurricane). The guide targets professional and collegiate sporting venues (e.g., baseball, football, basketball, hockey, soccer, car racing) in the United States (CCICADA, 2013).

The BPATS guide demonstrated expertise by using an integrative risk approach consisting of literature review, stadium security expert interviews, facility visits, and workshops. The literature review included incident After-Action-Reports, academic research reports, published articles, and special event operational procedures, among others. They also took advantage of best practices and research from other domains. The BPATS guide is one hundred fifty-five pages, and its Best Practices Matrix is another seventy-three pages. Approximately six-hundred feasible best practice risk treatments are identified in functional areas of risk assessment, staffing (e.g., leadership, organization, and authority), information management, operations, and communications. Risks meriting best practice treatment, or "protective measures," are rated from strongly recommend, recommend, to suggested. Metrics are also provided to evaluate performance for each best practice (CCICADA, 2013).

The second SME guideline is the National Center for Spectator Sports Safety and Security (NCS4) at the University of Southern Mississippi. The NCS4 developed best practices for collegiate and professional sporting event risks at annual workshops hosting event managers, law enforcement, medical, and other public safety representatives. Similar to the BPATS guide, NCS4 advocates continuous, or cyclical, improvement, and treats these guides as living documents. Their "2015 Intercollegiate Guide" is one hundred and seventy-two pages long and includes approximately seven hundred best practice recommendations. The NCS4 guide arranges best practices around nine functional areas: game day plan, crowd dynamics/management, emergency action planning, routine non-game day operations/measures, risk and threat assessment/vulnerabilities and planning, sport facility design/environment, staffing (e.g., performance, development, training, and certification), security and safety awareness culture, and technology use (e.g., implementation/innovation/information management) (NCS4, 2015).

As the NCS4 and BPAT guides use different methodologies, their results are not identical, although there is overlap in the list or risks and associated best practices. Both guides advocate use of the National Incident Management System's (NIMS) Incident Command System (ICS) during incident response. The ICS specifies a "Unified Command" doctrine to align and organize the response of incident commanders from law enforcement, fire, medical services, and venue security. The Unified Command promotes efficient interagency communications by operating from a common command center facility, staffed with representatives from each agency. One difference is that the BPAT guide includes metrics to evaluate compliance, although the NCS4 most likely provides this level of detail in their private consulting certification processes.

[1] List of National Planning Scenarios developed by the Federal interagency community https://emilms.fema.gov/IS800B/lesson5/NRF0105060t.htm

*Creative-Methods: Structured Analytics*

Next, new and emerging risks, and site-specific risks, can be creatively identified using structured analytics, such as divergent/convergent thinking, or the Delphi method. This builds upon the more than seven hundred known risks from the literature review and SME guideline information. For example, neither of the referenced SME best practice guides specifically address treatment of drone threats. Further, these creative methods can also test unproven risk treatments, such as those accompanying evacuations from mass-gatherings.

Delphi is one technique to conduct creative evaluations in general, with potential value for risk assessment. Rand Corporation developed Delphi to structure group communication of complex problems. The technique typically involves several rounds of communication, often conducted remotely, and with some degree of anonymity. The technique may begin with an initial phase contributing problem information, followed by a second phase discussing divergent group member views, followed by a final evaluating phase. Delphi has been recognized in risk analysis as both a method to identify risks, as well as to subjectively assess uncertainties ( Linstone & Turoff, 2002). Researchers applied Delphi research to man-made risks in global supply chains with uncertainty of type, location, and affected supply chain partners. They found the Delphi technique improved several areas, including risk identification and measurement (Markmann et al., 2012).

Structured brainstorming, or divergent/convergent thinking, is another creative technique permitting groups to identify and assess risks. This technique is conducted in two phases. The divergent phase lists as many ideas as possible, free of constraint or criticism. Techniques reduce "power of the pen" constraints, and groupthink. Successful divergent results are based on quantity. The convergent phase organizes the divergent results into related categories, and ranks them. Success in the convergent phase is an ordered list of risks (C.I.A., 2009). The two-phases of structured brainstorming effectively identifies new risks, as well as assigns relative importance to each (Yoe, 2011).

## MASS-GATHERING TERRORISM RISK

The recent terrorist attacks at the 2013 Boston Marathon bombing and the 2015 Stade de France attack contribute to our knowledge-base of mass-gathering security, but also provide opportunities to improve resilience planning using integrative risk identification. The protector-view is the crisis manager, and the scope is limited to mitigation plans following a terrorist attack, including use of social media and cell communications, and decisions to evacuate or shelter in place, and assign travel restrictions.

The Boston Marathon explosion was an isolated attack by two brothers that killed three civilians, and injured an estimated 264 others. The 2015 Stade de France attack was part of a more sophisticated series of attacks involving seven perpetrators in Paris and the city's northern suburb, Saint-Denis, killing 130 people, and injuring 368 others. Both events invoked public restrictions on movement and charted new territory in social media and public involvement in immediate crisis response and subsequent police investigation. While social media enhanced public awareness and response to the isolated Boston attack (Montgomery, Horwitz, & Fisher, 2013), poor cell service reduced panic in coordinated attacks at the Paris Stade de France (Borden, 2015). In Boston weapons included IEDs, a handgun, and a car. In Paris the attackers were more sophisticated using assault rifles, hand grenades, and suicide belts, in attacks outside the Stade de France, in cafés and restaurants, and inside the Bataclan theatre (de la Hamaide, 2015).

Following the Boston explosion, the Governor requested citizens to voluntarily "shelter in place" during the four-day manhunt controversially (and probably extra-constitutionally) halting commerce and travel in Boston, Watertown, and Cambridge. Eventually one perpetrator was killed, and his brother apprehended (Montgomery et al., 2013). Police initially attempted to use social media to enlist public support in the identification and location of the two persons of interest. Instead, officials needed to squelch ad hoc social media vigilante efforts, expressing concern that Twitter and Reddit users contributed to the exchange of bad information, heightened panic, and made public information that could compromise officers' position and safety (Chang, 2013).

The attack on the soccer game at the Stade de France could have been worse, had security not effectively blocked attacker access to the stadium, protecting French president Francois Hollande and 80,000 other fans. Further, poor stadium cell coverage permitted the game to continue without participant awareness of the attacks, avoiding panic. The need for more planning was evident at the end of the game when fans were initially herded to one of two exits, before being returned to the field to await further instruction (Borden, 2015). Similar to the Boston bombings, although more restrictive, France issued the first of five extensions of emergency powers to enhance police authority (BBC, 2016).

It is conceivable that the Paris Stade de France evacuation began as part of a structured resilience plan that was adapted in an agile response to new information of coordinated attacks, and determined safer to have fans wait in the stadium before receiving the all clear to exit. Although likely unplanned, it was fortuitous that poor cell

service reduced panic among unaware fans.

These events represent an evolving threat landscape for mass-gathering events, increasing in weapon sophistication and coordinated attacks. These represent an increased need for creative tabletop training exercises to prepare for both the known and possible.

## CONCLUSION

At this point benefits are evident in ongoing risk identification, and the need to grow a knowledge base from previous experiences. The integrative approach to increase identification of risks is a method to create lists of assets and associated threat/vulnerability pairs. Practice and creative-methods combine literature review, ethnography, and structured analytics to identify risks. In addition, the creative-methods can help investigate risks arising from proposed treatments.

Integrative risk identification derives value from creating resilience plans to identified risks, and as such creates long lists of risks that need managed. Additionally, resilience plans may combine to enhance flexibility for agile response in crises.

## ACKNOWLEDGMENTS

We would like to thank the reviewers for the positive and helpful comments.

## REFERENCES

Ahmed, N., & Abraham, A. (2015). Modeling cloud computing risk assessment using machine learning. In A. Abraham, P. Krömer, & V. Snasel (Eds.), Afro-European Conference for Industrial Advancement: Proceedings of the First International Afro-European Conference for Industrial Advancement (Vol. 334, pp. 315-325). Cham: Springer International Publishing.

Barthe-Delanoë, A.-M., Carbonnel, S., Bénaben, F., & Pingaud, H. (2012, April). Event-driven agility of crisis management collaborative processes. Paper presented at the 9th International ISCRAM Conference, pp. 1-5, Vancouver, Canada.

Barthe-Delanoë, A.-M., Ramète, G. M., & Bénaben, F. (2014). Agility of crisis response, from adaptation to forecast: Application to a French road crisis management use case. Paper presented at the ISCRAM-med 2014, pp. 157-164, Toulouse, France.

Barthe-Delanoë, A.-M., Truptil, S., & Bénaben, F. (2014, May). Agility of crisis response: Gathering and analyzing data through an event-driven platform. Paper presented at the 11th International ISCRAM Conference, pp. 255-259, University Park, PA.

BBC. (2016, Dec. 10). Paris attacks: State of emergency 'to protect elections'. BBC, p. 1. Retrieved from http://www.bbc.com/news/world-europe-38274200

Boehm, B., & Hansen, W. (2001). The Spiral Model as a tool for evolutionary acquisition. Crosstalk: The Journal of Defense Software Engineering, 14(5), 4-11.

Borden, S. (2015, Nov. 14). As Paris attacks unfolded, players and fans at soccer stadium remained unaware. The New York Times, p. 1. Retrieved from http://nyti.ms/1RVuVH2

C.I.A. (2009). A tradecraft primer: Structured analytic techniques for improving intelligence analysis. Washington DC: U.S. Government Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf.

CCICADA. (2013). Best practices in anti-terrorism security (BPATS) for sporting and entertainment venues: Resource guide. Rutgers University: Command, Control and Interoperability Center for Advanced Data Analysis (CCICADA) Retrieved from https://www.safetyact.gov/externalRes/refdoc/CCICADA%20BPATS.pdf.

Chang, A. (2013, April 22). Reddit apologizes for fueling Boston bombings online witch hunts. Los Angeles Times, p. 1. Retrieved from http://articles.latimes.com/2013/apr/22/business/la-fi-tn-reddit-apologizes-boston-bombings-witch-hunt-20130422

Comfort, L. K., Boin, A., & Demchak, C. C. (2010). The rise of resilience Designing resilience: Preparing for extreme events. Pittsburgh, PA, US: University of Pittsburgh Press.

de la Hamaide, S. (2015, Nov. 14). Timeline of Paris attacks according to public prosecutor. Reuters, p. 1. Retrieved from http://www.reuters.com/article/us-france-shooting-timeline-idUSKCN0T31BS20151114

Haynes, S. R., Kannampallil, T. G., Cohen, M. A., Soares, A., & Ritter, F. E. (2008). Rampart: A service and agent-based architecture for anti-terrorism planning and resource allocation. Paper presented at the First European Conference on Intelligence and Security Informatics, pp. 260-270 , Esbjerg, Denmark.

ISO/IEC. (2009). Risk management – Principles and guidelines ISO 31000:2009. Geneva, Switzerland: ISO International Standard.

Linstone, H. A., & Turoff, M. (2002). The Delphi method: Techniques and applications. Ann Arbor, MI: Addison Wesley.

Manunta, G. (1997). Towards a security science through a specific theory and methodology. [Dissertation]. University of Leicester.

Markmann, C., Darkow, I., & von der Gracht, H. (2012). A Delphi-based risk analysis — Identifying and assessing future challenges for supply chain security in a multi-stakeholder environment. Technological Forecasting & Social Change, 80(2013), pp. 1815-1833. doi:http://dx.doi.org/10.1016/j.techfore.2012.10.019

Milsten, A., Maguire, B. J., Bissell, R. A., & Seaman, K. G. (2002). Mass gathering medical care: A review of the literature. Prehospital and Disaster Medicine, 17(3), pp. 151-162.

Montgomery, D., Horwitz, S., & Fisher, M. (2013, Apr. 20). Police, citizens and technology factor into Boston bombing probe. The Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/inside-the-investigation-of-the-boston-marathon-bombing/2013/04/20/19d8c322-a8ff-11e2-b029-8fb7e977ef71_print.html

NCS4. (2015). Intercollegiate athletics safety and security: Best practices guide. Retrieved from http://www.nccpsafety.org/assets/files/library/2015_NCS4_Intercollegiate_Best_Practices_Guide.pdf

NIST. (2012). Guide for conducting risk assessments Special Publication 800-30 Revision 1. Washington DC: National Institute of Standards and Technology.

Ozgulbas, N., & Koyuncugil, A. S. (2011). Financial early warning system for risk detection and prevention from financial crisis. In A. S. Koyuncugil & N. Ozgulbas (Eds.), Surveillance technologies and early warning systems: Data mining applications for risk detection (pp. 76-108). Hershey, PA: Information Science Reference.

Pew, R. W., & Mavor, A. S. (2007). Human-system integration in the system development process: A new look, Committee on Human-System Design Support for Changing Technology. Washington, DC: National Academies Press.

Serwylo, P., Arbon, P., & Rumantir, G. (2011, May). Predicting patient presentation rates at mass gatherings using machine learning. Paper presented at the 8th International ISCRAM Conference, Lisbon, Portugal.

Snedaker, S., & Rima, C. (2014). Chapter 1 - Business Continuity and Disaster Recovery Overview. Business Continuity and Disaster Recovery Planning for IT Professionals (Second Edition) (pp. 1-28). Boston: Syngress.

Soomaroo, L., & Murray, V. (2012). Weather and environmental hazards at mass gatherings. PLoS Currents, 4, e4fca9ee30afc4. http://doi.org/10.1371/4fca9ee30afc4.

Tchankova, L. (2002). Risk identification – Basic stage in risk management. Environmental Management and Health, 13(2), pp. 290-298.

Wagner, D., & Disparte, D. (2016). Global risk agility and decision making. London: Macmillan Publishers Ltd.

Wang, B. Q., Zhou, X. Y., & Zhang, W. J. (2013). Data mining improves pipeline risk assessment. Applied Mechanics and Materials, 347-350, 2168-2172. doi:10.4028/www.scientific.net/AMM.347-350.2168

Xin, L., & Liu, X. (2015). Research of food safety risk assessment system based on data mining. Advance Journal of Food Science and Technology, 8(10), 707-710.

Yoe, C. (2011). Principles of risk analysis: Decision making under uncertainty. Boca Raton, FL: CRC Press.